RGPD

Mise en conformité de votre site E commerce : suivez le guide

Synolia

RGPD

Mise en conformité de votre site E commerce : suivez le guide

SOMMAIRE

Synolia

Dring Dring ! Ça y-est, l'heure de l'entrée en vigueur du RGPD a sonné. Vous n'êtes pas tout à fait au point ? Pas de panique, nous sommes là pour vous aider à dédramatiser. Il est en effet inutile de frémir : derrière son allure de Grand Méchant Loup, le RGPD constitue en réalité une véritable opportunité pour vos stratégies marketing et commerciales.

Oui, redonner à vos prospects et clients le contrôle sur l'usage de leurs données personnelles vous est désormais imposé.
Non, ceci n'implique pas que des contraintes mais bien des bénéfices : affinage de vos campagnes, meilleure image, consolidation de la confiance que vous accordent vos clients...

Synolia propose de vous accompagner dans cette démarche. Pour commencer, le récapitulatif ci-après devrait vous aider à y voir un peu plus clair...

Malgré des heures et des heures de lecture sur le RGPD, vous ne savez toujours pas si votre site est conforme ou ce que vous devez changer pour vous adapter à la nouvelle réglementation ? Ce récapitulatif est pour vous !

Synolia a analysé pour vous le RGPD afin de vous donner les clés pour mieux appréhender les points d'attention sur une plateforme E-commerce. Notre objectif ? Faciliter votre mise en conformité RGPD en mettant à votre disposition :

- ☐ **Une application des principes RGPD au secteur E-commerce**
- ☐ **Une segmentation par fonctionnalité**
- ☐ **Des informations complémentaires sur les outils à votre disposition**
- ☐ **Des exemples à suivre**
- ☐ **Une distinction précise entre les éléments obligatoires et recommandés**

CGV ET POLITIQUE DE CONFIDENTIALITÉ

Ce qui est obligatoire

☐ Inclure les aspects relatifs aux données personnelles dans les CGV ou une page dédiée (exemple : une page politique de confidentialité)

☐ Permettre de valider explicitement les CGV au moment du paiement (exemple : via une case à cocher)

☐ Informer vos clients par email de la mise à jour des CGV suite à l'entrée en vigueur de la RGPD

Exemple de communication

Cher(e) client(e),

Assurer la sécurité de vos données est très important pour nous. Nous avons donc mis à jour notre **Politique de Confidentialité** selon le nouveau Règlement Général sur la Protection des Données (RGPD).

Ce qui change:
Plus de transparence:
Nous sommes capables de vous montrer comment, quand et dans quelle mesure nous traitons vos données et nous vous garantissons une totale transparence de celles-ci.

Plus facile d'utilisation:
Pour que notre politique soit encore plus compréhensible, nous l'avons mise à jour en utilisant un langage encore plus clair et intelligible.

Vous pouvez dès aujourd'hui consulter notre nouvelle **Politique de Confidentialité**. La nouvelle déclaration sur la protection des données sera applicable à partir du 25 mai 2018 et viendra remplacer la précédente.

Lorsque vous vous rendrez sur notre site web après le 25 mai 2018, vous accepterez automatiquement les mises à jour.

Si vous avez la moindre question à ce sujet, nous serons ravis d'y répondre.

Note : les restaurants livrent selon des zones géographiques limitées.
Plus de restaurants sur www.foodora.fr

Complément d'information

Exemples de Politique de confidentialité :

https://www.zalando.fr/zalando-protection-donnees/
https://www.apple.com/legal/privacy/fr-ww/
https://www.bose.fr/fr_fr/legal/privacy_policy.html

