



Le règlement RGPD : principe de co-responsabilité et impacts dans les relations contractuelles entre clients et fournisseurs



GDPR
RATING

Laurent ZEITOUN
Directeur Général

21, rue de la Banque
75002 PARIS

Mobile : 06 20 48 09 25

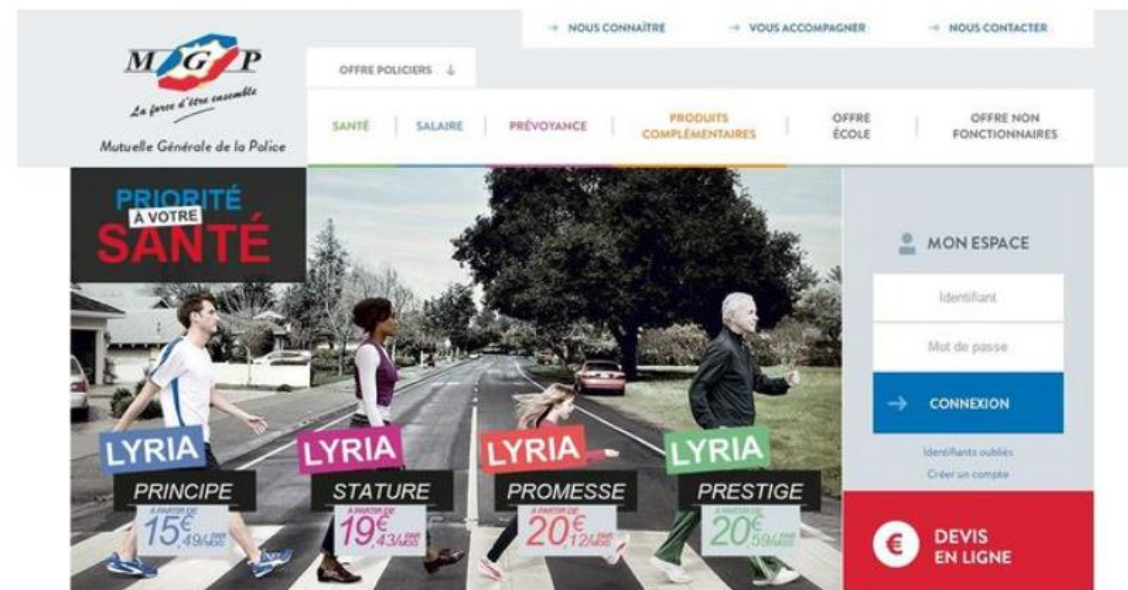
Email : laurent.zeitoun@gdpr-rating.eu

★ Mutuelle de police : 120 000 individus

- Issu d'un acte malveillant et intentionnel!
- Copie de fichiers d'un serveur sécurisé à un drive google...
- Enquête de police après l'assassinat de 2 policiers chez eux

Les données personnelles de 112.000 policiers ont fuité sur le web

Par  Caroline Piquet | Mis à jour le 27/06/2016 à 15:40 / Publié le 27/06/2016 à 14:18



The screenshot shows the website for MGSP (Mutuelle Générale de la Police). The header includes the logo and navigation links: "NOUS CONNAÎTRE", "VOUS ACCOMPAGNER", and "NOUS CONTACTER". Below the header is a menu with categories: "OFFRE POLICIERS", "SANTÉ", "SALAIRE", "PRÉVOYANCE", "PRODUITS COMPLÉMENTAIRES", "OFFRE ÉCOLE", and "OFFRE NON FONCTIONNAIRES". The main content area features a promotional banner for "LYRIA" health insurance with the slogan "PRIORITÉ A VOTRE SANTÉ". The banner shows four people holding signs for different plans: "PRINCIPE" (15€), "STATURE" (19€), "PROMESSE" (20€), and "PRESTIGE" (20€). On the right side, there is a "MON ESPACE" section with a login form containing fields for "Identifiant" and "Mot de passe", a "CONNEXION" button, and links for "Identifiants oubliés" and "Créer un compte". At the bottom right, there is a red button labeled "DEVIS EN LIGNE".

