Grant Thornton

Intervenant(s)
- Emmanuelle Muller-Schrapp
Associée, Finance & IT transformation
- Nicolas Rémy-Néris
Avocat, Correspondant Informatique & Liberté
- Jean de Laforcade
Directeur Associé, Risk management

Bienvenue aux

GRANT THORNTON ADVISORY DAYS

La Fraude : 50 nuances de Conseil

Jeudi 23 mars 2017

Sécuriser votre CRM et la gestion des données personnelles

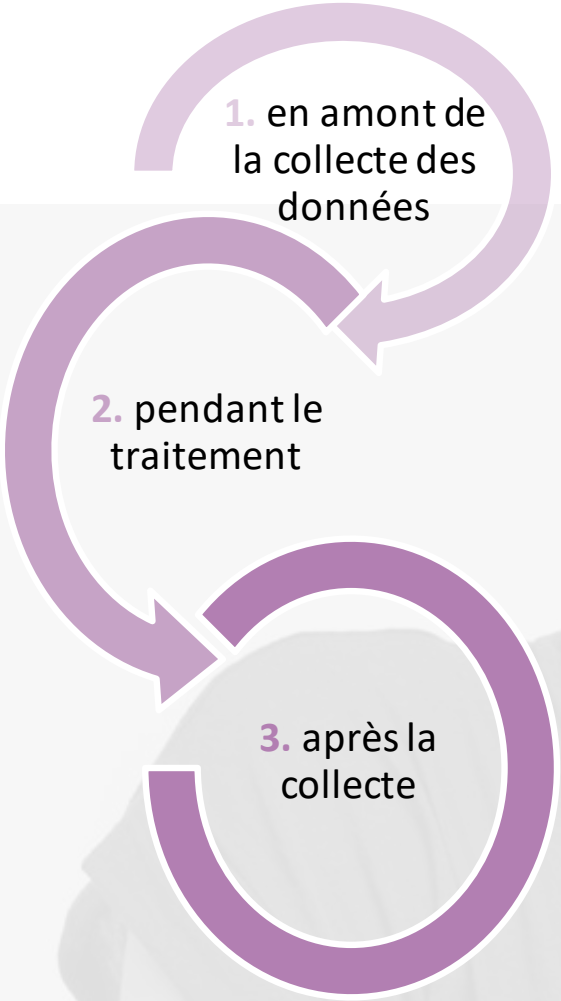
Fraude et digital média, quels enjeux face au renforcement de la législation?

Présentation du Règlement européen sur la protection des données personnelles (RGPD) n°2016/279

- Adoption le 27 avril 2016 et entrée en vigueur le 25 mai 2018 (application directe dans les pays de l'Union Européenne aux acteurs privés, publics et aux associations, ainsi qu'à leurs sous-traitants)

Vocation	Autorités compétentes
▪ **protéger les personnes résidentes d'un pays de l'UE** dont les données personnelles font l'objet d'une collecte et d'un traitement quelles que soient leur localisation (UE ou hors UE)	le **Comité européen de protection des données (CEPD)** et la **Commission nationale de l'informatique et des libertés (CNIL)** au niveau national
▪ **protéger les résidents non-UE** pouvant aussi bénéficier d'une protection sur la collecte et les traitements réalisés au sein de l'UE	

Durcissement de la législation



- information sur **l'usage des données**
- **consentement préalable** de la personne concernée

- **licéité** du traitement
- traitement limités aux **finalités acceptées par la personne** concernée
- **registre des activités** des traitements opérés

- droit à la **limitation du traitement**,
- droit **d'accès**, droit **de rectification**, droit **à l'oubli**
- droit à **la portabilité des données**, droit **d'opposition**
- **sécurité des traitements**
- **notification** sous 72h aux personnes concernées et à la CNIL en cas de failles de sécurité

Sanctions

Sanctions/alertes

avertissement, mise en demeure, limitation ou arrêt de traitement, suspension des flux, ordre de mise en conformité, ordre de retirer l'agrément/conformité émise par un tiers voire retrait direct

Sanction administrative

maximum de 20 millions d'euros d'amendes ou 4% du CA mondial consolidé.

Droit à réparation

pour les personnes lésées (actions de groupe possibles du fait de la "Loi sur la Modernisation de la Justice du 21ème siècle")

Réputation et Image

risque accru sur la réputation et l'image (perte de clientèle, chute du cours de bourse,…)

Collecte & Traitement de l'information

- Dans le cadre de la collecte et du traitement de l'information il faut satisfaire de nombreuses exigences et droits : **d'accès, de rectification, à l'oubli, à la limitation du traitement, à la portabilité des données, d'opposition, …**
- Pour garantir la conformité il faut **identifier la donnée collectée et son devenir**

Quelles sont les questions à se poser ?

Qui collecte l'information et par quel canal ?	Quelle forme prend l'output du traitement ? Où est-il localisé ?
Le consentement et l'information nécessaires sont-ils respectés ?	Qui utilise cet ouput, à quelle fin et qui d'autre en bénéficie potentiellement ?
Qui stocke l'information (où, quel format, quel système, en interne/externe) ?	L'accès aux informations respecte-t-elle des protocoles de sécurisation ?
Quels sont les transferts opérés au niveau de la donnée collectée ?	Combien de temps l'information est-elle ou doit-elle être détenue ?
Quels sont les différents traitements opérés et par qui sont-ils réalisés ?	L'information relative à cette collecte et traitement est-elle communiquée au CIL/DPD et répertoriée dans le registre des traitements ?

