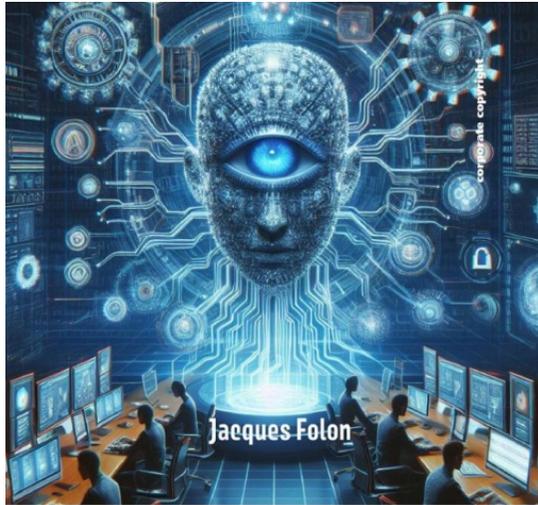


Marketing digital et RGPD Un couple impossible ?





RGPD 2024

la protection des données personnelles
à l'heure de l'Intelligence Artificielle

GUIDE PRATIQUE

Préface de Didier Reyniers, commissaire européen Justice

Editeur aux droits d'auteur

FINALIST
BELGIUM'S
CYBER SECURITY
Privacy Professional
of the Year



Jacques Folon

Co-founder & CEO
GDPRFOLDER.EU

Prof. Dr. Jacques Folon

@ Jacques@gdprfolder.eu

www.linkedin.com/in/folon

www.gdprfolder.com

+32 475 98 21 15

https://www.folon.com

- 
- LE GDPR EN RÉSUMÉ
 - LE SITE INTERNET
 - LES COOKIES
 - L'EMAILING ET LA PROSPECTION
 - LES RÉSEAUX SOCIAUX
 - ANALYSE DE RISQUES ET PRIVACY BY DESIGN
 - L'IA

2018 - 2024
6 ANS DE
RGPD
PETIT RAPPEL





Ce que je sais à propos du RGPD ?

Pourquoi je dois m'y intéresser pour le marketing digital?

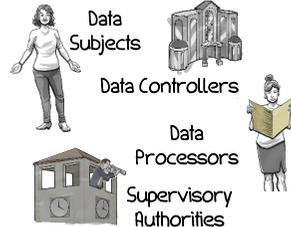
Un petit résumé des relations entre RGPD et marketing direct

TERRITORIAL SCOPE

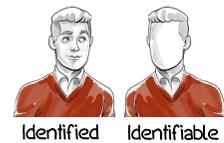


EU Establishments
 Non-EU Established Organizations
 Offer goods or services or engaging in monitoring within the EU.

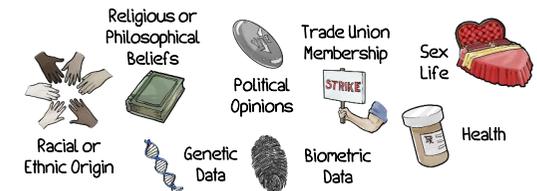
THE PLAYERS



PERSONAL DATA



SENSITIVE DATA



RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS



LAWFUL PROCESSING

Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for

- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



CONSENT



Consent must be freely given, specific, informed, and unambiguous.

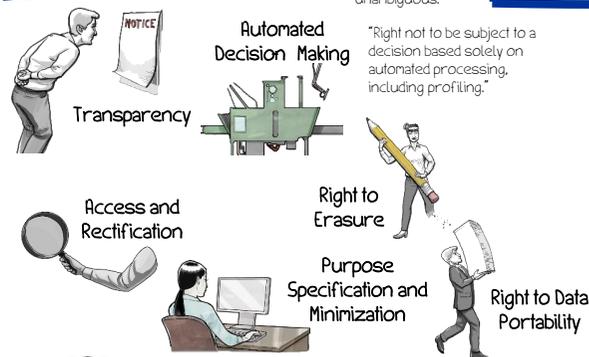


DATA BREACH NOTIFICATION

A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects
 Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS



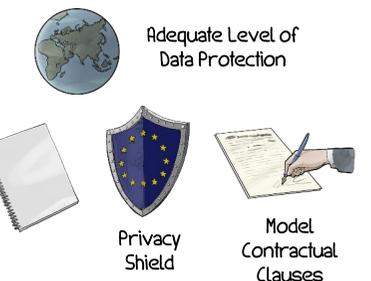
"Right not to be subject to a decision based solely on automated processing, including profiling."

ENFORCEMENT

Fines
 Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies:
 compensation for material and non-material harm.