BANDEAUX COOKIES AVEC COLLECTE DE DONNÉES PERSONNELLES

Ce qui est obligatoire

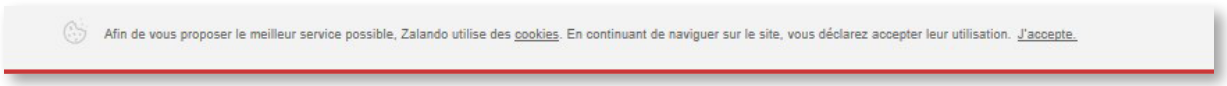
☐ **Afficher un bandeau cookie au moment de la première connexion**

☐ **Demander l'autorisation pour la collecte des données personnelles**

☐ **L'acceptation doit se faire par une action de la forme d'un opt-in de la part de l'utilisateur : case à cocher ou bouton « j'accepte »**

☐ **Communiquer sur la finalité des données récoltées**

→ Au sein même du bandeau cookies
(ex : « à des fins d'optimisation de votre parcours client »),
→ Dans la Politique de confidentialité, le plus explicitement possible
(ex : https://www.zalando.fr/zalando-protection-donnees/)



☐ **Indiquer la durée de validité du consentement à l'utilisateur.**

→ Soit au moment de l'acceptation
→ Soit dans les CGV ou dans la Politique de confidentialité

☐ **Communiquer à l'utilisateur la marche à suivre pour qu'il puisse retirer son consentement**

→ Dans les CGV ou dans la Politique de confidentialité
→ Exemple de marche à suivre :
https://www.bose.fr/fr_fr/legal/cookie_policy.html

Complément d'information

Il n'y a pas besoin d'historiser le consentement de l'utilisateur pour ce cas de figure, puisque le cookie lui-même a une durée de vie. Légalement, sa durée de conservation maximum est de 13 mois.

De nombreux sites embarquent des fonctionnalités déposant des cookies avec collecte de données personnelles (publicités, affiliation, tracking analytics, boutons réseaux sociaux etc.). Afin d'en simplifier la gestion, il existe des solutions centralisées de recueil de consentement aux cookies approuvés et disponibles sur le site de la CNIL : https://www.cnil.fr/fr/solutions-centralisees-de-recueil-de-consentement-aux-cookies-les-gestionnaires-de-tag

exemple : tarteaucitron.js - Source CNIL

Code pour paramétrer le bandeau tarteaucitron.js

```
<head>
<script type="text/javascript" src="/tarteaucitron/tarteaucitron.js"></script>
<script type="text/javascript">
 tarteaucitron.init({
"hashtag": "#tarteaucitron", /* Ouverture automatique du panel avec le hashtag */
"highPrivacy": false, /* mettre à true désactive le consentement implicite */
"orientation": "top", /* le bandeau doit être en haut (top) ou en bas (bottom) ? */
"adblocker": false, /* Afficher un message si un adblocker est détecté */
"showAlertSmall": true, /* afficher le petit bandeau en bas à droite ? */
"cookieslist": true, /* Afficher la liste des cookies installés ? */
"removeCredit": false /* supprimer le lien vers la source ? */ }) ;
</script>
</head>
```

Exemples de cookies couramment déposés sur des sites E-commerce : Criteo, facebook, twitter...

Il convient de distinguer ces cookies de collecte de données personnelles des cookies “standard” d’une solution E-commerce (Magento, PrestaShop). Dans ce dernier cas le recueil de consentement peut se faire avec un bandeau d’information dans la mesure où ceux-ci ne collectent pas de données personnelles. Leur acceptation peut être tacite si l’internaute poursuit la navigation sur le site.

FORMULAIRE DE CONTACT

Ce qui est obligatoire

☐ **Accompagner le formulaire de contact d'une mention de type :**
« Les informations mentionnées dans ce formulaire ne pourront être utilisées que conformément à la loi informatique et liberté 78-17 du 06/01/78. Vous disposez d'un droit d'accès et de modification et/ou suppression de ces données »
Exemple : https://www.cnil.fr/webform/nous-contacter

Vous pouvez mettre à jour la mention pour faire référence au Règlement Général Protection Données

☐ **Indiquer que la collecte des données sert uniquement à pouvoir répondre à la demande**

GESTION DES INSCRITS À UNE NEWSLETTER

Ce qui est obligatoire

☐ **Préciser la finalité de la newsletter (envoi d'offres promotionnelles, actualités etc.)**

☐ **L'inscription doit faire l'objet d'un opt-in explicite :**

→ Pas de case pré-cochée

→ Pas de négation dans la formulation : « ne pas s'inscrire »

→ Pas d'inscription induite par une action tierce.

