

PRINCIPES CNIL : RGPD ET E-PRIVACY

LES 3 RÈGLES À RESPECTER LORS DE LA MISE EN PLACE D'UN PROJET
ANALYTICS

SOMMAIRE

INTRODUCTION — QU'EST-CE QUE LA RÉGLEMENTATION RGPD ?

Page 04

RÈGLES N°1 — LA NON COLLECTE DE DONNÉES PERSONNELLES

Page 10

RÈGLES N°2 — RESPECTER LA DURÉE DE VIE DES COOKIES

Page 14

RÈGLES N°3 — METTRE À JOUR LES CONSENTEMENTS UTILISATEURS

Page 16

POUR ALLER PLUS LOIN — TOUTES LES ACTIONS RGPD À METTRE EN PLACE AU SEIN DE SON ENTITÉ

Page 22

VERSIONS DU DOCUMENT

Version	Date	Auteur	Société	Email	Commentaire
1.1	10/01/2017	Charlotte POULAIN	CONVERTEO	cp@converteo.com	Création du document

INTRODUCTION

QU'EST-CE QUE LA
RÉGLEMENTATION RGPD ?

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

❖ Le **RGPD ou GDPR** (Général Data Protection Régulation) entrera en vigueur le **25 mai 2018** :

- Mise en œuvre d'un « consentement éclairé et informé » / opt-in formel
- Les sanctions pourront aller jusqu'à **4% du chiffres d'affaires mondial du groupe ou 20M€**

❖ Les modalités pratiques de mise en œuvre sur le marché sont encore en discussion actuellement et nécessitent **une veille continue** jusqu'à la stabilisation du périmètre légal

❖ Dans tous les cas, le respect de cette réglementation devra nécessairement être pris en compte dans notre démarche :

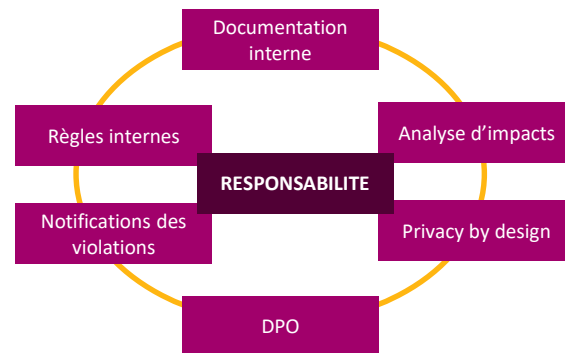
- Anonymisation de la donnée
- Protection et sanctuarisation de la donnée
- Législation européenne > Législation française > Législations locales

❖ Dans cette optique **la logistique autour de la donnée** est un des enjeux central des marques :

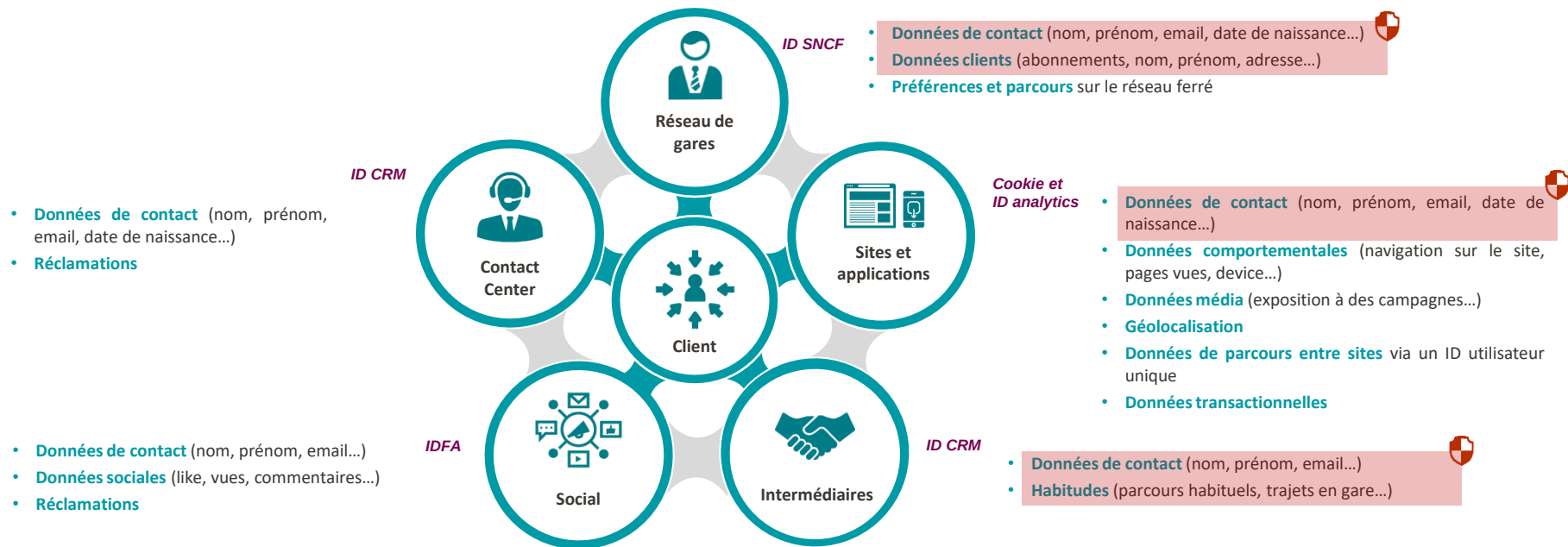
- Une portabilité des data opt-in et opt-out des utilisateurs vers ses partenaires
- Une traçabilité de ses actions



