LIVRE BLANC

RGPD, CCPA et au-delà :

Comment la gouvernance des identités aide les entreprises à se conformer et à améliorer la confiance des clients

Akamai

Résumé

Les réglementations en matière de confidentialité ayant un impact sur l'entreprise représentent une tendance mondiale en constante évolution. Le Règlement général sur la protection des données (RGPD) de l'Union européenne est entré en vigueur en 2018. Et, le 1er janvier 2020, le California Consumer Privacy Act (CCPA) entre en vigueur, affectant les entreprises qui exercent leurs activités en Californie, la cinquième économie mondiale.

Mais ce n'est que le début. Sous l'effet de violations de données, d'usurpations d'identité et de scandales connexes largement médiatisés, une législation en matière de confidentialité et de conformité est adoptée rapidement dans le monde entier. Rien qu'aux États-Unis, neuf États ont présenté ou adopté des lois imposant de lourdes obligations à l'égard des entreprises et des organisations afin de donner aux utilisateurs davantage de transparence et un contrôle accru sur les informations à caractère personnel.

Les entreprises ne peuvent pas se permettre d'ignorer ces nouvelles lois et réglementations en matière de confidentialité. Du seul point de vue financier, les amendes modérées qui ont été infligées au cours des 12 premiers mois du RGPD ont désormais laissé place à des pénalités financières de plus de 200 millions de dollars, qui sont encore loin du plafond légal de 4 % du chiffre d'affaires annuel global prévu par le RGPD. Mais le coût pour les multinationales est bien plus que financier. La confiance des utilisateurs est menacée.

Si les clients ne font pas confiance aux entreprises ou organisations pour protéger la confidentialité de leurs données, le pouvoir commercial et marketing de ces entités en pâtira. Aujourd'hui, les entreprises ont besoin d'un consentement exprès pour traiter des données personnelles. Et le consentement nécessite de la confiance. Sans confiance, il n'y a pas de consentement. Sans consentement, il n'y a pas de données. Et cela se traduit par des campagnes de vente ou marketing irrémédiablement inefficaces.

Le respect de la vie privée n'est pas seulement une question de conformité, c'est aussi un avantage commercial essentiel. La gouvernance de la confidentialité et des identités aide les entreprises et les organisations à instaurer des relations de confiance avec les utilisateurs et les clients, ce qui se traduit par une plus grande fidélité des clients et, au final, une augmentation des revenus de l'entreprise.

Cette publication est une présentation du RGPD, du CCPA et d'autres réglementations internationales connexes en matière de confidentialité. Elle permet de renforcer la confiance des clients grâce à la conformité réglementaire, à la gouvernance des identités et à la protection des données. Elle aborde également la nécessité de mettre en place des solutions de gestion des identités appropriées. Vous trouverez également des exemples montrant comment deux grandes marques ont atteint leurs objectifs de conformité en matière de confidentialité.

Règlement général sur la protection des données

Le 25 mai 2018, le RGPD est devenu partie intégrante de notre quotidien à l'échelle mondiale. L'objectif de cette législation générale sur la protection des données est d'harmoniser les lois locales sur la protection des données à travers l'Europe. La loi s'applique non seulement aux entreprises basées en Europe, mais également à toute entreprise ou organisation qui exerce des activités au sein de l'Union européenne.

Le RGPD définit de nombreuses exigences détaillées concernant la collecte, le stockage et l'utilisation des informations à caractère personnel, ainsi que la protection des données contre les accès non autorisés.[1] Cela implique non seulement l'identification et la sécurisation des données personnelles, mais également la façon de répondre aux nouvelles exigences en matière de transparence, de détecter et de signaler les violations de données personnelles et de former le personnel chargé de la confidentialité.

