



LIVRE BLANC

Confidentialité dès la conception

Comment les services Bot Manager Premier et Page Integrity Manager d'Akamai respectent les exigences européennes en matière de confidentialité

Présentation

Akamai comprend que la protection des données personnelles et le respect des exigences en matière de confidentialité sont essentiels pour établir la confiance en nos technologies et nos services. Ce livre blanc explique comment Bot Manager Premier¹ et Page Integrity Manager respectent la directive européenne « vie privée et communications électroniques » et le Règlement général sur la protection des données (RGPD)² afin que vous puissiez évaluer les risques associés au fonctionnement de ces services.

Bot Manager Premier est conçu pour détecter les demandes d'accès à vos propriétés Web automatisées générées par des (ro)bots qui imitent

le comportement humain pour collecter et exploiter les données de connexion des utilisateurs finaux. Page Integrity Manager détecte les JavaScripts injectés dans ces propriétés à des fins abusives. Une fois les bots et les scripts détectés, Akamai les classe comme activités non malveillantes ou malveillantes, conformément à vos instructions, aux connaissances communes et à nos informations sur les menaces. Les activités malveillantes seront bloquées et seuls les bots et les scripts non malveillants pourront accéder à vos serveurs, à votre infrastructure et à vos données d'origine.

Ces deux services protègent les données personnelles fournies par les utilisateurs finaux contre l'exfiltration et les utilisations abusives. L'importance de la protection contre de telles menaces a été démontrée par les récentes violations de sécurité et de données dont ont été victimes [British Airways](#) et [The North Face](#).

