HubSpot, vos données et vous

Introduction à la gestion des données dans l'Union européenne

Dernière mise à jour le 4 août 2017

Vous pouvez télécharger la version la plus récente de ce document et obtenir davantage d'informations sur l'approche adoptée par HubSpot en matière de respect de la vie privée à cette adresse : http://legal.hubspot.com/data-privacy.

La protection du respect de la vie privée dans l'Union européenne peut paraître complexe, tout particulièrement à la lecture du nouveau Règlement général sur la protection des données (RGPD). Tout repose pourtant sur un seul principe : la confiance. L'Union européenne et ses États membres ont mis en place des restrictions juridiques afin de s'assurer que les entreprises collectant des données personnelles se montrent honnêtes sur la raison de leur collecte, sur leur utilisation, sur leur hébergement et sur leur partage. Si des entreprises partagent ces données, par exemple en faisant appel à un sous-traitant pour leurs opérations quotidiennes, ces restrictions exigent aussi qu'elles demandent à leurs prestataires de services de respecter les mêmes exigences. Ces lois établissent ainsi un flux protégé de données entre des individus et les entreprises auxquelles ils font confiance, ainsi qu'entre ces mêmes entreprises et les prestataires de services auxquels elles accordent leur confiance.

AVERTISSEMENT : Ce document ne vise pas à présenter de manière exhaustive les lois européennes sur le respect de la vie privée, ni à offrir de conseils juridiques sur lesquels votre entreprise pourrait s'appuyer pour se mettre en conformité avec des règlements tels que le RGPD. Il fournit néanmoins des informations contextuelles permettant de mieux comprendre comment HubSpot gère certains points juridiques importants. Ces *informations* juridiques ne sont pas des *conseils* juridiques. Il est donc indispensable que vous consultiez votre propre conseiller juridique si vous souhaitez savoir comment interpréter ces informations ou vérifier leur exactitude. Vous ne pouvez pas utiliser ce document au titre de conseil juridique, ni même au titre de recommandation pour la compréhension d'une loi donnée.

Table des matières

Résumé historique 2

Garantie de conformité 4

Le RGPD 6

L'approche juridique adoptée par HubSpot 8

L'approche adoptée par HubSpot pour la sécurité 9

Cookies 9

Fonctionnalités des e-mails 10

Hébergement de données 11

Programme de sécurité 12

Modification des données et autres demandes liées au respect de la vie privée 12

Envisager l'avenir 12

Autres ressources 14

Résumé historique

La notion de « confiance » est entrée en scène juste après la Seconde Guerre mondiale. Dans un effort d'unification des pays européens, un groupe d'états signa alors un traité formant le Conseil de l'Europe en 1949. Peu après, le Conseil vota pour adopter la Convention européenne des Droits de l'Homme, un traité international énonçant la liste des droits et des libertés fondamentaux devant être garantis dans les États membres. L'engagement suivant figurait au huitième article de la Convention, et présentait ainsi un premier pas affirmé vers le concept de respect de la vie privée :

> **toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.**

En 1980, le Conseil réaffirma cet engagement et, avec l'Organisation de coopération et de développement économiques (OCDE), rédigea le Traité n°108 afin de réguler le « traitement automatique des données personnelles ». Le Traité présentait ainsi les principes fondamentaux du respect de la vie privée, qui apparaissent depuis dans de nombreuses lois abordant la question du traitement des données :

- Le devoir d'obtenir et de traiter les données personnelles de manière juste et légale
- Le devoir d'héberger les données personnelles uniquement dans un but indiqué et légitime

- Le devoir de collecter les données de manière appropriée, pertinente et non excessive au regard de ce but
- Le devoir de préserver l'exactitude des données, notamment par le biais de mises à jour
- Le devoir de préserver les données pouvant être reliées à une personne pour la seule durée strictement nécessaire à ce but
- Une restriction supplémentaire pour traiter les « catégories spéciales » de données à caractère personnel révélant l'origine raciale, les convictions religieuses ou l'état de santé des personnes concernées
- Une obligation de maintenir les « mesures de sécurité adéquates »
- Des droits supplémentaires afin que chaque individu puisse demander si ses données personnelles sont hébergées, et puisse demander à les mettre à jour ou les supprimer

Chaque État membre de l'UE a ratifié ce traité, qui représente ainsi un fondement important de la protection des données au sein de l'Union.

