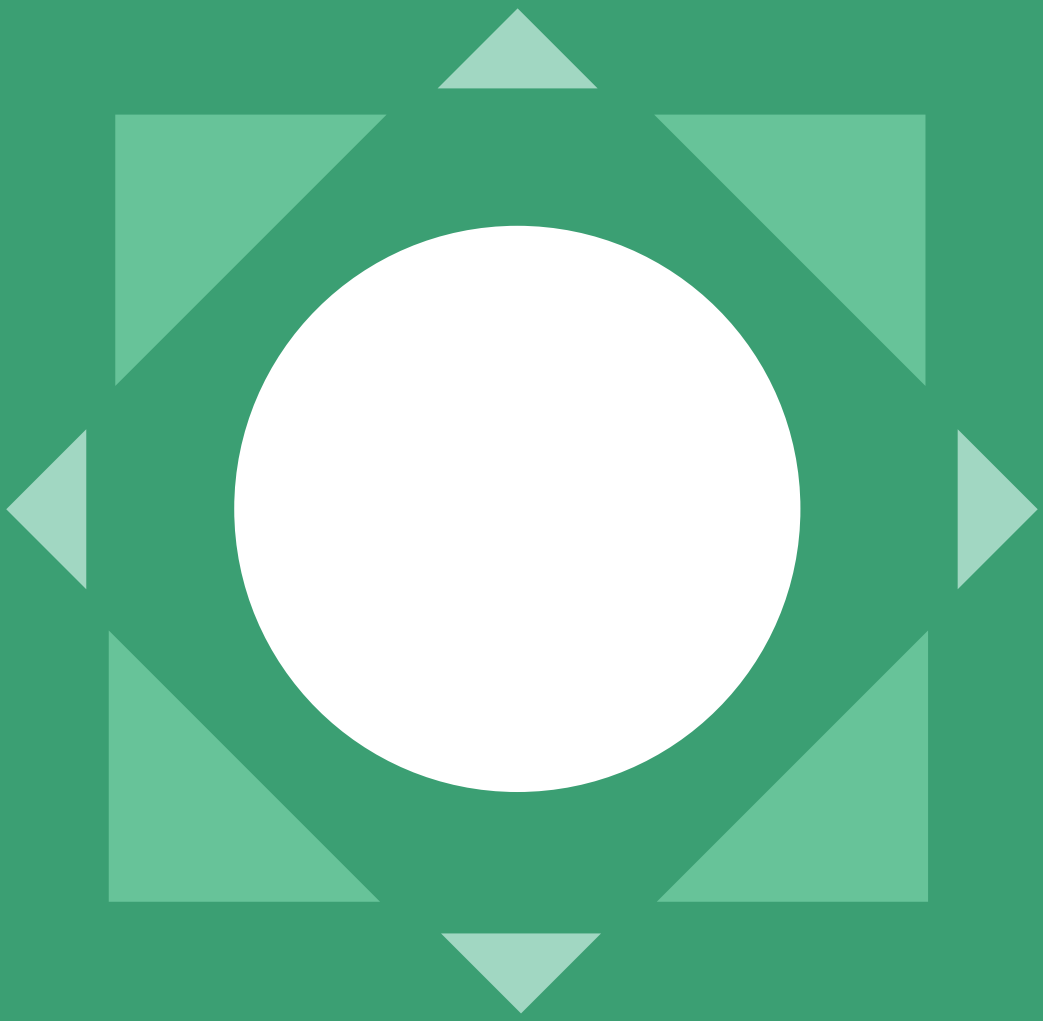
creditsafe

RGPD Creditsafe

Comment Creditsafe utilise le RGPD pour améliorer son business



creditsafe

Introduction

Qu'est ce que le RGPD ?

Le règlement général sur la protection des données (RGPD) fourni un ensemble solide de règles pour la collecte, le stockage et le traitement des informations personnelles et st entré 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 dans tous les États membres de l'UE. Information complémentaire à propos du Royaume-Uni : il sera toujours membre de l'UE en 2018, il s'applique donc au Royaume-Uni de la même manière, et s'appliquera également après le Brexit.

Qu'est ce que le RGPD ?

