creditsafe

Briefing client 2018 sur le RGPD

Comment Creditsafe utilise-t-elle le RGPD pour mieux piloter ses activités ?

creditsafe

Présentation

Qu'est-ce que le RGPD ?

Le RGPD (Règlement Général sur la Protection des Données) fournira un ensemble de règles solides pour la collecte, le stockage et le traitement des données à caractère personnel et entrera en vigueur le 25 mai 2018. Le RGPD est un règlement plutôt qu'une directive, ce qui signifie qu'il s'agit d'une législation unique qui s'applique à tous les États membres de l'UE.

Pourquoi le RGPD ?

Étant donné que les entreprises recueillent de vastes quantités de données sur les consommateurs, de l'analyse comportementale aux caractéristiques personnelles, le sujet de la vie privée et de la protection de celle-ci est devenu une préoccupation majeure. De nombreuses entreprises ont développé des modèles commerciaux extensifs qui donnent accès à leurs services moyennant échange d'informations personnelles. Offrant d'énormes opportunités pour les entreprises, ces modèles limitent néanmoins le contrôle des individus sur la façon dont leurs données sont utilisées et stockées et, par conséquent, pourraient les exposer à de possibles vols de données, fraudes et autres abus. En renforçant les mesures à ce sujet, l'UE s'efforce de restaurer la confiance et de réduire la menace globale pesant sur les individus.

La mise en place du RGPD reflète bien les avancées technologiques et les progrès en matière de traitement des données qui ont eu lieu au cours des deux dernières décennies. Il vise à harmoniser les lois sur le respect de la vie privée et la protection des informations personnelles à travers l'Europe en instaurant des règles du jeu uniformes et, plus important encore, en en simplifiant la compréhension, de sorte à ce que les entreprises puissent gérer elles-mêmes la manière de s'y conformer.

À qui le RGPD s'applique-t-il ?

Toutes les organisations qui détiennent des données personnelles sur les citoyens de l'UE seront touchées par le RGPD. Et ce peu importe l'endroit dans le monde où les données sont situées.

Le RGPD élargit la définition des *données personnelles* pour englober tout ce qui peut être utilisé pour identifier directement ou indirectement une personne. Cela couvre un large éventail de données allant des nom, photos, adresse e-mail, coordonnées bancaires et messages sur les réseaux sociaux aux informations médicales ou aux adresses IP par exemple. Le nouveau règlement vise à protéger ces données, que leur dépôt soit automatique ou manuel, papier ou électronique.

Lorsque l'on considère les données B2B vs B2C, et ce qui relève ou non du RGPD, la ligne séparant les données personnelles et professionnelles ne semble pas toujours clairement définie. Par exemple, les données de particuliers provenant d'entreprises non constituées en société, telles que les sociétés individuelles ou les sociétés de personnes, ou les données sur les administrateurs d'entreprises constitués en société devraient être considérées comme des données personnelles identifiables, selon la définition du RGPD.

creditsafe

Qui sont les acteurs clés du RGPD ?

Les organisations elles-mêmes devront rendre des comptes auprès des autorités de surveillance de la protection des données. Bien que leur responsabilité ne soit pas une nouvelle exigence, le RGPD exige que toutes les organisations enregistrent et documentent tous les aspects prouvant leur conformité aux dispositions applicables du RGPD. Le règlement confère davantage de droits aux particuliers en ce qui concerne leurs données, notamment un contrôle et une visibilité accrus sur la façon dont leurs données personnelles sont utilisées, et le droit de voir ces informations supprimées ou transférées sur demande.

Personne concernée

Les personnes concernées sont les particuliers (citoyens de l'UE) dont les données sont collectées et traitées, comme par exemple les dirigeants, actionnaires et chefs d'entreprise. Le RGPD offre aux personnes concernées des droits supplémentaires en ce qui concerne les données traitées et contrôlées par les entreprises. Ceci est généralement appelé *autonomisation* des personnes concernées.