En 1995, l'UE a voté la Directive sur la protection des données personnelles (95/46/EC) afin de protéger le droit à la vie privée de chaque individu et de réguler le traitement et l'échange de données personnelles. Cette Directive a été conçue pour donner davantage de substance aux droits établis dans le Traité n°108 et, depuis plus de 20 ans, demeure le principal accord juridique régissant la protection des données et le respect de la vie privée dans l'UE. En tant que Directive, elle a servi de modèle pour établir un ensemble de règles indispensables liées au respect de la vie privée que les États membres devaient intégrer à leurs propres lois nationales. Un réseau de lois européennes a donc été créé ; celles-ci comportent plusieurs points communs mais varient aussi légèrement d'un pays à l'autre.

La Directive s'attachait à établir des normes que chaque organisation devait suivre lors de la collecte et du traitement de données personnelles concernant des citoyens de l'Union européenne (« personnes concernées »). Elle imposa la plupart de ces normes aux organisations qui collectaient des données et choisissaient la manière de les utiliser (« responsables du traitement »), et établit aussi des règles pour les prestataires auxquels les responsables faisaient appel pour traiter ou héberger les données (« sous-traitant »). Ces règles couvraient de nombreux concepts familiers du respect de la vie privée, comme l'obtention de l'accord des personnes concernées avant l'utilisation de leurs données, l'application d'une attention toute particulière pour le traitement des données sensibles, la garantie de mesures de sécurité appropriées, l'examen des relations avec les prestataires qui pourraient aider les responsables à gérer ou à héberger des données (tout particulièrement

ceux basés en dehors de l'UE) et l'autorisation donnée aux personnes concernées pour contrôler l'utilisation de leurs données. La Directive exigeait aussi des États membres qu'ils établissent une ou plusieurs autorités nationales de régulation (« autorités responsables de la protection des données » ou « autorités de contrôle ») qui seraient chargées du contrôle et de l'application des lois sur le respect de la vie privée sur leur propre territoire.

Les pays extérieurs à l'UE ne proposaient généralement pas de protections similaires pour les données et les législateurs de la Directive choisirent de se concentrer plus particulièrement sur le transfert des données personnelles en dehors de l'UE. L'Article 25 de la Directive énonce ainsi un ensemble de restrictions géographiques pour le transfert des données, autorisant les transferts en dehors de l'UE seulement lorsque la Commission européenne détermine que le « pays tiers » peut assurer un « niveau de protection adéquat » (souvent qualifié de « caractère adéquat »). Sans pays au caractère adéquat (la liste n'en compte que neuf à ce jour), les responsables voulant transférer des données dans un pays tiers devaient adopter l'une des quelques autres options pré-approuvées (comme les Clauses contractuelles types) ou s'appuyer sur un accord personnalisé approuvé par les organisations gouvernementales concernées.

Garantie de conformité

Un acteur essentiel sur la scène mondiale n'apparaît pas sur la courte liste de caractère adéquat de l'UE : les États-Unis. Cette décision s'appuyait principalement sur le fait que les États-Unis adoptent une approche différente du respect de la vie privée, en choisissant de réguler des secteurs précis plutôt que d'appliquer des règles générales. Les transferts de données entre l'UE et les États-Unis ne sont autorisés que si un responsable s'appuie sur des Clauses contractuelles types ou si les États-Unis décident de signer un accord avec l'UE afin de garantir des niveaux de protection adéquats.