« Quels sont les risques éthiques et réglementaires liés aux données ? »

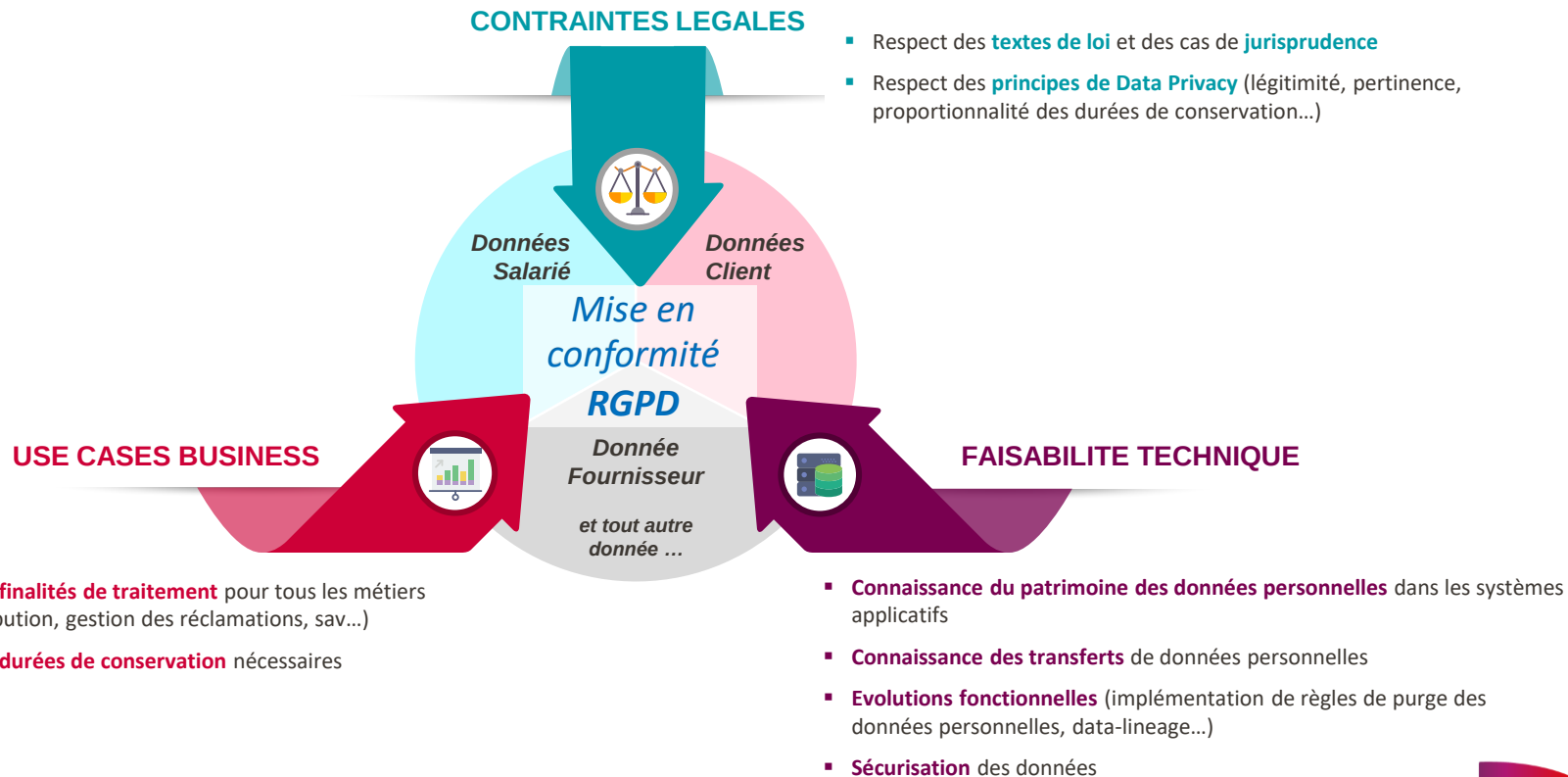


COLLECTER ET DE TRAITER UN FORT VOLUME DE DONNÉES CLIENTS DE NATURE TRÈS DIVERSES



SNCF souhaite définir et déployer une **stratégie Connaissance Client transverse** (cross-canal et cross-entités), conforme à la **réglementation RGPD**, incarnée par un **Comité dédié - DPO**