Les entreprises recueillant de nombreuses données personnelles sur les consommateurs, de l'analyse comportementale aux caractéristiques personnelles, la protection de la vie privée est devenue une préoccupation majeure. De nombreuses entreprises ont mis au point des modèles d'affaires complets qui reposent sur l'échange d'informations commerciales en échange d'un accès aux services. Bien que cela offre d'énormes possibilités, cela donne également aux individus peu de contrôle sur l'utilisation de leurs données, la façon dont elles sont stockées, par conséquent, pourrait les exposer à une menace de vol, de fraude et d'autres abus. En renforçant les mesures, l'UE s'efforce d'améliorer la confiance et de réduire la menace qui pèse sur les individus.

Le RGPD est mis en place afin de refléter les progrès de la technologie et des données au cours des deux dernières décennies. Il vise à harmoniser les lois sur la protection des données à travers l'Europe, en créant des règles du jeu équitables et, plus important encore, en simplifiant la compréhension et la gestion de leur propre conformité par les entreprises.

Qui est concerné par le RGPD ?

Toutes les organisations qui détiennent des données personnelles sur les citoyens de l'UE seront affectées par le RGPD. Peu importe où se trouvent les données dans le monde.

Le RGPD élargit la définition des données personnelles pour englober tout ce qui peut être utilisé pour identifier directement ou indirectement une personne. Il s'agit d'un large éventail de données allant des noms, photos, adresses électroniques, 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, qu'il s'agisse d'un dépôt automatique ou manuel, papier ou électronique.

Lorsque l'on considère les données B2B vs B2C, et ce qui relève ou non du mandat du RGPD, la limite entre données personnelles et commerciales ne semble pas toujours clairement définie. Par exemple, les données sur les particuliers provenant d'entreprises non constituées en société, comme les entreprises individuelles, les sociétés de personnes, ou les données sur les administrateurs d'entreprises constituées en société devraient être considérées comme des données personnelles identifiables au sens de la définition du RGPD.

creditsafe

Qui sont les acteurs clés du RGPD?

Les organisations seront responsables devant les autorités de contrôle de la protection des données. Bien que l'obligation de rendre compte ne soit pas une nouvelle exigence, le RGPD exige que toutes les organisations enregistrent et documentent la conformité à tous les aspects applicables du RGPD. Le règlement donne aux individus plus de droits en ce qui concerne leurs données, y compris plus de contrôle et de visibilité sur la manière dont leurs données personnelles sont utilisées, et le droit de faire supprimer ou déplacer ces informations si nécessaire.

Sujet des données

Les sujets de données sont les personnes privées (citoyens de l'UE) sur lesquelles des données sont collectées et traitées, par exemple les directeurs, les actionnaires et les propriétaires d'entreprises. Le RGPD fournit aux sujets des données plus de droits en ce qui concerne les données qui sont traitées et contrôlées par les entreprises. C'est ce qu'on appelle habituellement l'habilitation des sujets de données.

Contrôleur de données

Le responsable du traitement détermine les finalités et les moyens de traitement des données personnelles. Ils contrôleront la manière dont les données personnelles sont traitées, ce qui signifie qu'ils ont la propriété du «pourquoi» et du «comment» de tous les traitements de données. Les contrôleurs de données ne sont pas déchargés de leurs obligations lorsqu'un sous-traitant est impliqué - le RGPD impose d'autres obligations pour s'assurer que vos contrats avec les sous-traitants sont conformes au RGPD. Creditsafe est un contrôleur de données.

Processeur de données

Le responsable du traitement des données est responsable du traitement des données personnelles pour le compte d'un responsable du traitement. Le RGPD impose des obligations légales spécifiques aux responsables du traitement des données ; par exemple, ils doivent de tenir des registres des données personnelles et des activités de traitement. Les préposés au traitement des données auront une responsabilité légale s'ils sont responsables d'une violation.

Autorité de protection des données

Les DPA sont des autorités publiques indépendantes qui supervisent, par le biais de pouvoirs d'investigation et de correction, l'application de la loi sur la protection des données. Ils fournissent des conseils d'experts sur les questions de protection des données et traitent les plaintes déposées contre les violations du règlement général sur la protection des données et des lois nationales pertinentes. Il y en a un dans chaque État membre de l'UE.