Architecture de Bot Manager Premier

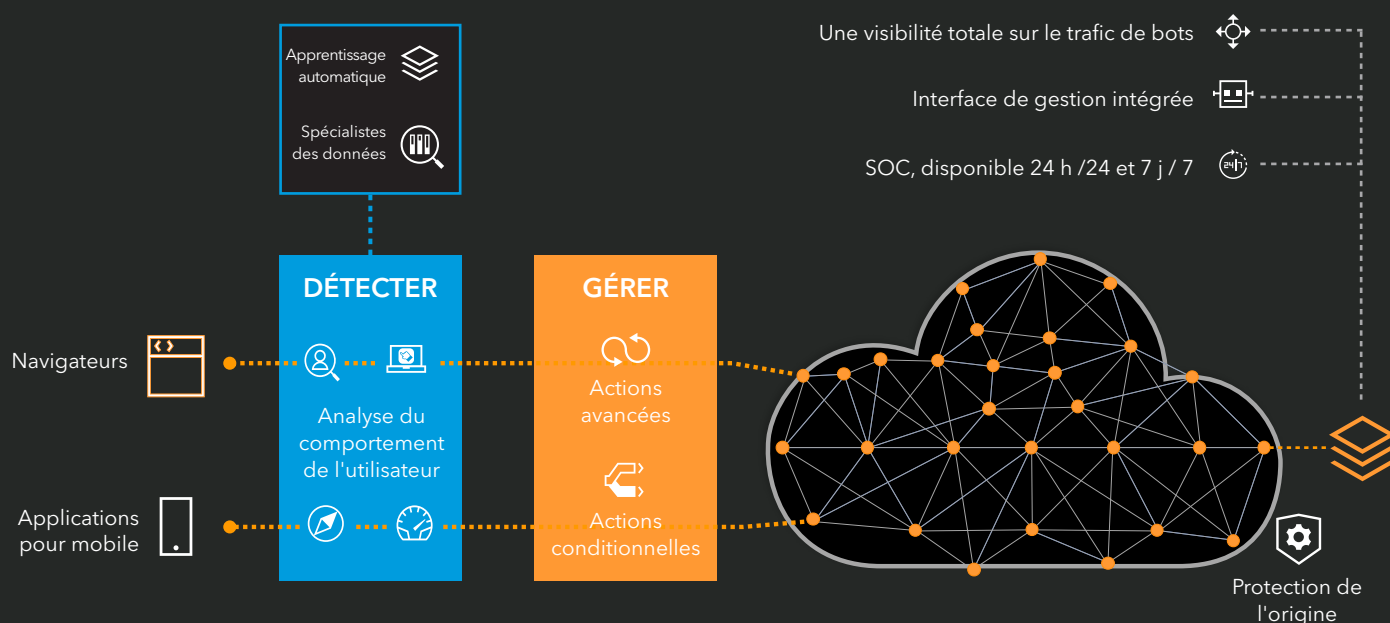


Fig. 1 : Architecture de Bot Manager Premier

Architecture de Page Integrity Manager

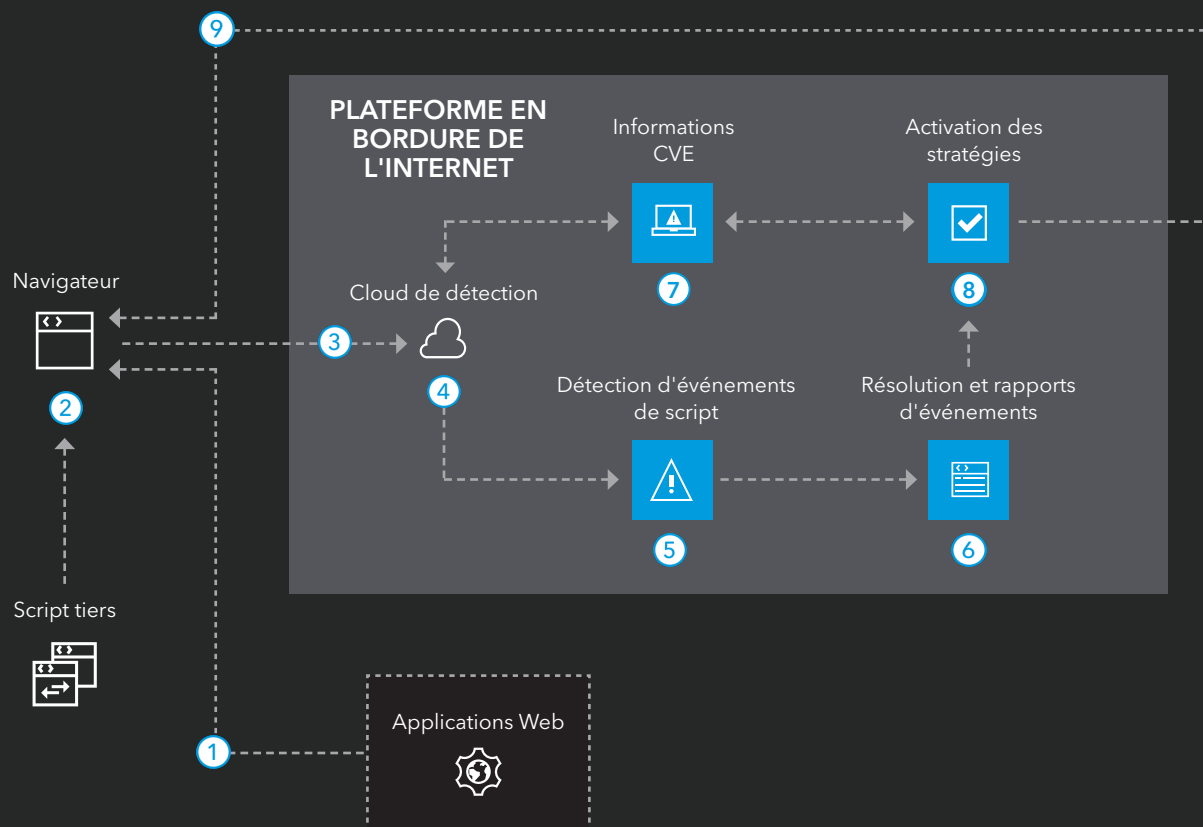


Fig. 2 : Architecture de Page Integrity Manager

D'un point de vue technique, la détection de bots et de scripts s'effectue via l'injection de JavaScript ou l'intégration du kit de développement logiciel (SDK) d'application pour mobile, ainsi que par le biais des analyses des données de comportement, de réseau et de navigateur recueillies. Bot Manager Premier analyse les données pour déterminer si l'activité provient d'un bot ou d'un humain, tandis que Page Integrity Manager identifie tous les scripts injectés dans les propriétés Web. Toutes les activités de bot et de script détectées sont alors classées comme activités malveillantes ou non malveillantes, et ces dernières sont bloquées afin d'éviter l'exfiltration des données.

