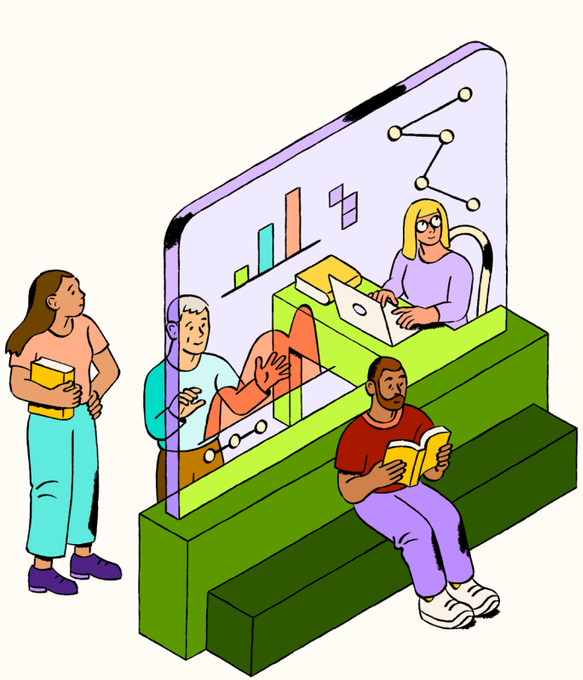
ZENDESK INSIGHTS

Faciliter la gestion des risques liés à la confidentialité des données de CX

zendesk
CX Trends 2024



Comme l'a révélé le rapport CX Trends 2024 de Zendesk, les responsables de l'expérience client (CX) sont désormais un moteur clé, avec leurs équipes informatique et juridique, dans la prise de décisions sur les données et la confidentialité, car ce sont les informations qui alimentent les expériences personnalisées et pilotées par l'IA. Si les clients réclament des expériences personnalisées, ils exigent également des pratiques à toute épreuve en matière de sécurité des données.

Cet enjeu est crucial, comme pourra vous le dire toute entreprise qui a déjà été victime d'une faille de sécurité. Les responsables de CX qui ne prennent pas la question à bras le corps pourraient, sans le savoir, exposer leur entreprise à des risques considérables.

Pour eux, trouver un équilibre entre l'exploitation des données clients et leur protection peut sembler particulièrement difficile. En effet, 61 %

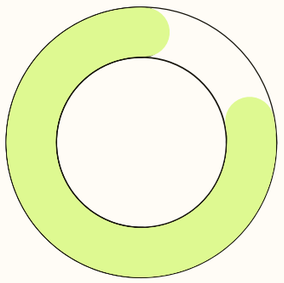
des responsables de la CX admettent qu'ils ont du mal à suivre le rythme des dernières exigences légales et réglementaires concernant les données des clients et la protection de la vie privée.

Par ailleurs, si 83 % d'entre eux pensent que leurs clients ont confiance dans leurs efforts de protection des données, les consommateurs ne partagent pas en réalité ce sentiment : ils sont 60 % à juger que les entreprises n'en font pas assez pour les protéger. Les entreprises vivent un moment charnière. Celles qui parviennent à assurer la transparence et la sécurité de leurs données pourront gagner la confiance de leurs clients. À l'inverse, celles qui n'y parviennent pas risquent de perdre du terrain face à la concurrence.

Les responsables de CX l'ont bien compris et œuvrent déjà en ce sens, notamment en optimisant la confidentialité des données dans leur service, en élaborant des plans stratégiques et en s'associant à des experts pour préparer sereinement l'avenir.

83 % des responsables de la CX déclarent que la protection des données et la cybersécurité sont des priorités absolues dans leur stratégie de service client

Zendesk sait que, même si aucune entreprise n'est confrontée aux mêmes problèmes, il existe des mesures que chaque responsable CX peut prendre pour réussir dans son nouveau rôle de gardien de la confidentialité des données. Dans ce guide, vous découvrirez un ensemble de pratiques développées par nos experts pour faciliter la gestion des risques liés à la confidentialité des données de CX tout au long de leur cycle de vie.



