ATiPiC AVOCAT

Technologies
Informations
Propriété
Intellectuelle
Commerce

CYBER CERCLE

Le GDPR pour les Nuls...

...et pour les autres aussi

François Coupez
Avocat à la Cour, associé

SPÉCIALISTE

Droit des nouvelles technologies, de l'informatique et de la communication
Chargé d'enseignement à l'Université de Paris II Panthéon-Assas, au CELSA et à l'Institut Léonard de Vinci

ATiPiC AVOCAT

Technologies Informations Propriété Intellectuelle Commerce

Conseille, forme et défend les entreprises en droit de l'immatériel

Marques, Brevets, Dessins & Modèles, Nom de domaine et droit d'auteur, Innovation et transformation numérique, Sécurité des SI, Données personnelles, Contrats informatiques, Dématérialisation, E-commerce, Evaluation, gestion et protection du patrimoine informationnel et actif immatériel, etc.

SPÉCIALISTE

Analyse juridique rigoureuse

Certificat de spécialisation en droit des nouvelles technologies, de l'informatique et de la communication

+

Compréhension du fonctionnement technique

+

Orientation business

- ✓ Anticiper les problématiques juridiques pour mieux les gérer
- ✓ Proposer des solutions juridiques innovantes prenant en compte l'ensemble des impératifs

2018 TROPHÉES DU DROIT PARIS
ÉQUIPES MONTANTES
Droit des nouvelles technologies

FIRM OF THE YEAR 2017 Cyber Security Law France
ACQ5.com

FIRM OF THE YEAR 2017 Technology Law France
ACQ5.com

HIGHLY RECOMMENDED INTERNET LAW

HIGHLY RECOMMENDED DATA PROTECTION

RECOMMENDED IT/SOFTWARE LAW

LEADERS LEAGUE 2017

Préambule

- Dès que des **données personnelles** sont traitées…
  - ✓ Donnée personnelle : donnée relative à une personne physique identifiée ou identifiable
  - ✓ Traitement : automatisé ou non automatisé si les données sont dans des fichiers
- … il faut respecter **un certain nombre de règles (loi du 6 janvier 1978 modifiée)**…
  - ✓ Aujourd'hui encore, effectuer les formalités auprès de la CNIL
  - ✓ Respecter la finalité du traitement des données, qui doit être légitime
  - ✓ Assurer la sécurité des données
  - ✓ Respecter les obligations d'information
- … qui sont **renforcées par l'arrivée d'un texte européen : le Règlement Général sur la Protection des Données (RGPD)**
  - ✓ Privacy by design
  - ✓ Privacy by default
  - ✓ Serveurs dans l'UE…
  - ✓ **Regardons dans le détail…**

Plan

GDPR ! GDPR ! GDPR ! GDRP ! RGPD ! RGDP !... Euh, vous voulez dire GDPR ?

- Mais au fait, c'est quoi ce texte ?
- Pourquoi est-il incontournable ? Pourquoi est-ce une bonne chose ?
- Légendes urbaines
- Et vous ? Faites-nous part de vos expériences !

Une idée répandue…

LE RGPD, UN AMI

Mais est-ce vraiment lui le coupable ?

QUI VOUS VEUT DU BIEN ?

GDPR, le bug de l'an 2018

- Les **points communs ?**
  - ✓ C'était prévisible et attendu
  - ✓ 40 ans pour avoir un début de conformité
  - ✓ Un manque actuel de main-d'œuvre compétente

- Une comparaison en réponse au marketing de la peur : un **réflexe de déni**, car
  - ✓ Les compétences qui manquent sont celles d'avenir, pas du passé
  - ✓ La réglementation est connue, les régulateurs n'ont aucune raison de ne pas l'appliquer
  - ✓ **La réglementation n'est pas ponctuelle, elle est conçue pour une conformité en mode PDCA pour les années à venir**

Petit rappel du front marketing…

UN EXPERT SMART GDPR® VOUS RAPPELLE SANS ENGAGEMENT

Nom *

Téléphone *

Société *

Email *

Être recontacté
SANS ENGAGEMENT

De : 3M <contact.3m@departement-commercial.com>
Date : jeudi 26 octobre 2017 à 11:26
À : 3M <contact.3m@departement-commercial.com>
Objet : 3M vous remercie de notre rencontre au Assises de la Sécurité

Bonjour,

Le 25 mai 2018, le RGPD (**Règlement Général sur la Protection des Données**) fixé par l'Union Européenne entrera en vigueur. Toutes les entités (entreprises et collectivités) qui collectent, stockent ou traitent des données personnelles de citoyens européens y seront soumises.