★ DARTY: 100 000€

- Accès libres à des dossiers clients
- Accès à des 900 000 fiches de clients non sécurisés
- Logiciel du sous-traitant défaillant
- Juillet 2017

La CNIL inflige à DARTY une amende de 100 000 euros pour une atteinte à la sécurité des données clients

LE MONDE DU DROIT | 8 FÉVRIER 2018

DÉCRYPTAGES



★ BOUYGUES : 250 000€

- 2 millions de client B&You exposés!
- Vulnérabilité de l'adresse URL sur le site web de BOUYGUES TELECOM
- Pas d'utilisation frauduleuse
- Erreur corrigé ensuite
- Décembre 2018

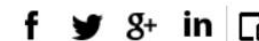
Amende de 250.000 euros : la Cnil sanctionne Bouygues Télécom

Par [latribune.fr](#) | 27/12/2018, 13:37 | 384 mots



SUIVRE LA TRIBUNE

Votre email



Hello bank!

par BNP PARIBAS

★ UBER : 400 000€ (en France...)

- Faille de sécurité!
- 57 millions de personnes touchées dont 1,4 en France !
- Pas assez de sécurité dans l'accès de leurs serveurs AWS
- Même type d'amende dans d'autres pays européens
- CA 6 milliard
- Déjà amende de 148 millions dollar aux US suite à des piratages
- Décembre 2018



★ GOOGLE : 50 000 000€

- 1^{er} amende au titre du RGPD !
- Issue de 2 plaintes (NOYB et Quadrature du net)
- Manque de transparence, information GDPR trop disséminées
- Problème de consentement, module de gestion données privées trop difficile à obtenir (plus de 5 à 6 niveaux)

RGPD: la Cnil impose à Google une sanction record de 50 millions d'euros

Par Lucie Ronfaut | Mis à jour le 21/01/2019 à 19:05 / Publié le 21/01/2019 à 16:28



LE RGPD c'est quoi ?





Comprendre le RGPD (GDPR)

Règlement Général sur la Protection des Données

C'est un règlement qui porte sur l'utilisation et la circulation de données personnelles pour permettre aux utilisateurs de maîtriser l'usage de leurs données privées.

Vous pourrez donc continuer à utiliser des données personnelles du moment où vous savez justifier le droit, l'usage, la collecte, et la sécurité de ces données et que vous avez suffisamment informé les personnes de leurs droits.

Droit d'accès, de rectification, de portabilité et d'oubli





Comprendre le RGPD (GDPR)

Donnée personnelle : toute donnée qui peut, directement ou indirectement, identifier une personne

- Bank Account
 - Bank Identifier Code (BIC)
 - IBAN
- Credit Card Number
 - American Express
 - VISA
 - MasterCard
 - Dinners Club
 - Discover
 - JCB
- Demographic Data
 - Name
 - Gender
 - Date of Birth
 - Age
 - Nationality
- Channels
 - Phone Number
 - Postal Address
 - City
 - Country
 - Email Address
- Government Identifiers
 - National Id
 - Passport Number
 - Social Security Number
 - Vehicle Registration Number
 - Driver License
- Digital Identifiers
 - IP Address (V4, V6)
 - MAC Address
 - X/Y Geographic Coordinate
- Social Media
 - Twitter Account
 - URL FaceBook
 - URL LinkedIn
 - URL Pinterest
 - URL Instagram
- Organization
 - HR Information
- Sensitive Data
 - Health, Sex
 - Political
 - Religious
 - Philosophical
 - Trade union member info
 - Genetic
 - Biometric
 - Race
 - Gender
 - Ethnicity
 - Children
- Pictures
- ...
- Footsteps ?

Copyright © SAS Institute Inc. All rights reserved.



Comprendre le RGPD (GDPR)

Quelles entreprises concernées ?

Toute entreprise Européenne ou étrangère qui manipule des données à caractère personnel de citoyens ou résidents étrangers vivants sur le sol Européen.

Quels traitements concernés ?

Le GDPR ne concerne pas qu'Internet, mais tous les traitements automatisés traitant des données personnelles, qu'ils concernent, **des consommateurs, des salariés**, des partenaires en BtoB, des **patients**, etc...

Dès qu'il y a des données personnelles et un traitement informatique ou manuel, le GDPR s'applique.