La première grande tentative pour trouver un accord politique était la Sphère de sécurité, approuvée par le Département du Commerce des États-Unis (« DoC ») et la Commission européenne en 2002. Les entreprises américaines pouvaient ainsi décider d'intégrer le programme de la Sphère de sécurité et devaient certifier au DoC qu'elles respecteraient plusieurs principes liés au respect de la vie privée. Ces principes exigeaient qu'elles (1) informent les personnes concernées de la collecte de leurs données personnelles et de la façon dont elles seraient utilisées ; (2) fournissent des mécanismes afin de refuser la collecte des données et leur transfert à des tiers ; (3) s'assurent que les sous-traitants offrent un niveau adéquat de protection ; (4) permettent aux personnes concernées d'accéder à leurs données

personnelles ; et (5) entreprennent des efforts raisonnables pour prévenir toute perte d'information et s'assurer que les données collectées sont pertinentes et utilisées dans l'unique but défini pour leur collecte. Les entreprises américaines respectant ces principes et certifiées dans le cadre du programme de la Sphère de sécurité étaient alors autorisées à recevoir des données en provenance de l'UE, conformément aux critères d'adéquation de la Directive.

Conscients que de nombreux pays tiers ne pourraient intégrer la courte liste des pays dont les lois offraient une protection adéquate sans avoir besoin de recourir à d'autres systèmes de protection, les législateurs de la Directive inclurent aussi une provision établissant que la Commission européenne aurait l'autorité d'approuver « certaines clauses contractuelles types » comme offrant des protections suffisantes pour permettre le transfert de données vers un pays tiers.

À ce jour, la Commission a approuvé trois ensembles de clauses, souvent qualifiées de « clauses contractuelles types ». Les deux premiers ensembles étaient conçus pour une relation entre un responsable au sein de l'UE et un responsable en dehors de l'UE/EEE (« responsable à responsable »), mais le troisième couvrait une relation de « responsable à sous-traitant », parfaite pour un fournisseur de services automatisés tels qu'un prestataire informatique ou logiciel. Approuvé par la Décision 2010/87/EU, le troisième ensemble agit comme modèle d'accord entre un responsable basé dans l'UE (« exportateur de données ») et un sous-traitant basé aux États-Unis (« importateur de données »). L'accord comprend une série de 12 clauses qui détaillent les obligations du sous-traitant et du responsable, ainsi que les droits des personnes concernées, et deux appendices contenant des lignes vierges afin que l'importateur indique quelles données seront collectées, comment il les traitera et quelles mesures de sécurité il a mises en place.

En octobre 2015, la Cour de justice de l'Union européenne (CJUE) a émis un jugement déclarant la non-validité de la Sphère de sécurité. Suite à une action en justice entreprise par Maximillian Schrems, étudiant autrichien en Droit, et Facebook, la Cour annonça que la Sphère de sécurité ne garantissait pas l'adéquation des transferts de données vers les États-Unis en raison de la faiblesse des recours proposés aux personnes concernées et de l'échec de gérer pleinement l'éventuelle surveillance du gouvernement américain. Des années étant souvent nécessaires pour mettre en place des solutions sur mesure pour garantir l'adéquation, les entreprises se hâtèrent alors d'appliquer les clauses contractuelles types pour des transferts de données autrefois couverts par leur participation au programme de la Sphère de sécurité.

Bien heureusement, les États-Unis et l'UE comprirent rapidement la nécessité d'une solution de remplacement, souvent qualifiée de « Sphère de sécurité 2.0 », et lancèrent des discussions pour mettre en place un nouveau cadre de travail. En juillet 2016, ils publièrent donc la version finale du nouveau système, dénommé bouclier de protection des données UE-États-Unis, qui permettait aux entreprises américaines de se certifier elles-mêmes à compter du 1er août 2016. Le bouclier de protection s'appuie sur les bases de la Sphère de sécurité, avec un processus de certification abordable pour les PME et une applicabilité « générale » à tous les transferts de données concernant les clients européens de toute entreprise américaine certifiée. Toutefois, pour gérer les failles identifiées par le cas *Schrems* dans la Sphère de sécurité, le bouclier de protection comporte de nouveaux engagements pour les droits des personnes concernées, une protection durant le transfert vers des sous-sous-traitants et une coopération entre l'UE et les États-Unis sur les supposées infractions et surveillance gouvernementale.