INTERNATIONAL DATA TRANSFER

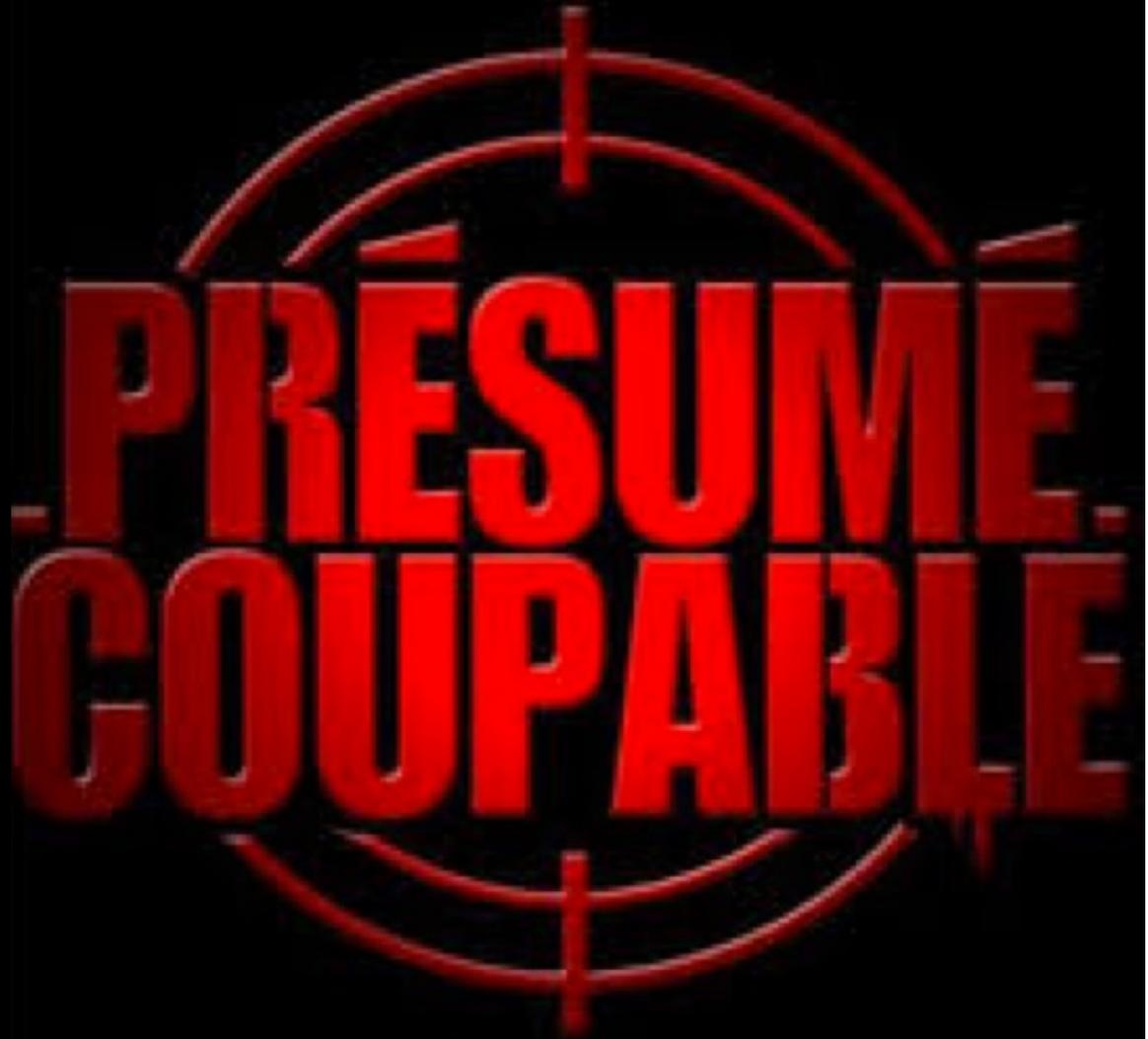




Accountability principle

- You must be compliant!
- You must show it !

Vous devez être capable de démontrer que vous êtes en règle par rapport au RGPD



**PRÉSUMÉ
COUPABLE**



I want to be GDPR compliant.
What do I need to do?

It's easy. Just buy a badge
and pin it on.