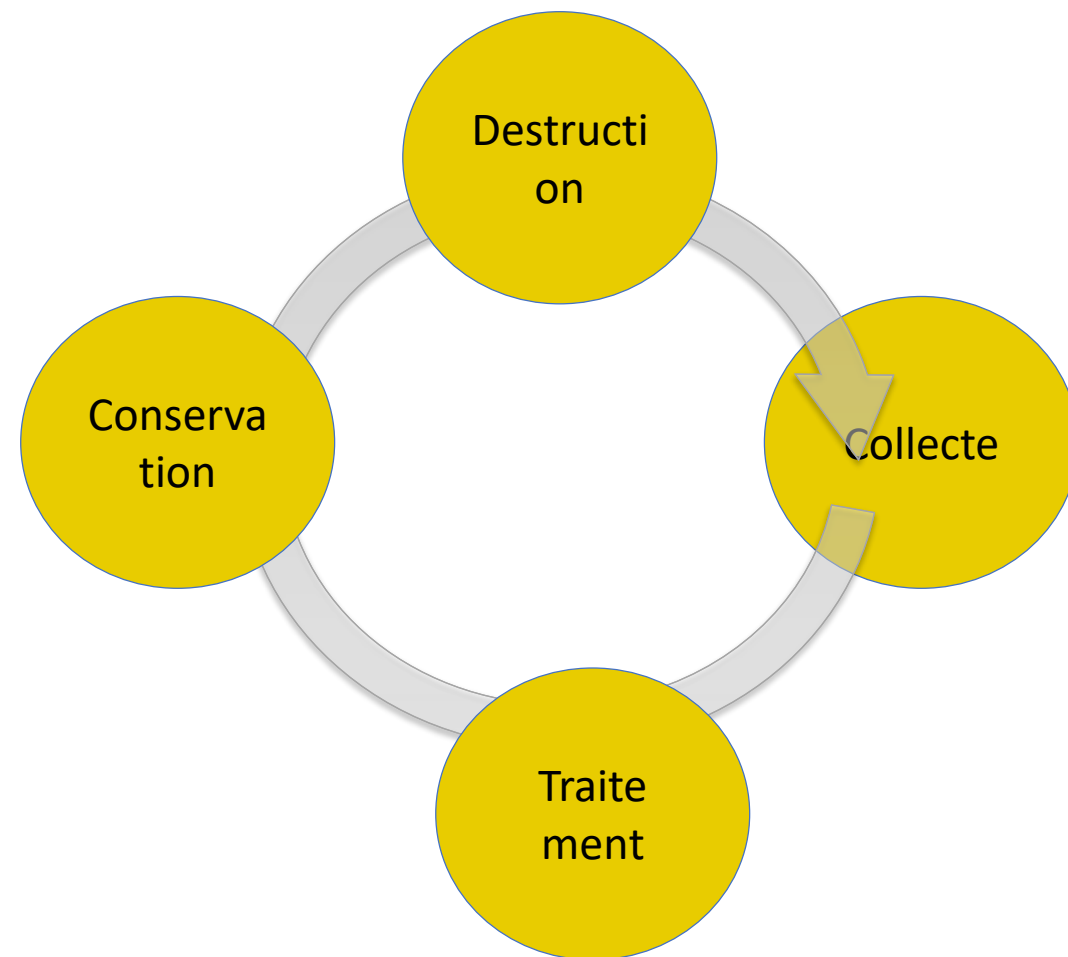
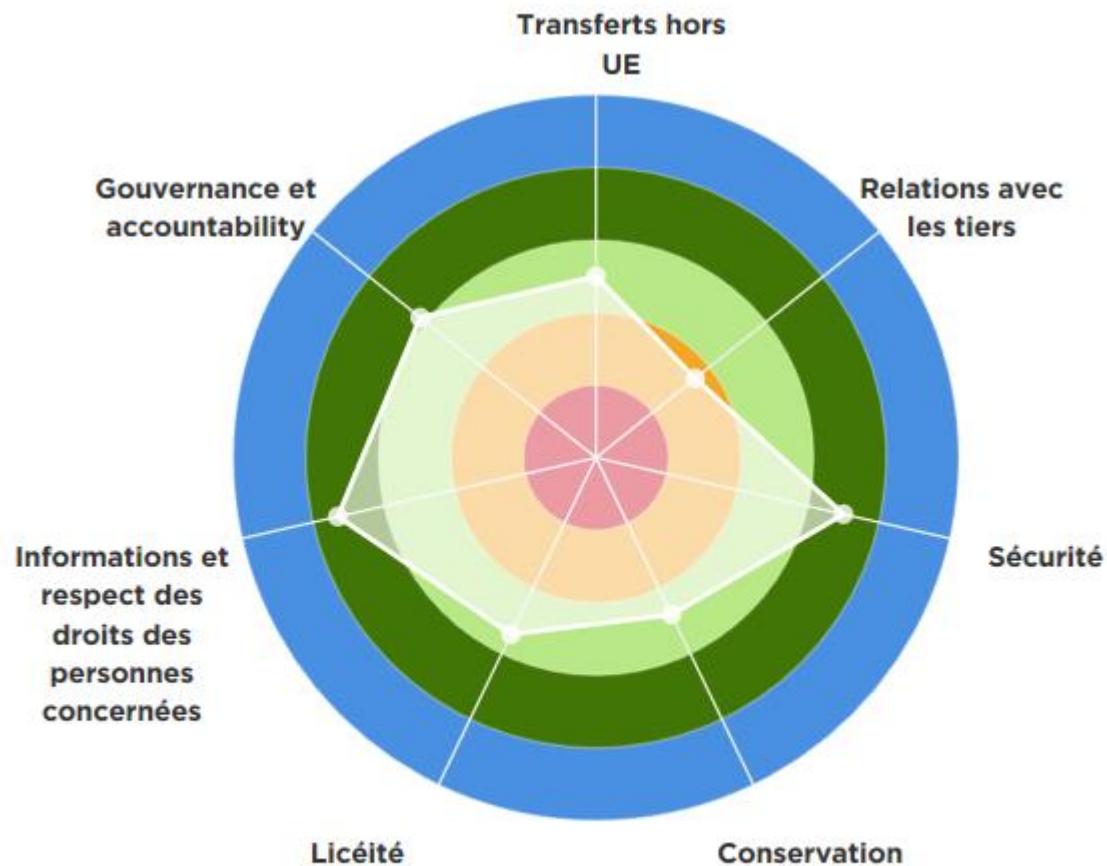
Règlement dissuasif : des risques forts