Les filtres de confidentialité 3M offrent une solution simple et efficace pour assurer la confidentialité de vos données privées, et répondre à cet ensemble de mesures.

Pour une conformité GDPR achetée, deux gratuites ?

Alexandre Eloy a commenté ceci

Franklin Brousse
L'Avocat des Directions Achats et des Directions Digitales
15 h · Modifié

Ale
mé
cac
cor
pre
l'ap
jus

Sulliman Omarjee
IP/ IT LEGAL COUNSEL - LECTURER IN CYBERLAW
3d · Edited

Les arnaques au RGPD se developpent meme à La Reunion avec des prestataires totalement inexperimentés dans le droit du numerique qui profitent d'un effet d'aubaine pour vendre leur services
Raison de plus pour faire confiance a notre equipe FIDAL pour vous accompagner dans la conduite de votre plan de conformité RGPD :)

spécialiste du RGPD et de la protection des données en quelques mois. Dès lors si des consultants se présentent à vous sans l'appui d'un juriste ou d'un avocat spécialisé, passez votre chemin !

Pour une conformité GDPR, merci de communiquer votre n° de CB

CNIL
@CNIL
Suivre

#StopArnaque - Vous êtes PME, artisan/commerçant et recevez actuellement des sollicitations par téléphone pour une « mise en conformité » de votre entreprise au règlement européen sur la protection des données (#RGPD) ? Lisez ce thread 👇

06:02 - 17 janv. 2018

600 Retweets 198 J'aime

6 600 198

Pour une conformité GDPR, merci de communiquer votre n° de CB

CNIL @CNIL · 17 janv.

1 Des entreprises peu scrupuleuses vendent une prestation « clé en main » qui vous garantirait la conformité de votre entreprise au #RGPD. Leur technique : insister sur les sanctions financières encourues ET se présenter comme «labellisé», «mandaté» ou «recommandé» par la @CNIL

3 79 27

CNIL @CNIL · 17 janv.

2 Ces messages peuvent avoir pour but de vous faire appeler un numéro surtaxé, de vous faire signer un engagement frauduleux ou de collecter des informations sur votre organisation pour préparer une escroquerie ou une attaque informatique #stoparnaque #RGPD

1 16 4

CNIL @CNIL · 17 janv.

3 N'y répondez pas ! La @CNIL n'est, bien entendu, pas à l'origine de telles démarches auprès des entreprises. En cas de doute, vous pouvez nous contacter au 01 53 73 22 22.

Plan

GDPR ! GDPR ! GDPR ! GDRP ! RGPD ! RGDP !... Euh, vous voulez dire GDPR ?

Mais au fait, c'est quoi ce texte ?

Pourquoi est-il incontournable ? Pourquoi est-ce une bonne chose ?

Légendes urbaines

Et vous ? Faites-nous part de vos expériences !

Rappel des notions fondamentales

- Données « à caractère personnel »
- Traitement
- Responsable de traitement
- Sous-traitant
- Application des règles à tous, sauf usage purement privé
- Cadre strict (finalités, etc.), formalisme (pré-GDPR), information des personnes, droits des personnes, sécurisation, etc.

Bien comprendre la conception antinomique des US

- **Dans les pays anglo-saxons, on est propriétaire de ses données**
  - ✓ On peut donc les céder… sans espoir de retour ni de contrôle
- **En France (et au niveau de l'UE), la protection des données personnelles fait partie des droits de la personnalité**
  - ✓ On n'en est pas « propriétaire », on ne peut donc s'en déposséder définitivement
  - ✓ On peut donc revenir sur son consentement…
  - ✓ D'où le terme de « data subject » (et non data owner)

Une Directive européenne 1995/46 insuffisamment efficace ?

- La principale critique : trop de libertés données aux États membres
- Une fragmentation, des disparités fortes :
  - ✓ En Allemagne, un très important formalisme
  - ✓ En Espagne, des sanctions très fortes
  - ✓ Au Royaume-Uni, des traitements possibles sans information préalable (contrôle clandestin des salariés)
  - ✓ Etc.
- Une application « européano-européenne »

Une modernisation nécessaire : Big Data, les sous-traitants ont pris le pouvoir, des sanctions financières peu élevées, etc.