Du point de vue de la confidentialité, l'injection de JavaScript et l'intégration du SDK sont classées comme « technologie de cookies » par les lois de l'UE et déclenchent donc l'application de la directive européenne « vie privée et communications électroniques ». En outre, certains des éléments de données recueillis, par exemple l'adresse IP de l'utilisateur final, sont classés comme des données personnelles et déclenchent l'application du RGPD.

Conformité aux lois européennes « vie privée et communications électroniques »

Pour utiliser la technologie de cookies Bot Manager Premier et Page Integrity Manager conformément aux lois européennes sur la protection de la vie privée, deux exemptions issues des règles générales s'appliquent : l'exemption de consentement et l'exemption de mécanisme de refus. Ces exemptions vous permettent de placer Bot Manager Premier et Page Integrity Manager sur vos propriétés Web pour une utilisation immédiate.

Application de l'exemption de consentement

Par défaut, la directive « vie privée et communications électroniques » exige de recueillir le consentement de l'utilisateur final pour l'utilisation de toute technologie de cookies et la collecte de données associée. Ce n'est que lorsque le cookie est strictement nécessaire pour fournir un service de la société de l'information (sur vos propriétés Web) explicitement demandé par un abonné ou un utilisateur (l'utilisateur final) que le consentement d'une personne pour l'utilisation du cookie n'est pas requis et que la technologie de cookie peut fonctionner sans délai.³

La plupart des pays membres de l'UE ont repris cette exception dans leurs lois locales de transposition de la directive « vie privée et communications électroniques ».

La technologie de cookies utilisée pour Bot Manager Premier et Page Integrity Manager est nécessaire au fonctionnement des services. Sans l'injection de JavaScript, aucune donnée ne peut être collectée et analysée, et les bots ou scripts ne seront pas détectés ni bloqués. Les données sont collectées dans le but de protéger les données personnelles fournies via vos propriétés Web contre les compromissions, l'exfiltration et les utilisations

abusives. Les autorités locales chargées de la protection des données ont confirmé que l'utilisation de la technologie de cookies pour la prévention contre la fraude et d'autres services de sécurité relève de l'exemption de consentement.⁴ Le tableau suivant indique comment l'Information Commissioner's Office (ICO) du Royaume-Uni décrit l'application de l'exemption de consentement pour les services de sécurité.⁵

Activité	Est-elle susceptible de remplir les conditions d'une exemption ?
Sécurité	En fonction de la limitation de finalité. Les cookies internes utilisés à des fins de sécurité peuvent bénéficier de l'exemption strictement nécessaire ; par exemple, les cookies utilisés pour détecter les tentatives de connexion échouées répétées. Leur durée peut également être plus longue que celle d'un cookie de session. Toutefois, les cookies liés à la sécurité d'autres services en ligne (les vôtres exclus) nécessitent un consentement. Cela est dû au fait que la fonctionnalité demandée par l'utilisateur est liée à votre service et non à ceux d'autres entités. Si vous utilisez les techniques d'empreinte des terminaux à des fins de sécurité spécifiques, vous pouvez également bénéficier de l'exemption strictement nécessaire. Toutefois, comme pour les cookies, si les informations sont traitées à des fins secondaires (par exemple, les informations relatives à la sécurité des services en ligne que l'utilisateur n'a pas demandé), le consentement est requis. Cela s'applique également lorsque les informations sont traitées à des fins de prévention contre la fraude, en particulier dans les cas où plusieurs services en ligne utilisent un seul service de prévention contre la fraude qui traite les informations des visiteurs de tous ces services.

Application de l'exemption de refus

Les lois « vie privée et communications électroniques » exigent que les entités proposent aux utilisateurs finaux un mécanisme permettant de refuser la collecte de données via la technologie de cookies. Cette exigence reflète le droit de contester cette collecte en vertu de l'article 21 du RGPD.⁶

Cependant, il existe un cas spécifique où ce droit de contrôle ne pourra être respecté et où son exercice dérogatoire empêchera l'exécution des activités de protection des données : l'exécution d'un service de sécurité basé sur la technologie de cookies.