70 %

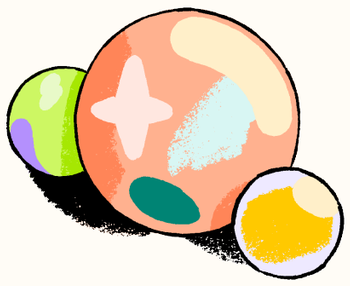
des consommateurs renoncent à acheter un produit ou un service s'ils jugent que l'entreprise n'est pas apte à protéger leurs données

BONNES PRATIQUES

1. Évaluer régulièrement toutes vos données pour ne garder que celles nécessaires pour une CX de qualité
2. Mieux protéger les données de vos clients en limitant l'accès au strict nécessaire
3. Maintenir un contrôle strict sur votre clé de chiffrement des données clients afin de pouvoir réagir aux menaces
4. Surveiller l'accès aux données des clients et mettre à jour les autorisations d'accès si nécessaire
5. Automatiser les protocoles et procédures de sécurité des données pour protéger efficacement la vie privée

BONNE PRATIQUE N° 1

Évaluer régulièrement toutes vos données pour ne garder que celles nécessaires pour une CX de qualité



Pour offrir des expériences personnalisées et immersives, il faut exploiter les données des clients, ce qui implique de les stocker correctement. Des informations de contact à l'historique des interactions, ces données doivent être facilement accessibles pour votre équipe. Cependant, toutes les données ne sont pas nécessaires pour assurer une CX de qualité. Pour protéger la vie privée des clients, vous devez faire le tri entre les éléments à conserver et ceux à supprimer.

Suivez les réglementations relatives à la suppression des données

De nombreuses réglementations, notamment le RGPD de l'Union européenne et le CPRA de la Californie, fixent des normes spécifiques quant au moment où les données des clients doivent être supprimées. La première étape, en tant que responsable de CX, est d'acquérir une compréhension approfondie de la manière dont ces normes s'appliquent à votre organisation, afin que votre entreprise reste conforme. N'oubliez pas que les lois et les règlements évoluent : vous ne cesserez jamais d'apprendre. Votre mission en tant que responsable de CX sera de rester à l'écoute de ces changements.

Définissez les données de CX à conserver et à supprimer

Au-delà de la réglementation, réfléchissez aux données que votre équipe de CX est plus ou moins susceptible d'exploiter. Existe-t-il certains types ou sujets de conversation avec les clients dont votre équipe a besoin pour fournir un service de qualité ? Y a-t-il des informations personnelles identifiables (PII) qui ne sont jamais importantes pour votre organisation de CX ? Si oui, il est préférable de les occulter dans les conversations avec les clients.

Appliquez un système de marquage

Pour gérer la conservation et la suppression des données à grande échelle, il faut pouvoir identifier et suivre facilement les informations pertinentes au sein de votre système de CX. Pour ce faire, il est possible d'utiliser des formulaires clients spécifiques, des balises de conversation ou encore des types de demandes.

Créez un calendrier de conservation et de suppression

Une fois identifiées les données à supprimer ou à conserver, déterminez à quelle fréquence le faire. Différents types de conversations doivent-ils être conservés pendant des durées différentes ? Par exemple, les sociétés de services financiers doivent supprimer les questions de routine, mais conserver la trace des modifications importantes apportées à un compte. Dans le domaine médical, les interactions sur la facturation doivent être conservées pendant une durée différente que les échanges portant sur des sujets personnels/médicaux.

TÉMOIGNAGE CLIENT

INDIGOV

Indigov utilise la plateforme Zendesk pour rapprocher les représentants élus des États-Unis de leurs électeurs, tout en préservant la confidentialité et la sécurité des données sensibles. C'est un véritable exploit si l'on considère que les élus reçoivent chaque année 5,1 milliards de messages de la part de leurs électeurs.