- des amendes allant jusqu'à 20M€ ou 4% du CA mondial prononcées par la CNIL,
- des peines de prison allant jusqu'à 5 ans d'emprisonnement / 300.000€ d'amende

et aussi un risque réputationnel

- mauvaise publicité
- perte de confiance des clients

★ Comprendre le RGPD (GDPR)





Comprendre le RGPD (GDPR)

De nouvelles obligations fortes et contraignantes

- Obligation d'**information** : toujours fournir la mention « CNIL » aux personnes concernées;
- Obligation de tenir compte du GDPR dans toute décision IT, projet, développement ou achat de solutions logicielles / prestations (« **privacy by design** »);
- Obligation de mettre en place une étude d'impact préalable (« **PIA** / *Privacy Impact Assessment* ») en cas de traitement *big data* ou de traitements sensibles;
- Obligation de **minimiser les données collectées** et de pouvoir prouver pour quoi les données sont collectées;
- Obligation de limiter dans le temps la conservation des données (politique de **purge obligatoire**);
- Obligation de **sécurité informatique** et de confidentialité et intégrité des données collectées;
- Obligation de prévenir la CNIL en cas de **faible de sécurité** dans les 72h;
- Obligation d'avoir un **contrat-type** avec les prestataires externes comprenant de nombreuses clauses imposées par le GDPR;
- Obligation de tracer les activités dans un **registre dédié**.

Chaque obligation doit donner lieu à une documentation spécifique



Comprendre le RGPD (GDPR)

Respect de la loi

Il n'y a plus de déclaration à la CNIL. C'est à chaque entreprise de s'assurer qu'elle respecte bien la loi.

Le GDPR est construit dans un esprit de *compliance* : la CNIL contrôlera de nombreuses sociétés qui devront prouver, sur une base principalement documentaire, son respect de la loi.