Le RGPD

Internet a énormément changé depuis l'adoption de la Directive il y a plus de vingt ans. De l'omniprésence de fournisseurs SaaS américains comme Google, Dropbox et Microsoft, à la croissance de l'« internet des choses », les données sont utilisées et partagées de façons inimaginables pour les législateurs de 1995, alors que nombre de foyers ne disposaient pas encore d'une connexion propre et que l'e-commerce peinait à faire des adeptes.

Au-delà de ces changements qui compliquèrent l'application de la Directive, l'UE comprit aussi que le modèle contractuel de la directive possédait une limite fondamentale : en dépit de son objectif d'harmonisation des lois européennes sur le respect de la vie privée, la flexibilité accordée à chaque pays avait donné naissance à des règles dont la rigueur variait grandement.

Les législateurs européens passèrent des années à développer une solution de remplacement qui permettrait d'améliorer l'approche de la Directive, et finirent par mettre en place le Règlement général sur la protection des données (RGPD) en mai 2016. Le RGPD, qui devrait être appliqué à compter de mai 2018, est conçu comme un règlement, et non comme une directive. Il s'applique donc directement à tous les États membres sans que ceux-ci ne doivent adapter leur propre législation. Il s'appuie sur de nombreuses exigences de la Directive pour le respect de la vie privée et la sécurité, mais comprend aussi plusieurs provisions nouvelles afin d'accroître les droits des personnes concernées et de durcir les pénalités en cas d'infraction.

Certains des nouveaux principes du RGPD ont donné lieu à de nombreuses discussions. La Directive s'appliquait aux organisations de l'UE, mais le RGPD concerne aussi les entreprises basées en dehors de l'UE qui vendent leurs produits à des citoyens de l'UE ou qui suivent le comportement de ces derniers. Le RGDP a étendu les normes de divulgation lors de l'obtention du consentement, exigeant que ce consentement se « manifeste de façon libre, spécifique, éclairée et univoque », et que les responsables utilisent des termes juridiques « clairs et simples » qui se « distinguent clairement » d'autres questions. Le règlement intègre aussi deux nouveaux droits pour les personnes concernées : un « droit à l'oubli » exigeant des responsables qu'ils informent les destinataires de telles demandes d'effacement, et un « droit à la portabilité des données » qui permet aux personnes concernées par des données de demander une copie de ces dernières dans un format couramment utilisé. Enfin, plusieurs nouveaux principes sont introduits pour les entreprises qui développent des logiciels et des systèmes gérant des données personnelles, y compris une exigence d'intégration du respect à la vie privée « dès la conception » lors du développement de nouveaux systèmes et une obligation d'effectuer une évaluation d'impact du respect de la vie privée lors du traitement de données par le recours à de « nouvelles technologies » ou susceptible d'engendrer un risque.

Du point de vue de la sécurité, le RGPD exigera de nombreuses entreprises qu'elles comptent en leur sein un Responsable du respect de la vie privée afin de surveiller les efforts liés à la conformité. Ce rôle sera très utile au regard des nouvelles exigences du règlement, qui impliquent que les responsables informent les autorités de contrôle de leur pays en cas de violation des données personnelles, et ce dans les 72 heures suivant le moment où ils en prendront connaissance. Le RGDP préserve actuellement les méthodes approuvées de la Directive pour s'assurer du « caractère adéquat » du transfert de données personnelles vers un pays tiers (y compris de la Sphère de sécurité et des clauses contractuelles types), mais les Responsables du respect de la vie privée permettront aussi de surveiller les relations des responsables avec les sous-traitants qui traitent et hébergent des données personnelles, en les aidant à évaluer les pratiques des sous-traitants en matière de sécurité et en informant les sous-traitants des demandes effectuées par les personnes concernées. La tâche des Responsables du respect de la vie privée devrait être simplifiée par une provision établissant que les entreprises comptant des bureaux dans plusieurs États membres de l'UE disposent d'une « autorité de contrôle chef de file » agissant comme point central de mise en œuvre, afin d'éviter toute incohérence posée par de multiples autorités de contrôle.