LES ENJEUX DE MISE EN CONFORMITÉ RGPD



RGPD : LE CONTEXTE ET LES PRINCIPES

LES ENJEUX



Enjeux

- **Responsabiliser les entreprises** sur la gestion des données personnelles
- **Harmoniser les réglementations européennes** et élargir les pouvoirs des autorités de contrôle
- **Renforcer les droits des personnes** à disposer de leurs données et à limiter leur collecte et leur usage



Périmètre

- Applicable lorsque **le responsable du traitement des données est basé dans l'UE**
- Ou lorsque **les personnes concernées se trouvent dans l'UE**



Pénalités

- Les amendes peuvent aller jusqu'à **4% du CA ou 20 M€**
- Un premier seuil de sanction à **2% du CA ou 10 M€** pour les infractions les moins graves

LES PRINCIPES DE PROTECTION DES DONNÉES PERSONNELLES



Finalité

- Le traitement doit être **licite** et **légitime**
- Les données doivent être **pertinentes** pour le traitement
- Il doit y avoir **proportionnalité** entre les données traitées et la finalité de traitement



Transparence

- Les personnes doivent bénéficier d'une **information préalable au traitement sur les droits dont elles disposent** (accès, rectification, opposition à prospection / profilage)
- Les personnes doivent être **informées du fondement juridique** sur lequel repose le traitement (AVEC ou SANS consentement)



Conservation

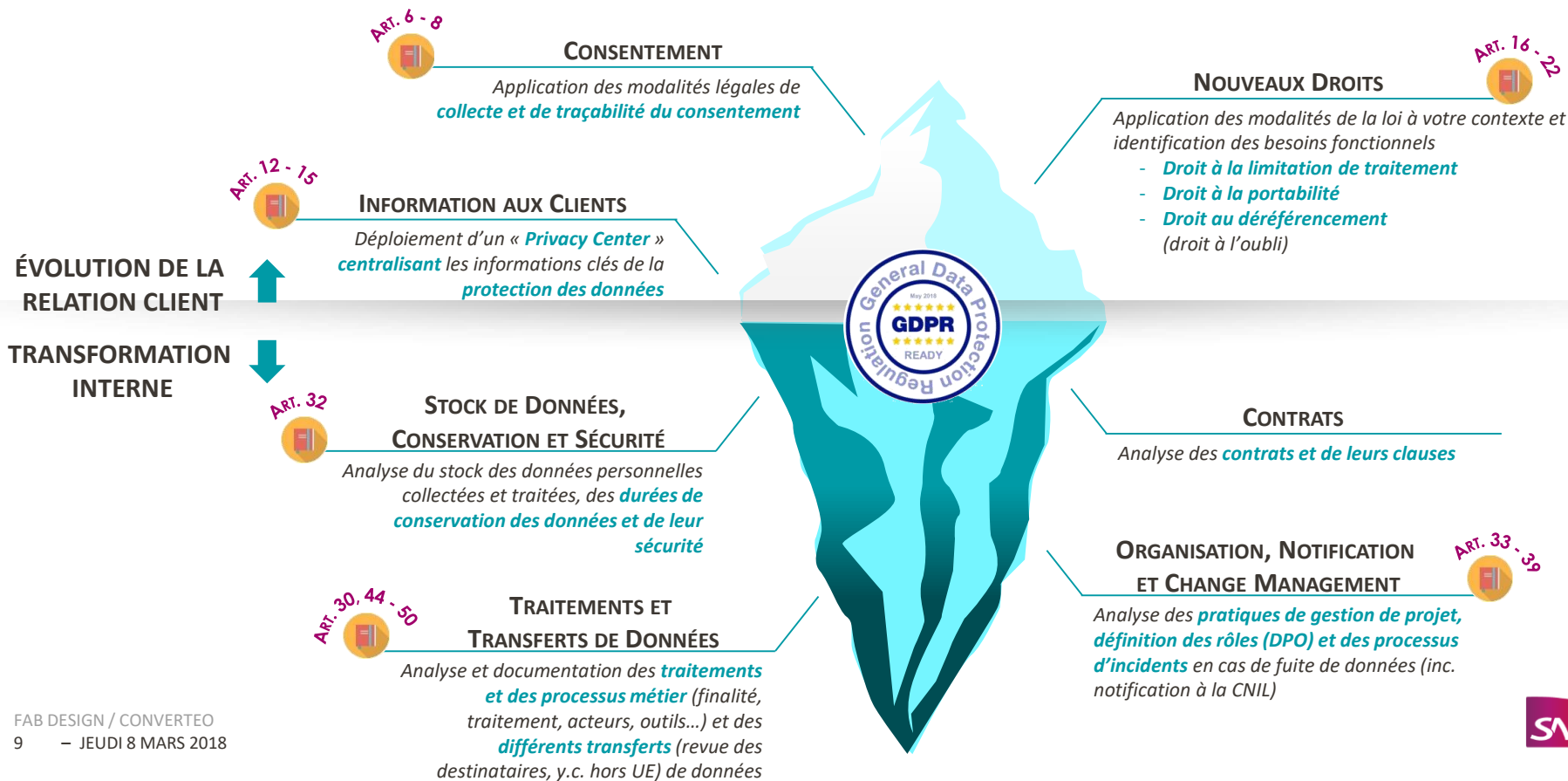
- Les données doivent être conservées pour une **durée adéquate**