L'entreprise a été en mesure de rester agile et de faire progresser ses objectifs de CX plus rapidement que prévu, grâce à la personnalisation et aux fonctionnalités de sécurité intégrées de Zendesk. Ses fonctions de sécurité prêtes à l'emploi ont permis à Indigov de répondre immédiatement à des normes fédérales strictes. Désormais, les clients d'Indigov opèrent en toute confiance grâce à une expérience omnicanal plus fluide, conçue pour répondre à leurs besoins, avec l'assurance que leurs données sont toujours protégées.

BONNE PRATIQUE N° 2

Mieux protéger les données de vos clients en limitant l'accès au strict nécessaire

Votre organisation de CX devra stocker certaines données clients, mais il est important de limiter leur accès aux employés qui en ont réellement besoin. Il s'agit là d'un concept important en matière de protection des données, connu sous le nom de *principe du moindre privilège*.

Limitez l'accès aux conversations des clients grâce à un contrôle d'accès basé sur les rôles

Il est fort probable que seuls certains employés aient besoin d'accéder aux conversations avec les clients. Pour filtrer les autorisations, rien de mieux qu'un système de contrôle des accès basé sur les rôles. Il garantit que les agents n'ont accès qu'aux données correspondant à leur rôle et leurs responsabilités. Par exemple, un agent du service de facturation n'a pas forcément besoin d'accéder aux demandes d'assistance technique. Cela permet non seulement de renforcer la sécurité des données, mais aussi de simplifier l'expérience utilisateur pour les agents, qui peuvent ainsi se concentrer sur leurs tâches.

Masquez les informations sensibles et personnelles

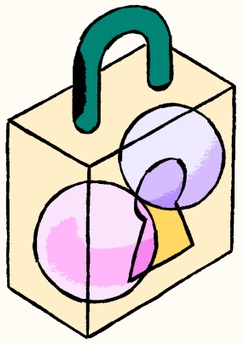
Le masquage des données permet de cacher les renseignements qui ne sont pas nécessaires à vos agents dans le cadre de leurs fonctions. Par exemple, un agent peut avoir besoin de connaître le nom et l'adresse e-mail d'un client, mais pas son adresse postale. Dans ce cas, vous pouvez occulter l'adresse postale du client tout en laissant apparaître ses autres informations grâce au masquage.

Menez des audits et des examens trimestriels des autorisations d'accès

Pour vous assurer que vos politiques d'accès aux données sont efficaces et à jour, vérifiez et révisez régulièrement vos autorisations. Une fois l'audit réalisé, mettez soigneusement en œuvre les changements requis afin que les employés aient uniquement accès aux données dont ils ont besoin. Cela permet d'éviter l'exposition inutile de données sensibles.

BONNE PRATIQUE N° 3

Maintenir un contrôle strict sur votre clé de chiffrement des données clients afin de pouvoir réagir aux menaces



Protéger la vie privée de vos clients, c'est empêcher que leurs données ne tombent entre de mauvaises mains. Le chiffrement des données, qui convertit les informations des clients en texte chiffré que les acteurs malveillants ne pourront pas consulter, constitue un garde-fou très efficace. Plus vous contrôlez le processus de chiffrement, plus il est facile d'utiliser cet outil pour sécuriser les données de vos clients.

Chiffrement BYOK

Vous pouvez mieux contrôler la clé de vos données clients grâce au cryptage BYOK (pour Bring Your Own Key), qui implique d'utiliser sa propre clé de chiffrement. Avec le BYOK, vous pouvez réduire le risque d'exposition des données de vos clients en modifiant et en révoquant régulièrement vos clés. Par exemple, au lieu de protéger toutes vos données clients à l'aide d'une même clé, vous pouvez sécuriser différentes portions de vos données à l'aide de clés distinctes. Ainsi, si une clé est compromise, toutes les données de vos clients ne sont pas exposées. Et si une clé est compromise, vous pouvez la révoquer pour qu'elle ne puisse plus être utilisée.