Le non-respect des principes du RGPD peut avoir une incidence importante sur la situation financière d'une entreprise, puisque le RGPD peut imposer des amendes. Bien que les premières violations de confidentialité aient donné lieu à de modestes amendes, le secteur est maintenant à l'affût, car les pénalités récemment imposées font les gros titres dans le monde entier. Deux amendes très élevées – l'une imposée à une importante compagnie aérienne[2] (230 millions de dollars) pour une violation de données qui a touché 500 000 personnes et l'autre à une multinationale hôtelière[3] (123 millions de dollars) pour le piratage des informations personnelles de 383 millions de clients – ont suscité une attention particulière auprès des multinationales.

California Consumer Privacy Act

Exerçant une pression supplémentaire sur les entreprises pour protéger la confidentialité, le compte à rebours final a commencé pour le California Consumer Privacy Act (CCPA)[4]. Le 1er janvier 2020, la plupart des grandes entreprises ou organisations qui travaillent en Californie devront se conformer à la nouvelle législation stricte de cet État, qui établit un droit légal et applicable en matière de confidentialité pour chaque résident californien. Comme pour le RGPD, ces nouveaux règlements ne s'appliquent pas seulement aux entreprises établies en Californie, mais aussi à toutes les entreprises qui exercent une activité dans cet État.

Le CCPA offre les protections suivantes aux données personnelles des utilisateurs californiens[5] :

- **Propriété.** Protège le droit des utilisateurs à demander à une entreprise de ne pas partager ni vendre d'informations personnelles.
- **Contrôle.** Permet aux utilisateurs d'exercer un contrôle sur les informations personnelles qui sont recueillies à leur sujet
- **Sécurité.** Tient les entreprises responsables de la protection des informations personnelles
- Toute entreprise ou organisation devra se conformer aux exigences du CCPA si elle répond à au moins un des critères suivants :
  - avoir un chiffre d'affaires supérieur à 25 millions de dollars
  - acheter, recevoir, vendre ou partager les informations personnelles de 50 000 utilisateurs, foyers ou terminaux ou plus à des fins commerciales
  - 50 % des revenus annuels proviennent de la vente d'informations personnelles d'utilisateurs

Alors que de nombreuses entreprises ont dû surmonter des obstacles importants l'an dernier pour se conformer au RGPD, elles doivent maintenant se mettre en conformité avec le CCPA. Et la date limite approche à grands pas. Les entreprises qui recueillent des données sur l'identité des clients en Californie et établissent des profils de clients pour des campagnes de marketing personnalisées doivent agir maintenant, sans quoi elles risquent des amendes importantes.

Quelle différence entre le RGPD et le CCPA ?

Bien que la portée du CCPA soit quelque peu différente de celle du RGPD, il accorde aux utilisateurs des droits similaires de contrôle et de refus quant à l'utilisation de leurs données. Les deux règlements exigent des entreprises qu'elles conservent les données en toute sécurité, qu'elles soient transparentes quant aux types de données personnelles recueillies et qu'elles gèrent les demandes de suppression de données personnelles des utilisateurs (souvent appelées « droit à l'oubli »), ce qui signifie qu'elles sont en mesure de supprimer des données personnelles de tous les systèmes de l'entreprise.

Lorsque le consentement est la base juridique du traitement des données, le CCPA diffère du RGPD car il requiert la possibilité pour les utilisateurs de se retirer, au lieu de demander un consentement explicite avant de collecter des informations à caractère personnel.

Réglementations internationales supplémentaires

Aussi importants soient-ils, le RGPD et le CCPA ne sont que le début de cette tendance mondiale. Dans le monde entier, de nombreuses lois sur la confidentialité et la conformité sont prises en compte ou déjà promulguées. Rien qu'aux États-Unis, les législateurs de neuf autres États ont mis en place des projets de loi qui imposeraient aux entreprises des obligations générales pour fournir aux utilisateurs une plus grande transparence et un meilleur contrôle sur les informations à caractère personnel.[6]

Au niveau international, la tendance à des réglementations plus strictes (et ayant un impact sur l'entreprise) en matière de confidentialité est un phénomène mondial que les entreprises et les organisations ne peuvent pas ignorer. Le tableau ci-dessous répertorie quelques-unes des réglementations nouvelles et en cours de mise en œuvre, telles que la loi PIPEDA (Personal Information Protection and Electronic Documents Act) du Canada.