**GDPR
COMPLIANCE**

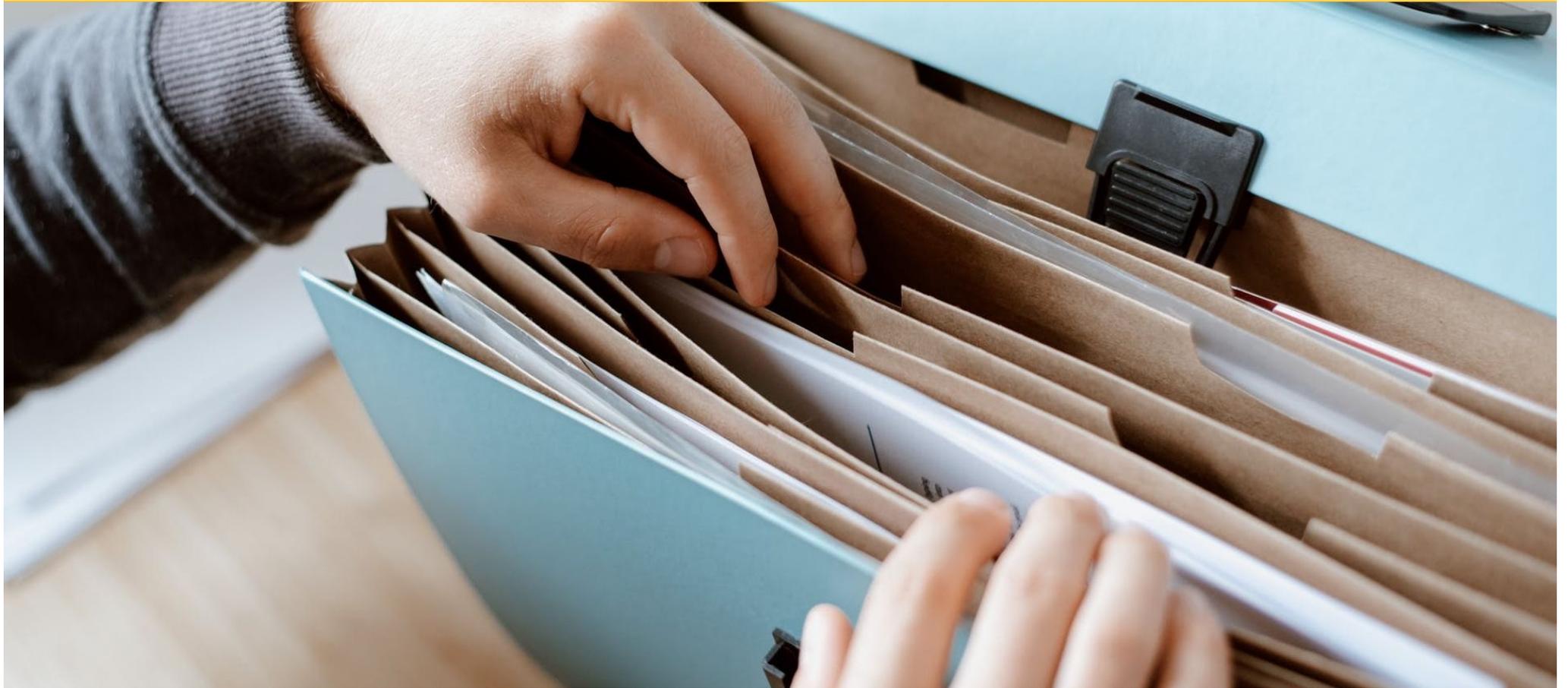
**GDPR
COMPLIANT**

Written by Daniel J. Solove

www.teachprivacy.com

Illustrated by Ryan Beckwith

le dossier rgpd



But à atteindre

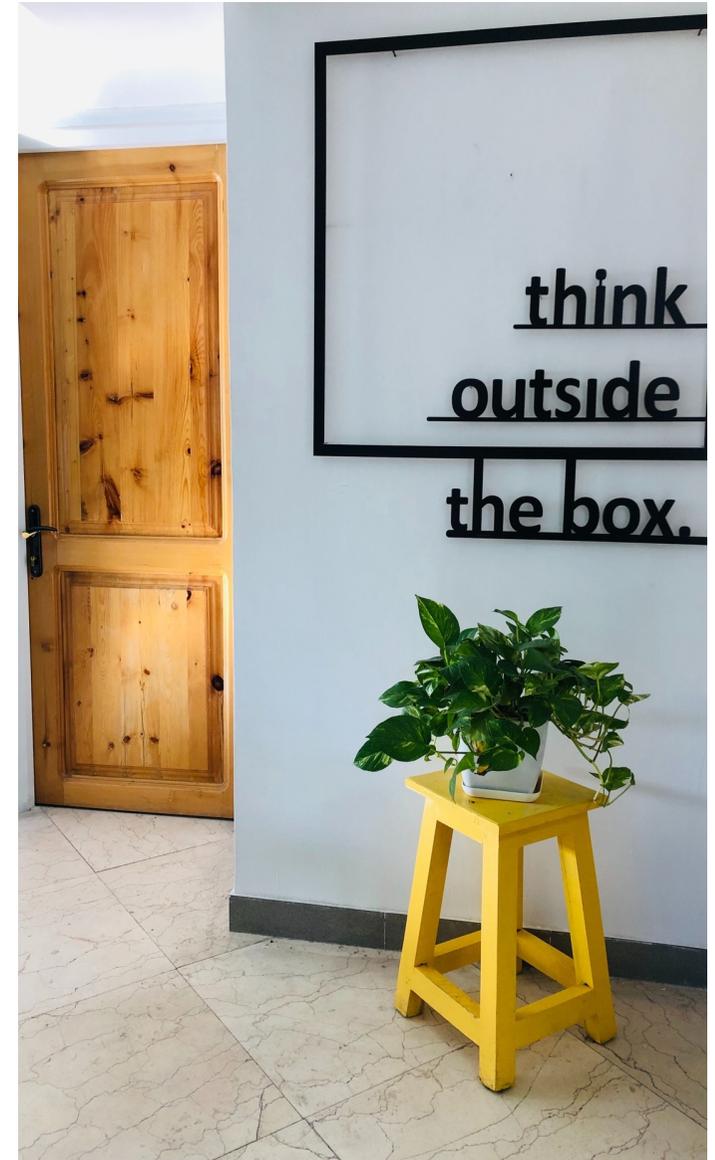
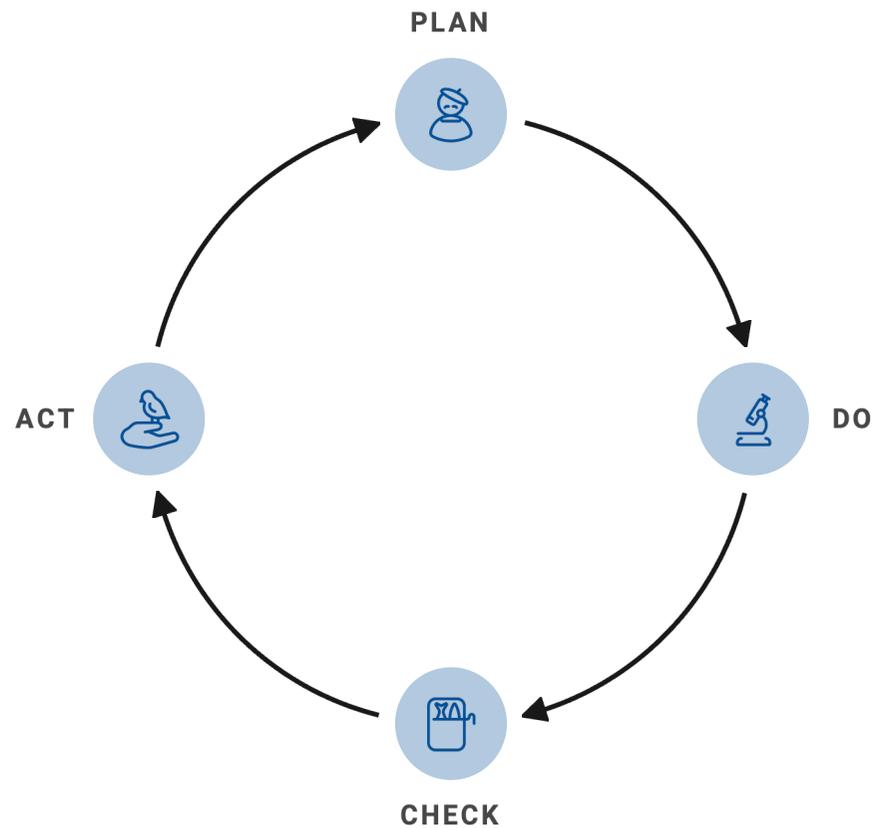
- Avoir un dossier complet
- Obligation de moyen
- La sécurité de l'information en fait partie
- Et la compliance est comprise dans ISO27002

LE DOSSIER RGPD

- 01 DPO
- 02 Contrats de sous-traitance et RT-RT
- 03 DPIA
- 04 RH
- 05 Site internet et portails
- 06 Registre des incidents
- 07 Registre des traitements
- 08 Mesures de sécurité techniques
- 09 Mesures de sécurité organisationnelles
- 10 gestion des droits des personnes concernées
- 11 Privacy by design
- 12 relations avec l'APD
- 13 Conventions
- 14 IA et RGPD
- 15 NIS2 ET RGPD
- 98 suivi des réunions



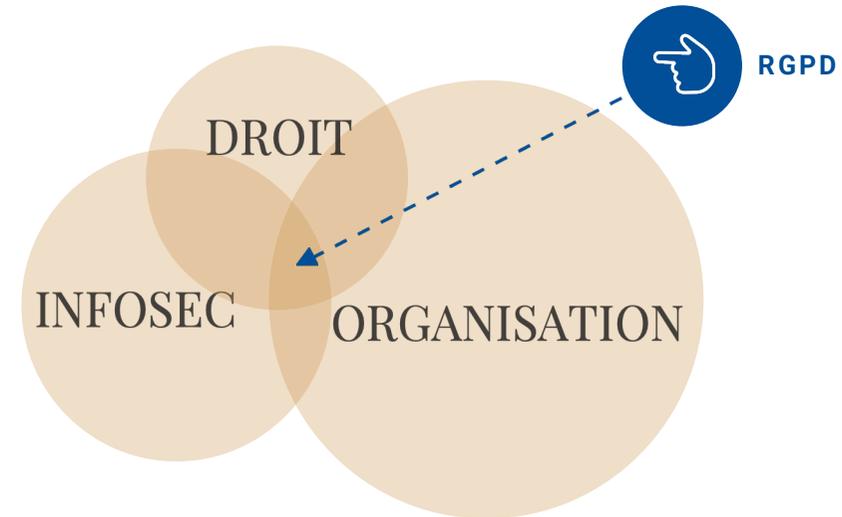
LE DOSSIER RGPD NE SERA JAMAIS FINI !