Un peu d'histoire (récente)

2012 : projet GDPR

adapter la protection des données personnelles aux nouveaux enjeux

4 ans de négociations, 173 considérants, 99 articles

2016 GDPR adopté

(ainsi que directive NIS)

G29 guidelines

25 mai 2018, entrée en application

Ne pas oublier le projet de règlement ePrivacy (application repoussée en 2019/2010 ?)

Les grands principes inchangés

- Loyauté, finalité, proportionnalité
- Les données sensibles
- Le consentement souvent nécessaire
- L'exception *made in France* : le NIR
- Les pouvoirs opérationnels de la CNIL
- L'analyse de risque pour les droits et libertés des personnes physiques
  (l'*accountability* – cf. plus loin – en renforce fortement l'exigence)
- Le CIL, qui devient DPO/DPD (Data Protection Officer / Délégué à la Protection des Données)

Rappel : quelques éléments saillants du GDPR

Un champ d'application mondial ?

Un sous-traitant partenaire de la sécurité, responsable conforme… ou rien !

Pseudo-anonymisation, minimisation, PIA, etc.

Quelles conséquences ?

Un "gardien du Temple GDPR" : le CEPD (ex-G29)

Traçabilité et conformité à tout moment

La notification des atteintes à l'intégrité, à la confidentialité et à la disponibilité

Renforcement des droits des personnes (portabilité, droit à l'oubli, etc.)

Des traitements de données Privacy by design / default

Des sanctions très fortement dissuasives

Protection des DCP : sanctions

- **En France, les grands principes existent depuis près de 40 ans !**
- Mais en pratique, les sanctions rares et faibles ont disqualifié le sujet au niveau de la direction / du COMEX
- Aujourd'hui, les montant des sanctions administratives x20
- **Demain**…

Hier (loi 1978)

150 000 €

Aujourd'hui
(loi République numérique)

3M €

Demain

Jusqu'à 4 % du CA mondial consolidé

Les droits renforcés des personnes dont les données sont traitées

Information

Opposition (dont profilage)

Portabilité

Droit d'accès

Effacement / Oubli

Directives *post mortem* (ajout franco-français)

Rectification / Mise à jour

Limitation du traitement

Les lois de « transposition »

- Les 57 renvois du GDPR au droit local…
- Le GDPR et le projet de loi « Informatique et libertés 3 » – vote par le Sénat aujourd'hui
- Les spécificités françaises
  - ✓ **Renforcement des pouvoirs de la CNIL** (pouvoirs, saisine…)
  - ✓ Age du consentement au traitement des données : **15 ans**
  - ✓ **Extension des effets de l'action de groupe** : possible d'obtenir non seulement la cessation du manquement (comme depuis la loi du 18 novembre 2016) mais des dommages et intérêts
- Et toujours le **buzz** : **des amendements voués à l'échec**
  - ✓ Patrimonialisation des données, dans une moindre mesure « amendement Qwant » ?

A METTRE A JOUR EN FONCTION ACTU – PAS DE SANCTION FINANCIERE POUR LES COLLECTIVITES ?

Les lois de « transposition »

- Un goût de déjà-vu : la loi pour une République numérique et la « surtransposition »
  - ✓ Droit à la portabilité des données non personnelles
  - ✓ Protection des données personnelles des personnes décédées indépendamment des droits existants des tiers (cf. droit des successions)
- Et à l'étranger ?
- **Des changements, jusqu'à quand ?**

Plan

GDPR ! GDPR ! GDPR ! GDRP ! RGPD ! RGDP !... Euh, vous voulez dire GDPR ?

Mais au fait, c'est quoi ce texte ?

Pourquoi est-il incontournable ? Pourquoi est-ce une bonne chose ?

Légendes urbaines

Et vous ? Faites-nous part de vos expériences !

« I am GDPR, resistance is futile, you will be assimilated ! »

Quelle que soit l'hypothèse…

- Etablissement du RT ou du ST dans l'UE

- Si offre de biens ou de services à des personnes dans UE
- OU si suivi de comportements au sein de l'UE

- Et les effets de bord pour leurs sous-traitants quelle que soit leur nationalité

Tous les chemins mènent au…

Des principes révolutionnaires ?