Contrôleur de données

Le contrôleur de données détermine les finalités et les moyens de traitement des données personnelles. Il contrôle la manière dont les données personnelles sont traitées, ce qui signifie qu'il est en charge du « pourquoi » et du « comment » de tout traitement de données. Les contrôleurs de données ne sont pas déchargés de leurs obligations lorsqu'un processeur de données est impliqué. Le RGPD impose d'autres obligations pour s'assurer que vos contrats avec les individus qui traitent des données pour votre compte soient conformes au RGPD. Creditsafe est un contrôleur de données.

Processeur de données

Il est chargé de traiter des données personnelles pour le compte d'un contrôleur. Le RGPD impose des obligations légales spécifiques : par exemple, les processeurs de données sont tenus de tenir des registres de données personnelles et des activités de traitement. Ceux qui traitent effectivement les données auront une responsabilité légale s'il s'avère qu'ils ont enfreint la réglementation en vigueur.

Autorité chargée de la protection des données

Les autorités chargées de la protection des données sont des autorités publiques indépendantes qui supervisent, via des mesures d'investigation et de rectification, l'application de la loi sur la protection des données à caractère personnel. Elles fournissent des conseils d'experts en matière de protection de la vie privée et traitent les plaintes déposées par rapport à d'éventuelles violations du règlement général sur la protection des données et des lois nationales d'application. Il y a une autorité compétente dans chaque État membre de l'UE.

Délégué à la protection des données

Le rôle principal du délégué à la protection des données (DPO) est de veiller à ce que l'organisation traite les données personnelles de ses travailleurs, clients, fournisseurs, ou de toute autre personne conformément aux règles applicables en matière de protection des données. Au sein des institutions et organes de l'UE, le règlement relatif à la protection des données qui est d'application (Règlement (CE) 45/2001) les oblige chacun à nommer un délégué à la protection des données. Creditsafe a nommé son délégué au niveau du groupe et a chargé des individus de protéger lesdites données puisque la réglementation et les bonnes pratiques des affaires l'imposent.

creditsafe

Les domaines clés du RGPD

1. **Responsabilité**

   Les contrôleurs de données doivent être en mesure de démontrer que les organisations se conforment bien au RGPD. Cependant, c'est la responsabilité des contrôleurs et des processeurs de données de s'assurer que les procédures adéquates soient suivies.

2. **Transparence**

   Les entreprises devront être honnêtes et transparentes sur les raisons pour lesquelles elles collectent des données personnelles et sur ce qu'elles ont l'intention d'en faire. Cela signifie qu'elles doivent expliquer à la personne concernée comment ses données vont être utilisées avant d'obtenir son consentement.

3. **Traitement des données personnelles**

   Les données personnelles ne peuvent être recueillies qu'à des fins précises, explicites et légitimes, et ne peuvent être traitées à d'autres fins que celles qui ont été prédéfinies. Par conséquent, les données légitimement collectées dans un certain but ne peuvent pas être utilisées à d'autres fins, à moins d'obtenir le consentement de la personne concernée ou d'avoir un but légitime pour le faire.

4. **Droit de regard**

   Les individus concernés ont le droit d'accéder à leurs données personnelles endéans les 30 jours suivant leur demande. Les organisations sont ainsi obligées de s'assurer que les données inexactes soient mises à jour ou effacées, et de donner aux personnes concernées un droit de correction et de modification des informations personnelles conservées à leur sujet.

5. **Droit à l'oubli numérique**

   Les individus ont également le droit de demander que leurs données personnelles soient supprimées, à condition qu'il n'y ait aucun motif légitime pour les conserver.

6. **Analyse d'impact relative à la protection des données (DPIA)**

   Le RGPD impose également l'évaluation de la quantité de données et de la durée pour laquelle celles-ci sont détenues. Dans les cas présentant un risque élevé, une évaluation des impacts sur la vie privée peut être requise. Le règlement indique également que, si des données personnelles sont collectées sur un individu, l'organisation ne peut pas en collecter davantage que ce qui est nécessaire pour l'exécution des finalités prévues.