Tableau. Exemples de réglementations existantes, à venir ou proposées en matière de protection des données et de confidentialité

AMÉRIQUES	EMEA	ASIE-PACIFIQUE
Argentine : PDPL/Projet de loi n° MEN-2018-147-APN-PTE[7] USA : Californie : CCPA (AB 375) Canada : PIPEDA[8] Hawaï : SB 418[9] Maryland : SB 0613[10] Massachusetts : SD 341[11] Mississippi : HB 2153[12] Nouveau Mexique : SB 176[13] New York : S00224[14] Dakota du Nord : HB 1485[15] Rhode Island : S0234[16] Texas : HB 4518[17]	Union européenne : RGPD Russie : Loi fédérale N° 152-FZ[18]	Australie : Privacy Act 1988 / Information sur les principes de confidentialité (IPP)[19] Chine : Spécifications de sécurité des informations personnelles[20] Inde : Projet de loi en matière de protection des données personnelles[21] Japon : APPI[22]

Au-delà de la conformité réglementaire : instaurer la confiance

Avec toutes ces réglementations, instaurer la confiance auprès des utilisateurs est devenu encore plus important pour les entreprises et les organisations du monde entier. Le RGPD, le CCPA et la législation connexe exigent des entreprises, le cas échéant, qu'elles demandent le consentement des clients avant de recueillir et d'utiliser leurs données, et bien sûr, de conserver un enregistrement de ce consentement.

Au-delà de la conformité réglementaire, la confidentialité est également cruciale pour les entreprises qui souhaitent établir des relations numériques solides et fiables avec leurs clients. Les clients ont des exigences de plus en plus élevées quant à la confidentialité et à la sécurisation de leurs données personnelles. Les nombreux cas largement médiatisés d'abus de données, d'atteinte à la protection des données et d'usurpation d'identité ont placé la barre plus haut, et on exige désormais des entreprises qu'elles soient des détentrices de données personnelles dignes de confiance. Lorsque les clients stockent des données dans une entreprise, ils concluent un contrat de confiance. Si cette confiance est rompue, il est généralement très difficile de la rétablir.

Les employés ne donnent leur consentement pour traiter leurs données que si l'entreprise offre de la valeur en retour, mais aussi uniquement s'ils font confiance à la marque. Sans confiance, il n'y a pas de consentement. Sans consentement, pas de données, ce qui dévalue tous les efforts en termes de vente et de marketing ou les rend inefficaces. La confiance est considérée comme la « nouvelle monnaie » pour les entreprises qui cherchent à obtenir des données clients.

L'importance du consentement : repenser l'expérience utilisateur

Dans le cadre du RGPD et du CCPA, les clients doivent pouvoir consulter, modifier et même révoquer leur consentement à tout moment. En d'autres termes, les entreprises qui fournissent des formulaires Web faciles à utiliser pour recueillir le consentement, puis compliquent volontairement la révocation du consentement en demandant aux personnes de suivre un processus bureaucratique complexe, ne seront pas conformes. De plus, les entreprises doivent clairement expliquer aux personnes pourquoi elles recueillent les données et à quoi elles vont servir.

Pour les organisations marketing, cela a quelques implications. Par exemple, le RGPD prévoit que les entreprises ne peuvent plus utiliser de cases pré-cochées sur les pages de destination pour le contenu de génération des leads régulé afin d'obtenir le consentement des utilisateurs. L'utilisateur doit donner activement son consentement plutôt que de devoir refuser chaque autorisation pré-cochée. C'est-à-dire que les clients doivent cocher la case pour accepter. En vertu du CCPA, cependant, le consentement implicite est toujours autorisé, les cases pré-cochées sont donc toujours conformes. Cette différence de législations peut être un vrai casse-tête pour les acteurs mondiaux confrontés à la perspective de s'adresser à deux marchés majeurs avec des sites Web et des applications qui doivent afficher différents formulaires d'inscription. Le problème est le même lorsqu'il s'agit de déployer des sites Web et des applications entièrement distincts afin de répondre aux besoins de différentes régions. Cela multiplie les efforts nécessaires au développement et à la maintenance du code.