Voyons…

- ✓ **Cartographier** les données traitées
- ✓ **Evaluer** les risques
- ✓ **Sécuriser** de façon proportionnée aux risques
- ✓ Assurer la **traçabilité** des opérations
- ✓ Avoir des relations contractuelles claires avec un **sous-traitant responsable** des prestations fournies
- ✓ **Respecter des principes légaux existant depuis 40 ans**
- ✓ **Etre soutenu par la direction / le Comex** pour appliquer ces principes

Des idées révolutionnaires ? **Ou des principes connus mais peu appliqués ?**

Se conformer ou… se conformer

- ✓ L'art. 28 RGPD et la **pression sur les ST**
- ✓ L'art. 28 RGPD et le **contrôle des demandes** des RT
- ✓ **En pratique, le contrôle mutuel devient la règle, les demandes sur l'état de la mise en conformité se multiplient…**

Evoluer… ou évoluer ?

Se conformer n'est plus une option

Ce qui compte : quels efforts pour combler le gap ? / d'où part-on ?

En pratique…

- Une mise en conformité souvent plus aisée pour les petites entités que pour les grandes…

- **Les priorités :**
  - ✓ les données RH
  - ✓ les données clients/administrés
  - ✓ mais également les contrats avec les sous-traitants

- **Une contrainte… mais également un potentiel avantage concurrentiel**

- **Le 25 mai 2018, winner takes all ?**

Rappel : comment se préparer au RGPD selon la taille des entités et leur niveau de maturité

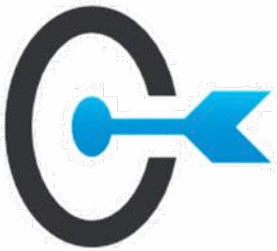
Préparer la Direction aux impacts… et aux opportunités !

Désigner une organisation (pérenne?), soutenue par un sponsor

Sensibiliser les services et les différents acteurs internes aux changements à venir

Auditer à 360° / Cartographier les traitements / Réaliser l'analyse d'écart

Se conformer en mode matriciel



Prioriser (quick win, etc.)

Intégrer dès l'origine les principes de base (Privacy by design, documentation, analyse de risque, etc.)

Intégrer la protection des DCP au cœur des process de l'entité

Sensibiliser, former, vérifier… et recommencer !

Les coûts estimés

30 M € par société du CAC40 en moyenne ? (Sia Partners)

35 M € par groupe international ? (Wavestone)

- **Cher ? Mais pour certains, les coûts sont à mutualiser avec d'autres mises en conformité ;-)**

« Même avec beaucoup de bonne volonté et de moyens, certaines entreprises auront du mal à tout mener de front.

À moyen terme, tout cela va naturellement converger.

La somme NIS + RGPD est inférieure à la somme des deux pris séparément. »

Guillaume Poupard, Directeur général de l'ANSSI

Plan

GDPR ! GDPR ! GDPR ! GDRP ! RGPD ! RGDP !... Euh, vous voulez dire GDPR ?

Mais au fait, c'est quoi ce texte ?

Pourquoi est-il incontournable ? Pourquoi est-ce une bonne chose ?

Légendes urbaines

Et vous ? Faites-nous part de vos expériences !

Info ou intox ?

- *« C'est à partir du 25 mai 2018 que nous aurons deux ans pour nous mettre en conformité. Tout va bien, on a le temps »*

C'est tout simplement faux

- Origine : Considérant 171 « *La directive 95/46/CE devrait être abrogée par le présent règlement. Les traitements déjà en cours à la date d'application du présent règlement devraient être mis en conformité avec celui-ci dans un délai de deux ans après son* ***entrée en vigueur*** ».
- **Oui mais… Art 99** « *1. Le présent règlement* ***entre en vigueur le vingtième jour suivant celui de sa publication*** *au Journal officiel de l'Union européenne.* **[25 mai 2016]**

  2. Il est applicable à partir du 25 mai 2018 »

Info ou intox ?