Gestion et rotation des clés

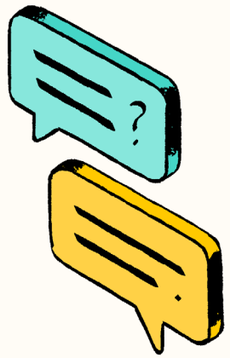
Envisagez l'utilisation d'un système automatisé de gestion des clés pour éviter les erreurs humaines en assurant la rotation des clés de chiffrement selon un calendrier déterminé. Cette organisation est importante car toute rotation oubliée par inadvertance peut augmenter le risque d'une violation de données coûteuse. Méfiez-vous aussi des solutions BYOK qui exigent que vos clés de chiffrement soient stockées sur la plateforme d'un fournisseur : vous devez garder la main sur vos clés.

Contrôle des clés d'accès

Veillez à établir un plan de contrôle strict précisant qui peut accéder aux clés de chiffrement, les modifier ou les gérer. Cela permet de garantir que seul le personnel autorisé peut manipuler ces éléments de sécurité critiques.

BONNE PRATIQUE N° 4

Surveiller l'accès aux données des clients et mettre à jour les autorisations d'accès si nécessaire



De nombreuses organisations de CX suivent les changements critiques, y compris la mise à jour des informations et des paramètres du compte, des utilisateurs, des applications, des widgets web, des règles de gestion, des tickets et des organisations. Afin de protéger la vie privée des clients, les responsables de CX doivent également conserver une trace de l'accès des agents aux données des clients dans un journal des accès.

Examinez les journaux d'accès pour identifier les risques de confidentialité

Ces journaux permettent d'identifier les comportements suspects tels que les recherches répétées d'informations sensibles (comme les détails d'une carte ou l'accès à des données depuis un lieu inhabituel).

Optimisez les autorisations des agents selon l'accès aux données

L'examen des données que les agents consultent régulièrement peut vous aider à comprendre à quelles informations ils doivent avoir accès. Vous pouvez utiliser ces renseignements pour optimiser les politiques d'autorisation appliquées aux agents.

Identifiez les données à supprimer (et à conserver)

Comprendre les types de données auxquelles les agents accèdent régulièrement peut vous aider à déterminer les données à conserver et à supprimer. Par exemple, si vous constatez que les agents ne reviennent jamais vers certains types de données passé un certain délai, elles peuvent être supprimées.

BONNE PRATIQUE Nº 5

Automatiser les protocoles et procédures de sécurité des données pour protéger efficacement la vie privée

Pour réduire les frais de gestion de la confidentialité des données de CX, automatisez au maximum les politiques et les procédures de protection de la confidentialité. En intégrant l'automatisation dans votre stratégie, vous faciliterez la tâche de votre équipe tout en garantissant le respect des politiques et des procédures. La bonne nouvelle, c'est que bon nombre des bonnes pratiques abordées dans ce guide peuvent être automatisées à l'aide d'outils existants sur le marché.

Suppression et conservation des données

Vous pouvez définir des politiques automatisées de conservation pour garantir que les données des clients ne sont stockées que pour la durée requise et sont ensuite supprimées, conformément à des réglementations telles que le RGPD. Vous pouvez ainsi réduire les risques de manquements éventuels.

Masquage des données

Utilisez des outils automatisés pour repérer les données personnelles dans vos conversations avec les clients et les masquer, en particulier lorsque vous partagez des informations avec d'autres équipes ou que vous les exportez dans des rapports. Vous pouvez ainsi préserver la confidentialité des clients tout en garantissant que les agents et les équipes n'accèdent qu'aux renseignements nécessaires à leur mission.