Le fait de refuser l'utilisation de la technologie de cookies utilisée pour détecter les bots et les scripts malveillants interrompt les services de sécurité qui protègent les données personnelles contre les accès non autorisés. À condition que la technologie de cookies soit utilisée uniquement à des fins de sécurité, l'absence de contrôle sur la collecte des données par le biais de la technologie de cookies ne porte pas atteinte aux droits et libertés de l'utilisateur final. En revanche, cette absence de contrôle garantit le fonctionnement continu de la technologie de cookies qui protège les données personnelles contre les accès non autorisés.

Les professionnels de la protection de la vie privée du monde entier s'entendent sur l'exigence de cette exemption de refus : lorsqu'un mécanisme de contrôle des données proposé aux individus (utilisateurs finaux) peut ne pas être appliqué afin de permettre l'accès aux données de manière non autorisée, le mécanisme de contrôle des données est inutile et ne doit pas être mis en place. En d'autres termes, il est logique qu'un fonctionnement fluide de services de sécurité de pointe l'emporte sur la nécessité de proposer un mécanisme de contrôle des données (dérogation) lié à la technologie de cookies.⁷

Conformité aux lois européennes en matière de protection des données

Bot Manager Premier et Page Integrity Manager traitent les données conformément au RGPD et aux autres lois applicables en matière de protection des données ou de la vie privée, y compris le type de données personnelles recueillies et le but de la collecte.

Type de données personnelles

Bot Manager Premier et Page Integrity Manager collectent des données de réseau, de navigateur et de comportement telles que la session TCP, la session TLS, l'ID de session, l'agent utilisateur, l'en-tête de demande, les URL visitées, l'horodatage, l'adresse IP de l'utilisateur final, les paramètres du navigateur et les données de géolocalisation des serveurs en bordure de l'Internet, ainsi que les données de comportement telles que les sélections d'écran, les mouvements de la souris et les pressions sur les touches du clavier.

Objectif

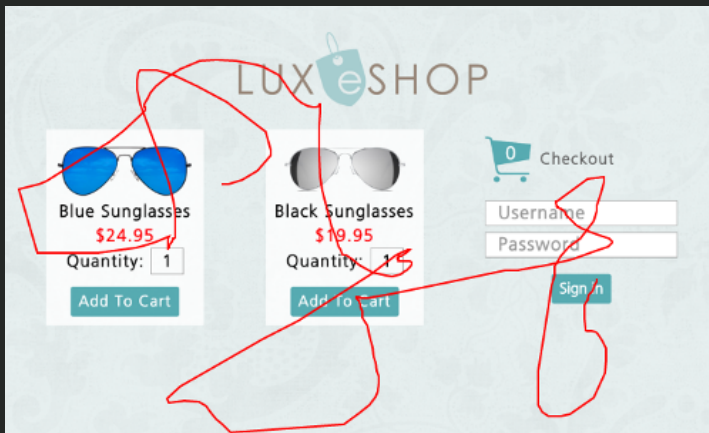
Le but de la collecte et de l'analyse des données est de détecter les bots et les scripts malveillants imitant le comportement humain dans vos propriétés Web, ainsi que d'éviter que ces derniers exfiltrent les données en vue de les utiliser à des fins abusives.

Pour ce faire, Akamai analyse la façon dont un terminal est utilisé lors de l'accès à vos propriétés Web. Akamai n'identifie pas l'utilisateur final lors de cette analyse ni lors de la création de profils d'utilisateurs finaux. En outre, les données sur le comportement recueillies ne sont pas utilisées dans le but d'identifier une personne de manière unique. Les données n'ont donc pas besoin d'être classées comme données biométriques dans le cadre du RGPD.⁸ Il ne s'agit donc ni de données sensibles (en termes américains) ni de catégories spéciales de données (en termes européens).

Akamai collecte et analyse les données de comportement afin de déterminer si l'accès à votre propriété Web est réalisé par un bot ou un humain, comme indiqué dans les figures ci-dessous.