Sécurité

- Les données doivent être **protégées** et la **confidentialité assurée**

L'ÉVOLUTION DE LA RELATION CLIENT & LA TRANSFORMATION INTERNE



RÈGLES N°1

LA NON COLLECTE DE DONNÉES
PERSONNELLES

QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?



QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

QU'EST CE QU'UNE DONNÉE PERSONNELLE ?

Toute information relative à une **personne physique** permettant de l'identifier **directement ou indirectement**. Ces données peuvent être **privées ou professionnelles**.



Données d'état-civil ou d'identification : Nom, prénom, identifiant (login, etc.), adresse, numéro de téléphone, adresse mail...



Données de connexion : Adresse IP, logs, conso téléphonique, historiques des sites consultés/téléchargements...



Données de localisation : Déplacements, données GPS, GSM...



Vie personnelle : Pièces justificatives d'identité (CNI, passeport,...), date de naissance, situation familiale, adresse domicile, habitudes de vie, etc.



Vie professionnelle : Niveau de poste, coefficient, diplômes, formations, haut potentiel...



Informations d'ordre économique et financier privées et professionnelles : revenus du foyer, fiscalité, rémunération, bonus, avantages en natures, frais...



Données sensibles réglementées : n° de sécurité sociale, opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciale ou ethnique, données biométriques, contour de la main



Données bancaires : RIB, code IBAN, code guichet...

QU'EST CE QU'UN TRAITEMENT ?

Suite d'**opération structurées**, manuelles ou automatisées, sur les données personnelles

Constituent notamment un traitement :



la collecte;



l'enregistrement et le stockage;



l'extraction, l'adaptation ou la modification;



la consultation;



l'utilisation;



la communication par transmission, la diffusion;



l'effacement ou la destruction;



le verrouillage;

...

Les transferts sont des traitements très fréquents : hébergement en cloud...



LORSQUE JE CRÉE MON PLAN DE TAGGAGE, JE PENSE À...

1 JE NE COLLECTE AUCUNE DONNEE PERSONNELLE

Exemple de données personnelles : Nom, prénom, numéro de téléphone, numéro de carte bancaire...

- Google Analytics, comme l'ensemble des solutions sur le marché veille à ce qu'aucune donnée personnelle ne soit collectée dans leurs outils. Mais il en tient de votre responsabilité lors de la création et de l'implémentation de votre plan de marquage, de ne pas faire afficher, stocker ou suivre des « données personnelles » dans ce type d'outil.

2 J'ANONYMISE OU PSEUDONIMISE LES DONNÉES À CARACTÈRE PERSONNEL OBLIGATOIRES

Exemple de données à caractère personnel : adresse email, user id, genre...

- Pour collecter certaines données indispensables aux besoins de web analyse, il est possible de les récupérer dans le plan de marquage uniquement si ces variables sont 'encryptées' (illisible dans retravail de la donnée via une clé personnalisée)



Mettre à jour les consentements utilisateurs sur ces données encryptées

RÈGLES N°2

E-PRIVACY - RESPECTER LA
DURÉE DE VIE DES COOKIES

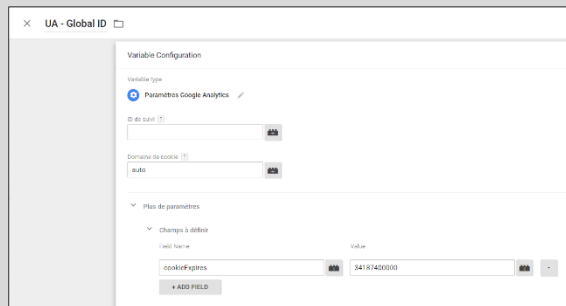
LORSQUE JE PARAMÈTRE MON CONTENEUR GTM, JE PENSE À...