Responsabilités

Le GDPR a posé des principes de responsabilité :

- lorsque deux responsables de traitements (partenaires par ex) utilisent des données personnelles en ayant déterminé la finalité, **la responsabilité est conjointe**;
- lorsqu'un sous-traitant (prestataire par ex) viole le GDPR, le responsable du traitement et le sous-traitant sont **tous les deux responsables** à l'égard de la personne concernée.

La responsabilité pénale est toujours personnelle.

GDPR et SOUS-TRAITANCE





Définitions

Le responsable de traitement est celui qui « *détermine les finalités et les moyens du traitement* »

Le sous-traitant est celui qui « *traite des données à caractère personnel pour le compte du responsable du traitement* »

En qualité de **responsable de traitement** (client), vous devez vous assurer que vos **sous-traitants** gérant des données personnelles soient en **conformité avec le RGPD**. Si ce n'est pas le cas, la responsabilité vous en incombera.

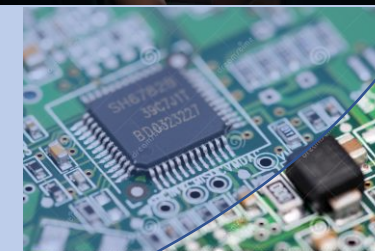
★ La co-responsabilité



ECOSYSTEME DE RESPONSABILITE



Equipements



Sous-traitants

Obligations du sous-traitant

Transparence et traçabilité

- Contrat (article 28)
- Obligation d'instructions
- Accord du client obligatoire si sous-traitant de rang 2
- Mise à disposition d'information (exemple : audit CNIL)

Privacy by design

- Garantir que les traitements offrent les garanties nécessaires de respect du RGPD (DPO, Registre...)

Garantir la sécurité des données traités:

- Moyens humains, physiques et IT
- Notification des violations de données
- Suppression de données au terme du traitement.

Obligation d'assistance d'alerte et de conseil

★ Les instructions du client

CE QUE PRÉVOIT LE RGPD

L'article 82

Le sous-traitant est responsable s'il a manqué à ses obligations ou agit en dehors des instructions **licites** du responsable de traitement

L'article 28

Le sous-traitant ne traite les données à caractère personnel **que sur instructions documentées** du responsable du traitement

Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une **instruction constitue une violation du RGPD**

CE QUI EST CONSTATÉ EN PRATIQUE

- Les contrats font toujours référence aux instructions documentées du client
- Mais très peu de donneurs d'ordres formalisent leurs instructions
- Les moyens permettant d'informer le client sur l'illicéité d'une instruction ne sont jamais prévus
- Que faire en cas désaccord avec le client concernant la licéité d'une instruction

★ Les mesures de sécurité

CE QUE PRÉVOIT LE RGPD

L'article 32

Le sous-traitant doit mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque

L'article 28

Le sous-traitant « *aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant* »

CE QUI EST CONSTATÉ EN PRATIQUE

- Les contrats ne définissent pas les traitements de données (nature, portées, objet) qui sont confiés au sous-traitant
- Les clients ne sont pas toujours exhaustifs dans la liste des données qui sont confiées au sous-traitant
- Le sous-traitant n'est pas informé de l'évolution du traitement
- Les clients n'apprécient pas les risques pour les individus, notamment à travers une DPIA

Le contrat

- Ce contrat doit définir :
 - l'objet et la durée de la prestation que vous effectuez pour le compte de votre client.
 - la nature et la finalité du traitement
 - le type de données à caractère personnel que vous traitez pour le compte de votre client
 - les catégories de personnes concernées
 - les obligations et les droits de votre client en tant que responsable de traitement
 - vos obligations et vos droits en tant que sous-traitant tels que prévus à l'article 28 du règlement
- Pour aller plus loin :
 - https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

GDPR RATING

CONTACT



GDPR
RATING

Laurent ZEITOUN
Directeur Général

21, rue de la Banque
75002 PARIS

Mobile : 06 20 48 09 25

Email : laurent.zeitoun@gdpr-rating.eu

KEEP IN TOUCH !



GDPR Rating



@GDPR.Rating



www.gdpr-rating.eu/fr/



GDPR Rating



[@gdpr_rating](https://twitter.com/gdpr_rating)