Événements de la souris

Exemple humain



Exemples de bot

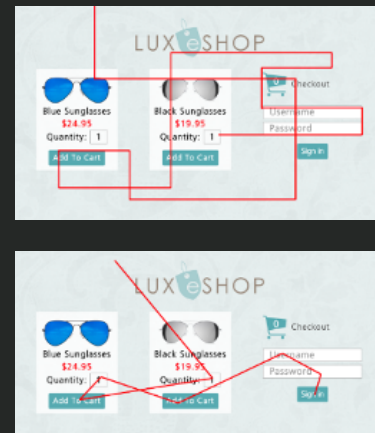
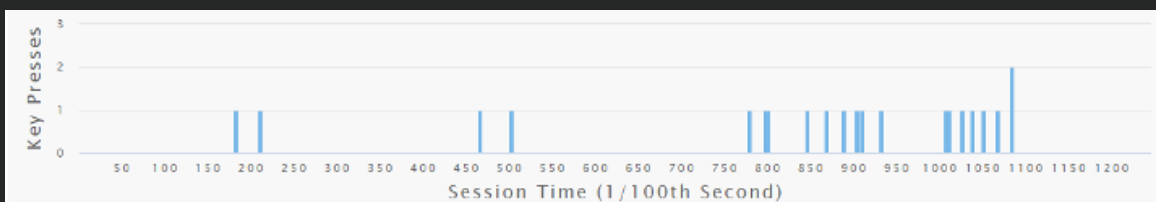


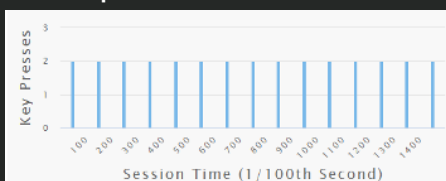
Fig. 3 : Les bots sophistiqués tenteront de passer inaperçus en déclenchant des mouvements de la souris. Ils sont conçus pour imiter l'interaction d'un utilisateur. Toutefois, après un certain nombre de mouvements, un motif se distingue. Akamai est en mesure de détecter ces motifs pour identifier un bot.

Détection du motif de pression des touches

Pressions de touches initiées par un humain



Exemple de pressions de touches initiées par un bot



Exemple de pressions de touches initiées par un bot

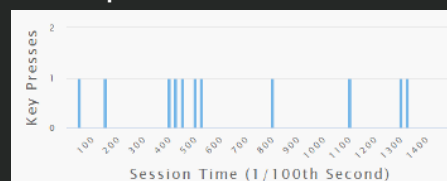


Fig. 4 : Les pressions de touches initiées par des humains sont généralement plus aléatoires qu'un bot, même sophistiqué. En examinant la vitesse et la cadence des pressions de touches d'un humain, Akamai est ensuite capable de déterminer si un utilisateur est un bot.

Base juridique

La base juridique pour le traitement des données est l'intérêt légitime d'Akamai de fournir des services de sécurité de réseau et de l'information sous forme de détection et de blocage de bots et de scripts malveillants. L'intérêt légitime est une base juridique reconnue pour l'exécution de services de sécurité dans le cadre du RGPD.⁹

Akamai diffuse et sécurise jusqu'à 30 % du trafic Internet total. Sans ses services de gestion de scripts et de bots, il y aurait beaucoup plus d'exfiltration et d'abus de données en ligne qui porteraient atteinte aux droits et aux libertés des utilisateurs finaux.

Évaluation de la nécessité et de la proportionnalité

Le traitement des données est nécessaire pour que les services de sécurité de réseau et de l'information d'Akamai soient considérés comme des services de pointe en vertu des lois sur la protection de la vie privée. En analysant les données collectées sur le réseau, le navigateur et le comportement, Akamai peut identifier précisément les actions et les scripts initiés par un bot ou un humain injectés dans une propriété Web.

L'analyse de tous les éléments de données recueillis est proportionnelle à la sophistication des bots et des scripts actuels. La réduction de la collecte de données a un impact sur la précision de l'analyse, ce qui se traduit par une détection moins efficace des activités malveillantes. Les bots ne peuvent pas être détectés en analysant uniquement les adresses IP des utilisateurs finaux. Bien que les informations sur le navigateur et le réseau renseignent sur l'utilisation du terminal, elles sont limitées aux mécanismes passifs basés sur des signatures et sont sujettes à des taux élevés de faux positifs et de faux négatifs. La sécurité de pointe pour les propriétés Web¹⁰ s'étend à la détection des bots sophistiqués. Les bots actifs qui imitent le comportement humain ne sont détectés qu'une fois les données de comportement analysées.