... ADAPTER LA DURÉE DE VIE DES COOKIES AUX PRINCIPES E-PRIVACY DE LA CNIL

1 Paramétrages Google Analytics

Au sein de votre **variable de paramétrage** 'Google Analytics' positionné sur tous vos tags à destination de cet outil de données comportementale :

1. Diriger vous dans les **paramétrages avancés**
2. Ajouter un « **champ à définir** »
3. Ajouter la variable par défaut Google Tag Manager « **cookieExpires** ».



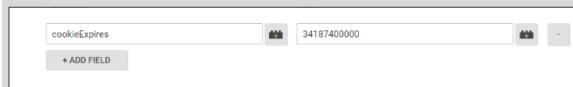
2 Ajuster la durée de vie

La **durée de vie des cookies** d'outil comportemental doit être de **13 mois (imposé par la CNIL)**.

Pour ce faire, en face de votre variables « **cookieExpires** » appliqué en secondes la durée de vie de 13 mois.

13 mois = 34 187 400 secondes

Enregistrez ensuite vos paramétrages.

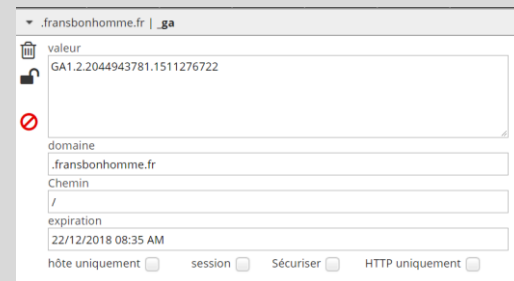


Faites attention de bien appliqué sur paramétrage sur toutes vos variables de paramétrages Google Analytics.

3 Vérifier mon paramétrage

Après la **publication** ou la **prévisualisation** de ces nouveaux paramétrages, je vais **vérifier** sur mon site que le **cookie utilisateur Google Analytics est bien limité à 13 mois** :

1. Je télécharge le plugin Chrome « **EditThisCookie** »
Lien de téléchargement :
<https://chrome.google.com/webstore/detail/editthiscookie/fngmhnnpilhplaeedifhccceomclgfbg?hl=fr>
2. Je vais sur la **première page de mon site** (après avoir rafraichit et effacer les cookies déjà en place sur mon navigateur)
3. Je vérifie la **durée de vie du cookie « _ga »** :



RÈGLES N°3

METTRE À JOUR LES
CONSENTEMENTS UTILISATEURS

PERMETTRE AUX UTILISATEURS DE CONSENTIR OU NON À LA COLLECTE DES DONNÉES COMPORTEMENTALES

1. La pose du cookie Google Analytics

À l'arrivée de l'utilisateur sur le site, lui laisser la possibilité d'appliquer ou non sur le site le tag de suivi Google Analytics contenant tous les cookies de suivi (utilisateur, session, campagne...).

Attention : Le cookie ne doit être déposé que si l'utilisateur accepte de poursuivre sa navigation avec.

2. La collecte de données à caractère personnel

La donnée collectée via Google peut être sensible. Il est indispensable de prévenir de façon explicite la collecte des données via Google Analytics et l'utilisation qui en est faite par la suite.

Exemple : Lors de la collecte de l'email encrypté dans un formulaire de souscription newsletter pour du Retargeting (recommandation produit sur d'autres domaines).

Exemple de privacy center – Gestion des cookies France TV

Gérer l'activation des cookies

Le terme de cookies couvre l'ensemble des traceurs déposés sur votre ordinateur et/ou sur vos appareils mobiles lors de la consultation d'un site internet ou d'une application mobile ou lors de la consultation d'une publicité. Ils ont notamment pour but de collecter des informations relatives à votre navigation sur les sites et de vous adresser des services personnalisés.

francetélévisions

CATÉGORIE	DESCRIPTION	ÉTAT
TAGS ANALYTICS	Ces cookies permettent de mesurer de manière anonyme et agrégée l'audience des contenus présents sur le site et d'en améliorer le fonctionnement.	
TAGS DE PERSONNALISATION	Ces cookies permettent d'interagir avec les modules sociaux et de partager les contenus de ce site avec d'autres personnes ou de les informer de votre consultation ou opinion sur celui-ci lorsque vous cliquez sur "partager", "aimer" sur Facebook et Twitter, par exemple.	☒
TAGS PUBLICITAIRES CIBLÉS	Ces cookies permettent de vous présenter des publicités adaptées à vos centres d'intérêt et à mesurer l'efficacité des campagnes publicitaires. Le fait de refuser la publicité ciblée n'entraîne pas l'arrêt de son affichage mais de ne plus tenir compte de vos préférences.	☒