Exemple : à la création de compte, « en créant votre compte, vous acceptez d'être inscrit à la newsletter ».

☐ **Historiser le consentement : vous devez garder une trace de la date d'inscription**

☐ **Recueillir de nouveau le consentement ou supprimer de la base un abonné si ce dernier n'a pas manifesté d'intérêt positif depuis plus de 36 mois :**

→ Un clic sur un lien présent dans la newsletter est considéré comme un intérêt positif (contrairement à l'ouverture seule d'une newsletter dans sa boîte mail).

→ Pour renouveler un opt-in, vous pouvez envoyer un email type :

« Cela fait longtemps que nous n'avons pas été en contact, êtes-vous toujours intéressé par nos offres...

☐ **Proposer un lien de désinscription fonctionnel à l'utilisateur pour qu'il puisse révoquer son consentement à tout moment.**

→ Prendre en compte le désabonnement sous un délai de 30 jours.

En cas de dépassement, il est nécessaire d'en informer l'utilisateur et de préciser les raisons justifiant un délai supplémentaire.

→ Rappeler la marche à suivre pour se désabonner dans les CGV ou dans la Politique de confidentialité.

Ce qui relève de la best practice

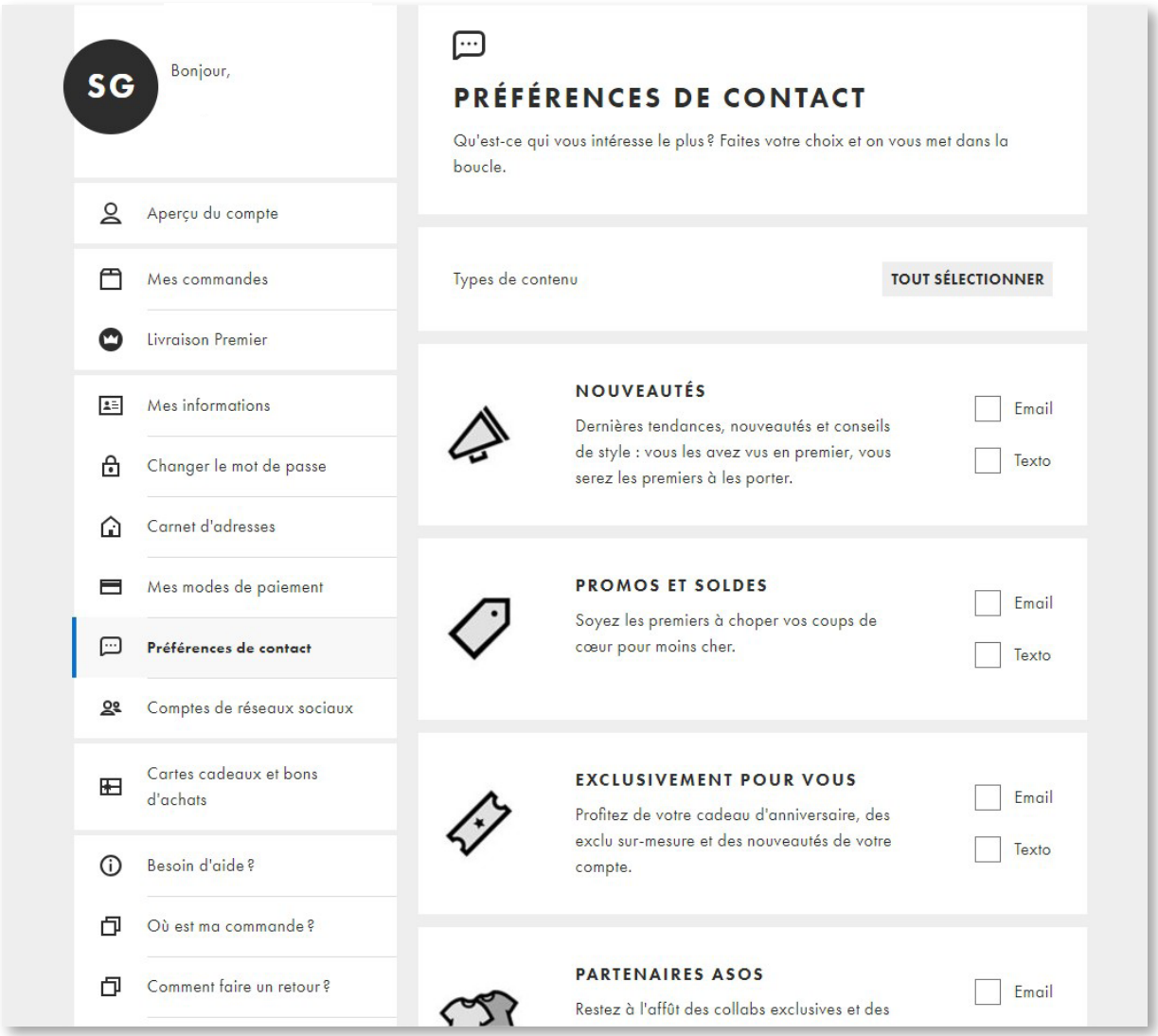
☐ **Mettre en place un double opt-in en demandant la confirmation de l'inscription par email**

