RGPD* & Cyber Sécurité

(*Règlement Général sur la Protection des Données)

FRANCE
QUALITE PERFORMANCE
GRAND-EST

28/04/2023

RGPD n’est qu’un prétexte ...

Quelques exemples

IKEA, victime d'une cyber-attaque

Els Bellens
Els Bellens est redactrice chez Data News.

Le géant du meuble IKEA est aux prises avec une cyber-attaque exploitant des mails d'hameçonnage ('phishing') internes pour toucher les collaborateurs. IKEA a confirmé l'attaque.

Cybersécurité. « L'attaque cyber a failli faire disparaître notre entreprise »

Stéphane Tesson, directeur général de Collectivision. / DR

Montpellier : victime d'une cyberattaque, Orchestra contraint ses salariés au télétravail

Une équipe pluridisciplinaire à votre service (6 salariés)

- Juristes en protection des données
- Ingénieur informatique
- Chef de projets
- Consultants techniques

AUDIT **ANALYSE** **CONSEIL**

Inkivari → Une entreprise régionale

INKIVARI

Objectifs de cette présentation

INKIVARI

Trois axes principaux :

- Rappel des principes généraux RGPD et des impacts dans vos entreprises
- Comment réduire la surface d'attaque
- Liens entre RGPD et cybersécurité


CASH
INVESTIGATION
NOS DONNÉES PERSONNELLES VALENT DE L'OR !

Avantages du RGPD

- Être dans la légalité
- Établir et renforcer la relation de confiance (Salariés, Clients, Partenaires, ...) : création de valeur
- Éviter de provisionner une amende
- Éviter de se faire bloquer une vente de son entreprise
- Éviter de se faire bloquer par un prospect/client
- Travailler son Hygiène informatique (Cyber Sécurité) et son Hygiène Juridique
- Suppression de la grande majorité des formalités CNIL
- Avantages en ce qui concerne l'image commerciale
- Valoriser les données de l'entreprise
- Fin d'une distorsion de concurrence

Le RGPD en 10 minutes !

Contexte

- **Règlement Général sur la Protection des Données « RGPD »**
- **S’inscrit dans la continuité de la loi « LiL » de 1978 et remplace la directive de 1995**
- **« Règlement Européen » est entré en vigueur en mai 2016 et applicable depuis le 25 mai 2018**

Il encadre la mise en œuvre des données à caractère personnel

L'occasion de travailler dans les règles (Hygiène informatique, Cadre juridique, …)

Génère de la confiance

Il concourt à la protection des droits et libertés des personnes

Le RGPD se mondialise

Rééquilibre de la concurrence pour acteurs européens et mondiaux

Qui doit s’y conformer ?

- Les entreprises (TPE, PME, ETI et GE)
- les administrations
- Les collectivités
- Les associations

Tous les organismes publics ou privés, quels que soient leur taille ou leur secteur d'activité, manipulant des données personnelles concernant des Européens, doivent se conformer au RGPD …

Le RGPD concerne aussi les sous-traitants qui traitent des données personnelles pour le compte d’autres organismes

CNIL.

- Informer & Protéger les droits
- Accompagner la conformité & conseiller
- Anticiper et innover
- Contrôler & Sanctionner
  - Sur place
  - Sur pièce
  - Sur audition
  - En ligne
  - Amende : 4 % du CA mondial – 20 M€

SANCTIONS

247 contrôles en 2020) :

- Dont 3 en Lorraine
- Dont 53 en ligne
- https://blog.alan.com/tech-et-produit/controles-par-la-cnil

Qu’est-ce qu’une donnée personnelle ?

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Ces données nous sont confiées pour une finalité précise, les personnes concernées doivent en conserver la maîtrise.

Une personne physique peut être identifiée :

- **Directement** → Nom, Prénom…
- **Indirectement** → numéro de sécurité sociale, ou de téléphone, Identifiant de connexion informatique...
- **Par croisement de données** → Géolocalisation, Centres d’intérêt, adresse... l’identification de la personne peut être facilement réalisée (notamment avec l’aide d’un algorithme)

Qu’est-ce qu’une donnée personnelle sensible ?

