



Petit Déjeuner E Business :

Le Règlement Général sur la Protection des Données (RGPD)

Jeudi 15 février 2018



Les intervenants

-> Erick Bullier



- Consultant senior en Cybersécurité,
- Enseignant à l'université de Montpellier (DU Cybercriminalité) et à l'Université Technologique de Troyes (Master Big Data),
- Fondateur et dirigeant du cabinet de conseil SCIURUS
- Président de l'association WOCSA (Worldwide Open Cyber Security Association)



Les intervenants

-> Jean-François Escala



- Master II en droit des Contrats et de la responsabilité des professionnels.
- Juriste d'affaires au sein de la Direction juridique d'un groupe industriel multinational (5 ans)
 - Droit des sociétés, Droit des affaires, Droit des contrats, Droit de la propriété intellectuelle.
 - Conformité « Informatique et Libertés » du groupe
- Consultant « Informatique et Libertés » (2 ans).





Plan

1. Présentation générale
 1. Le RGPD
 2. Une véritable nouveauté?
 3. Des notions qui fâchent...
 4. Les obligations
2. Suis-je concerné
 1. Comment
 2. Avec qui?
3. Déroulement type d'une démarche
 1. Inventaire
 2. Analyse
 3. Gestion du risque
4. Bilan



1. RGPD - Présentation générale



- Règlement Général sur la Protection des Données.
- Règlement européen entrant en vigueur fin mai 2018
- Un cadre juridique **unifié** pour l'ensemble de l'UE
- Un renforcement des **droits des personnes**
- Une conformité basée sur la **transparence** et la **responsabilisation**
- Des responsabilités partagées et précisées
- Des sanctions encadrées, graduées et **renforcées**



1.2 Une nouveauté?



- Pas véritablement.
 - > s'appuie sur des textes existant déjà
 - > Le règlement étend et renforce la DPD de 1995
- En fait, il remplace les 28 lois nationales sur la protection des données qui déclinent la directive européenne sur la protection des données de 1995 (DPD) et entend uniformiser leur application.





1.3 Des notions qui fâchent...

- DPO (Data Privacy Officer) ou DPD (délégué à la protection des données)
- Privacy by Design
- Privacy by Default
- Droit à l'oubli
- Droit à la portabilité, à la rectification, à l'effacement, etc.
- Responsabilité du commanditaire (« pas » de délégation)





1.4 Les obligations

- Tenir et maintenir un registre de traitement des données
- Effectuer une analyse d'impact
- Mettre en œuvre les procédures et les mesures de sécurité
- Informer en cas de faille ou de fuite de données (72h)
- Mettre en œuvre l'ensemble des procédures pour traiter les demandes des individus (rectification...)



1.4 Les obligations (ed)



- Recueillir le consentement express et explicite des individus
- Sensibiliser les personnels à la protection des données
- S'assurer du respect des obligations du GDPR de bout en bout
- Être en mesure de démontrer que le traitement est conforme au RGPD par la mise en œuvre de mesures techniques et organisationnelles appropriées dès l'origine





En fait, suis-je réellement
concerné?





2. A priori oui...

- **Applicable à toute personne** (physique/morale)
- **Pas d'exception hors traitements « domestiques »** ou secteur police/justice (*directive ad hoc*) ; loi impérative
- **Raisons d'être de la loi :**
 - Renforcer la protection des droits des citoyens
 - Libre circulation corrélative des DCP
 - Assurer son respect par des amendes TRÈS dissuasives pouvant aller jusqu'à...
 - 20 millions d'euros
 - 4% du chiffre d'affaires monde
 - Attention aux procès qui vont devenir monnaie courante...





2. Pourquoi?

- Bénéfices d'une mise en conformité :
 - **Éviter le risque judiciaire** (*amende, emprisonnement..*) et d'atteinte à la réputation / à l'image (*publication des sanctions, baisse de confiance, des ventes...*)
 - **Inspirer la confiance et prévenir les arrêts de production** par la qualité des traitements de données, la sécurité de l'information et du SI → solidité pratique et démonstration de la capacité à gérer correctement les DCP utilisées
 - **Augmenter les opportunités de contrats**, de plus en plus nombreux à exiger la conformité (ex. marchés publics, U.E.), et optimiser les conditions de cession d'entreprise (non-conformité = levier de négociation du prix)





2.1 Se mettre en conformité

- Une démarche globale et un véritable investissement
- Ne doit plus être du ressort de la DSI ou du RSSI, mais de la DG
- Avant tout chose, il faut désigner un pilote (qui peut être le DPO/DPD)
-> Se faire accompagner ou former une ressource interne
- La démarche est itérative (donc, doit faire l'objet d'un véritable suivi) et doit générer des traces (enregistrements)



2.1 Se mettre en conformité (ed)



2.2 Se mettre en conformité?



- Seul
 - Site web de la CNIL
 - Associations
 - Oui, mais...
- En se faisant accompagner
 - Beaucoup d'acteurs très opportunistes
 - Très peu de spécialistes
 - Nécessite des compétences croisées en « informatique et liberté, droit (privacy) et sécurité des SI »
 - Coût souvent élevé.
 - Surbooking des (bons) prestataires à prévoir avec l'arrivée de l'échéance...