- « *L'objectif est d'être prêt pour le 25 mai 2018* »

Pourquoi ce n'est pas suffisant :

- ✓ le GDPR met en place un suivi de conformité dans la durée, fait pour durer,
- ✓ la réglementation peut évoluer, les efforts de suivi seront donc **constants**

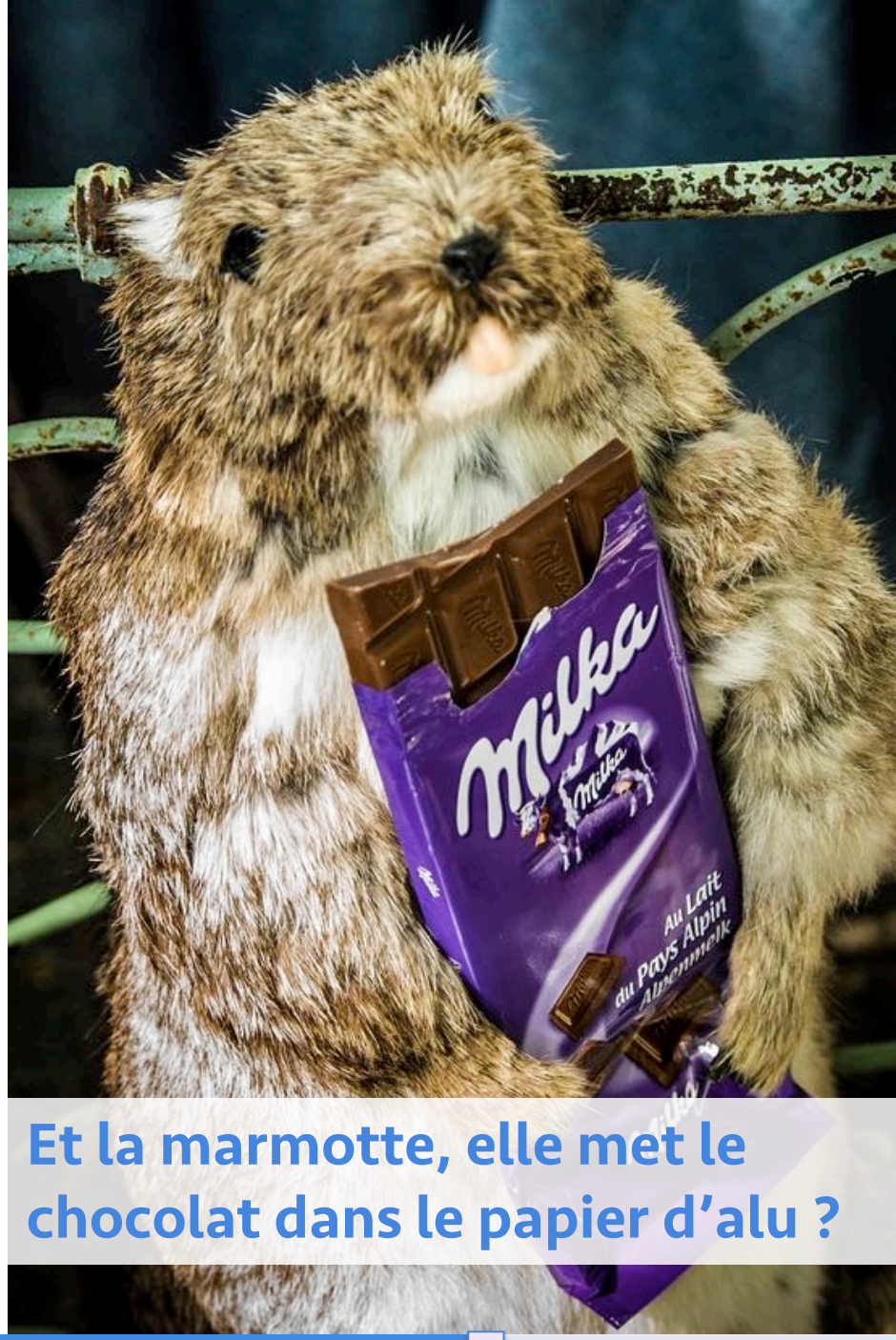
Le 25 mai 2018 ne marque que le début d'une étape !

Info ou intox ?

- *« Le GDPR ne s'appliquera pas le 25 mai 2018. Le délai sera repoussé et les sanctions ne s'appliqueront pas »*

Pourquoi on n'y croit pas :

- Les règles de base existent depuis 40 ans en France, les ajustements ne seraient pas difficiles si elles étaient parfaitement suivies… (cf. contre-exemple de l'Allemagne).
- **Le modifier est juridiquement irréaliste dans le délai**
- Repousser l'application du GDPR brouillerait le message du paquet européen sur la cybersécurité



Et la marmotte, elle met le chocolat dans le papier d'alu ?