☐ **Distinguer les consentements en fonction du traitement qu'implique cette inscription**

→ Par type de communication : une newsletter actualité marque, une newsletter offres partenaires, une newsletter promotions ou bons plans etc.

→ Par canal de communication : courrier, email, SMS.

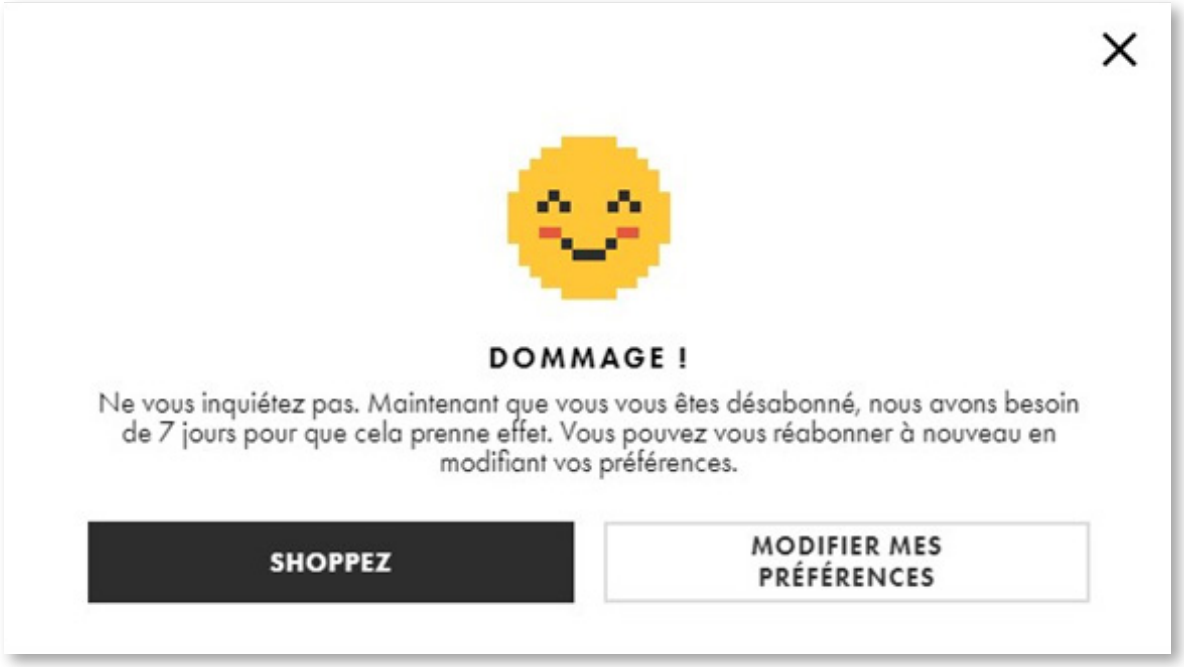
Exemple à suivre, Asos



☐ **Préciser si un délai de prise en compte est nécessaire avant la désinscription effective.**

Exemple : « les changements peuvent prendre jusqu'à X jours pour être pris en compte ».

Exemple à suivre, Asos



Complément d'information

Base existante : il est recommandé de procéder à un nettoyage de votre base afin de supprimer les abonnés qui n'auraient pas manifesté d'intérêt positif (pas de clic sur un lien présent dans la newsletter) depuis plus de 36 mois.

Alternativement, il est également possible de demander à vos inscrits un renouvellement de l'opt-in avant de les supprimer.

Exemple


asos
Mettez à jour avant le 25 mai ou vous risquez de manquer
Les exclusivités et offres ASOS
METTRE À JOUR ›
OOJOURS OO.OO.OO
Vous êtes probablement au courant, mais nous modifions nos règles de confidentialité. Ce qui signifie que si vous ne mettez pas à jour vos préférences, vous ne recevrez plus nos alertes promos, dernières tendances et toutes nos exclusivités à ne pas manquer. Pour continuer à recevoir de nos nouvelles, mettez à jour vos préférences contact dès maintenant.
J'APPROUVE ›
CHANGEZ MES PRÉFÉRENCES ›
DÉSABONNEZ-MOI ›

CRÉATION D'UN COMPTE CLIENT

Ce qui est obligatoire

☐ **Limiter la collecte de données personnelles au nécessaire pour votre activité**

☐ **Distinguer les champs facultatifs des champs obligatoires (* ou mention facultatif/obligatoire)**