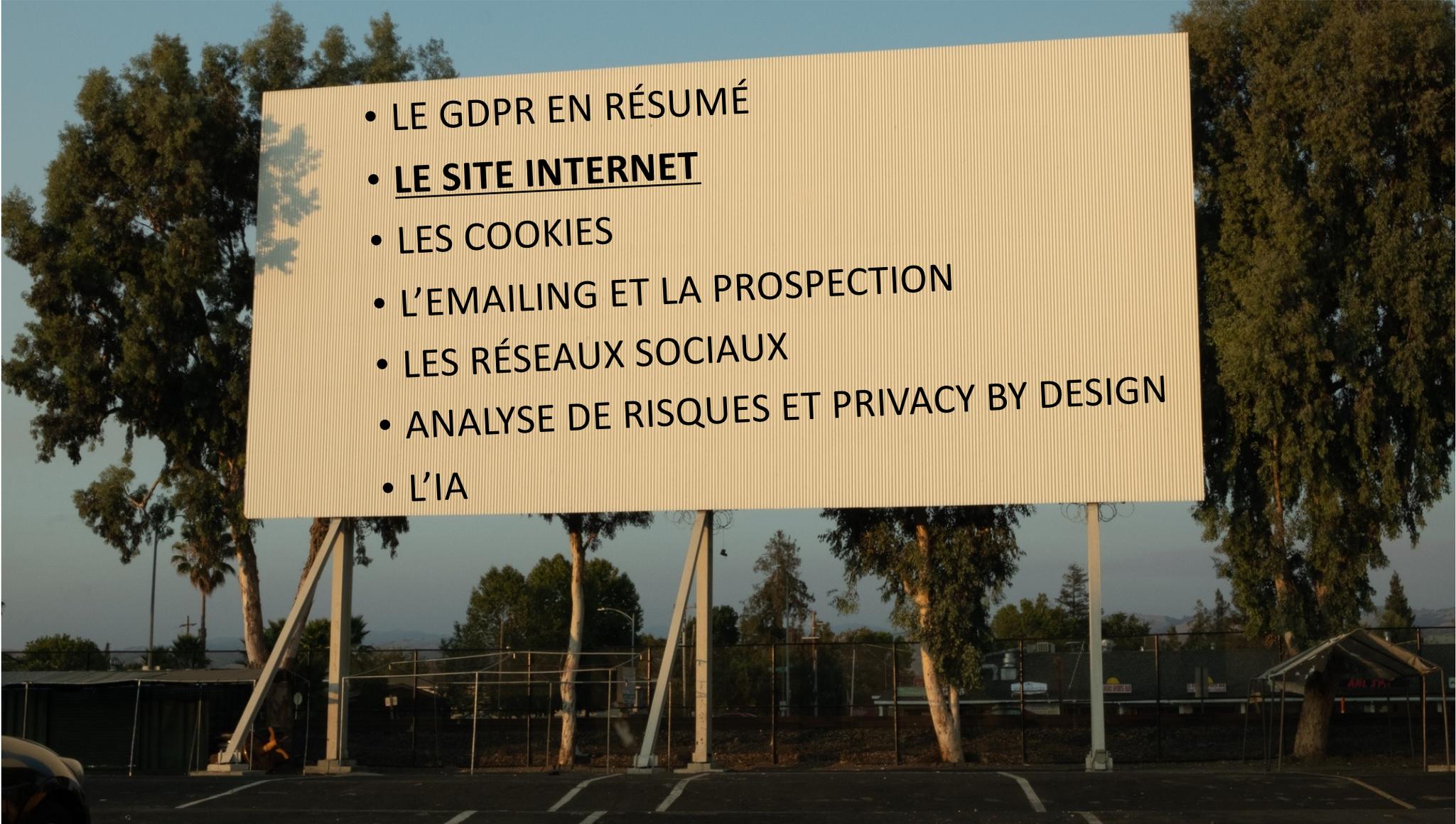
RGPD = ce n'est pas que du droit!!

Combinaison de 3 éléments



2 DIFFERENT WORLDS ? NOT REALLY THEY ARE NEARLY THE SAME !



- 
- LE GDPR EN RÉSUMÉ
 - LE SITE INTERNET
 - LES COOKIES
 - L'EMAILING ET LA PROSPECTION
 - LES RÉSEAUX SOCIAUX
 - ANALYSE DE RISQUES ET PRIVACY BY DESIGN
 - L'IA

Site internet



SONDAGE

Votre employeur lance un site internet de vente en ligne B2C de vêtements et accessoires.

Combien d'éléments devez-vous prendre en compte pour respecter le RGPD?

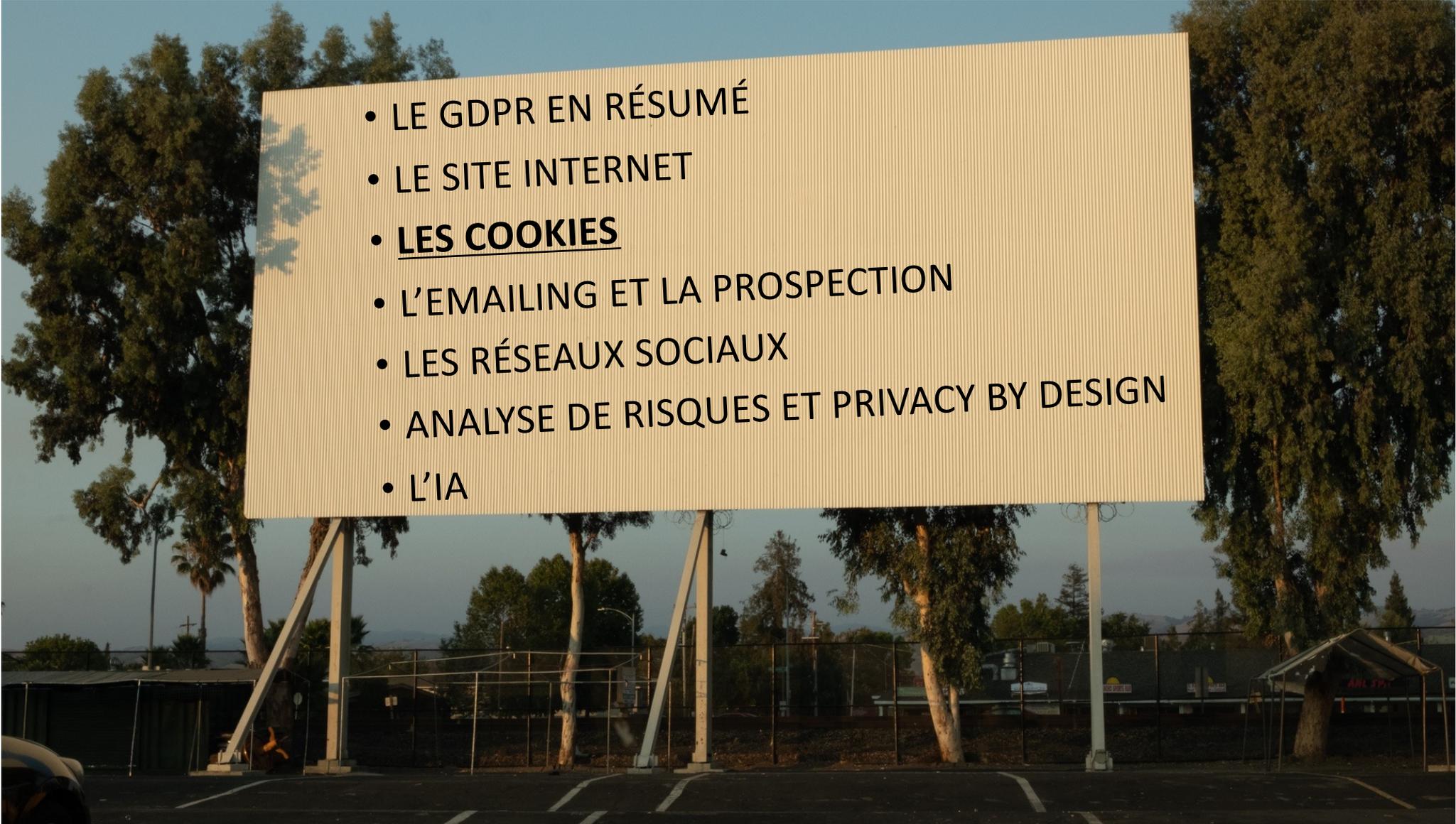
1. Cookies bandeau
2. Cokkies policy
3. Privacy policy
4. Droits des personnes
5. Durée de conservation des données
6. Etc.



le site internet est très visible...



