



# FAQ sur le Règlement général sur la protection des données (RGPD)



## 1. Quand le RGPD entrera-t-il en vigueur ?

Le RGPD est en vigueur depuis le 25 mai 2016. Il sera applicable à partir du 25 mai 2018.

## 2. Y a-t-il une période de transition ?

Nous sommes déjà dans la phase de transition. C'est pourquoi les e-commerçants doivent dès à présent prendre les mesures nécessaires pour respecter le RGPD afin d'être prêts lorsque le règlement prendra effet le 25 mai.

## 3. Est-ce que la réglementation en vigueur va subir d'importants changements ?

Non, les principes de base qui sont déjà énoncés à travers la directive 95/46/CE se retrouvent dans le RGPD. Il s'agit par exemple du principe de minimisation des données ou de leur affectation à un but précis. Aujourd'hui viennent s'y ajouter de nouveaux principes comme la protection des données par défaut (« privacy by default ») et la protection de la vie privée dès la conception (« privacy by design »).

## 4. Concrètement, qu'est-ce qui change pour les e-commerçants ?

L'un des principaux changements réside dans la mise en place du principe de responsabilité : celui-ci oblige les entreprises à prouver qu'elles respectent le RGPD. Ceci implique une augmentation des obligations en termes de documentation et de preuves : il faut tenir un répertoire des activités de traitement, effectuer des analyses d'impact de la protection des données et consigner les incidents en matière de protection des données.

De plus, en cas de non-respect du règlement sur la protection des données, les risques encourus sont nettement plus importants : les infractions peuvent être punies d'une amende allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel total réalisé dans le monde.

D'autres modifications sont également à prendre en compte :

- ▶ Les obligations d'information envers les personnes concernées (par exemple la déclaration de protection des données) sont plus nombreuses,
- ▶ Le droit à la portabilité des données et les délais de traitement des demandes pour exercer les droits des personnes concernées doivent être respectés.
- ▶ L'utilisation de cookies et d'outils publicitaires devra généralement être justifiée par une mise en balance des intérêts – sous réserve d'une disposition contraire émanant du règlement ePrivacy à venir ;
- ▶ Les contrats avec des sous-traitants doivent respecter des exigences plus strictes.



## **5. Quelles modifications les e-commerçants doivent-ils effectuer, et à quel endroit ?**

Les e-commerçants doivent effectuer les modifications suivantes :

- ▶ Les processus impliquant le traitement de données personnelles doivent être consignés dans un répertoire recensant ces activités
- ▶ La déclaration de protection des données doit être mise à jour
- ▶ Les déclarations de consentement autorisées jusqu'à présent par le droit français restent valides dans la mesure où elles respectent les nouvelles exigences plus strictes en matière de consentement volontaire. Dans le cas contraire, les personnes devront donner à nouveau leur consentement, conformément aux nouvelles exigences.
- ▶ Les contrats de sous-traitance doivent être vérifiés et, le cas échéant, retravaillés ;
- ▶ Les e-commerçants doivent analyser l'impact de la protection des données lorsque le responsable traite des données présentant un risque élevé pour les droits et les libertés des personnes concernées
- ▶ Les processus internes doivent être modifiés pour garantir les droits d'accès, de rectification, de suppression et d'opposition ainsi que le nouveau droit à la portabilité des données. À cet égard, les demandes des personnes concernées doivent généralement être traitées dans le délai d'un mois ;
- ▶ Un plan de réaction en cas de violations de données doit être mis en place afin de signaler tout incident aux autorités de surveillance dans les 72 heures qui suivent sa découverte.

## **6. Une boutique en ligne porte la marque de confiance Trusted Shops : cela signifie-t-il qu'elle remplit dès aujourd'hui les critères du RGPD ?**

Non, car les exigences du RGPD ne sont pas toutes contrôlées dans le cadre de l'attribution de la marque de confiance. Ainsi, l'examen ayant lieu dans ce cadre n'implique pas de vérification des documents internes comme la liste de processus.

## **7. La marque de confiance peut-elle être retirée si la boutique en ligne n'a pas effectué les modifications à la date limite ?**

La marque de confiance n'est pas automatiquement supprimée. Nous recommandons toutefois de préparer les modifications en amont afin de pouvoir les appliquer directement dans la boutique le jour de la mise en application du RGPD.

Veuillez noter que même après avoir été vérifiée par Trusted Shops, votre boutique doit toujours respecter les dernières conditions-cadres juridiques ainsi que les lignes directrices du programme TS.