Légendes urbaines

Info ou intox ?

- *« 2 ou 4 % du CA comme sanction ? Ils n'oseront pas, cela coulerait les boîtes »*

Pourquoi on n'y croit pas :

- **La CNIL a sanctionné le 16/11/2017 pour défaut de sécurité une entreprise de 760 000 EUR de CA à… 25 000 EUR d'amende (3,3 % de son CA)**
- Les régulateurs allemands et espagnols ne sont pas connus pour leur souplesse

Info ou intox ?

- *« Seules les entreprises de plus de 250 salariés sont dans l'obligation de désigner un DPO »*

C'est tout simplement faux

- Ce critère a existé dans une version du projet de texte… **mais n'a pas été retenu**
- Il est fait mention d'un critère de 250 salariés mais sur un autre sujet (registre de traitement – exception en elle-même très restreinte)
- Une mention de certaines dispenses liées à ce seuil figure pourtant - à tort - dans le rapport sénatorial…

Pour rappel sur les DPO

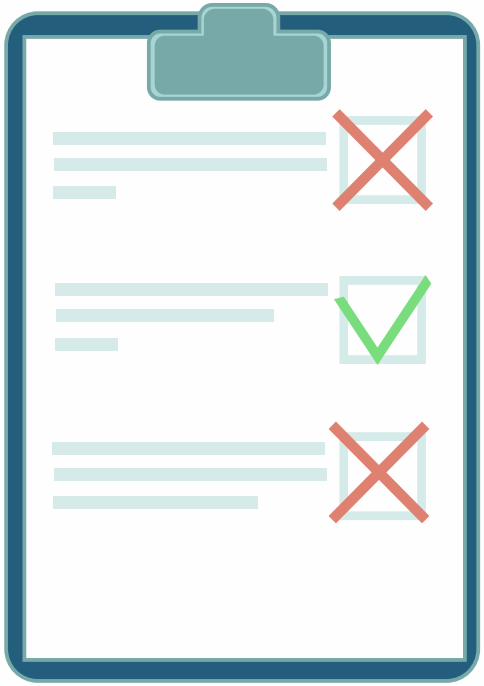
- **Désignation facultative, sauf…**

Si le traitement est effectué par une **autorité** ou un **organisme public**

OU si le droit local l'exige

OU si les activités du responsable consiste en des **traitements sur des catégories particulières de données** (données sensibles) ou touchant aux condamnations criminelles

OU si les activités du responsable consistent en des traitements exigeant un **suivi régulier et systématique des personnes** concernées



Et si le client le réclame ?

Légendes urbaines

Info ou intox ?

- *« Il existe d'ores et déjà des outils (logiciel, solution hardware) certifiés RGPD dont l'achat permet au responsable de traitement d'être automatiquement et à 100 % conforme… »*

Abracadabra ! Et il est à vous pour la modique somme de…

- La labellisation au niveau européen est prévue, mais n'est pas encore en place. Le label n'est d'ailleurs qu'un indice de conformité
- Et de toute façon, **la conformité GDPR passe par un ensemble de facteurs** (processus organisationnels, sensibilisation des personnels, clauses contractuelles, etc.)

Info ou intox ?

- *« Le DPO est responsable pénalement et personnellement des non-conformités des traitements du responsable de traitement qui l'a nommé… »*

Comment dire… Non !

En réalité le responsable de traitement reste… responsable !

Plan

GDPR ! GDPR ! GDPR ! GDRP ! RGPD ! RGDP !... Euh, vous voulez dire GDPR ?

Mais au fait, c'est quoi ce texte ?

Pourquoi est-il incontournable ? Pourquoi est-ce une bonne chose ?

Légendes urbaines

Et vous ? Faites-nous part de vos expériences !

Partageons nos expériences !

Avez-vous des questions ?

Merci de votre attention !

François COUPEZ

Avocat à la Cour, Associé

Droit des nouvelles technologies, de l'informatique et de la communication

f.coupez@atipic.legal

31, boulevard Malesherbes, 75008 Paris
01 80 48 11 25

@f_coupez