2.3 Concrètement...

- Une approche globale et une révision complète des processus de l'entreprise:
 - Nécessite une **vision et une expertise à 360°** (informatique et liberté, juridique, analyse d'impact, et cybersécurité),
 - **quelle que soit la phase abordée**, il faudra la traiter avec le même sérieux et la même compétence
 - Ne supporte pas l'industrialisation du processus:
 - Personnalisation du travail indispensable
 - Accompagnement des collaborateurs



3. Prérequis indispensable



- Il faut désigner et (éventuellement) former un pilote
- Ce pilote pourra être désigné DPO/DPD (ce n'est pas une obligation dans le texte)
- Si vous disposez déjà d'un CIL, c'est lui qui peut être naturellement désigné.
- Il est possible de déléguer la fonction de DPO à un prestataire externe.



3.1 Inventaire





3.1 Cartographie des traitements

- Cartographier, c'est la première étape de toute démarche conformité
- Il faut recenser précisément dans un **registre** dédié les différents **traitements de données personnelles** mis en œuvre.

Exemples de traitements de données personnelles :



Fichier clients



Outils métiers



CV



Dossier pro



Organigramme



Site web



Mailing



Planning



Outils métiers



Gestion terminaux



Réseaux sociaux



Jeux - Lotteries



vidéosurveillance



Badges



Tracking GPS



3.1 Cartographie des traitements



- Pour chaque traitement de données personnelles, il faut identifier :
 - **Qui?** Les acteurs qui traitent ces données.
 - Internes : Salariés
 - Externes : Fournisseurs, Prestataires et sous-traitants ;
 - **Quoi?** Les catégories de données personnelles traitées
 - **Pourquoi?** Les objectifs poursuivis le traitement de données (la finalité)
 - **Où? Jusqu'à quand? Comment?**
 - Les moyens mis en œuvre
 - Les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne.
 - Les destinataires des données
 - Les durées de conservation

3.1 Cartographie des traitements



DÉROULEMENT DE LA PRESTATION

Étape préalable : Nécessité de communiquer en amont sur la nature et la teneur de l'intervention en utilisant un média adapté à la culture d'entreprise afin de favoriser une remontée d'information qualitative par les personnes interviewées.



3.1 Cartographie des traitements



BÉNÉFICES DE LA CARTOGRAPHIE

- Sur la base du registre des traitements, vous identifierez les actions à mener pour vous conformer aux obligations actuelles et à venir.
- Vous pourrez prédéterminer la priorité des actions à mener au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.
- Pour les traitements réellement à risque, il faudra passer par l'analyse d'impact (PIA)



3.2 Analyse



3.2.1 Définitions: PIA/DPIA = AIPD



- Définition (DPIA): analyse de l'impact des opérations de traitement envisagées sur les droits et libertés des personnes.
- Définition (PIA): analyse de l'impact d'un projet ...



3.2.2 AIPD: Objectifs

- Objectifs : (imposés par le RGPD)
 - Démontrer la « nécessité » et la « proportionnalité » du/des traitements compte tenu de leur finalité (= *tests de N. et P.*)
 - Identifier les risques générés par les traitements sur les données traitées et les droits et libertés (= *analyse de risques*)
 - Identifier ...
 - Les mesures envisagées pour traiter ces risques ...
 - dont des garanties et mesures de sécurité visant à ...
 - protéger les DP
 - prouver la conformité au RGPD (= *test de conformité + risques de non-conformité*)
 - ... qui inclut un test de « compatibilité » et d' « intérêt légitime » (= *tests + risques de non-conformité*)
 - ... compte tenu de l'ensemble des personnes affectées (= *protection des tiers aux données*)



3.2.3 DPIA - Comment procéder?



- **Étape 1 :**

- Détermination des personnes qui
 - décident de la conduire, de ses termes et conditions, des ressources dédiées, du temps alloué,
 - en approuveront les résultats (+ procédés de prise de décision),
 - décideront de la manière dont les résultats seront mis en œuvre,
 - contribueront à l'étude, la manière dont elles seront sélectionnées, les méthodes de communications externes / internes
- Les personnes en charge de l'AIDP doivent agir en toute indépendance professionnelle ... elles doivent :
 - avoir l'expertise, les ressources et le temps nécessaires
 - s'efforcer de reconnaître et formaliser leur potentielle subjectivité
 - Idéalement, être indépendantes de l'entité ou du consortium à l'origine du traitement / projet (une supervision indépendante peut être une alternative).