7. **Amendes pour atteinte à la vie privée ou violation du règlement**
   Des amendes allant jusqu'à 4 % du chiffre d'affaires annuel ou 20 millions d'euros (montant le plus élevé des deux) pourraient être imposées en cas de violation du RGPD.

8. **Signalement des infractions**
   En cas de fuite de données susceptible d'avoir un impact sur l'individu concerné ou de lui causer un préjudice, le contrôleur de données est tenu de notifier l'autorité de contrôle au plus tard 72 heures après la détection de cette fuite de données.

L'impact du RGPD sur les services d'information Creditsafe

En tant qu'organisation, Creditsafe est tenue de recueillir des données sur les entreprises et leur comportement historique afin de pouvoir évaluer la solvabilité des sociétés. Creditsafe fournit à ses clients des données leur permettant de prendre des décisions financières et de gérer leurs risques commerciaux. Les informations personnelles identifiables (IPI) qui sont traitées par Creditsafe concernent uniquement les personnes qui sont directement liées à une entité commerciale.

Creditsafe opère dans un environnement business to business (B2B). Elle dispose des IPI des individus dans deux cas : dans le cadre d'une organisation, comme par exemple un directeur, ou en tant que personne unique, lorsque l'individu est l'entreprise. Creditsafe évalue uniquement la capacité de l'entité commerciale à (continuer à) mener des affaires et à exécuter des contrats en fonction de ses performances actuelles et passées. En tant que tel, le type et la qualité des données fournies aux clients ne changeront pas après l'introduction du RGPD.

Lorsque les données recueillies par Creditsafe ont été jugées impropres à l'utilisation ou ne semblent pas avoir le consentement approprié, ces données seront supprimées.

Intérêt légitime pour fournir des services d'information

L'article 6:F du RGPD autorise le traitement aux fins de l'intérêt légitime poursuivi par le contrôleur ou par une tierce partie. Il indique en outre que les responsables du traitement des données peuvent, lorsqu'il existe une raison authentique et légitime, traiter des données à caractère personnel sans le consentement préalable. Cela peut notamment inclure des avantages commerciaux, sauf lorsque ces intérêts sont remplacés par les intérêts ou les droits et libertés fondamentaux de la personne concernée qui requièrent la protection des données personnelles.

L'intérêt légitime de Creditsafe réside dans le fait que nous aidons les entreprises à prendre des décisions financières relatives à la gestion des risques afin de permettre à nos clients de prendre de meilleures décisions commerciales et économiques. En tant que tel, nous maintenons également l'intérêt légitime de sensibiliser les entreprises à cette capacité.

Relation contrôleur-contrôleur

Creditsafe offre plusieurs types de solutions à ses clients. Elle utilise sa propre base de données pour fournir ses services et peut décider à quelle autre fin utiliser ces données. En d'autres termes, Creditsafe agit comme un contrôleur de données. Ce poste est décrit dans nos Conditions Générales de base.

Creditsafe agit en tant que contrôleur de données chaque fois qu'elle fournit des services au client : elle utilise ses propres données et décide elle-même de ce qu'elle veut en faire ; elle a la flexibilité nécessaire pour déterminer comment la tâche sera exécutée, quelles données seront incluses et quels sont les points importants à compiler dans le rapport. Cela signifie que Creditsafe est entièrement responsable de toutes ses activités de traitement et doit donc s'assurer de ne partager des données personnelles que lorsque la loi le permet.

En résumé, toute donnée fournie par Creditsafe dans nos produits et services donnera lieu à une relation de contrôleur à contrôleur avec nos clients pour laquelle *aucune clause de traitement n'est requise*. Malgré l'existence

d'une relation de « contrôleur à contrôleur » avec ses clients, Creditsafe inclut les clauses relatives à la protection des données dans ses conditions générales de vente.