Catégories particulières de données à caractère personnel « données sensibles »

L'origine raciale ou ethnique

Infractions et condamnations pénales

Données santé/génétiques, empreinte digitale

Les opinions politiques ou l'appartenance syndicale

Les convictions religieuses ou philosophiques

Le règlement européen interdit de recueillir ou d’utiliser ces données, sauf, dans certains cas

Qu’est-ce qu’un traitement de données personnelles ?

« Est un traitement toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel {…} »

Concrètement, quels types d’opérations ?

- La collecte, l'enregistrement
- L'organisation, la conservation
- L'utilisation sous toutes ses formes : consultation, modification, extraction,
- La communication selon toute forme de mise à disposition
- L’archivage
- L’effacement ou la destruction …

C’est donc une notion très large, que ce soit au format **papier ou numérique**

Le responsable de traitement / le sous-traitant

- **Le responsable de traitement** à un rôle central, c'est lui qui détermine :
  - le « pourquoi » c'est-à-dire les objectifs poursuivis
  - le « comment » conditions techniques, matérielles et organisationnelles des opérations de traitements

- Le sous-traitant traite les données personnelles **pour le compte et sur instruction du responsable de traitement**, qui conserve la responsabilité du respect des obligations RGPD

« Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »

Exemples d'incidents :
Mauvais destinataire(s) de mail, cambriolage, perte d'un ordinateur ou d'un dossier, …

En cas de violation constatée qui présente un risque pour les personnes concernées :

- Notifier à la CNIL sous 72h (Article 33)
- Notifier à la personne concernée (Article 34) ;
  Si "efforts disproportionnés" -> communication publique
- Suspension du traitement
- Mettre à jour le registre des violations (Article 5.f)

Les acteurs de la conformité

- Le **responsable de traitement** doit mettre en œuvre des mécanismes et procédures pour démontrer le respect des règles (Accountability)
- Votre **référent/DPO**, vous conseille et vous accompagne en étroite relation avec la DSI et le service juridique (Notre référent est régulièrement le responsable Qualité)

La démarche de conformité RGPD est un projet dynamique et continu porté par tous :

- La direction
- Chaque collaborateur

Les 10 règles d'or à appliquer pour tout traitement

INKIVARI

- Licéité du traitement : 6 bases légales
  (Consentement – Contrat – obligat. Légale- intérêt légitime – service public – intérêts vitaux)
- Finalité du traitement : doit être définie précisément et légitime
- Minimisation : seules les données pertinentes et nécessaires sont traitées, de plus les données doivent être exactes et tenues à jour
- Protection particulière des données sensibles : ne peuvent être traitées que dans certaines conditions
- Conduire une Analyse d'impact relative à la protection des données (AIPD) quand requise
- Une conservation pendant une durée limitée : dès que la finalité est atteinte, elles sont archivées, supprimées ou anonymisées
- Obligation de sécurité des données traitées
- Transparence : définition des finalités et communication en cas de violation (Article 5.1.a)
- Droits des personnes (usager-agent) : informées de l'utilisation de leurs données et de la manière d'exercer leurs droits
- Validation des « partenaires » (conventions, contrat, CGV...)

La non-application de ces règles est passible de sanction par la CNIL

Liens entre RGPD et cybersécurité

INKIVARI

- Protection des données personnelles
  - Article 5.1.f
    - traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle
  - Article 25
    - Protection des données dès la conception et protection des données par défaut
  - Article 32
    - Sécurité du traitement
  - Article 35
    - Analyse d’impact relative à la protection des données

- Disponibilité + Intégrité + Confidentialité + Traçabilité

Sujet générateur de confiance et de croissance

- 71% des Français ont le sentiment que les données personnelles qu'ils communiquent sur Internet sont mal protégées (Odoxa – Janvier 2021)
- Établir et renforcer la relation de confiance (Salariés, Clients, Partenaires, etc.)
- Création de valeur
- Avantages en ce qui concerne l'image commerciale
- Valoriser les données de l'entreprise
- Pérenniser l'activité (ne pas rater un AO : délais/clauses)

Sécuriser les données

- Avoir des sauvegardes (Externalisée, chiffrées et testées)
- Avoir un PCA/PRA
- Réaliser des tests d'intrusion et audits de sécurité
- Se préparer à réagir à une violation de données
  - Qui prévenir ? Dans quel ordre ? Dans quel délai ?
    - CNIL
    - Personnes concernées
    - Élaborer le plan de communication
  - Comment réagir techniquement ?
    - Elaborer un Plan de Réponse à Incident
  - S'entraîner
  - Consigner et documenter pour renforcer et améliorer
- Pensez aux données papier !