Recueillir davantage de données serait excessif, car cela n'améliorerait pas les analyses.

Évaluation des risques

Le risque pour les droits et les libertés des utilisateurs finaux associé aux activités de traitement de Bot Manager Premier et de Page Integrity Manager est faible. Les données de navigateur, de réseau et de comportement ne sont pas classées comme hautement confidentielles, sensibles ou comme une catégorie spéciale de données personnelles.¹¹ Les activités de traitement d'Akamai liées à Bot Manager Premier et à Page Integrity Manager sont décrites dans la [Déclaration de confidentialité d'Akamai](#) et rendues transparentes pour les parties intéressées. Akamai respecte le principe de minimisation des données, en collectant uniquement les données nécessaires à la détection des bots et de JavaScript.

Akamai a mis en place des mesures techniques et organisationnelles appropriées en vue de protéger les données personnelles traitées contre tout accès tiers non autorisé. Ces mesures sont également publiées de manière transparente sur notre site Web : [Programme InfoSec d'Akamai](#) et [Mesures techniques et organisationnelles d'Akamai](#).

Les analyses pour la détection de bots et de scripts sont effectuées sur les systèmes Akamai déployés aux États-Unis. Par conséquent, lorsque les utilisateurs finaux européens accèdent à des propriétés Web protégées par Bot Manager Premier et Page Integrity Manager, les analyses nécessitent le traitement de données personnelles de l'UE aux États-Unis. Pour garantir une protection des données suffisante lorsque leur traitement est réalisé aux États-Unis, Akamai a adopté les Clauses contractuelles standard de l'UE au sein du groupe Akamai, avec nos clients et nos sous-traitants, et mis en œuvre des mesures de protection techniques supplémentaires afin de protéger les données personnelles contre les accès tiers lorsqu'elles sont traitées aux États-Unis.

Akamai applique la même exigence de protection des données à toutes les entités du groupe, indépendamment de l'emplacement de l'entité Akamai. Nous avons mis en place des mesures supplémentaires pour protéger les données transférées contre les accès tiers. De plus, selon Akamai, les données transférées aux États-Unis par Akamai pour Bot Manager Premier et Page Integrity Manager ne sont pas le type de données auquel les agences de surveillance (américaines) s'intéressent lors de leurs opérations de surveillance.¹² La plupart des données sont en libre accès, car elles sont nécessaires pour établir une connexion Internet et un tiers n'a pas besoin de se rapprocher d'Akamai pour recueillir ces données. Il existe de nombreux autres moyens plus pratiques que les tiers peuvent utiliser pour accéder à ces données. Par conséquent, Akamai a estimé que les risques d'accès tiers aux données transférées aux États-Unis pour Bot Manager Premier et Page Integrity Manager étaient minimes. Plus de détails sont fournis dans la [Déclaration de transfert de données d'Akamai](#) disponible via le Centre de confiance pour la protection de la vie privée d'Akamai.

Conformément au principe de minimisation et de sécurité des données, Akamai a fixé la période de conservation à 90 jours. Cette période est appropriée compte tenu de la nécessité d'analyser les données de réseau, de navigateur et de comportement sur une certaine période dans toutes les régions pour permettre la détection de bots et de scripts la plus efficace.

Les services de détection et de gestion de bots et de scripts d'Akamai assurent non seulement la sécurité de vos propriétés Web, mais améliorent également l'état général d'Internet. En détectant et en bloquant les bots et les scripts sur l'Intelligent Edge Platform d'Akamai, nous empêchons non seulement l'exfiltration et l'utilisation à des fins malveillantes de vos données personnelles d'utilisateur final, mais nous nous efforçons également d'obtenir des informations sur les menaces pour les services de réseau et de sécurité au profit de millions d'utilisateurs finaux.

Mesures d'atténuation

Akamai a atténué tous les risques identifiés pour les droits et les libertés du sujet des données lors de l'exécution des services Bot Manager Premier et Page Integrity Manager, où qu'ils se trouvent. Lors de la collecte des données de comportement, l'utilisateur final n'est pas identifié. En outre, Akamai a correctement sécurisé les données personnelles et mis en place des mesures supplémentaires pour garantir que les données transférées sont protégées de manière adéquate contre les accès tiers.