Les nouvelles réglementations interdisent également les collectes de données excessives. Les entreprises ne peuvent collecter que les données personnelles nécessaires au service ou au produit qu'elles proposent. Il n'est plus possible de demander le numéro de téléphone ou le sexe d'une personne pour envoyer une lettre d'information par e-mail ou activer le téléchargement d'un livre blanc. Cela signifie que les entreprises doivent repenser et restructurer leur expérience utilisateur et éliminer tous les champs de données des pages d'inscription et d'autres formulaires qui pourraient être considérés comme une collecte excessive de données.

Un détaillant mondial met en œuvre une solution centralisée pour simplifier la conformité aux lois actuelles et futures sur la confidentialité

Une entreprise de vente au détail internationale a récemment remédié à ses exigences de conformité en matière de confidentialité en déployant Akamai Identity Cloud. La solution a permis à l'entreprise de fournir à ses clients une transparence et un contrôle sur leurs données personnelles. Pour ce faire, elle a dû réduire les informations à caractère personnel capturées lors de l'inscription et demander l'autorisation avant de traiter les données.

Identity Cloud fournit à l'entreprise des expériences utilisateur entièrement personnalisables en matière d'inscription et de connexion, ainsi que des formulaires de consentement qui peuvent être invoqués progressivement selon les besoins. Cela a permis aux utilisateurs de l'entreprise de comprendre facilement la finalité des données dont ils autorisent l'utilisation, ainsi que le service duquel ils se sont désinscrits. Les clients peuvent consulter, modifier et révoquer leurs paramètres de consentement à tout moment.

L'entreprise s'appuie sur les fonctionnalités d'accès définies par Identity Cloud pour restreindre l'accès aux enregistrements de données (et à des champs spécifiques au sein des enregistrements), en fonction du rôle du personnel de l'entreprise qui accède aux données d'identité. Cela signifie qu'un représentant du service clientèle dispose de droits d'accès différents de ceux attribués au personnel marketing ou aux développeurs, par exemple. Cette fonctionnalité unique réduit les risques liés à l'exposition des données des clients et offre un niveau de sécurité des données inégalé.

En fournissant un référentiel central pour les données clients avec un contrôle d'accès granulaire, la solution peut limiter la prolifération des données d'identité « toxiques » (par exemple, les données qui sont toujours stockées dans la base de données après la révocation du consentement du client ou la demande de suppression). Le référentiel central simplifie également la suppression des données dans le cadre de demandes portant sur le « droit à l'oubli ».

Enfin, tous les paramètres de consentement sont stockés avec le profil du client dans un formulaire d'audit, ainsi que dans des journaux de modifications et des journaux d'audit indiquant qui a accédé à quelles ressources et quand.

Assurer la protection des données

La conformité va bien au-delà des problèmes de confidentialité. Garantir la sécurité des données des clients et les protéger des acteurs malveillants est impossible sans la confidentialité des données. Puisque les données d'identité personnelles peuvent être facilement utilisées et exploitées, elles sont devenues une cible majeure pour les attaques de piratage. Le rapport 2018 sur le coût des violations de données[23], mené par le Ponemon Institute et sponsorisé par IBM Security, a révélé que 48 % des organisations interrogées ont identifié la cause fondamentale d'une violation de données comme étant une attaque malveillante ou criminelle, avec un coût moyen d'environ 157 $ par dossier concerné.

Comme les violations concernent souvent des centaines de milliers (voire des millions) de dossiers, le coût qui en découle peut nuire gravement à une entreprise, et ce, avant la perte de revenus liée à la réputation, à la perte de confiance des clients et aux amendes potentielles de la part du RGPD et du CCPA.