- Double opt-in recommandé
- Conservation des accords
 - Contrat
 - consentement
- Cookies !
- Analytics
- Durée de conservation
- Privacy policies (pour chaque finalité)
 - Visiteurs
 - Newsletter
 - Achat
 - ...

- 
- LE GDPR EN RÉSUMÉ
 - LE SITE INTERNET
 - **LES COOKIES**
 - L'EMAILING ET LA PROSPECTION
 - LES RÉSEAUX SOCIAUX
 - ANALYSE DE RISQUES ET PRIVACY BY DESIGN
 - L'IA

LES COOKIES

- C'est quoi ?
- Comment ça marche?
- Ca sert à quoi ?
- Que doit-on mettre sur le site ?





Quel est la base légale pour utiliser les cookies ?

Les cookies doivent être acceptées par l'internaute et il s'agit donc d'un consentement au sens du RGPD



Le consentement



Consentement préalable

- ✓ Je ne dépose (ni ne me procure accès à) aucun cookie qui ne soit pas strictement nécessaire avant d'avoir obtenu le consentement valable à cet effet ;



Site web

Si vous souhaitez autoriser le dépôt de cookies sur votre appareil, vous pouvez cliquer sur le bouton "Tout accepter". Si vous souhaitez refuser un tel dépôt, vous pouvez accéder au niveau suivant en cliquant sur "Paramètres".

Tout accepter

Paramètres



Site web

Si vous souhaitez autoriser le dépôt de cookies sur votre appareil, vous pouvez cliquer sur le bouton "Tout accepter". Si vous souhaitez refuser un tel dépôt, vous pouvez accéder au niveau suivant en cliquant sur "Paramètres".

Tout accepter

Tout refuser

Paramètres

Consentement libre

- ✓ Je n'utilise pas de "cookie walls"²;
- ✓ Je ne prévois pas de bouton "accepter tous les cookies" (ou similaire) sans prévoir au même "niveau" un bouton "refuser tous les cookies non essentiels" (ou similaire)³;
- ✓ Je n'utilise pas de techniques pouvant être qualifiées de "deceptive design"⁴ (par ex. l'incitation par l'utilisation de la couleur)⁵;





Autorité de protection des données
Gegevensbeschermingsautoriteit



Consentement spécifique

- ✓ Je prévois, au plus tard dans un deuxième "niveau", la possibilité d'accorder (ou non) le consentement séparément pour chaque finalité spécifique ;
- ✓ J'utilise des catégories de cookies délimitées de la manière la plus claire et la plus précise possible, en me basant sur les finalités spécifiques pour lesquelles ils sont utilisés ;
- ✓ Je tiens compte également du fait que l'utilisation à des fins de publicité/profilage propre et celle à des fins de publicité/profilage de tiers doivent être considérées comme des finalités distinctes⁶;
- ✓ Je tiens également compte à cet égard du fait que l'utilisation de cookies pour partager, liker ou suivre une page sur des réseaux sociaux et l'utilisation de cookies pour personnaliser des publicités visent des finalités différentes ;
- ✓ J'évite l'utilisation d'un même cookie pour plusieurs finalités⁷;
- ✓ Je donne la possibilité, le cas échéant dans un "niveau" inférieur, d'accepter (ou non) l'utilisation de cookies par "partenaire" (responsable conjoint du traitement) ;





Consentement éclairé

- ✓ Je renseigne dans le premier "niveau" d'une façon très claire et concise les différentes finalités pour lesquelles le consentement est demandé (par ex. en utilisant une mise en évidence en gras, des puces, etc.) ;
- ✓ Je fournis en outre dans le premier "niveau", d'une façon claire et concise, au moins des informations sur :
 - ✓ l'identité de l'entité (des entités) responsable(s) du dépôt ou de la lecture des cookies (le cas échéant avec indication du nombre de partenaires et un hyperlien vers la liste complète répartie par catégorie) ;
 - ✓ la manière dont les cookies peuvent être acceptés ou refusés ;
 - ✓ les conséquences du refus ou de l'acceptation de cookies ;
 - ✓ l'existence du droit de retirer le consentement et la manière dont on peut le faire ;
- ✓ Je fournis en outre, dans un "niveau inférieur", la liste complète des cookies utilisés, classés par catégorie, y compris leur finalité, durée et les destinataires de ces cookies²;



Consentement univoque et actif

- ✓ Je ne déduis pas un consentement de la poursuite de la navigation sur le site Internet ou de la fermeture d'une bannière, ni de toute autre forme d'inactivité ;
- ✓ Je n'utilise pas de case précochée afin d'obtenir le consentement, que ce soit dans un premier "niveau" ou dans un "niveau" inférieur ;
- ✓ Je ne lie pas la demande de consentement à l'acceptation de conditions générales, ni à l' "acceptation" (ou la confirmation de prise de connaissance) d'une politique de confidentialité ;
- ✓ Je ne déduis pas le consentement des paramètres du navigateur d'un "visiteur" ;



Retrait du consentement

- ✓ Je prévois un mécanisme par lequel il est aussi simple de retirer le consentement que de le donner, comme en plaçant un lien ou un bouton clairement visible permettant de gérer le paramétrage des cookies et de retirer le consentement en un seul clic ;
- ✓ Je m'assure que ce retrait de consentement a effectivement l'effet escompté et qu'il n'a pas pour seule conséquence que ce cookie ne sera plus placé à l'avenir ;



Responsabilité

- ✓ Je veille à ce que les cookies destinés à l'enregistrement des préférences en matière de cookies du "visiteur" ne soient conservés que pendant une durée limitée (l'Autorité de protection des données estime qu'un délai de 6 mois est en principe raisonnable)⁹;
- ✓ Je conserve des informations démontrant la façon dont mon mécanisme de consentement (comme une bannière) a été adapté au fil du temps, je conserve les versions précédentes de ma politique en matière de cookies, j'indique une date et un numéro de version dans ma politique en matière de cookies)¹⁰;





Quand ne faut-il pas de consentement ?