Synthèse

Les services Bot Manager Premier et Page Integrity Manager d'Akamai sont conformes aux lois européennes sur la protection des données. La technologie de cookies utilisée pour le fonctionnement des services est strictement nécessaire et permet la protection des données personnelles de l'utilisateur final. Les exemptions de consentement obligatoire et de mécanisme dérogatoire sont donc applicables.

La collecte de données requise pour exécuter les services est légitime, nécessaire et proportionnelle. De plus, les mesures d'atténuation mises en place garantissent que le risque envers les droits et les libertés des utilisateurs finaux relatif aux activités de traitement est très faible. Les avantages de l'exécution de Bot Manager Premier et de Page Integrity Manager pour vos utilisateurs finaux et d'autres utilisateurs en ligne l'emportent sur les risques, car tout le monde bénéficie d'un Internet plus sécurisé.



Akamai Technologies
Dr. Anna Schmits, EMEA DPO

Sources :

1. Les déclarations ci-après s'appliquent également à Akamai Service Bot Manager Standard, à l'exception de la portée de la collecte de données, qui est limitée aux données du réseau et du navigateur. En savoir plus sur Akamai Bot Manager : https://learn.akamai.com/en-us/products/cloud_security/bot_manager.html
2. Voir « Protection de la vie privée digitale », disponible à l'adresse : <https://ec.europa.eu/digital-single-market/en/online-privacy>
3. Voir la modification de l'article 5 (3) de la directive 2002/58/CE « vie privée et communications électroniques » par la directive 2006/24/CE, disponible à l'adresse suivante : <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN>.
4. Voir, par exemple, les directives relatives aux cookies de l'ICO du Royaume-Uni, disponibles à l'adresse <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules9>, les directives de la CNIL, disponibles à l'adresse <https://www.cnil.fr/en/cookies-and-other-tracking-devices-council-state-issues-its-decision-cnil-guidelines>, ou les directives du Comité des autorités allemandes (en allemand uniquement), disponibles à l'adresse https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.
5. Voir les conseils sur les cookies de l'ICO, disponibles à l'adresse suivante : <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply16>.
6. Voir l'article 21 (1) du RGPD, disponible à l'adresse suivante : <https://gdpr-info.eu/art-21-gdpr/>.
7. Voir, par exemple, les conseils de l'ICO, disponibles à l'adresse suivante : <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules9>.
8. Voir l'article 9 (1) du RGPD, disponible à l'adresse suivante : <https://gdpr-info.eu/art-9-gdpr/>.
9. Voir le préambule 49 du RGPD, disponible à l'adresse suivante : <https://gdpr-info.eu/recitals/no-49/>
10. Comme l'exige l'article 32 du RGPD, disponible à l'adresse suivante : <https://gdpr-info.eu/art-32-gdpr/>
11. Voir l'article 9 du RGPD, disponible à l'adresse suivante : <https://gdpr-info.eu/art-9-gdpr/>
12. U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II, septembre 2020. Disponible à l'adresse : <https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF>



Akamai sécurise et diffuse des expériences digitales pour les plus grandes entreprises du monde entier. L'Intelligent Edge Platform d'Akamai englobe tout, de l'entreprise au cloud, afin d'offrir rapidité, agilité et sécurité à ses clients et à leurs entreprises. Les plus grandes marques mondiales comptent sur Akamai pour les aider à concrétiser leur avantage concurrentiel à travers des solutions agiles qui augmentent la puissance de leurs architectures multiclouds. Akamai place les décisions, les applications et les expériences au plus près des utilisateurs, et au plus loin des attaques et des menaces. Les solutions de sécurité en bordure de l'Internet, de performances Web et sur mobile, d'accès professionnel et de diffusion vidéo du portefeuille d'Akamai s'appuient également sur un service client exceptionnel, des analyses et une surveillance 24 h/24 et 7 j/7, 365 jours par an. Pour savoir pourquoi les plus grandes marques internationales font confiance à Akamai, visitez www.akamai.com, blogs.akamai.com ou @Akamai sur Twitter. Vous trouverez nos coordonnées dans le monde entier à l'adresse www.akamai.com/locations. Publication : 03/21.