Délégué à la protection des données

Le rôle principal du délégué à la protection des données (DPD) est de veiller à ce que l'organisation traite les données personnelles de son personnel, de ses clients, de ses fournisseurs ou de toute autre personne dans le respect des règles applicables en matière de protection des données. Dans les institutions et organes de l'UE, le règlement applicable en matière de protection des données (règlement (CE) n° 45/2001) les oblige à désigner chacun un délégué à la protection des données. Creditsafe a nommé un DPD au niveau du groupe et dispose d'un personnel local qui soutient le rôle du DPD lorsque la réglementation ou les pratiques commerciales le jugent nécessaire.

creditsafe

Les domaines clés du RGPD

1. Responsabilité

Les contrôleurs de données doivent être en mesure de démontrer la conformité de l'organisation au RGPD. Toutefois, il incombe à la fois aux transformateurs et aux contrôleurs de veiller à ce que les bonnes procédures soient suivies.

2. Transparence

Les organisations devront être transparentes sur les raisons pour lesquelles elles collectent des données personnelles et sur ce qu'elles ont l'intention d'en faire. Il s'agit d'expliquer au sujet des données ce pourquoi ses données sont collectées pour obtenir son consentement.

3. Traitement des données personnelles

Les données personnelles ne peuvent être collectées qu'à des fins spécifiques, explicites et légitimes, et ne peuvent être traitées à aucun autre titre ne répondant pas à ces finalités. Par conséquent, les données recueillies légitimement pour une finalité ne peuvent être utilisées pour un autre objectif à moins qu'elles n'obtiennent le consentement de la personne concernée ou n'aient un but légitime pour le faire.

4. Droit d'accès

Les sujets de données ont le droit d'accéder à leurs données personnelles dans les 30 jours suivant une demande. Les organisations ont la responsabilité de veiller à ce que les données inexactes soient mises à jour ou effacées ; donner aux sujets le droit de vérifier et de modifier les renseignements personnels qu'ils détiennent à leur sujet.

5. Droit à l'oubli

Les sujets de données ont également le droit de demander la suppression de leurs données personnelles, à condition qu'il n'existe aucune raison légitime de les conserver.

6. Protection des données par défaut (Evaluation des facteurs relatifs à la vie privée)

Le RGPD demande que nous évaluions la quantité et la durée pendant laquelle nous détenons des données personnelles. Dans des circonstances qui posent un risque élevé, une évaluation des facteurs relatifs à la vie privée peut être requise. Il stipule également que si des données personnelles sont recueillies sur une personne, l'organisation ne devrait pas recueillir plus de données que ce qui est nécessaire aux fins prévues.

7. Amendes pour atteinte à la vie privée ou violation du droit à la vie privée

Des amendes allant jusqu'à 4 % du chiffre d'affaires annuel ou 20 millions d'euros, le montant le plus élevé étant retenu, pourraient être infligées en cas de violation du RGPD.

8. Signaler les atteintes à la vie privées

En cas d'atteinte à la protection des données qui pourrait avoir un impact sur la personne ou causer un préjudice, le responsable du traitement est tenu d'informer l'autorité de contrôle d'une atteinte importante au plus tard 72 heures après que l'atteinte à la protection des données a été détectée.

creditsafe

RGPD et Creditsafe

En tant qu'entreprise, Creditsafe a l'obligation de collecter des données sur les entreprises et leur comportement historique afin d'évaluer la solvabilité des entreprises. Creditsafe fournit à ses clients des données qui leur permettent de prendre des décisions financières et de gérer les risques commerciaux. Les renseignements personnels identifiables (RPI) qui sont traités par Creditsafe ne concernent que les personnes qui sont directement liées à une entité commerciale[1].

Creditsafe opère dans un environnement interentreprises (B2B) et aux RPI des individus soit en tant que membre d'une organisation telle qu'un administrateur, soit en tant que commerçant unique où l'individu est l'entreprise. Creditsafe évalue uniquement la capacité de l'entité commerciale à exercer et à continuer à exercer ses activités et à exécuter les contrats sur la base des performances actuelles et historiques. La qualité des données fournies aux clients ne sera pas affectée après la mise en place du RGPD.

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

Intérêt légitime à fournir des services d'information

L'article 6:F du RGPD autorise le traitement aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers. Il stipule en outre que les responsables du traitement des données à caractère personnel peuvent traiter les données à caractère personnel sans consentement donné s'il existe une raison réelle et légitime.