L'importance des nouvelles provisions du RGPD est soulignée par les nouvelles pénalités imposées en cas d'infraction. Selon le type d'infraction constatée, les responsables et les sous-traitants qui géreraient mal des données personnelles ou violeraient le droit au respect de la vie privée pourraient avoir à payer une amende allant jusqu'à 20 millions d'euros, ou égale à 4 % de leur chiffre d'affaires annuel global (la somme la plus importante étant retenue).

L'approche juridique adoptée par HubSpot

En 2012, lorsque HubSpot a attiré l'attention d'une audience internationale plus vaste qu'auparavant, ses directeurs ont décidé d'obtenir une certification dans le cadre du programme de la Sphère de sécurité. La société est donc entrée en partenariat avec TRUSTe, une grande entreprise mondiale de gestion du respect de la vie privée qui a certifié ses pratiques afin de se conformer aux termes du programme de la Sphère de sécurité de l'UE. Pour les clients allemands en quête d'un niveau supérieur de protection conforme à la Loi fédérale sur la protection des données, HubSpot proposait aussi un appendice de traitement des données faisant référence à plusieurs exigences de la législation allemande, et notamment à certaines protections applicables au transfert intracommunautaire de données de clients allemands vers le bureau irlandais de HubSpot.

Lorsque la Sphère de sécurité fut attaquée devant la Cour de justice et que ses clients potentiels commencèrent à poser des questions sur les options possibles, HubSpot se mit à rechercher d'autres solutions. Elle opta pour les Clauses contractuelles types, jugées comme étant la meilleure option, offrit ainsi des protections contractuelles étendues à ses clients et établit des délais de mise en place relativement rapides par rapport à d'autres options, dont certaines pouvaient exiger des années. Une fois le nouveau programme de bouclier de protection annoncé, HubSpot prit également la décision de se certifier.

Aujourd'hui, la société maintient sa Certification au bouclier de protection auprès du Département du Commerce américain afin de s'assurer que les protections adéquates sont mises en place lorsque des données personnelles sont transférées entre l'UE et les États-Unis. Elle a également intégré des informations sur sa certification au bouclier de protection dans ses conditions générales d'utilisation (section relative au Traitement des données UE/États-Unis) et dans ses clauses de confidentialité.

À l'approche de mai 2018, HubSpot se concentre aussi sur ses efforts de mise en conformité avec le RGPD. Au cours la période de mise en œuvre du règlement, la société évalue les nouvelles exigences et restrictions imposées et entreprendra toutes les actions nécessaires

pour s'assurer qu'elle gérera les données de ses clients dans le respect de la législation applicable dès mai 2018. D'ici cette date, elle publiera des informations sur les étapes entreprises pour s'assurer que ses processus et ses produits sont conformes aux termes du RGPD bien avant sa date d'application, et conseille aux parties intéressées de consulter sa page du respect de la vie privée pour se tenir informées des mises à jour effectuées. Elle procédera aussi à une mise à jour de ses documents juridiques avant l'échéance afin de refléter tous les changements apportés aux produits et de s'assurer qu'en tant que sous-traitant des données personnelles de ses clients, elle répond aux exigences applicables au regard du règlement.

Chaque entreprise étant différente, et le RGPD adoptant une approche basée sur le risque de la protection des données, les entreprises devraient donc évaluer leurs propres pratiques de collecte et d'hébergement de données (y compris les façons dont elles utilisent les logiciels HubSpot Marketing et HubSpot Sales), en consultant leurs propres avocats afin de s'assurer que leurs pratiques professionnelles sont conformes aux termes du RGPD.

