

RGPD : CHECK (& WAKE) UP !

INNOVATION, AUDIT, SÉCURITÉ, ACCOMPAGNEMENT, RESPONSABILITÉS ET BÉNÉFICES

#CYBERDAY | 20.02.19

Intervenants :

- **Marie de Fremerville** (ex-Directrice de la gouvernance des filiales / **AIRBUS GROUP**)
- **Matthieu Grall** (Directeur de l'expertise technologique / **CNIL**)
- **Fabian Guion** (Consultant RGPD / **GAC GROUP**)



SOMMAIRE

01 | INTRODUCTION

02 | 5 QUESTIONS À LA CNIL

03 | TABLE RONDE

04 | CONCLUSION



1

INTRODUCTION



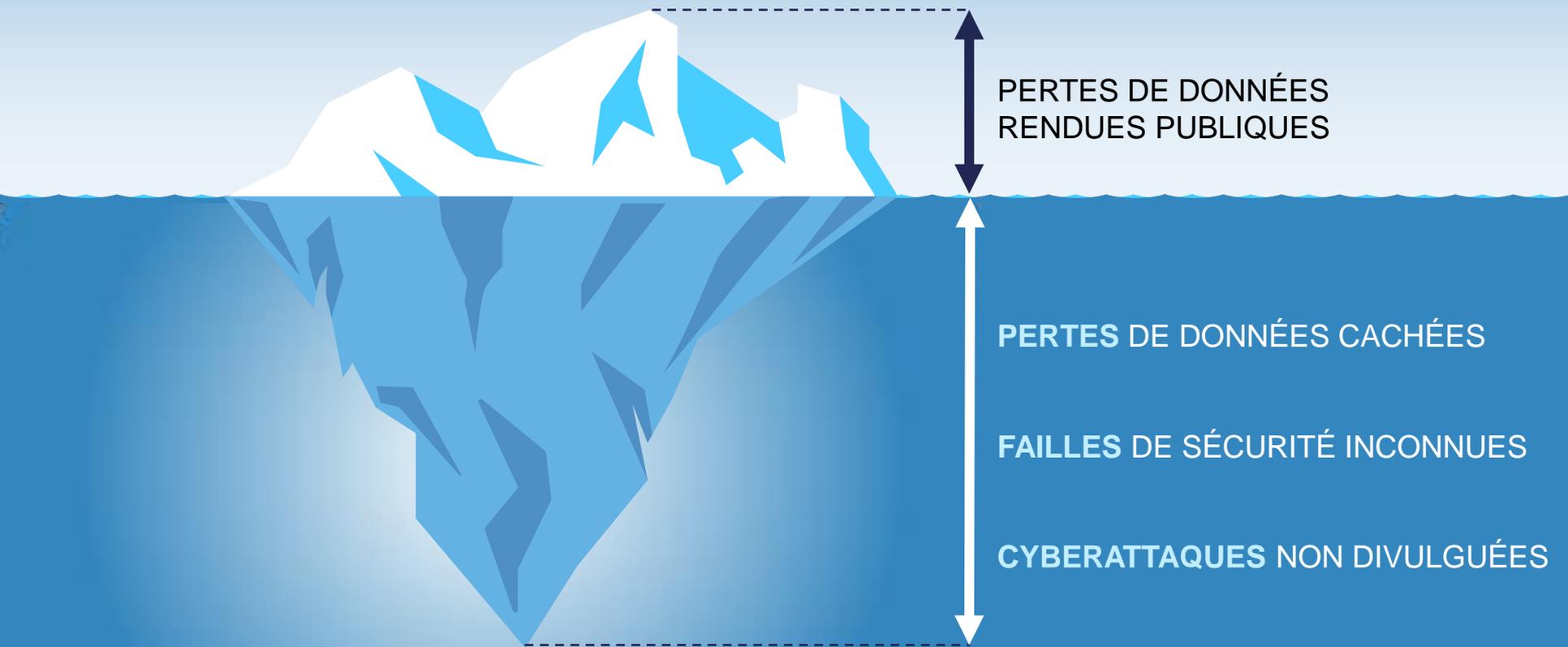
CYBERSÉCURITÉ & RGPD, PERSONNE N'EST PARFAIT !