La question n'est pas « est-ce que je vais être attaqué » mais « quand est-ce ... »

Les 6 étapes de la conformité RGPD

INKIVARI

1 **Désigner un pilote** qui exercera une mission d'information, de conseil et de contrôle en interne

2 **Cartographier** vos traitements de données personnelles à travers la création d'un registre des traitements

3 **Prioriser les actions** à mener pour vous conformer aux obligations définies dans le réglement

4 Gérer les risques à travers une **analyse d'impact sur la protection des données (PIA)**

5 **Organiser les processus internes** afin de garantir la prise en compte de la **protection des données à tout moment** lors de tout traitement

6 **Documenter** la conformité en **maintenant à jour** les actions et les documents réalisés à chaque étape à travers leur **réexamination et actualisation**

Analyse de sites internet

INKIVARI

Nombre de sites des membres	141	
Nombre de sites avec :		
- Faille de sécurité importante (à corriger au plus vite) :	19	13,48 %
- Faille de sécurité potentielle :	86	60,99 %
- Cookie avec durée invalide :	88	62,41 %

Check list RGPD du responsable - Interne

INKIVARI

- RH (Fiches de paie, Contrats salariés, NDA Stagiaires, ...)
- Points d'alertes
  - Géoloc, vidéo surveillance, NIR, données « sensibles »
  - Utilisation du mot « anonyme »
- Collecte de données sans mentions RGPD
- Appliquer le Privacy by design
  - mieux vaut changer un word qu'un code ou un process validé
- Sensibilisation des équipes (surtout ceux en contact des clients)
- Procédures
  - Reconnaître une VDD et réagir
  - réagir en cas d'exercice de droit
  - réagir en cas de contrôle CNIL / demandes clients, prospects, investisseurs / Accountability
- Besoin d'un DPO, d'un registre ?
- Sécurisation données papiers et numériques
  - Sauvegarde des données
    - Lieu, fréquence, tests
    - (sauvegarde de ce qui est uniquement « dans le cloud »
  - PCA/PRA

Check list RGPD du responsable - Externe

INKIVARI

- Vente : Vos contrats / CGU / CGV
- Votre site, votre app mobile
- Avoir une documentation « commerciale » à jour
  - Avoir un Plan d'Assurance Sécurité (PAS)
  - Registre de sous-traitance
- Conformité de vos sous-traitants / partenaires
  - Transfert Hors UE, Contrats, …
- Conventions entre filiales
- Attention aux mélanges de « vos casquettes »
  - Mandataire d'une entreprise et d'une
- Règles de prospection
- Choix des outils (Hubspot, Stripe, ...)

Présentation d’un Registre

INKIVARI

- 1 - Ressources Humaines ** 19
- 2 - Adminstration des ventes - Gestion Commerciale ** 2
- 3 - Achat - Fournisseurs ** 1
- 4 - Marketing & Communication ** 4
- 5 - Production
- 6 - SAV
- 7 - SI ** 4
- 8 - Gestion statutaire ** 1
- 9 - Gestion administrative - comptable - budgétaire ** 1
- 10 - Fonctionnement courant des services ** 2
- 11 - Hygiène Sécurité Environnement ** 1
- 12 - Qualité ** 1

Démo DPO Assist – index du registre

REGISTRE

DES ACTIVITÉS DE TRAITEMENT

DE Inkivari

Coordonnées du responsable de l'organisme :

Inkivari
RUE GENERAL DE REFFYE 88000 EPINAL

Coordonnées du délégué à la protection des données (DPD/DPO) :