## **8. La boutique en ligne doit-elle nommer un délégué à la protection des données ?**

L'art. 37 al. 1 c du RGPD dispose que les e-commerçants doivent nommer un délégué à la protection des données si leur activité principale consiste à traiter intégralement certaines catégories de données. En dehors de ces cas limitativement énumérés, la désignation d'un délégué à la protection des données est recommandée mais non obligatoire.



## **9. Dans quelle mesure un e-commerçant doit-il être vigilant concernant l'activité de de ses prestataires (outil d'envoi de newsletter, solution e-commerce, prestataires de paiement, outils de suivi...) ?**

Les prestataires doivent fournir suffisamment de garanties indiquant qu'ils respectent le RGPD à l'aide de mesures techniques et structurelles appropriées.

Si vous trouvez un prestataire adapté, vous devez conclure avec lui un contrat de sous-traitance qui remplisse les exigences de l'art. 28 al. 3 du RGPD.

## **10. Quelles questions l'e-commerçant doit-il poser à ses prestataires ?**

L'e-commerçant doit découvrir si le prestataire garantit suffisamment le respect des exigences du RGPD. La distinction par une certification relative à la protection des données est un indicateur important qui signale qu'un prestataire respecte les exigences du RGPD.

De plus, vous devez vous assurer de conclure avec le prestataire un contrat de sous-traitance qui contienne les informations obligatoires mentionnées au sein de l'art. 28 al. 3 du RGPD. Par exemple, le contrat de sous-traitance doit mentionner si, et dans quelles conditions, il est possible de faire appel à des sous-traitants.

Il convient également de vérifier s'il y a une transmission de données personnelles dans des États non membres de l'Union européenne : les données restent-elles dans l'UE ou sont-elles transmises dans un ou plusieurs États étrangers ? Pour les transmissions de données internationales, vous devez vérifier la présence de garanties pour assurer un niveau de protection des données adapté.

## **11. Comment une boutique en ligne peut-elle savoir si sa déclaration de protection des données est suffisante ?**

En premier lieu, vous devez procéder à un examen des traitements de données actuellement réalisés dans votre boutique en ligne (outils de suivi, newsletters, contrôle de solvabilité, transmission de données à des tiers). La déclaration de protection des données doit informer de ces traitements de données. Les indications obligatoires concernant ces traitements, et devant être mentionnées dans la déclaration de protection des données, sont les suivantes :

- ▶ Nom et coordonnées du responsable et, le cas échéant, du délégué à la protection des données
- ▶ Bases juridiques envisagées
- ▶ Intérêts justifiés de la personne responsable
- ▶ Destinataire des données ou catégories de destinataires des données
- ▶ Informations relatives à la transmission dans des pays étrangers
- ▶ Délais de suppression ou critères pour leur détermination
- ▶ Informations sur les droits d'accès, de modification, de blocage, de suppression, d'opposition et de portabilité des données
- ▶ Droit de porter plainte auprès des autorités de surveillance
- ▶ Information sur le droit de retrait des consentements accordés à tout moment
- ▶ Pour les processus décisionnels automatisés, y compris le profiling, la logique appliquée ainsi que l'ampleur et les effets escomptés du traitement



- ▶ Si les données ne sont pas recueillies auprès de la personne concernée (par exemple à partir d'une source publique), la provenance des données.

## **12. Le scoring est-il encore autorisé ?**

Le scoring reste autorisé sous certaines conditions. Les autorisations pour les e-commerçants restent les mêmes: le scoring ne peut avoir lieu qu'avec le consentement exprès de la personne concernée ou s'il est nécessaire à la conclusion ou à l'exécution du contrat. Enfin, on peut citer par exemple le cas où un client choisit de payer sur facture ou en plusieurs fois. La nouveauté est que la personne concernée doit être informée de la logique appliquée ainsi que de l'ampleur et des effets escomptés du traitement.

## **13. Comment seront appliquées les amendes dans la pratique ?**

L'art. 83 du RGPD prévoit des amendes nettement plus élevées que celles en vigueur actuellement. Ainsi, pour certaines infractions, les amendes peuvent atteindre 20 millions d'euros ou 4% du chiffre d'affaires annuel d'une entreprise. Il est difficile de savoir à l'avance dans quelle mesure les autorités de surveillance vont faire appliquer ces sanctions. Toutefois, il faut s'attendre à une hausse substantielle des amendes en cas de violation de la protection des données.