L'intérêt légitime de Creditsafe est que nous aidons les entreprises à prendre des décisions financières basées sur les risques afin de permettre à nos clients de prendre de meilleures décisions commerciales et économiques. À ce titre, nous maintenons également l'intérêt légitime de sensibiliser les entreprises à cette capacité.

Relation contrôleur - contrôleur

Creditsafe offre de nombreux produits différents parmi lesquels les clients peuvent choisir. Creditsafe utilise sa propre base de données pour fournir les services et peut décider à quoi d'autre il utilise les données. Creditsafe agira en tant que contrôleur de données, ce poste sera couvert dans les conditions générales de vente.

Creditsafe agit en tant que contrôleur de données chaque fois qu'il fournit des services au client : Creditsafe utilise ses propres données dont il peut décider de l'utilisation ; il dispose d'une certaine souplesse pour décider de la manière d'exécuter la tâche, des données à inclure et de ce qui est important en termes de compilation du rapport. Cela signifie que Creditsafe sera entièrement responsable de toutes ses activités de traitement et qu'elle doit s'assurer qu'elle ne partage les données personnelles que lorsqu'il est légal de le faire.

Malgré l'existence d'une relation «contrôleur-contrôleur» avec les clients, Creditsafe inclut les clauses de protection des données dans les conditions générales de nos clients.

[1] Les activités de Creditsafe en Suède et en Norvège collectent et traitent également des données sur les consommateurs en vertu des dispositions des lois sur les références de crédit.

En tant que responsable du traitement, Creditsafe doit s'assurer qu'elle ne partage des données personnelles que lorsqu'il est légal de le faire et, par conséquent, Creditsafe définit dans les termes et conditions le cadre pour le partage des données personnelles et une reconnaissance par le client que pour utiliser nos services, ils doivent avoir une base légale pour le faire. Dans les termes et conditions de Creditsafe il y a une liste des raisons pour lesquelles un client peut utiliser nos produits.

Certains services d'information spécifiques sont les suivants :

Nettoyage des données et données sur les paiements commerciaux

Creditsafe consiste à « contrôler » les corrections apportées à ces données et les informations ou données supplémentaires qui doivent être ajoutées dans le cadre du service. Creditsafe a la flexibilité de décider comment effectuer la tâche, nous sommes un « contrôleur » de ces données.

Nos clients peuvent-ils utiliser nos informations ?

Oui, toutes nos données et produits sont conformes aux exigences et nous utilisons les données conformément au consentement ou à l'intérêt légitime.

Le client est responsable d'établir la base légale pour le traitement des données personnelles obtenues dans le cadre de l'utilisation des services d'information de Creditsafe et de maintenir le respect de la législation sur la protection des données en relation avec ces données. Le client doit également reconnaître que l'accès aux données personnelles par l'utilisation des services d'information de Creditsafe n'est autorisé que si le client dispose d'une base légale pour ce faire.

Ce qui signifie, par exemple, que le client ne doit utiliser les services d'information Creditsafe qu'à des fins de vérification de crédit, de prospection, de marketing direct, de vos vérifications clients, de conformité, de vérification et d'amélioration des données, d'autres buts légaux de diligence raisonnable ou de toute autre activité commerciale ayant un intérêt légitime au regard du RGPD.

creditsafe

Comment Creditsafe s'est conformé au RGPD

Creditsafe a adopté une approche commerciale globale du RGPD et a examiné tous les processus d'affaires et les processus de données pour s'assurer qu'ils s'alignent sur les intérêts légitimes de notre entreprise afin d'aider les clients à prendre des décisions financières fondées sur des évaluations factuelles des risques. Ce processus nous a permis d'examiner les sources et l'utilisation de toutes nos données afin de nous assurer que nous pouvons fournir à nos clients les services qu'ils désirent, tout en nous assurant qu'aucune de nos pratiques ne causera de tort ou de préjudice aux personnes identifiées dans nos ensembles de données

Comprendre nos sources de données et leur stockage

Pour toutes les étapes de la conservation des données, nous cherchons à identifier ce que nous faisons avec les données, comment nous protégeons les données et comment nous nous assurons de ne pas empiéter sur les droits du sujet de ces données. Cela signifie notamment que les données à caractère personnel ne peuvent être obtenues qu'à des fins déterminées et licites et ne peuvent faire l'objet d'aucun traitement ultérieur incompatible avec cette finalité ou ces finalités.