Pas de DPO désigné

Version publique

Table des matières

- **Activité 1 - Achat - Fournisseurs**
  - Activité 1.1 - 1410-Suivi administratif des contrats
- **Activité 2 - Adminstration des ventes - Gestion Commerciale**
  - Activité 2.1 - 1413-Gestion de la relation client
  - Activité 2.2 - 1421-Réalisation d'actions de prospection commerciale
- **Activité 3 - Fonctionnement courant des services**
  - Activité 3.1 - 1942-Traitements nécessaires au fonctionnement courant des Services
  - Activité 3.2 - 1955-Sinistres des véhicules
- **Activité 4 - Gestion administrative - comptable - budgétaire**
  - Activité 4.1 - 1901-Gestion administrative comptable-budgétaire
- **Activité 5 - Gestion statutaire**
  - Activité 5.1 - 1419-Organisation et fonctionnement des assemblées
- **Activité 6 - Hygiène Sécurité Environnement**
  - Activité 6.1 - 1945-Prévention des risques professionnels
- **Activité 7 - Marketing & Communication**
  - Activité 7.1 - 1411-Site Web

Kiitos !

INKIVARI

cyril@inkivari.com

03 74 11 71 96

Slides supplémentaires

L’exercice des droits des personnes

INKIVARI

Exercice des droits à prévoir selon la base légale du Traitement : 1 mois pour répondre

	Droit d’accès	Droit de rectification	Droit à l’effacement	Droit à la limitation du traitement	Droit à la portabilité	Droit d’opposition
Consentement	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	Retrait du consentement
Contrat	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Non**
Intérêt légitime	**Oui**	**Oui**	**Oui**	**Oui**	**Non**	**Oui**
Obligation légale	**Oui**	**Oui**	**Non**	**Oui**	**Non**	**Non**
Intérêt public	**Oui**	**Oui**	**Non**	**Oui**	**Non**	**Oui**
Intérêts vitaux	**Oui**	**Oui**	**Oui**	**Oui**	**Non**	**Non**

La base légale d’un traitement

La base légale d’un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de traiter des données à caractère personnel. On peut également parler de « fondement juridique » ou de « base juridique » du traitement.

[Art 6 .1 a]	**le consentement**	*la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques.*
[Art 6 .1 b]	nécessaire à l'**exécution d'un contrat** ou aux mesures pré-contractuelles	*le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures pré-contractuelles prises à la demande de celle-ci.*
[Art 6.1 c]	l'**obligation légale** à laquelle le responsable de traitement est soumis	*le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis et qui impose la mise en œuvre du traitement de données.*
[Art 6 .1 e]	la **mission d’intérêt public** dont le responsable de traitement est investi	*le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.*
[Art 6 .1 f]	l'**intérêt légitime** du responsable de traitement	*le traitement est nécessaire à la poursuite d’intérêts légitimes de l’organisme qui traite les données ou d’un tiers, dans le strict respect des droits et intérêts des personnes dont les données sont traitées. A moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.*
[Art 6 .1 d]	la sauvegarde des **intérêts vitaux**	*le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.*

Respecter les droits des personnes concernées

INKIVARI

Article 15

"La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel [...]"

Article 16

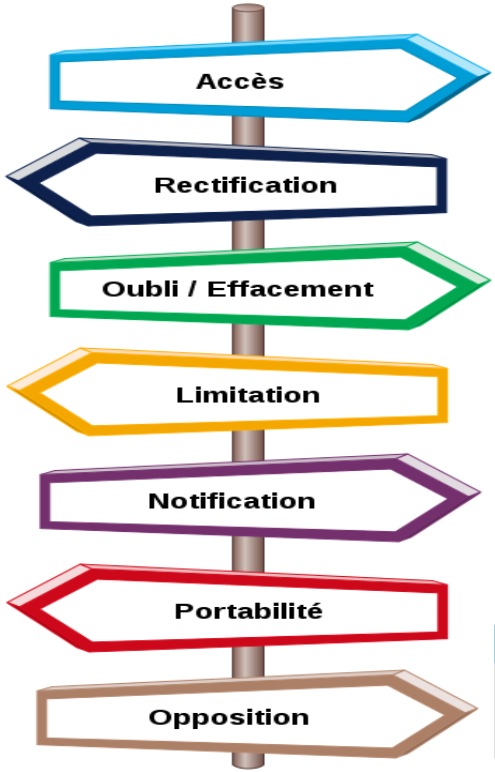
"La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes."

Article 17

"La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais [...]"

Article 18

"La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement [...]"



Article 19

"Le responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement [...]"

Article 20

"Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement [...]"

Article 21

"La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant [...]"