L'approche adoptée par HubSpot pour la sécurité

Au regard de la complexité des lois européennes relatives au respect de la vie privée, les clients de HubSpot posent souvent des questions sur des aspects des produits ou sur le programme de sécurité de la société. Lorsqu'ils comprennent mieux la technologie HubSpot, ils peuvent ainsi travailler avec leur avocat pour vérifier que leur propre entreprise se conforme aux lois applicables.

Cookies

En 2002, l'UE a adopté la Directive sur la vie privée et les communications électroniques (2002/58/EC). Cette Directive s'appuie sur la directive sur le respect de la vie privée en se concentrant sur la protection applicable aux communications électroniques, comme les données liées au trafic et les e-mails non sollicités. Elle établit, en particulier, un régime d'abonnement au regard duquel le consentement préalable du destinataire est requis avant l'envoi d'e-mails. Cette première Directive fut amendée en 2009 (2009/136/EC) pour exiger la divulgation et le consentement pour l'usage autorisé des cookies.

HubSpot utilise des cookies pour améliorer l'expérience des visiteurs et des utilisateurs de sa plateforme. La société divulgue tous les cookies employés et fournit toutes les informations nécessaires dans sa documentation. Elle utilise généralement des cookies afin de fournir une expérience sécurisée aux utilisateurs connectés au portail, et pour aider à mesurer l'engagement des visiteurs du site avec le contenu publié sur des portails HubSpot.

La plateforme HubSpot utilise aussi des cookies pour aider ses clients à comprendre comment les visiteurs de leur site web et leurs prospects s'engagent avec le contenu produit. Un cookie est un petit fichier enregistré sur l'ordinateur des personnes consultant un site web. Lorsqu'un visiteur parvient sur un site, HubSpot enregistre ainsi un cookie sur son ordinateur afin de l'identifier de manière unique. Les cookies servent aussi à activer des fonctionnalités comme le contenu intelligent, grâce auquel les visiteurs voient un contenu personnalisé en fonction de leurs visites précédentes.

La plateforme HubSpot peut ainsi indiquer avec quelles parties d'un site les visiteurs interagissent ou lesquelles ils consultent. Si un visiteur choisit volontairement de fournir ses coordonnées, le cookie enregistré dans son navigateur sera associé à la fiche d'informations nouvellement créée pour ce contact. Les informations de navigation sont ainsi disponibles dans les portails des clients et dans la fiche d'informations de chaque contact. Les cookies ne peuvent pas servir à identifier une personne qui a choisi de ne pas fournir ses coordonnées. Les informations liées aux visites ultérieures ne sont associées à des contacts que s'ils ont décidé de fournir leurs coordonnées.

Les visiteurs d'un site attachent beaucoup de valeur à la transparence des entreprises concernées. Afin de soutenir les efforts de transparence, la plateforme HubSpot permet à ses utilisateurs d'activer les notifications de respect de la vie privée. Pour en savoir plus sur ces notifications, vous pouvez consulter cet article sur les fenêtres contextuelles de respect de la vie privée.

Fonctionnalités des e-mails

L'outil E-mails de HubSpot comporte différentes fonctionnalités qui peuvent améliorer l'efficacité des équipes marketing et commerciales, et réduire le nombre de communications non sollicitées par vos destinataires et par vos prospects potentiels.

La plateforme HubSpot permet ainsi de configurer votre portail de façon à s'assurer que les contacts sont intéressés par votre contenu. Avec la fonctionnalité de confirmation d'inscription

aux e-mails, vous savez réellement que vos contacts souhaitent recevoir vos messages. Pour en savoir plus sur l'activation de cette fonctionnalité, consultez cet article sur la confirmation d'inscription aux e-mails. Les contacts peuvent ainsi confirmer qu'ils s'intéressent à votre contenu. Les nouveaux contacts montrent leur intérêt en fournissant leurs coordonnées sur vos pages de destination. Avant de lire votre premier e-mail, ils doivent confirmer leur désir de recevoir vos communications. Lorsque la fonctionnalité de confirmation d'inscription aux e-mails est activée dans votre portail, vous pouvez affirmer que votre audience et votre société se portent un intérêt mutuel.