Accès des agents aux données personnelles

Tirez parti de l'automatisation pour accorder ou révoquer l'accès des agents en fonction de leur rôle. Le contrôle dynamique des accès réduit le risque de violation des données et garantit que les informations des clients sont uniquement consultées par les bonnes personnes.

Suivi des accès

Les outils de surveillance tels que les journaux d'accès peuvent automatiquement capturer les événements d'accès aux données et vous indiquer les profils de clients qui ont été ouverts, les tickets d'assistance consultés ou encore la liste complète des recherches. Tout accès inapproprié aux données est ainsi signalé en temps utile, ce qui permet de réagir rapidement.

Restez à la pointe des tendances

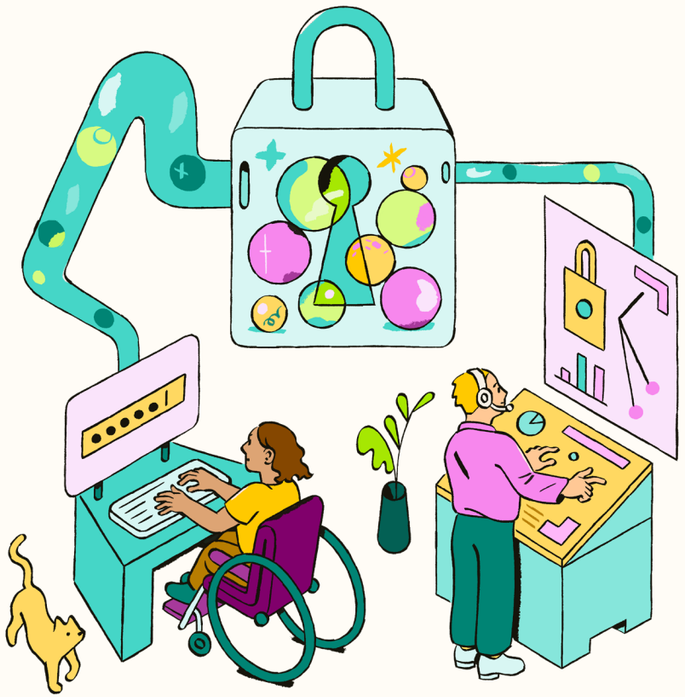
Les responsables de CX deviennent les champions de la confidentialité des données dans un paysage complexe, jalonné de défis critiques pour leurs entreprises. Même si ces problèmes peuvent sembler insurmontables, il existe des outils conçus pour vous aider.

C'est notamment le cas de la plateforme Protection et confidentialité avancées des données de Zendesk, qui permet de mettre en œuvre des politiques et des contrôles simples mais robustes, notamment des clés de chiffrement autogérées, une journalisation des accès et des outils complets de minimisation des données. Pour les responsables de CX aux prises avec les obligations de sécurité des données, il peut s'agir d'un outil précieux permettant à leur organisation de gérer efficacement les risques liés à la protection de la vie privée tout au long du cycle de vie des données.

Chez Zendesk, nous nous engageons en faveur de la confidentialité des données dans l'expérience client afin que les organisations soient équipées pour protéger efficacement les données des clients tout en s'adaptant à l'évolution des normes en vigueur. En intégrant les solutions de Zendesk, les entreprises peuvent gérer de manière réactive la confidentialité des données, en maintenant à la fois la conformité et la confiance des clients sur un marché en constante évolution.

Méthodologie

Les résultats CX Trends présentés dans ce rapport proviennent de deux sources : une enquête mondiale menée auprès de 2 500 consommateurs dans 20 pays et une seconde enquête mondiale avec près de 4 500 participants (dont 1500 entreprises et 1000 consommateurs dans la région EMEA).



Pour en savoir plus sur la façon dont vous pouvez gérer les risques liés à la confidentialité des données, contactez Zendesk dès aujourd'hui.

zendesk