Renforcer le contrôle interne autour de la conformité

Définir un **mode de gouvernance** adapté

Mettre en œuvre des **évaluations** à titre de **contrôles périodiques** en interne ou externe

Cartographier tous les **traitements** ainsi que toutes les **parties prenantes** concernées

Déployer un **contrôle interne permanent ciblé**

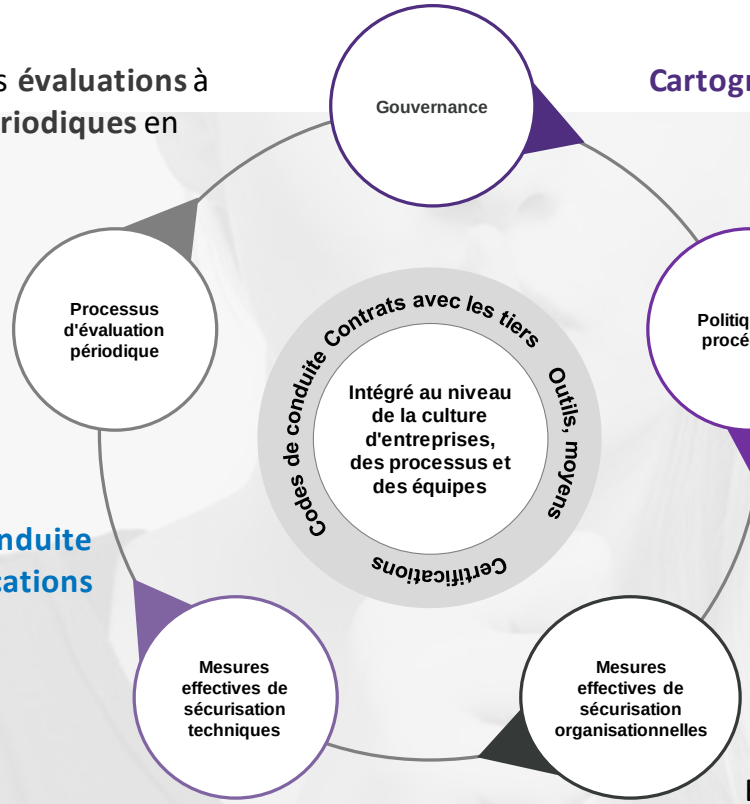
Cadrer le fonctionnement cible par des **politiques, procédures et contrats**

Adhérer à des **codes de conduite** ou préparer des **certifications**

Déployer de nouveaux **processus mesurables et contrôlables**

Sécuriser les **Systèmes d'Informations**

Etre en mesure d'apporter les **preuves de conformité** attendues à son niveau ainsi qu'au niveau des sous-traitants



Sécuriser les SI - Focus sur la Cyber sécurité

- Il vous sera impossible de **garantir une parfaite sécurité de votre système d'information** vis-à-vis d'intrusions par des personnes malintentionnées en interne ou externe. L'intrusion devant être déclarée à l'autorité de contrôle sous 72 heures.
- Néanmoins, l'absence de mesures de sécurité effectives sera considérée comme **une négligence** et donc comme **un facteur de nature à aggraver la sanction administrative.**

Quelles diligences apparait-il nécessaire de mettre en œuvre ?

- Un **corpus documentaire** axé sur la sécurité des SI (politiques, procédures, chartes…) supportant des processus opérationnels
- **Des activités portant sur l'existence** :
  - d'une veille relatives aux failles de sécurité
  - d'un processus d'application des correctifs sécurité (OS, SGBD, applications) des tests internes de détection de vulnérabilités (ex : scan de vulnérabilités)
  - d'un dispositif de détection d'un incident de sécurité
  - d'une revue de code de sites web, d'applications mobiles
- La mise en œuvre périodique **de tests d'intrusions tant internes qu'externes**
- La réalisation **d'audits internes ou externes** axés sur la sécurité du SI

Conformité des sous-traitants - Diligences vis-à-vis des tiers

Qui est concerné ?

- Tout prestataire de services impliqués dans la fourniture de solutions (application Saas), l'hébergement (mode Cloud), et la réalisation de traitements en lien avec les données personnelles du client (Big Data)

Exemples de prestataires

amazon web services™ · salesforce · Google · OVH.com · Microsoft Azure

Comment se protéger au mieux ?

Revoir et enrichir les contrats en vigueur

- Détenir une clause d'auditabilité pour mener des audits de vérification le cas échéant
- Intégrer des engagements clairs aux contrats: *responsabilité, obligation de mise en conformité, sécurité,, information en cas d'atteinte aux données*
- Imposer de nouveaux indicateurs de SLA *(délai pour être prévenu en cas d'atteinte aux données...)*

Disposer d'un confort supplémentaire sur la conformité du prestataire

- La preuve d'une attestation externe *(ex: ISAE 3402, SOC 2 ou 3 avec un focus Privacy)*
- L'obtention de certifications *(ISO 27001 Sécurité, ISO 27018 Cloud Privacy)*