☐ **Préciser la finalité de(s) traitement(s).**

Exemples :

→ Date de naissance : « Nous pourrons vous envoyer des offres anniversaire »

→ Date de naissance : « Nous souhaitons nous assurer que vous avez plus de 16 ans »

☐ **Restreindre la collecte de données personnelles en fonction de l'âge de l'utilisateur :**

→ Mineur de moins de 13 ans : la récolte de données personnelles est strictement interdite

→ Mineur de moins de 16 ans : la récolte de données personnelles est autorisée sous réserve d'un accord parental.

☐ **Proposer un lien vers la page acceptation de la « Politique de confidentialité »**

☐ **Veiller à ce que les mots de passe client ne soient pas stockés en clair dans la base.**

→ Ils ne sont donc pas visibles depuis le back-office

→ Ils ne sont donc pas envoyés par mail en cas de mot de passe oublié, mais sous forme de lien de réinitialisation du mot de passe.

Ce qui relève de la best practice

☐ **Vérifier si l'utilisateur est majeur : il est préférable d'utiliser une case à cocher de type « je certifie avoir plus de 16 ans » plutôt que de faire une vérification sur une date de naissance.**

☐ **Éviter les informations sous forme d'info-bulles, qui vont manquer de visibilité pour l'utilisateur.**

☐ **Nettoyer la base clients afin de ne pas conserver des données personnelles plus longtemps que nécessaire.**

→ Un compte sans commande est considéré comme un prospect, il est recommandé de supprimer les données personnelles le concernant après 36 mois d'inactivité

→ Un compte avec commande est un client, il est recommandé de ne pas conserver les données du client si celui-ci ne s'est pas connecté depuis 36 mois.