[Découvrez nos engagements pour protéger vos données](#)

J'accepte

TROIS BONNES PRATIQUES DE GESTION DES DONNÉES PERSONNELLES ET DES COOKIES À RETENIR

1 Adopter une **communication pédagogique**

2 Communiquer en toute **transparence sur les traitements**, leurs **finalités**, leur **fondement juridique** & les **durées de conservation**

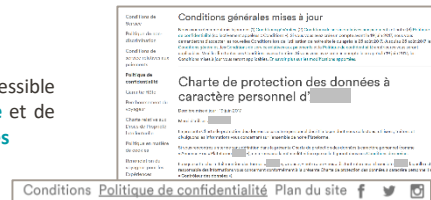
3 Mettre à disposition des utilisateurs des **solutions simples de gestion des informations** désormais **obligatoires et des nouveaux droits**

1. ADOPTER UNE COMMUNICATION PÉDAGOGIQUE, SIMPLE, ACCESSIBLE ET TRANSPARENTE

1

Rédiger une politique de gestion des données personnelles clairement séparée des mentions légales ou des CGV/CGU

La politique de confidentialité de l'acteur est accessible depuis le footer, sur n'importe quelle page du site et de manière clairement séparée des conditions générales

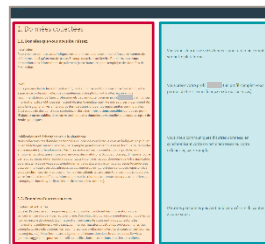


2

Communiquer à la fois de manière simple et complète

La Politique de confidentialité d'un acteur majeur des réseaux sociaux est scindée en 2 parties :

- La partie gauche contient l'intégralité des informations pertinentes et le **détail de la politique**
- La partie droite **synthétise les informations clés**



3

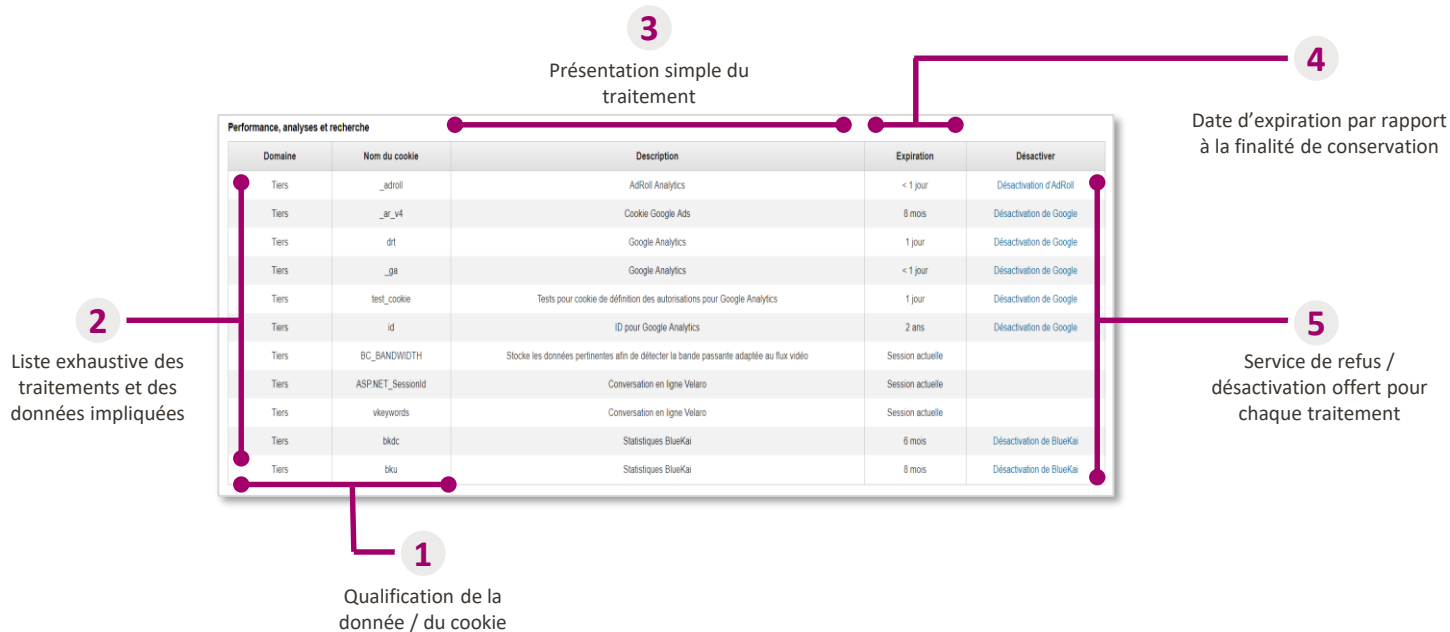
Développer du contenu dédié et pédagogique, sous des formats innovants