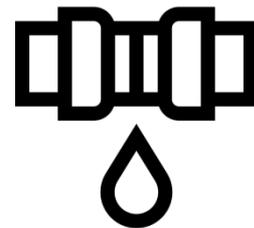
Dans cette liste figuraient par exemple, le directeur de la sécurité informatique de l'Elysée, le responsable infrastructure de l'Autorité de sûreté nucléaire ou encore deux cent entreprises que le gouvernement a jugé « critiques pour le bon fonctionnement de la Nation ».

Pour y accéder, [une simple requête dans le moteur de recherche](#) du site du club avec les termes Clusif et CSV suffisait à ouvrir « la caverne d'Ali baba ».

LE TITANIC ÉTAIT UN PAQUEBOT RÉPUTÉ « INSUBMERSIBLE » »



2018, UNE ANNÉE RICHE...EN FUITE DE DONNÉES !



Faille majeure pour Facebook, près de 50 millions de comptes exposés à des pirates

Le Nouvel Obs – 28/09/2018

Google ferme son réseau social Google+ après une faille ayant exposé des données personnelles pendant trois ans

Usine Digitale – 09/10/2018

Les données personnelles d'un millier d'élus allemands (dont la chancelière Angela Merkel) ont été piratées et publiées sur Twitter avant Noël.

Kaspersky Lab 01/19

2018, UNE ANNÉE RICHE...EN CYBERATTAQUES !



48 heures après la SSII Altran, c'est au tour du géant de l'aérien et de la défense, Airbus, d'être victime d'une piratage informatique. Deux attaques qui interviennent une semaine après le FIC !

Le Monde Informatique / 02/19

Cyberattaque à Atlanta: une rançon demandée en bitcoins !
Les hackers ont utilisés un logiciel élaboré par la NSA.
L'attaque aurait coûté 10 millions de dollars à la ville.

AFP – 02/18

Les cybercriminels délaissent le pillage des particuliers depuis des imitations de Paypal pour dévaliser les entreprises avec des contrefaçons de sites Office 365.

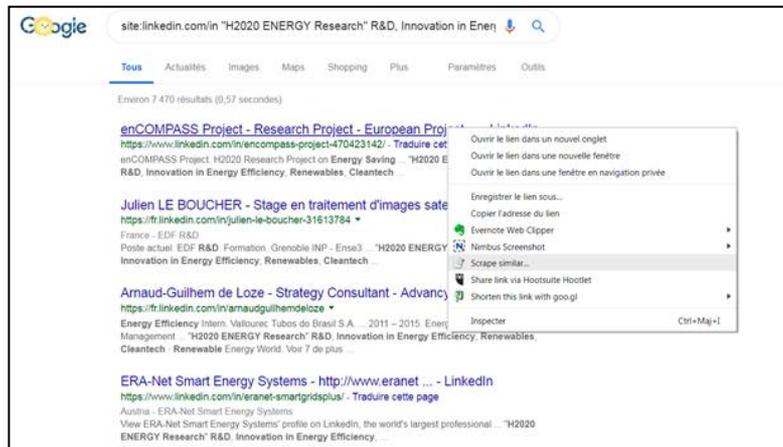
Vadeseure – 10/18

2018, UNE ANNÉE RICHE...EN SPAM !



COMMENT EXTRAIRE LES MEMBRES D'UN GROUPE LINKEDIN SANS EN FAIRE PARTIE ?

- 1- Ajoutez [l'extension Chrome « Scrapper »](#)
- 2- Ouvrez un fichier Google Excel
- 3- Affichez un groupe sur LinkedIn
- 4- Copiez / collez le nom du groupe sur Google avec cette manière d'écrire : « `site: linkedin.com/in` « NOM DU GROUPE »
- 5- Tous les résultats s'affichent (ne pas hésitez à débloquent le curseur d'affichage / page)
- 6- Cliquez droit sur la première URL puis sur « Scrapper »
- 7- Copiez « to clipboard » puis collez dans Google Excel



The screenshot shows a Google search interface with the search query "site:linkedin.com/in "2020 ENERGY Research" R&D, Innovation in Ener". The search results are displayed in a list format. The first result is "enCOMPASS Project - Research Project - European Proj" with the URL "https://www.linkedin.com/in/encompass-project-470423142/". A right-click context menu is open over this first result, showing options such as "Ouvrir le lien dans un nouvel onglet", "Ouvrir le lien dans une nouvelle fenêtre", "Ouvrir le lien dans une fenêtre en navigation privée", "Enregistrer le lien sous...", "Copier l'adresse du lien", "Evernote Web Clipper", "Nimbus Screenshot", "Scrape similar...", "Share link via Hootsuite Hootlet", and "Shorten this link with googl". The "Scrape similar..." option is highlighted. Below the first result, other search results are visible, including "Julien LE BOUCHER - Stage en traitement d'images sate" and "Arnaud-Guilhem de Loze - Strategy Consultant - Advancy".