Comprendre notre utilisation des données

Aux fins spécifiques pour lesquelles des données ont été collectées comme pour la finalité spécifique pour laquelle les données ont été collectées, comme l'intérêt légitime, les enregistrements de traitement, le consentement, la garantie que les données sont adéquates, pertinentes et non excessives par rapport à la finalité ; Creditsafe évalue systématiquement ses données pour vérifier l'intérêt légitime.

Protéger les droits de l'individu

Creditsafe a mis en place des processus pour traiter tous les droits des individus, y compris les demandes d'accès par sujet, le droit à l'oubli, la correction des données, le changement de consentement lorsqu'il a été donné, et le transfert des données vers une autre plate-forme pour une utilisation individuelle.

Intégrité et transparence des données

Le processus Data Vault de Creditsafe gère et tamponne les données, ce qui garantit une traçabilité totale de toutes les données Creditsafe. En montrant clairement d'où proviennent les données et tout changement apporté avec la raison du changement.

Mettre en oeuvre les mesures techniques et organisationnelles appropriées

Pour protéger les données personnelles contre le traitement non autorisé ou illégal et contre la perte accidentelle ou la destruction ou l'endommagement, Creditsafe met en œuvre des technologies qui nous permettront d'abord d'identifier et ensuite d'étiqueter les informations d'identification personnelle sensibles, es données seront alors protégées en totalité. Cela garantit que les données ne sont pas utilisées à mauvais escient ou supprimées en dehors du réseau Creditsafe par des actions non autorisées.

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

• Pare-feu - Tous les points d'entrée/sortie du réseau sont protégés par un pare-feu.
• DMZs - Bien défini pour les serveurs ouverts au public, avec une segmentation interne du réseau utilisée pour isoler davantage les ressources sensibles
• HIDS/NIDS - Activé aux principaux points d'étranglement du réseau.
• SIEM - Réseaux surveillés par SIEM, avec enregistrement et analyse des événements de sécurité, alertes et alarmes automatisées en place.
• Antivirus - Tous les points finaux compatibles couverts par un logiciel antivirus, avec des mises à jour automatiques via un serveur de mise à jour et Internet.
• Balayage réseau/hôte - Balayage régulier à la recherche de configurations vulnérables.
• Tests de pénétration, tests d'applications Web et analyse des vulnérabilités - Un programme de gestion des menaces et des vulnérabilités est en place pour gérer les résultats.
• Prévention des pertes de données : Creditsafe a mis en place des contrôles pour protéger les données contre la sortie de son réseau, à moins qu'elles ne soient autorisées à la fois sur les réseaux et via des sources de médias externes.

Mettre en place des contrôles appropriés

Creditsafe opère pour éviter les transferts de données vers un pays ou 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 rapport au traitement des données à caractère personnel.

Etre prêt à répondre

Creditsafe a mis en place des processus qui permettront une réponse rapide et efficace à tout incident suspect, y compris les violations qui pourraient avoir un impact sur les données d'identification. Creditsafe est prêt avec des plans de communication clairs et concis pour les clients, les sujets de données et les autorités réglementaires dans le cas d'un incident qui aura pour résultat toute personne affectée.

Protection de la vie privée dès la conception

Creditsafe se rend compte que le RGPD n'est pas un événement unique dans l'histoire, mais qu'il est plutôt utilisé comme une ligne directrice pour nos futures affaires avec la protection de la vie privée par la conception adoptée dans nos interactions avec les individus. Il est également utilisé dans notre stratégie d'affaires, en s'assurant que toutes les décisions et développements futurs de l'entreprise tiennent compte de l'impact sur l'individu avant d'entamer son évolution.

creditsafe

FAQ

Est-ce que Creditsafe est entièrement conforme au RGPD ?

Creditsafe est engagé dans un programme complet de RGPD pour s'assurer que nos opérations et nos services sont en pleine conformité avec la réglementation.