L'espace de confidentialité France Télévisions met à disposition de ses utilisateurs du **contenu vidéo illustrant la politique de gestion de données personnelles** du groupe



2. COMMUNIQUER EN TOUTE TRANSPARENCE SUR LES TRAITEMENTS, LEURS FINALITÉS, LEUR FONDEMENT JURIDIQUE & LES DURÉES DE CONSERVATION

Extrapoler ce que font certains acteurs vis-à-vis de leurs cookies sur la gestion des données à caractère personnel



3. METTRE À DISPOSITION DES UTILISATEURS DES SOLUTIONS SIMPLES DE GESTION DES DONNÉES, DANS LE PROLONGEMENT DE CE QUI EXISTE DÉJÀ CÔTÉ COOKIES

Les annonceurs ont adopté 3 approches distinctes afin de permettre à leurs utilisateurs de gérer efficacement les cookies :

Module tiers « externalisé »

Le site de l'annonceur intègre un lien qui renvoie vers un module tiers de gestion des données détaillant pour chacun le nom, la finalité et le statut d'accord avec la possibilité d'opt-out

Forces :

- Simplicité de mise en place

Limites :

- Faible intégration avec le site de l'annonceur
- Complexité de gestion pour l'utilisateur avec potentiellement plusieurs dizaines de données répertoriées (non nécessairement pertinentes à l'échelle de l'annonceur)

Accepter ou refuser les sociétés une par une

Société	Activé / Désactivé	Statut	Indice
1plusX	edg	Actif	1
33Across	edg	Actif	1
4W MARKETPLACE SRL	edg	Actif	1
Accordant Media	edg	Actif	1
Acxiom	edg	Actif	1
ad4mat	edg	Actif	1
ADARA	edg	Actif	1
Adrain LTD	edg	Actif	1
Addien+	edg	Actif	1
AddThis (formerly Clearspring)	edg	Actif	1
ADEX	edg	Actif	1
Adform	edg	Actif	1
ADITION	edg	Actif	1

Accepter toutes les sociétés

Refuser toutes les sociétés

Module de gestion des cookies proposé par Your on line Choices

Module tiers « intégré »

Le site de l'annonceur intègre un module de gestion des données détaillant pour chacun le nom, la finalité et le statut d'accord avec la possibilité d'opt-out

Forces :

- Simplicité de mise en place
- Bonne intégration avec le site de l'annonceur

Limites :

- Faible ergonomie et répétitivité pour chaque annonceur

Outil de gestion des cookies

Les sociétés stockant ou pouvant voir des données via ce site sont :

Nom	But Du Cookie	Statut D'Accord
Essentiel		
Publicitaires		
Analytique Et Personnalisation		
Utilitaires	Non divulgué	aller au site
Ad Target	Non divulgué	aller au site
Adxela Analytics	Servent publicitaires, ciblage publicitaires, personnalisation	aller au site

Appliquer les modifications Fermer

Module de gestion des cookies d'un retailer Français par Evidon



Module « sur mesure »

Les données sont regroupées par type de traitement / durée de conservation et l'utilisateur peut gérer les données à cette granularité

Forces :

- Simplicité d'utilisation et transparence vis-à-vis de l'utilisateur

Limites :

- Complexité de mise en place avec des développements sur mesure

Gestion des cookies

Lorsque vous naviguez sur notre site internet, des informations sont susceptibles d'être enregistrées, ou lues, dans votre terminal, sous réserve de vos choix. Par défaut, vos cookies sont activés.

- ☐ Acceptez-vous le dépôt et la lecture de cookies afin que nous et nos partenaires puissions analyser vos centres d'intérêts pour vous proposer des publicités personnalisées ?
- ☐ Acceptez-vous le dépôt et la lecture de cookies afin d'analyser votre navigation et nous permettre de mesurer l'audience de notre site internet ?
- ☐ Acceptez-vous le dépôt et la lecture de cookies pour vous permettre de partager des contenus de notre site avec d'autres personnes ou de faire connaître à ces autres personnes votre consultation ou votre opinion (boutons "J'aime" de Facebook par exemple) ?