2018, UNE ANNÉE RICHE...POUR FACEBOOK !



L'autorité de la concurrence allemande a demandé à Facebook de cesser de collecter et combiner les données personnelles des utilisateurs de ses différentes plateformes, à savoir Instagram et WhatsApp.

Journal du Geek 02/19

Facebook a payé des utilisateurs âgés de 13 à 35 ans pour obtenir des données précises quant à l'utilisation de leur smartphone (messages privés, photos, vidéos, mails, sites consultés ou encore recherches effectuées).

Clubic 01/19



Leur CA 2018 a bondi de 47% et atteint 40,6 Mds !
Le nombre d'utilisateurs est « conforme aux attentes » : 2,13 Mds
Les recettes publicitaires mobiles : 89% des recettes totale.

Ouest France 01/19

2018, UNE ANNÉE RICHE...EN PRISE DE CONSCIENCE !



**60% des consommateurs jugent que la protection des données personnelles n'est pas une priorité pour les entreprises.
80% estiment que la mauvaise gestion des données personnelles menace leur liberté fondamentale !**

OpinionWay 12/18

Le réseau social « Skred » permet de passer des appels, d'échanger des textos et de transférer des fichiers de manière sécurisée. L'échange se déroule donc de « pair à pair », sans laisser aucune trace !

Les Echos 11/18

Safran va utiliser Qwant le moteur de recherche européen qui respecte la vie privée et ne collecte pas les données personnelles de ses utilisateurs, par défaut sur l'ensemble des 91K postes de travail ayant un accès internet.

Global Security Mag 01/19

EN SYNTHÈSE...PERSONNE N'EST (VRAIMENT) PRÊT & À JOUR !

35 % des foyers

détiennent jusqu'à 10 appareils connectés

(Source : Global Security Mag 01/19)

+150 % d'attaques

de type « cheval de Troie bancaire »

(Source : Global Security Mag 01/19)

42 % des entreprises

ont été touchées par des logiciels malveillants (vs 20,5 % en 2017)

(Source : Rapport Check Point 07/18)

Les **infrastructures dans le Cloud** sont de plus en plus utilisées donc ciblées

(utilisées par plus de 50 % des entreprises françaises / AWS)

EN SYNTHÈSE...PERSONNE N'EST (VRAIMENT) PRÊT & A JOUR !

65% des collaborateurs

craignent de se faire « voler »
leur identité numérique

(Source : Sailpoint - 10/18)

1 entreprise sur 10

a mis en place un véritable
programme de cyber-résilience

(Source : CESIN / OpinionWay – 01/19)

6 000 postes ouverts vs. 1 200 pourvus

chez les spécialistes de la
cybersécurité :

(Source : Le Télégramme 01/19)

Industrialisation d'attaques de type « **cyber-Pearl Harbour** » en 2019 ?

(A l'occasion du FIC de Janvier 2019, l'ANSSI y a fait allusion)

2018 : L'ANNÉE DE L'ENTRÉE EN VIGUEUR DU RGPD !

190 000 d'appels

reçus par la CNIL

8 millions de visites

sur le site de la CNIL

9 700 plaintes

1 000 notifications

de violations de données reçues
(environ 7 par jour)

Seuls 54% des français

comprennent ce que le RGPD
change

Le RGPD en Europe

95 000 plaintes / 255 enquêtes / **3 amendes** (dont Google par la CNIL)

RAPPEL DU THÈME : RGPD : CHECK (& WAKE)-UP !

Ce règlement nécessite de **faire travailler ensemble des domaines, disciplines et compétences désormais complémentaires**.

Ad minima, cinq d'entre eux sont nécessaires : innovation, SI, sécurité, juridique et organisationnel.

Tous les métiers seront appelés à mieux appréhender les cadres, contraintes et avantages vers lesquels ils devront s'orienter.