Les produits HubSpot permettent de connaître les taux d'ouverture et de lecture des e-mails, et ainsi de prendre des décisions informées. Pour en savoir plus sur la façon dont HubSpot a utilisé les informations liées à l'engagement de ses abonnés pour supprimer des milliers d'entre eux de sa liste de destinataires, consultez cet article de blog sur le greymail.

Afin de fournir des données sur le niveau d'engagement des destinataires des e-mails, les produits HubSpot s'appuient sur un outil dénommé « pixel de suivi ». Celui-ci utilise des images comme ressources afin de savoir si les destinataires ouvrent les e-mails envoyés via un produit HubSpot. Lorsqu'un e-mail est envoyé avec les logiciels HubSpot Marketing et HubSpot Sales, une balise d'image pour une image minuscule est intégrée dans le corps du texte. Lorsque l'un de vos destinataires ouvre l'e-mail concerné, son client de messagerie, s'il est configuré pour cela, effectue une demande auprès de la plateforme HubSpot afin d'afficher l'image, ce qui se traduit par le taux d'ouverture affiché dans votre portail. Ces demandes de pixels ne comprennent pas de données personnelles pouvant servir à identifier un destinataire, et elles sont obscurcies par une chaîne de requête aussi longue qu'aléatoire.

Hébergement de données

La plateforme HubSpot et les données enregistrées par HubSpot sont hébergées par des fournisseurs de centre de données tiers de confiance basés aux États-Unis. HubSpot travaille avec les plus grands fournisseurs de centres de données au monde pour fournir ses services. À ce jour, l'infrastructure primaire de HubSpot est hébergée par Amazon Web Services dans la région USA Est (Virginie du Nord). Amazon Web Services possède les certifications ISO 27001, SOC 2 Type II et plusieurs autres pour témoigner de la rigueur appliquée à son programme d'hébergement et de gestion d'infrastructure. Pour en savoir plus à ce sujet, vous pouvez consulter la page des programmes de conformité d'AWS.

Programme de sécurité

HubSpot est responsable de la sécurité des données qui lui sont confiées et la société s'attache à être transparente dans la manière dont elle protège les données de ses clients. Vous pouvez prendre connaissance des informations relatives à son programme de sécurité sur la page Protection des données et systèmes à grande échelle de HubSpot, ainsi que dans votre portail, dans la section Paramètres > Comptes et facturation > Centre de documentation > Présentation des risques et de la sécurité.

Le programme de sécurité de HubSpot comprend un système avancé de détection et de prévention des risques et des attaques, un système de suivi et de notification assuré 24h/24 et 7j/7 ainsi qu'un système avancé de découverte des bugs. La plateforme intègre différents niveaux de redondance et de basculement. Elle est hébergée dans des centres de données qui sont réputés pour leur fiabilité. L'expérience HubSpot s'appuie sur une distribution de contenu ultramoderne afin que vos visiteurs et vous-même puissiez vous déplacer rapidement sur des pages web, et ce à tout endroit du monde.

Modification des données et autres demandes liées au respect de la vie privée

Chaque personne fournissant ses coordonnées à HubSpot est en droit de demander à ne pas être contactée ou de demander à corriger les informations qui la concernent. L'équipe chargée du respect de la vie privée, joignable à l'adresse privacy@hubspot.com, a pour rôle de s'assurer que HubSpot joue en permanence une influence positive sur les communautés de la vente et du marketing de contenu.

Les demandes envoyées à HubSpot sont automatiquement transmises à un spécialiste d'astreinte. Chaque demande est ensuite suivie au cours de son cycle de vie entier, de sa réception à sa conclusion, et HubSpot peut faire appel à des ressources complémentaires si les circonstances l'exigent. Davantage d'informations sur l'approche adoptée par HubSpot sont disponibles dans les clauses de confidentialité de la société.