3.2.3 AIPD – Comment procéder?



- **Contenu de l'AIPD :**

- Description des opérations envisagées
- Analyse de conformité aux principes de « nécessité » et de « proportionnalité » (référence : CEDH)
- Analyse de conformité au RGPD
- Identification et analyse des risques (conforme aux normes internationales de gestion des risques dont ISO/IEC 27001 – appliquées aux DP/DL)
- Évaluation des risques
- Mesures de traitement des ...
 - ... faiblesses en termes de nécessité et proportionnalité
 - ... faiblesses de conformité au RGPD
 - ... risques, incluant ceux menaçant la conformité RGPD



3.2.4 Une obligation?

- **Cas de PIA obligatoire : (RGPD, art. 35)**
 - Risques élevés pour les DL - notamment en cas de recours à de nouvelles technologies en fonction des natures, portées, contextes et finalités du traitement.
 - Exigé pour
 - **Évaluation systématique** et approfondie d'aspects personnels
 - **Traitements à grande échelle** de catégories particulières de données sensibles
 - **Surveillance systématique** à grande échelle d'une zone accessible au public
 - La CNIL peut dresser une liste complémentaire





3.2.4 Une obligation?

- **Cas de PIA obligatoire : (hors RGPD, art. 35)**

Tous traitements, s'agissant ...

- De la **démonstration de conformité RGPD** (art.24)

Obligation de mise en œuvre « des mesures techniques et organisationnelles » permettant de s'assurer + être en mesure de démontrer la conformité RGPD

- Du **test de compatibilité / d'intérêt légitime** (art. 6 1f & 4)

+ identification des risques : le test de compatibilité doit tenir compte des conséquences possibles du traitement pour les droits et libertés

- Du **test de nécessité** (et de proportionnalité)

Art 6 : le traitement doit être « nécessaire aux fins des intérêts légitimes poursuivis » + nombreux autres articles faisant référence à cette notion

- De l'**identification / traitement des risques** (art. 32)

Compte tenu de l'état des connaissances, coûts (...), nature / portée / contexte / finalités du traitement et risques pour les DL [et leur degré de probabilité], resp. + sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.



3.3 Mise en place mesures « correctives » et préventives



3.3.2 Obligation globale de sécurité



- Les organisations ont pour obligations de mettre en place les **mesures techniques et organisationnelles appropriées** afin de garantir un niveau de sécurité adapté aux données personnelles.
- Les risques pour les individus résultent notamment de:
 - la destruction,
 - la perte,
 - l'altération,
 - la divulgation non autorisée de données à caractère personnel.



3.3.3 Mise en place mesures correctives (..ed)



- A titre d'orientations pratiques, le texte met l'accent sur :
 - la pseudonymisation (vs anonymisation),
 - le chiffrement des données tout au long de leur cycle de vie
 - l'évaluation régulière des mesures de sécurité,
-> audits



3.3.2 Mise en place mesures correctives (..ed)



- La cartographie et la PIA effectuées en phase 1 et 2, permettent :
 - d'**identifier les actifs** à protéger,
 - de les **ordonner par priorité** (importance du risque).
- Le traitement du risque (phase 3) va essentiellement consister en deux actions:
 1. **Documenter** (actions, analyses et décisions),
 2. Mettre en place les **mesures techniques** pour...
 - réduire à un niveau acceptable le risque pesant sur les données personnelles.
 - viser la conformité au texte.



3.3.2.1 Documenter

- Mise en place/adaptation d'un **système de gestion documentaire**:
 - Il revient à l'entreprise **d'assurer la traçabilité** des données et des mesures de sécurisation mises en œuvre.
 - L'entreprise doit mettre en place les procédures internes adaptées pour **la gestion et la notification des incidents de sécurité**.
 - L'analyse d'impact (puis de risque) doit être **révisée régulièrement**. Elle contribue à la preuve du « privacy by design » et « by default »
 - Les mesures mises en place doivent **générer des enregistrements** qui doivent être **conservés**.



3.3.2.2 Mettre en place les mesures techniques



- Mise en place d'un « système de management de la sécurité de l'information ».
 - **Adapté** à votre taille et vos moyens.
 - Seul capable de garantir **dans le temps** :
 - l'amélioration continue de la sécurité des données
 - la cohérence des mesures avec les traitements de données (qui évoluent)
 - **Impose les bonnes pratiques:**
 - Documentation,
 - Qualité des mesures implémentées
 - Cohérence des mesures déployées et déployables
 - Transparence des actions



Conclusion



- Une démarche conséquente, mais qui va dans le bon sens.
- L'application du règlement concerne toutes les entreprises, quelle que soit leur taille.
- Elle est abordable par tous. Il vaut mieux faire peu avec ses moyens que de ne rien faire.
- Attention: ne pas gérer le risque d'une atteinte à la sécurité des données privées que vous gérez pourrait demain vous coûter beaucoup plus qu'une amende.
- N'hésitez pas à venir nous voir, et prenez garde aux vendeurs de rêves...