Appliquer les modifications

Module de gestion des cookies d'un fournisseur d'énergie Français





POUR ALLER PLUS LOIN

TOUTES LES ACTIONS RGPD À
METTRE EN PLACE AU SEIN DE
SON ENTITÉ

ZOOM SUR LES NOUVEAUX PRINCIPES DE LA RÉGLEMENTATION RGPD

New ! Accountability	▪ Responsabilisation des organismes de traitement : les responsables de traitement devront être en mesure de démontrer à leur autorité de contrôle qu'ils se conforment à leurs obligations en matière de protection des données personnelles et mener des Privacy Impact Assessment (PIA) sur les traitements critiques
Consentement	▪ Consentement aux traitements : les entreprises devront collecter et tracer les consentements libres, spécifiques, éclairés et univoques prouvant que les personnes ont accepté par un acte positif clair que leurs données fassent l'objet d'un traitement
Gestion de crise	▪ Notification des violations : en cas de violation, la notification devra être effectuée auprès de la CNIL dans un délai de 72 heures au plus tard après la prise de connaissance de la violation. La CNIL pourra alors demander au responsable de traitement de prévenir les personnes concernées
Le rôle du Data Protection Officer	▪ Data Protection Officer : nommé pour les entreprises dont l'activité consiste intrinsèquement à traiter des données personnelles (ex : assureur...) ou qui traitent un volume de données personnelles à l'échelle régionale ou supérieure ▪ Le DPO aura pour mission principale d'informer et de délivrer des conseils dans le cadre de la mise en œuvre des traitements ▪ En dernier lieu, le DPO sera le point de contact avec l'autorité de contrôle avec laquelle il devra collaborer
Encadrement de la sous-traitance	▪ Contrôle des sous-traitants : les sous-traitants hors UE, traitant des données de ressortissants européens devront désigner un représentant au sein de l'UE ▪ Les sous-traitants devront désormais tenir un registre des traitements mis en œuvre pour le compte du responsable de traitement ▪ Les obligations contractuelles sont renforcées
Consécration de nouveaux droits	▪ Droit à la portabilité des données : les personnes pourront récupérer les données qu'elles ont communiquées ou en demander la transmission à un autre prestataire de service par exemple via des API ▪ Droit à la limitation du traitement de données personnelles ▪ Droit à l'oubli numérique : sur demande, après retrait du consentement, données non utiles pour le traitement...

4 DÉFINITIONS CLÉS À RETENIR ET LEUR ILLUSTRATION DANS UN CONTEXTE MARKETING

Rappel : Art. 4.1.

Données à caractère personnel

Toute information se rapportant à une **personne physique identifiée ou identifiable** [...]

Est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, **directement ou indirectement**, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale

Exemples marketing :

Ex 1 : Données **CRM** (nom, prénom, date de naissance, données de contact, adresse, données sociodémographiques...) et **transactionnelles** (historique d'achat)

Ex 2 : Données **comportementales web** et clé de matching avec le fichier clients (id client unique...)

Rappel : Art. 4.2.

Traitement

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et **appliquées à des données ou des ensembles de données à caractère personnel**, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction

Exemples marketing :

Ex 1 : La **collecte** des données comportementales on-site (rattachées à un id client) avec un outil d'Analytics puis l'**hébergement** et l'**analyse** dans un DataLake constituent a minima 3 traitements

Ex 2 : L'historisation et l'archivage des dossiers clients papier

Rappel : Art. 4.4.

Profilage

Toute forme de **traitement automatisé de données à caractère personnel** consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour **analyser ou prédire** des éléments concernant le rendement au travail, la situation économique, la santé, **les préférences personnelles, les intérêts**, la fiabilité, **le comportement**, la localisation ou les déplacements de cette personne physique

Exemples marketing :

Ex 1 : L'analyse des données comportementales et **le calcul de scores d'appétences/de chaleur dans les outils de marketing automation**

Ex 2 : Le calcul de **probabilité de conversion ou de churn** par les data scientists

Rappel : Art. 4.5.

Pseudonymisation

Le traitement de données à caractère personnel de telle façon que celles-ci **ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires**, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable

Exemples marketing :

Ex 1 : Données comportementales uniquement rattachées à un id cookie

Ex 2 : Données calculées (score d'appétence, score de pression marketing...) uniquement rattachées à un id client et non stockées dans l'outil CRM

MERCI DE VOTRE ATTENTION

JORDAN CHARLET – DIGITAL DESIGN & ECOSYSTÈME CLIENT - SNCF

Email : jordan.charlet@sncf.fr

Tel : [+33 \(0\)6 09 05 20 87](tel:+33(0)609052087)

CONSULTANTS EXTERNES :

ALEXANDRE CHIRAKHI – CONSULTANT DIGITAL & DATA - CONVERTEO

Email : ac@converteo.com

Tel : [+33 \(0\)6 84123053](tel:+33(0)684123053)

CHARLOTTE POULAIN – CONSULTANT SENIOR DIGITAL & DATA - CONVERTEO

Email : cp@converteo.com

Tel : [+33 \(0\)6 84 16 06 568](tel:+33(0)6841606568)