Envisager l'avenir

Le respect de la vie privée est un sujet qui évolue en permanence au sein de l'UE, et qui a connu des modifications à un rythme rapide au cours des dernières années. La société HubSpot se tient informée des mises à jour dans ce domaine, en s'appuyant sur des relations

privilégiées avec des cabinets juridiques régionaux et des prestataires de services spécialisés dans la sécurité des données, comme TRUSTe, afin de s'assurer que ses produits et ses processus demeurent conformes à la législation lorsque des règlements sont adoptés ou supprimés. Les membres de l'équipe juridique de HubSpot partagent également les mises à jour avec la société entière lorsque des modifications de la législation affectent son travail ou ses clients.

HubSpot pense que la meilleure approche possible consiste à proposer aux clients basés dans l'UE/EEE des clauses supplémentaires dans ses conditions générales d'utilisation afin de mentionner sa certification au bouclier de protection. Au fil de la transition entre le programme de la Sphère de sécurité et celui du bouclier de protection, HubSpot évaluera toutefois les nouvelles options disponibles pour s'assurer de la conformité du transfert de données à l'extérieur de l'UE. Au cours des mois qui précéderont mai 2018, la société intégrera les efforts liés au respect du RGPD dans ses opérations quotidiennes et dans ses produits, et publiera les mises à jour correspondantes sur la page http://legal.hubspot.com/data-privacy.

La société se voit parfois demander si elle envisage d'ouvrir un centre de données dans l'UE. Cette question se pose car HubSpot fait appel aux services d'AWS, une entreprise basée aux États-Unis, pour l'hébergement de ses données, comme mentionné plus haut. HubSpot étudie actuellement la possibilité d'héberger des données dans l'UE et, sans pouvoir toutefois proposer de date précise, tiendra ses clients informés dès qu'elle en saura davantage sur les options disponibles.

HubSpot se tiendra également informée de chaque nouveau développement lié aux lois sur le respect de la vie privée, aux meilleures pratiques en matière de sécurité et aux plateformes logicielles internationales, afin de préserver la sécurité des données de ses clients et de s'assurer de sa conformité avec la législation applicable. Lorsqu'une nouvelle loi est applicable, HubSpot travaille avec des avocats et d'autres ressources externes afin de vérifier que son plan d'action couvre toutes les modifications nécessaires. Au-delà de toutes ces considérations, l'objectif ultime de HubSpot est de s'assurer qu'elle préserve ce qui lui importe le plus : la confiance de ses clients.

Autres ressources

Si vous avez d'autres questions, n'hésitez pas à consulter ces ressources apportant des réponses plus détaillées :

- **Généralités**
  - Protection des données, Commission européenne
  - Manuel de droit européen en matière de protection des données, Agence des droits fondamentaux de l'Union européenne (2014)

- **Transfert de données en dehors de l'Union européenne**
  - Clauses contractuelles types pour le transfert de données personnelles vers des pays tiers, Union européenne (2010)
  - Updated EU Model Clauses, WilmerHale (2010)
  - The Demise of the US-EU Safe Harbor, Hunton & Williams (2015)
  - Privacy Shield Program Overview, U.S. Département du Commerce (2016)
  - GDPR - Cross-border data transfers, Loyens Loeff (2017)

- **Règlement général sur la protection des données de l'Union européenne**
  - Régulation (UE) 2016/679 [RGPD], Union européenne (2016)
  - A Brief History of the GDPR, IAPP (2016)
  - General Data Protection Regulation Guide, Jones Day (2017)
  - A Guide to the General Data Protection Regulation, DLA Piper (2016)
  - Unlocking the EU General Data Protection Regulation, White & Case (2016)
  - GDPR Compliance Update: Which Government Authorities Have Issued Official GDPR Guidance?, Proskauer (2017)

- **Cookies et adresses IP**
  - IP Addresses as Personal Data, Orrick (2016)
  - EU regulators welcome stricter rules on cookies and direct marketing, White & Case (2017)