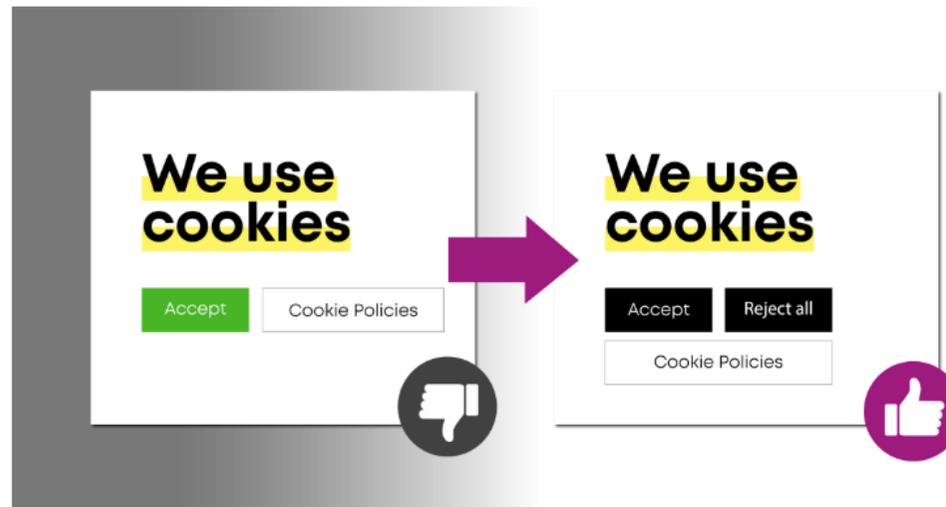
- ✓ J'ai contrôlé la catégorisation des "cookies techniques essentiels"¹¹ (tels que ceux pour le load balancing) ;
- ✓ J'ai contrôlé la catégorisation des "cookies fonctionnels strictement nécessaires" (tels que les cookies pour la conservation temporaire du choix de la langue, les préférences en matière de cookies ou le contenu du panier). Ceci inclut uniquement les cookies qui sont strictement nécessaires pour fournir un service¹² explicitement demandé par le "visiteur" ;
- ✓ J'ai veillé à ce qu'aucun autre cookie que ceux ci-dessus ne soit placé sans l'obtention préalable du consentement valable du "visiteur".



226 plaintes déposées contre des bannières de cookies trompeuses

⚠ This page has been translated automatically. [Read the original](#) or [leave us a message](#) if something is not right.

[Cookie Banners](#) / Tue 09/08/2022 - 10:35



"Les conceptions de bannières de cookies trompeuses tentent de forcer l'accord de l'utilisateur en rendant le refus des cookies incroyablement pénible. Le GDPR exige en fait un choix équitable entre oui et non, pas des marathons de clics insensés." -

Ala Krinickytė, avocat spécialisé dans la protection des données chez noyb



Autorité de protection des données
Gegevensbeschermingsautoriteit

1/33

Chambre Contentieuse

Décision quant au fond 131/2024 du 11 octobre 2024

Numéro de dossier : DOS-2023-03283

Objet : Plainte relative à la bannière cookies présente sur le site Internet de RTL Belgium

[Aide et contact](#) [Concours](#) [Castings](#)

[Mentions légales](#) [Conditions générales d'utilisation](#) [Espace de confidentialité](#) [Gestion des cookies](#)



RTL info.

Avec votre accord, [nos partenaires](#) et nous utilisons des cookies ou technologies similaires pour stocker et accéder à des informations personnelles comme votre visite sur ce site. Vous pouvez retirer votre consentement à tout moment en cliquant sur "En savoir plus" ou dans notre [politique en matière de cookies](#) sur ce site.

Avec nos partenaires, nous traitons les données suivantes en nous basant sur votre consentement :

Cookies essentiels, Données de géolocalisation précises et identification par analyse du terminal, Publicités et contenu personnalisés, mesure de performance des publicités et du contenu, données d'audience et développement de produit, Réseaux sociaux, Stocker et/ou accéder à des informations sur un terminal

[EN SAVOIR PLUS →](#)

[ACCEPTER & FERMER](#)

- 
- A large billboard with a white corrugated metal surface is mounted on several tall, light-colored metal poles. The billboard is positioned in an outdoor parking lot area, with a chain-link fence and trees in the background. The sky is clear and blue. The text on the billboard is in black, sans-serif font, and is arranged in a list format. The fifth item in the list, 'L'EMAILING ET LA PROSPECTION', is underlined and bolded.
- LE GDPR EN RÉSUMÉ
 - LE SITE INTERNET
 - LES COOKIES
 - **L'EMAILING ET LA PROSPECTION**
 - LES RÉSEAUX SOCIAUX
 - ANALYSE DE RISQUES ET PRIVACY BY DESIGN
 - L'IA



EMAILING, PROSPECTION ET RGPD

Au niveau RGPD il faut penser à quoi ?

LES QUATRE ÉTAPES POUR UNE CAMPAGNE D'EMAILING « LÉGALE »



4. DROITS DES PERSONNES

3. UNSUSCRIBE

2. PREUVE
DU CONSENTEMENT

1. CONSENTEMENT

La publicité par courrier électronique est possible à condition que les personnes aient explicitement donné leur **consentement** avant d'être démarchées.

Le **consentement** doit être **libre, spécifique, éclairé et univoque**. Il requiert, pour être valable, une action positive et spécifique de la personne concernée (par exemple, une case à cocher dédiée et qui ne soit pas pré-cochée). L'acceptation de conditions générales d'utilisation ne peut suffire. L'accord doit être libre.

Exemple d'information sur un site web :

J'accepte que mes informations soient utilisées pour de la prospection commerciale.

Deux exceptions à ce principe :

- **Si la personne prospectée est déjà cliente de l'entreprise et si la prospection concerne des produits ou services similaires fournis par la même entreprise.**

Comme la CNIL l'a rappelé dans une décision de **sanction**, cette exception ne peut pas être mobilisée lorsqu'aucune vente ou prestation de service n'a été effectuée, y compris lorsque le client a créé un compte en ligne (par exemple sur un site de commerce en ligne). En effet, la simple création d'un compte ne signifie pas qu'il y aura une commande éventuelle de produits ou de services auprès de la société.

- **Si la prospection n'est pas de nature commerciale (caritative par exemple).**

Dans ces deux cas, la prospection peut être fondée sur **l'intérêt légitime** de l'organisme. **La personne doit, au moment de la collecte** de son adresse de messagerie :

- **être informée** que son adresse électronique sera utilisée à des fins de prospection ;
- **être en mesure de s'opposer** à cette utilisation de manière simple et gratuite lorsque les données sont collectées, et à tout moment notamment lors de chaque envoi d'un courrier électronique de prospection.





La prospection vers les professionnels peut être fondée sur **l'intérêt légitime** de l'organisme.