## **14. Les enfants bénéficient-ils de droits particuliers en matière de protection des données ?**

Les enfants doivent jouir d'une protection particulière ; le RGPD contient donc des dispositions spécifiques pour les enfants. Par exemple, le traitement des données personnelles d'enfants de moins de 16 ans n'est autorisé que si et dans la mesure où le tuteur légal de l'enfant a donné son consentement à cet égard.



# FAQ sur le Règlement général sur la protection des données et les produits Trusted Shops



## **1. Trusted Shops doit-il aussi s'adapter en matière de protection des données ? Si oui, de quelle façon ?**

Comme toutes les entreprises européennes, Trusted Shops s'efforce déjà d'appliquer les exigences du RGPD à ses propres activités. Ceci implique de retravailler le répertoire des traitements et d'autres documents, mais aussi de modifier les déclarations de protection des données sur nos pages Internet et de mettre à jour la formation de nos salariés par rapport au RGPD.

## **2. Trusted Shops propose-t-il de conclure un contrat de sous-traitance ?**

Avec le lancement du RGPD et en lien avec les modifications des exigences légales qui en découlent, Trusted Shops va proposer de conclure un contrat de sous-traitance avec les boutiques en ligne qui utilisent des produits Trusted Shops.

Nous sommes actuellement en train de créer une ébauche de modèle que nous allons mettre à la disposition des clients intéressés avant que le RGPD ne prenne effet. Merci de bien vouloir comprendre qu'au vu du nombre de ses clients, Trusted Shops ne peut pas proposer de contrôler et de valider toutes les ébauches de contrat de tous ses clients.

Bien entendu, le document proposé par Trusted Shops respectera les dispositions légales et tiendra compte des intérêts de nos clients.

## **3. Est-ce qu'un e-commerçant doit mentionner l'utilisation des produits Trusted Shops dans sa déclaration de protection des données ?**

Dans la mesure où le changement de la législation va aussi augmenter les obligations d'information des propriétaires de sites Internet, une boutique en ligne devra aussi indiquer dans sa déclaration de protection des données si elle transmet des données personnelles à Trusted Shops ou si elle autorise que Trusted Shops recueille de telles données sur le site de la boutique en ligne – après consentement de l'acheteur ou dans le cadre du contrat de sous-traitance avec Trusted Shops.

Les informations contenues dans la déclaration de protection des données doivent décrire la collecte et le traitement des données et indiquer les catégories de données qui sont collectées. L'e-commerçant doit alors évoquer explicitement Trusted Shops GmbH en tant que sous-traitant de la boutique en ligne. De plus, la déclaration de protection des données doit expliciter l'objet du traitement ainsi que les bases juridiques sur lesquelles repose le traitement. Si les données personnelles sont transmises à Trusted Shops sur la base d'un consentement, l'e-commerçant doit également informer du droit de rétractation, ou sinon du droit d'opposition.



## **4. Quelles sont les données collectées lors de l'utilisation des produits de Trusted Shops dans une boutique en ligne ?**

### **A. Une boutique en ligne qui utilise des produits de Trusted Shops en passant par l'API mise à disposition :**

Lorsqu'une boutique en ligne utilise des produits de Trusted Shops en passant par l'API de Trusted Shops, alors les paramètres individuels de l'API déterminent quelles données personnelles d'un acheteur sont transmises à Trusted Shops et à quel moment.

C'est pourquoi, il n'est pas possible d'indiquer, pour tous les cas, les données transmises entre la boutique en ligne et Trusted Shops dans le cadre de l'utilisation d'une API de Trusted Shops. Vous trouverez plus de détails sur les API mises à disposition par Trusted Shops sur [api.trustedshops.com](https://api.trustedshops.com).

Veuillez noter que la transmission des données personnelles d'acheteurs à Trusted Shops nécessite toujours le consentement préalable des personnes concernées même en cas d'utilisation d'une l'API, car il s'agit d'une transmission de données à des fins de marketing. La boutique en ligne a donc l'obligation d'obtenir au préalable le consentement nécessaire.

### **B. Une Boutique en ligne intégrant le Trustbadge :**

#### **a) Transmission de données lors de la visite d'une boutique en ligne intégrant le Trustbadge :**

De la même manière que lors de l'accès à une page internet, l'accès à un Trustbadge intégré à une boutique en ligne par le navigateur Web du client (et ainsi simultanément l'accès à la page de la boutique en ligne) entraîne automatiquement une inscription d'entrée du navigateur internet. Dès lors qu'il s'agit d'un format standard unique, les informations sur le navigateur Web du client qui y accède (date, heure, referrer, adresse IP du client, user-agent) y sont présentes. Il s'agit de données d'utilisation qui sont générées lors de chaque transfert de données sur Internet. Une telle transmission de données se produit en particulier pour chaque intégration de contenus tiers.