En tant que contrôleur, Creditsafe doit veiller à ne partager ses données personnelles que lorsque le cadre légal le permet. Par conséquent, les conditions générales de Creditsafe esquissent le cadre pour le partage des données personnelles et rappellent que le client s'engage, en utilisant nos services, à avoir une base légale pour le faire. Les conditions générales reprennent une liste des raisons pour lesquelles un client peut utiliser nos solutions.

Parmi nos services d'information, l'on retrouve :

Les mots clés recherchés

Le point de vue non contraignant de l'Autorité pour la Protection des Données était que les termes recherchés n'étaient pas pertinents - la société propriétaire de la base de données était un contrôleur de données et, lorsqu'elle envoyait des informations au client via un rapport, celui-ci devenait à son tour contrôleur de données de ce rapport. Par conséquent, il s'agit de savoir si vous pouvez ou non partager légalement ces informations - les mots clés recherchés sont un faux-fuyant.

Nettoyage des données/Ajout des données relatives au comportement de paiement commercial

Creditsafe « contrôle » les corrections qui sont apportées à ces données et détermine les informations/données supplémentaires qui doivent être ajoutées dans le cadre de son service. Creditsafe a la flexibilité nécessaire pour déterminer de quelle façon elle va effectuer la tâche ; nous sommes donc « contrôleurs » de ces données.

Nos clients peuvent-ils utiliser nos informations ?

Oui, toutes nos données et produits sont conformes aux exigences et nous utilisons nos données en respectant le consentement reçu ou l'intérêt légitime.

Il appartient au client d'établir la base légale pour le traitement des données personnelles obtenues suite à l'utilisation des services d'information de Creditsafe et de respecter la législation sur la protection des données en lien avec ces informations. Le client reconnaît également que l'accès aux données personnelles via l'utilisation des services d'information de Creditsafe n'est autorisé que s'il dispose d'une base légale pour le faire.

Cela signifie par exemple que le client n'utilisera les services d'information Creditsafe qu'à des fins de vérification de crédit, de prospection, de marketing direct, de vérification des clients, de conformité, de vérification et d'amélioration des données, d'autres contrôles légaux ou de toute autre affaire ayant un intérêt légitime, conformément au RGPD.

Comment Creditsafe s'est-elle alignée avec le RGPD ?

Creditsafe a adopté une approche commerciale globale pour le RGPD et a examiné tous les processus d'affaires et de données pour s'assurer qu'ils correspondent aux intérêts légitimes de notre entreprise : aider le client à prendre des décisions financières basées sur des évaluations de risques factuelles. Ce processus nous a permis d'examiner les sources et l'utilisation de toutes nos données afin de pouvoir offrir à nos clients les services qu'ils désirent, tout en veillant à ce qu'aucune de nos pratiques ne nuise ou ne porte préjudice aux personnes identifiées dans nos ensembles de données.

Comprendre nos sources de données et leur stockage (mappage de données)

À chaque étape de la collecte de données, nous cherchons à identifier ce que nous faisons avec les données, comment nous les protégeons et comment nous veillons à ne pas enfreindre les droits des individus à qui elles appartiennent. Ceci comprend le fait que les données personnelles doivent être obtenues uniquement à des fins définies et licites, et ne doivent pas être traitées d'une manière incompatible avec ces finalités.

Comprendre l'utilisation de nos données

Lorsque des données ont été collectées via intérêt légitime, enregistrement ou consentement, Creditsafe s'assure que ces données soient adéquates, pertinentes et non excessives par rapport à l'objectif fixé. CreditSafe évalue systématiquement ses données pour vérifier leur intérêt légitime.

Protéger les droits de l'individu

Creditsafe a mis des processus en place pour gérer tous les droits des individus, y compris les demandes d'accès à l'information, le droit à l'oubli, la correction des données, le changement du consentement donné et le transfert des données vers une autre plateforme pour un usage individuel.

Intégrité des données et transparence

Les processus du système de données de Creditsafe gèrent et « estampillent » les données, ce qui assure une traçabilité complète de toutes nos données. Ceci nous permet de démontrer clairement d'où proviennent les données et d'identifier tout changement apporté avec la raison de celui-ci.