Creditsafe, en tant qu'entreprise, a l'obligation de collecter des données sur les entreprises et leur conduite historique afin d'évaluer et de fournir à ses clients des données leur permettant de prendre des décisions financières et de gérer les risques d'affaires. Les IIP traitées par Creditsafe ne concernent que les personnes qui sont directement liées à une entité commerciale.

Creditsafe opère dans un environnement interentreprises (B2B). Lorsque nous avons les identifications de personnes physiques, soit en tant que membre d'une organisation, comme un administrateur, soit en tant qu'entreprise individuelle, où l'entreprise est l'individu. Nous n'évaluons que la capacité de l'entité commerciale d'exercer et de continuer d'exercer ses activités et d'exécuter les contrats en fonction de son rendement historique. Ainsi, le type et la qualité des données fournies aux clients ne changeront pas après l'introduction du RGPD. Lorsque les données collectées par Creditsafe ont été jugées impropres à l'utilisation ou ne semblent pas avoir le consentement approprié, ces données seront alors effacées.

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

- Creditsafe est certifié ISO27001, réglementé par la FCA et enregistré en tant que contrôleur de données auprès du bureau du Commissaire à l'information du Royaume-Uni
- Creditsafe opère par le biais d'un centre de données Tier3+ UK, qui est audité selon les normes ISO9001, ISO14001, ISO27001, ISAE3402, SSAE16 et PCI DSS
- Sécurité physique complète du centre de données, y compris la conception d'un mur à 6 couches, des patrouilles de campus 24/7, des clôtures militaires, des fils de déclenchement numériques, de multiples tours de vidéosurveillance IR et est construit selon les normes californiennes en cas de tremblement de terre.

Les contrôles de sécurité Creditsafe incluent:

- Pare-feu - Tous les points d'entrée/sortie du réseau sont protégés par un pare-feu.
- DMZs - Bien défini pour les serveurs ouverts au public, avec une segmentation interne du réseau utilisée pour isoler davantage les ressources sensibles.
- HIDS/NIDS - Activé aux principaux points d'étranglement du réseau.
- SIEM - Réseaux surveillés par SIEM, avec des événements de sécurité enregistrés et analysés, des alertes et des alarmes automatisées sont également en place.
- Antivirus - Tous les points finaux compatibles couverts par un logiciel antivirus, avec des mises à jour automatiques via un serveur de mise à jour et Internet.
- Cryptage des données.
- Tests de pénétration habituels, tests d'applications Web et analyse des vulnérabilités - Programme de gestion des menaces et des vulnérabilités en place pour gérer les sorties.
- Sauvegarde des données : les données sont répliquées toutes les 5 minutes depuis l'environnement de production Creditsafe jusqu'à un environnement dédié à la continuité de l'activité. La plate-forme est dimensionnée et configurée pour utiliser une haute disponibilité, permettant le basculement automatisé des serveurs.

creditsafe

Données Marketing Creditsafe

Comment Creditsafe prépare ses données marketing dans le cadre du RGPD ?

Creditsafe est engagé dans un programme complet de RGPD en s'assurant que toutes les données sont collectées et utilisées avec l'autorisation appropriée, qu'il s'agisse d'un consentement ou d'un intérêt légitime. L'utilisation des données est entièrement cartographiée dans l'ensemble de l'entreprise et fait l'objet d'évaluations rigoureuses des risques et de l'incidence des données sur la protection de la vie privée.

Quel consentement Creditsafe demande-t-il aux entreprises auprès desquelles nous recueillons des renseignements ?

En tant qu'entreprise BtoB, l'Article 6:F du RGPD permet le traitement aux fins des intérêts légitimes poursuivis par le contrôleur ou par un tiers. L'intérêt légitime de Creditsafe est que nous aidons les entreprises à prendre des décisions financières fondées sur le risque afin de permettre à nos clients de prendre de meilleures décisions commerciales et économiques. À ce titre, nous maintenons également l'intérêt légitime de sensibiliser les entreprises à cette capacité, y compris lorsqu'elles sont à la recherche de nouvelles opportunités d'affaires.

Où sont hébergées toutes les données auxquelles nous avons accès, s'agit-il du Royaume-Uni ?

Toutes les données Creditsafe sont stockées soit au Royaume-Uni, soit dans l'EEE sur des serveurs sécurisés qui sont entièrement protégés pour la récupération en cas de catastrophe.