Quelles sont **les conditions** d'une mise en œuvre réussie ?

POUR EN PARLER, NOUS AVONS L'HONNEUR D'ACCUEILLIR...



Matthieu Grall

Directeur de l'expertise technologique

@CNIL



Marie de Freminville

Ex-Directrice de la gouvernance des filiales

@AIRBUS



Fabian Guion

Consultant RGPD / IT

@GAC GROUP



2

5 QUESTIONS À LA CNIL

POURRIEZ-VOUS FAIRE UN BILAN DES ACTIONS MISES EN PLACE PAR LA CNIL DEPUIS L'ENTRÉE EN VIGUEUR DU RGPD EN MAI 2018 ?

En plus d'avoir ardemment **travaillé à l'interprétation du texte**, nous avons élaboré divers outils.

La CNIL a aussi **adopté 2 référentiels** pour la certification de compétences des délégués à la protection des données (DPO).

Nous envisageons **la délivrance des premiers agréments**.

Nous travaillons aussi à **l'élaboration d'une dizaine de codes de conduite**.

QUELS SONT LES MOYENS QUE LA CNIL VA UTILISER POUR RENFORCER SES ACTIONS ?

En 2018, la CNIL c'est 8 millions de visites, 190.000 appels reçus et 12.000 plaintes...

Mais c'est aussi juste une **amende** record (Google) vs. **avertissements** et mises en demeure auprès de plus petites structures

Doit-on considérer que **seuls les géants du web ont à s'inquiéter financièrement** d'une mise en conformité au RGPD ?

COMMENT LA CNIL PEUT-ELLE DÉMONTRER QUE L'ON EST « PERFORMANT ET EFFICACE » LORSQU'ON SE CONFORME AU RGPD ?

« *Le RGPD menace les capacités d'innovation des startups européennes et surtout françaises* » (source : Gary Shapiro, organisateur du CES de Las Vegas)

77 % des entreprises sont plus préoccupées par leur cybersécurité que par leur conformité

87 % des entreprises connaissent des retards dans leur cycle de vente en raison des préoccupations des clients ou des prospects en matière de confidentialité (Source : Cisco 01/19)

La **transparence** et le **respect des droits** des personnes
sont bons pour le business

COMMENT ÉVALUERIEZ-VOUS LE NIVEAU DE MATURITÉ ACTUEL DES ENTREPRISES FRANÇAISES ?

59 % des entreprises répondent aux exigences du RGPD (Source : Cisco 01/19)

78 % des français affirment être préoccupés par l'utilisation et la protection de leurs données personnelle (source : KPMG 2017)

Les **risques de violations** de données et le **coût lié à ces violations** pourraient diminuer pour les entreprises si elles venaient à observer totalement les exigences réglementaires du RGPD

(source : KPMG 2017)

Devenir une entreprise **plus sûre, innovante et rentable**

QUELLES MESURES ET SOLUTIONS SONT POUR VOUS NÉCESSAIRES POUR RÉPONDRE EFFICACEMENT AUX EXIGENCES DU RÈGLEMENT ?

Les mesures citées dans le RGPD – chiffrement, pseudonymisation, etc. – ne sont que des exemples, qui ne sont pas des arguments de protection suffisants.

Il convient d'intégrer sécurité et protection de la vie privée **dès la conceptualisation des projets**.

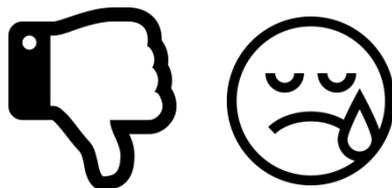
Mesures de base, **mesures d'hygiène informatique**
et étude de risques de sécurité

3

TABLE RONDE

QUELS SONT LES RISQUES POUR UNE ENTREPRISE D'ÊTRE VICTIME D'UNE CYBERATTAQUE OU D'UNE PLAINTE À LA CNIL ?

“ La question n'est pas « est-ce nous allons être victimes d'une cyberattaque ? », mais « quand allons-nous être victimes d'une cyberattaque » ?



Perte de **crédibilité** (dégradation d'image...)

Perte de **business** (perte de CA, ransomware...)

COMMENT AVEZ-VOUS FAIT ÉVOLUER LES USAGES DE VOS CLIENTS EN MATIÈRE DE CYBERSÉCURITÉ POST RGPD ?

La première évolution est celle des **mentalités** et de la **prise de conscience**.