La personne doit, au moment de la collecte de son adresse de messagerie :

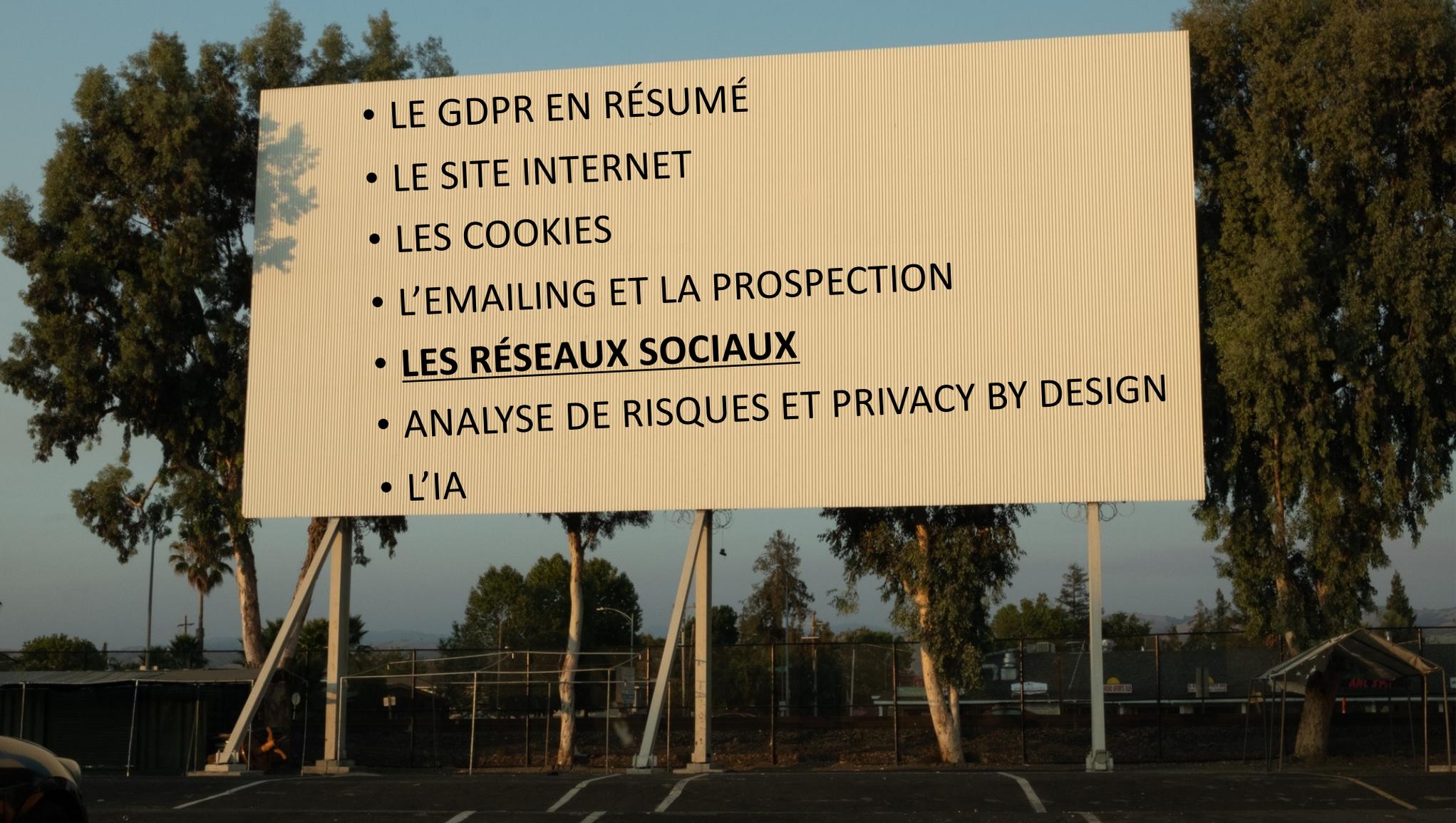
- **être informée** que son adresse électronique sera utilisée à des fins de prospection par voie électronique ;
- **être en mesure de s'opposer** à cette utilisation de manière simple et gratuite.

Lorsque les données sont déjà en possession de la société ou acquises auprès de tiers, il faut s'assurer que la personne concernée a été informée du traitement et est en mesure de s'y opposer.

L'objet de la sollicitation doit être en rapport avec la profession de la personne démarchée.

Exemple : message présentant les mérites d'un logiciel à paul.toto[@]nomdelasociété, directeur informatique.

Les adresses professionnelles génériques de type info[@]nomsociete.fr, contact[@]nomsociete.fr ou commande[@]nomsociete.fr sont des coordonnées de personnes morales. Elles ne sont pas soumises aux principes rappelés ci-dessus.

- 
- LE GDPR EN RÉSUMÉ
 - LE SITE INTERNET
 - LES COOKIES
 - L'EMAILING ET LA PROSPECTION
 - **LES RÉSEAUX SOCIAUX**
 - ANALYSE DE RISQUES ET PRIVACY BY DESIGN
 - L'IA



RGPD ET RESEAUX SOCIAUX

Que doit-on faire à votre avis ?

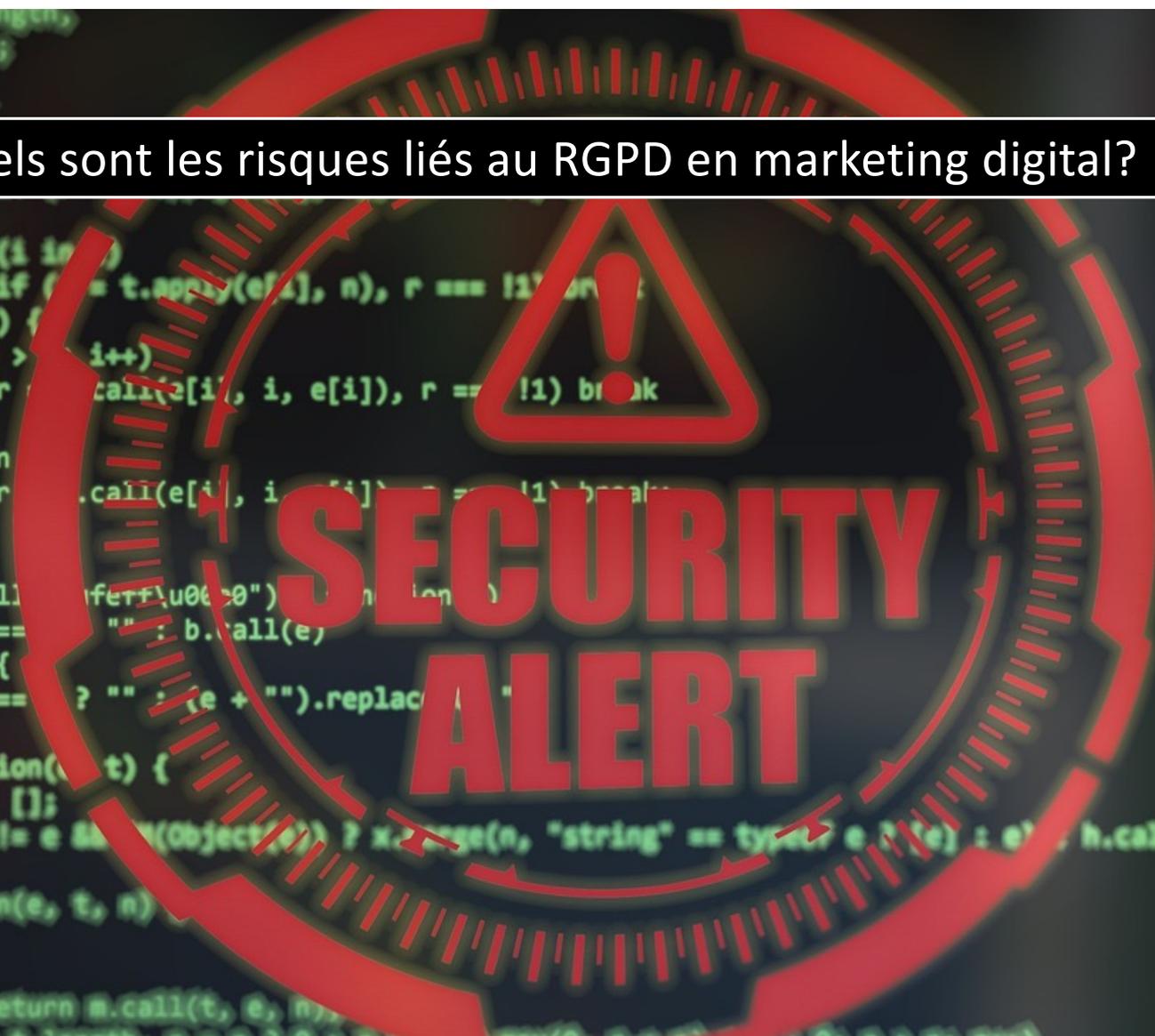
- 
- A close-up photograph of a person's hand holding a white rectangular card. The person is wearing a dark suit jacket and a white shirt. The background is dark and out of focus. The card contains a bulleted list of three French terms.
- RESPONSABLE CONJOINT
 - INFORMATION AUX PERSONNES
 - POLITIQUE DE VIE PRIVÉE