Trusted Shops n'établit aucun profil d'utilisation issu de ces données d'utilisation et ne fait aucune déduction sur les visiteurs des pages internet. Ces données sont exploitées dans le seul but de garantir un bon fonctionnement du système.

De surcroît, la seule consultation d'une page d'une boutique en ligne intégrant le Trustbadge n'entraîne aucune transmission et aucun enregistrement automatique de données personnelles (par exemple: nom, adresse email etc...).

#### **b) Transmission de données lors d'une commande sur une boutique en ligne :**

Dans le cas où l'acheteur n'utilise pas lui-même le produit de Trusted Shop, l'intégration du Trustbadge conduira seulement à transmettre le numéro de commande à Trusted Shops, afin de vérifier les garanties ou avis ultérieurs.



Les autres données, en particulier les données personnelles, ne seront transmises que si le client de la boutique utilise activement les produits Trusted Shops pour acheteurs et qu'il consent à une telle transmission de données ou si, dans le passé, il y a déjà consenti pour ses futurs achats.

Les seules données collectées sont celles nécessaires à minima à une utilisation de nos produits. En règle générale, ces données sont les suivantes pour l'utilisation de la "garantie Trusted Shops avec avis site": date de la commande, numéro de la commande, le cas échéant le numéro de client existant, le montant de la commande, la devise, le cas échéant la date de livraison attendue, le moyen de paiement et l'adresse email de l'acheteur. En cas d'intégration des avis clients par la boutique, les données supplémentaires collectées sont les suivantes: l'URL du produit et de son image, la description du produit, le SKU du produit, les GTIN et MPN, ainsi que le fabricant.

Seuls le numéro de commande et l'adresse email sont nécessaires dans le cas où un rappel à évaluation est envoyé sans la "garantie acheteur Trusted Shops". Trusted Shops ne reçoit pas d'autres données de l'utilisateur par ce biais.

Trusted Shops vérifie automatiquement si l'acheteur est déjà enregistré pour une utilisation du produit au moyen d'un paramètre neutre, l'adresse email hachée, qui a une fonction cryptologique unidirectionnelle (procédure MD 5). Avant sa transmission, l'adresse email sera convertie en une valeur hachée indéchiffrable pour Trusted Shops. Si aucune correspondance n'est trouvée, le paramètre est rejeté. L'adresse email sera seulement collectée si, par la suite, l'acheteur décide d'utiliser les produits Trusted Shops. Il n'y a pas de transmission automatique de l'adresse email en clair de l'acheteur ou d'autres données le concernant.

Les données reçues seront exclusivement utilisées pour le bon déroulement du contrat conclu et sauvegardées en interne pour la durée de l'exécution réciproque du contrat. Ensuite, les données seront verrouillées afin d'éviter toute autre utilisation et définitivement supprimées après l'écoulement de tous les délais légaux et fiscaux de conservation.

Dans le cas où l'acheteur n'utilise pas les produits Trusted Shops pour acheteurs et s'il quitte la page, les données ne seront ni transmises à Trusted Shops, ni sauvegardées ni traitées par Trusted Shops.



## 5. Quelles sont les conditions à respecter lors de l'envoi d'une invitation à évaluation?

### L'invitation à évaluation est de la publicité

Lors de l'envoi d'un email de rappel à évaluation, il convient de respecter les dispositions relatives au droit des données personnelles et au droit de la concurrence, puisqu'il s'agit d'une utilisation de données personnelles à des fins de publicité. Le rappel à évaluation envoyé est de la publicité.

Il existe de nombreuses décisions judiciaires (*en Allemagne: LG Hamburg, Urt. v. 30.6.2006 – 309 S 276/05 - Umfragen zu Marktforschungszwecken stellen Werbung dar; AG Hannover, Urt. v. 3.4.2013 – 550 C 13442/12 sowie AG Düsseldorf, Urt. v. 27.10.2014 – 20 C 6875/14 sowie LG Leipzig, Urt. v. 13.11.2015 – 02 HK O 888/15 - Feedbackanfragen sind Werbung; OLG Dresden, Urt. v. 24.04.2016 - Az.: 14 U 1773/13 - Kundenzufriedenheitsanfragen sind unerlaubte E-Mail-Werbung*) qui précisent qu'en matière de Feedback ou de demande d'évaluation, il s'agit de publicité au sens du § 7 Abs. 2 Nr. 3 de la loi allemande sur la répression de la concurrence déloyale. Ces actions "importunent" le plaignant de la même manière que toute autre publicité par email.