Mettre en œuvre des mesures techniques et organisationnelles appropriées

Pour lutter contre le traitement non autorisé ou illégal de données personnelles et contre la perte accidentelle, destruction ou l'endommagement de celles-ci, Creditsafe met en œuvre des technologies qui nous permettront d'identifier puis d'étiqueter les informations personnelles identifiables (IPI) sensibles de sorte à les protéger. De cette manière, nous nous assurons que les données ne sont ni utilisées abusivement ni retirées du réseau de Creditsafe par le biais d'actions non autorisées.

Voici quelques mesures que nous prenons pour protéger nos systèmes et nos données :

- Pare-feu – Tous les points d'entrée et de sortie du réseau sont protégés par un pare-feu.
- DMZ – Des serveurs bien définis pour un accès au public, isolés du réseau interne pour écarter davantage les ressources sensibles.
- HIDS/NIDS – Activé au niveau des principaux goulots d'étranglement du réseau.
- SIEM – Des réseaux surveillés par un logiciel de supervision informatique, avec enregistrement et analyse des événements de sécurité et des alertes et alarmes automatisées en place.
- Antivirus – Tous les points terminaux compatibles sont protégés par un logiciel antivirus, avec des mises à jour automatiques via un serveur de mises à jour et Internet.
- Balayage réseau/hôte – Balayage régulier permettant de détecter les configurations vulnérables.
- Tests de pénétration, tests d'application Web et scans de vulnérabilité réguliers – Programme de gestion des menaces et de la vulnérabilité en place pour gérer les données sortantes.
- Prévention de la perte de données : Creditsafe a mis en place des contrôles pour empêcher les données de quitter son réseau, sauf si elles sont autorisées à la fois sur des réseaux et via des sources de média externes.

Mettre en place des contrôles appropriés

Creditsafe met tout en œuvre pour éviter que les données ne soient transférées vers un pays ou un territoire en dehors de l'Espace Économique Européen, à moins que ce pays ou territoire n'assure un niveau adéquat de protection des droits et libertés des personnes concernées par le traitement de leurs données personnelles.

Être prêt à répondre

Creditsafe a mis en œuvre des processus qui permettront une réponse rapide et efficace face à tout incident suspect, y compris toute violation qui pourrait avoir un impact sur les données IPI. Creditsafe a préparé des plans de communication clairs et concis vis-à-vis des clients, des personnes concernées et des autorités de régulation dans le cas d'un incident qui impliquerait un individu.

Confidentialité dès la conception

Creditsafe se rend compte que le RGPD n'est pas un événement unique dans l'histoire, mais plutôt une ligne directrice pour nos futurs modèles d'affaires. La nouvelle approche veut que la confidentialité dès la conception régisse toutes nos interactions entre individus. C'est aussi le cas dans notre stratégie d'entreprise, par laquelle nous voulons faire en sorte que toutes les décisions futures et les prochains développements tiennent compte de l'impact sur les individus avant d'être mis en œuvre.

creditsafe

FAQ

Creditsafe est-elle entièrement compatible avec le RGPD ?

Creditsafe est impliquée dans un programme de RGPD complet, et nos activités et services sont par conséquent en parfaite conformité avec la réglementation.

Creditsafe en tant qu'entreprise a l'obligation de recueillir des données sur les entreprises et leur comportement historique afin d'évaluer et de fournir à ses clients des données leur permettant de prendre des décisions financières et de gérer les risques commerciaux. Les informations personnelles identifiables (IPI) qui sont traitées par Creditsafe concernent uniquement les personnes qui sont directement liées à une entité commerciale.

Creditsafe opère dans un environnement business to business (B2B). Lorsque nous détenons les IPI de particuliers, soit en tant qu'administrateur ou en tant que commerçant unique, soit en tant qu'entreprise, nous n'évaluons que la capacité de l'entité commerciale à (continuer à) mener des activités et à exécuter des contrats sur la base de performances historiques. En tant que tel, le type et la qualité des données fournies aux clients ne changeront pas après l'introduction du RGPD. Lorsque les données recueillies par Creditsafe ont été jugées impropres à l'utilisation ou ne semblent pas avoir le consentement approprié, elles seront supprimées.