- 
- LE GDPR EN RÉSUMÉ
 - LE SITE INTERNET
 - LES COOKIES
 - L'EMAILING ET LA PROSPECTION
 - LES RÉSEAUX SOCIAUX
 - ANALYSE DE RISQUES ET PRIVACY BY DESIGN
 - L'IA

A green rectangular sign with white text is suspended from a dark metal pole. The sign is centered horizontally and features the text "ANALYSE DE RISQUES + PRIVACY BY DESIGN" in a bold, sans-serif font. The background is a blurred city street scene with a clock tower visible in the lower right.

ANALYSE DE RISQUES + PRIVACY BY DESIGN

Quels sont les risques liés au RGPD en marketing digital?



**SECURITY
ALERT**

Commencer par identifier les risques
Et puis pour chaque risque...

		Niveau de gravité			
		Insignifiant	Marginal	Critique	Catastrophique
Probabilité	Très probable	A gérer	Inacceptable	Inacceptable	Inacceptable
	Probable	A gérer	A gérer	Inacceptable	Inacceptable
	Possible	Négligeable	A gérer	A gérer	Inacceptable
	Peu probable	Négligeable	Négligeable	A gérer	Inacceptable
	Très improbable	Négligeable	Négligeable	A gérer	A gérer

Le but d'une analyse de risques est de pouvoir démontrer

1. que l'ensemble des dangers ont été identifiés,
2. que les risques qui en découlent ont été évalués e
3. comment un risque inacceptable est rendu acceptable par la mise en œuvre des mesures préventives

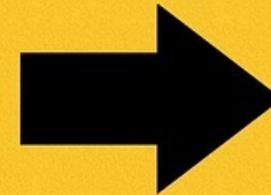
N°	Niveau de gravité	Description	Quelques exemples concrets
1	Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments qu'elles surmonteront sans difficulté	Maux de tête passagers Réception de SPAMS Sentiment d'atteinte à la vie privée
2	Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	Refus d'un service administratif ou commercial (ex : refus de prêt bancaire) Publicité ciblée sur un aspect que la personne souhaiterait garder confidentiel (ex : traitement pharmaceutique...)
3	Importante	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter mais avec des difficultés réelles et significatives	Chantage Interdiction bancaire Blessure physique Divorce Phishing
4	Maximale	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles ne pourraient pas surmonter	Décès Sanction pénale Perte de preuve dans le cadre d'un contentieux



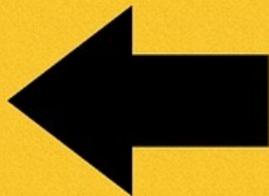
Il faut donc, pour chaque risque, mettre en place les mesures de sécurité pour limiter

- **La probabilité**
- **La gravité**

AVANT DE LANCER LE
TRAITEMENT DE
DONNEES, IL FAUT FAIRE LE
PRIVACY BY DESIGN



AUSSI AVANT SI NECESSAIRE, IL
FAUT FAIRE UNE ANALYSE
D'IMPACT





EN CAS DE VIOLATION DE DONNEES

- REAGIR DANS LES 72 HEURES
- PRENDRE DES MESURES CORRECTIVES

- 
- A large billboard with a white, vertically-ribbed background is mounted on several metal poles. The billboard is positioned in an outdoor parking lot area, with trees and a chain-link fence visible in the background. The text on the billboard is a list of topics, with the last item, 'L'IA', underlined.
- LE GDPR EN RÉSUMÉ
 - LE SITE INTERNET
 - LES COOKIES
 - L'EMAILING ET LA PROSPECTION
 - LES RÉSEAUX SOCIAUX
 - ANALYSE DE RISQUES ET PRIVACY BY DESIGN
 - L'IA

**ARTIFICIAL
INTELLIGENCE**

TIPPA





RGPD

AI

A votre avis c'est possible une IA qui respecte le RGPD ?

IA ET RGPD

- QUI EST RESPONSABLE DE TRAITEMENT ?
 - QUELLES DONNÉES PERSONNELLES ?
 - QUELLE EST LA BASE LÉGALE ?
 - QUELLE EST LA FINALITÉ ?
 - PRIVACY BY DESIGN
 - MINIMISATION ET MACHINE LEARNING
 - ARCHIVAGE ET DURÉE DE CONSERVATION
 - MESURES TECHNIQUES ET ORGANISATIONNELLES
 - DROITS DES PERSONNES CONCERNÉES
 - PRISES DE DÉCISIONS AUTOMATISÉES
- BREF CA DEVRAIT ÊTRE INTERDIT ! 😊



c o n c l u s i o n

LA COMPATIBILITÉ ET LA LÉGALITÉ DU MARKETING DIGITAL
PAR RAPPORT AU RGPD
EST POSSIBLE !





VOS CLIENTS ET
VOS ACTIONNAIRES
SERONT CONTENTS

Marketing digital et RGPD : no excuses :JUST DO IT