→ **Sensibiliser**

→ Mettre en place les **bonnes pratiques**

→ Insuffler une **culture** de la protection de la donnée (cyber et usages)

*« Les autres (grandes) entreprises sont exposées,
la mienne ne risque rien »*

COMMENT AVEZ-VOUS IMPLÉMENTÉ LES PRINCIPES DE *PRIVACY BY DEFAULT* ET *PRIVACY BY DESIGN* CHEZ VOS CLIENTS ?

Privacy by default = protection des données personnelle par défaut

Privacy by design = protection des données personnelles dès la conception

Nécessite :

- un **référent** en charge de piloter le sujet (**DPO**)
- une **implication continue** sur les projets de l'entreprise (nouvelle offre, nouveau produit...)
- des **procédures** de revue de conformité tout au long du **cycle** (checklists...)

Processus de **vérification continu**

QUELS SONT VOS CONSEILS EN MATIÈRE DE SÉCURITÉ VIS-À-VIS DE LA SOUS-TRAITANCE / FOURNISSEURS ?

Il est important de **fiabiliser** la gestion des données transférée aux sous-traitants

- Clauses contractuelles types
- Référentiels et normes (ISO 27000, etc.)
- Audits externes

Assurer un **niveau de protection équivalent** et **suffisant** quel que soit le nombre d'acteurs impliqués

POURQUOI ET COMMENT IMPLIQUER L'ENSEMBLE DES FONCTIONS DE L'ENTREPRISE DANS LA POLITIQUE DE CYBERSÉCURITÉ ET LE RGPD ?

La gestion des données (personnelles ou non) concerne l'ensemble des services d'une entreprise. La connaissance de **toutes ses activités et ses usages** est nécessaire pour maîtriser ses risques.

“ *Le risque cyber est un **meta-risque**, qui touche toutes les fonctions de l'entreprise : la direction générale, la direction financière, la direction juridique, la direction des risques, la direction informatique, etc.*

Maîtriser toute **la chaîne de traitement** des données
pour mieux la **protéger**

4

CONCLUSION

CYBERATTAQUES : COMMENT LES ANTICIPER ?

Votre besoin : protéger en permanence votre réseau contre les intrusions indésirables

Votre problème : trop de choix, pas assez d'expertise, des solutions trop complexes, trop cher et un manque de temps et de visibilité



Solution simple et complète de sécurité réseau

Monitoring > Détection > Alerte > Solution

RGPD : COMMENT EN FAIRE UNE OPPORTUNITÉ ?



GAC
GROUP



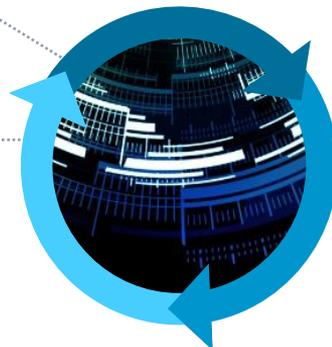
CONFORMITÉ RGPD

- ▶ Diagnostic et cartographie des traitements
- ▶ Mise en conformité
- ▶ Accompagnement CNIL



MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

- ▶ Analyse de risques / écarts ISO 27000
- ▶ Security Operating Center
- ▶ Tests d'intrusion



CONSEIL & ACCOMPAGNEMENT

- ▶ Formation / Sensibilisation
- ▶ Externalisation du Data Protection Officer (DPO)
- ▶ Conseil organisationnel

Innovation

Pragmatisme

Excellence



RDV À 15H/15H45 - MASTER CLASS

COMMENT PASSER DE L'OBLIGATION À L'OPPORTUNITÉ BUSINESS ?

Faute de temps et de coordination interne, vous avez finalement décidé de véritablement traiter le sujet en 2019 ?

Ne cédez plus au « marketing de la peur » : concentrez-vous uniquement sur les stricts moyens nécessaires à votre conformité pour éviter de perdre du CA à cause du RGPD



Mettre en place un plan d'action pragmatique et structuré

Coordonner vos équipes commerciales, marketing, RH et DSI

Répondre à vos obligations en BtoB et BtoC



CONTACT

Fabian GUION

Consultant RGPD

fguion@group-gac.com

01 44 82 22 03



GAC GROUP

11-13 Rue René Jacques

92130 Issy-les-Moulineaux



www.group-gac.com