Quels logiciels de sécurité et cryptage avez-vous mis en place pour protéger toutes les données que Creditsafe a recueillies et/ou traitées ?

- Creditsafe est certifiée ISO27001, réglementée par la FCA et enregistrée en tant que contrôleur de données auprès du bureau du Commissaire britannique à l'information.
- Creditsafe fonctionne via un centre de données britannique Tier3+, dont la conformité aux normes ISO9001, ISO14001, ISO27001, ISAE3402, SSAE16 et PCI DSS est contrôlée par audit.
- Sécurité physique complète du centre de données, qui comprend une conception de mur à six couches, des patrouilles sur site 24 heures sur 24 et 7 jours sur 7, une clôture de qualité militaire, des fils de détente numériques, plusieurs tours CCTV à infrarouges et dont la construction répond aux normes sismiques californiennes.

Les contrôles de sécurité de Creditsafe comprennent :

- DMZ – Des serveurs bien définis pour un accès au public, isolés du réseau interne pour écarter davantage les ressources sensibles.
- HIDS/NIDS – Activé au niveau des principaux goulots d'étranglement du réseau.
- SIEM – Des réseaux surveillés par un logiciel de supervision informatique, avec enregistrement et analyse des événements de sécurité et des alertes et alarmes automatisées en place.
- Antivirus – Tous les points terminaux compatibles sont protégés par un logiciel antivirus, avec des mises à jour automatiques via un serveur de mises à jour et Internet.
- Balayage réseau/hôte – Balayage régulier permettant de détecter les configurations vulnérables.
- Tests de pénétration, tests d'application Web et scans de vulnérabilité réguliers – Programme de gestion des menaces et de la vulnérabilité en place pour gérer les données sortantes.
- Les données sont répliquées toutes les 5 minutes entre l'environnement de production Creditsafe et un environnement dédié dans la continuité des opérations. La plateforme est dimensionnée et configurée pour offrir une grande disponibilité, permettant le basculement automatisé d'un serveur à l'autre.

Données marketing Creditsafe

Comment Creditsafe prépare-t-elle ses données marketing pour le RGPD ?

Creditsafe s'investit dans un programme de RGPD complet garantissant que toutes les données sont recueillies et utilisées avec la permission appropriée, qu'elles fassent l'objet d'un consentement ou qu'elles aient un intérêt légitime. L'utilisation des données est entièrement cartographiée dans toute l'entreprise et soumise à des évaluations rigoureuses des risques et de la confidentialité des données.

Quel consentement Creditsafe demande-t-elle aux entreprises ?

Le consentement obtenu par Creditsafe est pertinent pour l'utilisation des données recueillies à ce moment, c'est-à-dire le consentement à l'utilisation, le consentement à la commercialisation, le consentement à l'appel et le consentement pour la mise à jour des dossiers pour un contact futur.

Lorsque le consentement n'est pas disponible, l'Article 6:F du RGPD permet le traitement aux fins de l'intérêt légitime poursuivi par le contrôleur ou par une tierce partie. L'intérêt légitime de Creditsafe réside dans le fait que nous aidons les entreprises à prendre des décisions financières fondées sur les risques afin de permettre à nos clients de prendre de meilleures décisions commerciales et économiques. En tant que tel, nous maintenons également l'intérêt légitime de faire prendre conscience aux entreprises de cette capacité, y compris lorsqu'elles recherchent de nouvelles opportunités commerciales.

Où sont hébergées toutes les données auxquelles nous avons accès, est-ce au Royaume-Uni ?

Toutes les données Creditsafe sont stockées au Royaume-Uni ou dans l'EEE sur des serveurs sécurisés entièrement protégés contre les sinistres.