### L'obtention du consentement

C'est la raison pour laquelle l'envoi d'une demande d'évaluation nécessite toujours l'obtention préalable du consentement explicite du destinataire. La seule présence de l'adresse email dans la banque de données de la boutique en ligne ne suffit pas. Cette condition vaut également lorsque l'adresse est transmise à un tiers, afin que ce dernier envoie le rappel à évaluation. Ainsi, c'est par exemple le cas lors de l'utilisation du collecteur d'avis ou de la collecte automatique par Trusted Shops. Au sein des Conditions générales pour ses Membres, Trusted Shops oblige contractuellement le commerçant en ligne à recueillir les consentements appropriés et ce de manière opposable. Dans l'hypothèse où se produit une transmission sans recueil préalable des consentements, il s'agit alors non seulement d'une violation par le commerçant en ligne d'un engagement contractuel mais également, en cas de dommages, d'un motif de demande d'indemnisation au commerçant en ligne par Trusted Shops.

Au sens du § 7 Abs. 2 Nr. 3 de la loi allemande sur la répression de la concurrence déloyale et de l'article L34-5 du Code français des postes et de communications électroniques, il est nécessaire d'avoir une déclaration séparée de l'acheteur pour recueillir un consentement qui soit opposable. La déclaration de consentement ne doit pas être liée à d'autres déclarations. Par ailleurs, il est nécessaire que le client effectue une action et ce uniquement par le biais d'une case à cocher, d'un clic sur un bouton séparé portant accord à recevoir un rappel à évaluation ou du remplissage d'un espace dédié à l'inscription au rappel à évaluation.



## **Etendue et portée**

L'étendue et la portée du consentement doivent être explicites: quelles données vont être transmises et à qui, par qui vont-elles être utilisées, pour quel objectif, de manière régulière ou une seule fois etc. Si un tiers doit envoyer la demande d'évaluation, alors la déclaration de consentement doit aussi contenir la transmission de l'adresse email aux fins d'envoi d'une demande d'évaluation à ce tiers. Lorsque le rappel à évaluation est envoyé par Trusted Shops, la déclaration obtenue par la boutique en ligne doit donc contenir que l'adresse email sera transmise à Trusted Shops à des fins d'envoi du rappel à évaluation. En outre, il convient de toujours informer que le consentement peut être retiré à tout moment. La délivrance du consentement doit être documentée et consignée pour preuve.

## **Exemple: le consentement donné par une case à cocher dans le compte-client**

### **Consentement par le biais d'une case à cocher**

je souhaiterais recevoir, par email et de manière unique, un rappel à évaluation après mes achats et consens à ce que mon adresse email soit transmise à cette fin à la société Trusted Shops GmbH.

ou (pour l'envoi d'un rappel à évaluation par la boutique en ligne elle-même)

je veux évaluer mes achats. Veuillez à chaque fois m'envoyer un email pour me permettre d'évaluer mes achats.

A ce sujet, le recueil du consentement dans le compte client ou par un lien dans l'email de confirmation de commande offre l'avantage que, dans le premier cas, l'adresse email a déjà, le cas échéant, été confirmée; dans le deuxième cas, seul le titulaire de l'adresse email accède au lien. Dans les deux cas, un double opt-in à titre de preuve serait superflu.

## **Les cartes postales d'évaluation**

L'utilisation d'une carte postale d'évaluation est sans risque en droit allemand. Il peut également s'agir par exemple d'un flyer avec un lien raccourci vers un profil de boutique. Les règles strictes valant pour la publicité par email ne s'appliquent pas à ce mode d'expédition. En France, il convient toutefois de vérifier que la personne n'a pas refusé d'être démarchée par voie postale (listes anti-prospection).

Dans le cas d'un contact personnel, un client peut également directement être sollicité pour donner une évaluation. Dans ce cas, aucun email n'est envoyé à cette fin et le recueil du consentement préalable n'est pas nécessaire.

Trusted Shops is Europe's  
trustmark in e-commerce.



Vous avez des questions sur les solutions de confiance de Trusted Shops ?  
L'équipe Trusted Shops est là pour vous aider.

 +33 (0)1 70 70 70 50

[members@trustedshops.com](mailto:members@trustedshops.com)