→ Il peut exister des contraintes annexes, qui peuvent justifier une durée de conservation plus longue (la durée de garantie des produits, le secteur...)

Complément d'information : exemples de best practice

Cas 1 : Un E-commerçant qui vend des chaussures peut demander de renseigner la taille ou le genre. Ce ne sont pas des données personnelles, il n'y a pas de restriction.

Cas 2 : Un E-commerçant qui vend des chaussures peut demander la date de naissance pour envoyer par exemple une offre anniversaire. Il faudra alors qu'il précise la finalité du traitement (envoyer des offres « Anniversaire ») au moment de la récolte de la donnée.

Cas 3 : Un E-commerçant qui vend des vêtements enfant souhaite récolter des informations sur les enfants d'un client à des fins marketing :

Il est préférable de demander l'âge et non la date de naissance des enfants de moins de 13 ans.

☐ **Le E-commerçant doit préciser la finalité de traitement : exemple : envoyer des offres adaptées à l'âge**

☐ **Le nom & prénom n'apporte aucune valeur ajoutée : ils ne doivent pas être demandés**

☐ **Le genre peut être demandé car il ne permet pas d'identifier directement un individu**

Cas 4 : Un E-commerçant qui vend de la lingerie n'a pas nécessairement besoin à la création de compte de demander une adresse postale. Cet élément peut être renseigné par la suite dans le cas d'une commande.

Ressources complémentaires

https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

https://www.cnil.fr/fr/limiter-la-conservation-des-donnees

COMPTE CLIENT

Ce qui est obligatoire

Permettre au client de :

☐ **Demander la portabilité de ses informations personnelles :**

→ Soit depuis son compte client (exemple : télécharger une archive)

→ Soit avoir la possibilité de faire une demande depuis le formulaire de contact ou via une adresse email dédiée (ex : mesdonneesperso@monsite.com)

→ L'export des données doit se faire dans un format facile à utiliser afin de permettre un traitement (CSV, XML etc.)

☐ **Consulter et modifier ses informations personnelles :**

→ Soit depuis son compte client

→ Soit avoir la possibilité de faire une demande depuis le formulaire de contact ou via une adresse email dédiée (exemple : mesdonneesperso@monsite.com)

☐ **Supprimer son compte et l'ensemble des informations personnelles le concernant**

→ Soit depuis son compte client
(exemple : depuis un bouton « supprimer mon compte »)

→ Soit avoir la possibilité d'en faire la demande depuis le formulaire de contact ou via une adresse email dédiée (exemple : mesdonneesperso@monsite.com)

→ Il ne sera plus possible d'effectuer de traitements sur ces données (marketing, profiling...)

Les modifications et suppressions doivent être répercutées partout où les données sont présentes (archives, bases, solutions tierces interconnectées...)

Ce qui relève de la Best practice

☐ **Ne pas enregistrer les données bancaires.**

☐ **Dans le cas contraire s'assurer :**

→ D'avoir demandé le consentement explicite

→ D'être en mesure d'assurer la sécurisation du stockage des données

Complément d'information

En dépit de l'obligation de supprimer les données personnelles lorsque l'utilisateur en fait la demande, il est à noter que le cadre juridique en France impose de conserver les pièces comptables (factures, commandes) pendant une durée de 10 ans minimum.

Certains éditeurs ont anticipé le travail de mise en conformité par l'intermédiaire de modules disponibles sur les marketplaces des solutions. Exemple module PrestaShop : https://addons.prestashop.com/fr/legislation-loi-hamon/28991-gdpr-suite.html

SÉCURISER LES DONNÉES PERSONNELLES DE VOS UTILISATEURS

Ce qui est obligatoire

☐ **Cartographier précisément les flux de données personnelles (type de données, lieux de stockage, transfert, synchronisation)**

☐ **Limiter en interne et en externe l'accès aux données personnelles (dans les bases de données) uniquement aux personnes légitimes**

☐ **Limiter le transfert des données personnelles vers des solutions tierces (Éditeur de modules, Agences, Marketplaces, Prestataires...**

→ Limiter le transfert de données personnelles au strict nécessaire

→ Anonymiser les données qui peuvent l'être

☐ **Veiller à ce que vos partenaires (solutions tierces, consultants, freelance...) soient bien en conformité avec le RGPD**

☐ **Activer le protocole https sur les écrans comportant des données personnelles**

☐ **Créer des accès individuels pour les solutions manipulées si ces outils permettent d'accéder ou de modifier des données personnelles (CMS E-commerce, ERP, CRM etc.)**

☐ **Si malgré tout, des données personnelles constituant un risque au regard de la vie privée des personnes concernées viennent à fuiter, il est nécessaire de :**

→ Prévenir les personnes concernées sous un délai de 72h

→ Avertir la CNIL : https://notifications.cnil.fr/notifications/index

Ce qui relève de la Best practice

☐ **Limiter les droits en créant des rôles précis par métier (Admin, Marketing, Service Client, prestataire etc.)**

☐ **Sécuriser les mots de passe des utilisateurs :**

→ Administrateurs

→ Utilisateurs : voir les recommandations de la CNIL (https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires)

☐ **Verrouiller les sessions sur les postes**

☐ **Appliquer régulièrement les patchs de sécurité de l'éditeur des solutions techniques utilisées (Ex : Magento, PrestaShop...)**

☐ **Penser les développements dans une logique privacy par design, privacy by default.**

→ Exemples : Mise en place de logs

- Éviter d'inclure des données personnelles dans des logs (privacy by design)
- Être en mesure de nettoyer les logs des données personnelles

HÉBERGEMENT ET TRANSFERT

S'assurer que la gestion des données personnelles d'utilisateurs Européens se fasse dans des conditions respectant le RGPD. Le transfert de ces données est possible si celui-ci est fait vers :

☐ **Un autre pays Européen (UE)**

☐ **Un pays disposant d'accords spécifiques avec l'UE sur la question des données personnelles:**

→ Liste des pays compatibles : https://linc.cnil.fr/fr/la-protection-des-donnees-dans-le-monde.

→ Si un pays n'est pas sur la liste, il faut l'accord explicite de la personne dont on récolte les informations personnelles.

Complément d'information

Cas 1 : Il est possible pour un site E-commerce américain certifié Privacy Shield de livrer en France et de stocker sur le sol américain des données personnelles d'utilisateurs français. Le site doit toutefois le préciser et respecter le RGPD.

Cas 2 : Dans le cas d'un E-commerçant qui sous-traite son service client à une société localisée dans un pays étranger qui n'a pas d'accord ou qui n'a pas encore d'accord avec l'Union Européenne sur la régulation des données personnelles :

☐ **Il est autorisé d'ouvrir l'accès aux données personnelles (hébergées en Europe ou dans un pays avec un accord avec l'Europe) à ce service client situé à l'étranger. Il ne s'agit pas ici de transfert de données hors de l'Europe, mais d'accès à des données.**

☐ **Il reste néanmoins nécessaire de garantir contractuellement que le sous-traitant est en conformité avec le RGPD et que le contrat mentionne bien les traitements qui sont confiés au sous-traitant.**

Maintenant que vous connaissez tout le spectre d'ajustements qu'induit l'entrée en vigueur du RGPD, il vous reste à respirer profondément et... à vous lancer ! Pour tout renseignement complémentaire, n'hésitez pas à nous contacter.

Contact
Lyon - Paris - Bordeaux

Adresse siège : 59 rue de l'Abondance 69003 Lyon

Tél. : 04 27 70 53 70

Email : contact@synolia.com

Suivez nos actualités

Site web : www.synolia.com
Twitter : @Synolia
LinkedIn : @Synolia