La nécessité de la gouvernance des identités

Les identités personnelles sont des ressources précieuses, non seulement pour les entreprises qui collectent et compilent des informations à caractère personnel, mais également pour les utilisateurs qui possèdent les informations et qui ont une volonté affirmée de les protéger et de ne pas en autoriser une utilisation abusive.

De plus en plus d'aspects de la vie personnelle des utilisateurs se déplacent dans le domaine numérique. Les données personnelles se retrouvent dans les données de profil de l'entreprise, allant du nom, de l'adresse, du téléphone, du sexe, des informations de paiement et des préférences personnelles, aux historiques d'achats et de navigation, ainsi qu'à d'autres données comportementales. La nécessité pour les entreprises de sécuriser et de protéger les données vitales a considérablement augmenté, et les organismes de réglementation du monde entier réagissent à ce besoin sous la forme de réglementations de plus en plus strictes.

La conformité réglementaire et la sécurité sont des facteurs majeurs qui ajoutent énormément à la complexité et à l'importance de la gestion des identités. Toutefois, les solutions de gestion des identités à l'échelle de l'entreprise peuvent offrir aux clients une transparence et un contrôle sur leurs données personnelles en minimisant les données capturées lors de l'inscription et en demandant leur consentement avant de traiter les données.

Grâce à une gestion adéquate des identités, les entreprises peuvent regagner la confiance des utilisateurs.

Une marque de boissons mondiale se conforme rapidement au RGPD

Une entreprise internationale de boissons a dû faire face à un délai très court de deux mois pour mettre en œuvre la conformité aux exigences en matière de confidentialité du RGPD pour tous ses clients européens avant l'échéance du RGPD. L'entreprise avait précédemment mis en œuvre Identity Cloud, mais elle a dû assurer rapidement la conformité aux réglementations changeantes en matière de confidentialité des utilisateurs.

La conformité a été assurée en deux mois seulement, du début à la fin. L'accent de l'entreprise a été mis sur l'obtention du consentement explicite des utilisateurs pour l'utilisation de leurs données à des fins de marketing et de personnalisation, conformément aux exigences du RGPD. Identity Cloud fournit à l'entreprise des formulaires de consentement hautement personnalisables et précis que l'on peut invoquer progressivement sur n'importe quelle propriété digitale : des sites Web aux applications pour mobile en passant par les terminaux connectés à l'IoT. En plus de permettre la conformité au RGPD, cette fonctionnalité puissante a permis à la marque de boissons de gagner en confiance auprès de ses clients en leur permettant de comprendre et de gérer facilement leurs préférences en matière de consentement.

L'un des aspects les plus difficiles du déploiement mondial a été d'équilibrer l'aspect relatif au « droit à l'oubli » du RGPD avec l'obligation légale de conserver les données pendant la durée d'une promotion auprès des utilisateurs. Identity Cloud a fourni la capacité nécessaire pour que l'entreprise s'assure que les données étaient conservées pour la durée légale, puis effacées à la fin de cette période, et pour qu'elle puisse communiquer sur cet aspect auprès de ses clients.

Akamai Identity Cloud

Identity Cloud est la solution d'Akamai pour la gestion des identités et des accès des clients. La plateforme fournit tout ce dont les entreprises ont besoin pour permettre à leurs clients de créer des comptes personnels et de se connecter en toute sécurité sur des sites Web, à des applications pour mobile ou à des applications basées sur l'IoT. Identity Cloud fournit des outils qui peuvent être utilisés pour réduire de manière significative les efforts de conformité en matière de confidentialité, tout en fournissant aux entreprises un référentiel de profil client hautement sécurisé et en offrant une vue à 360 degrés du client.

Identity Cloud offre des fonctionnalités et des expériences utilisateur spécifiques qui peuvent aider les entreprises à répondre aux exigences de réglementation. Les fonctionnalités de protection et de confidentialité d'Identity Cloud incluent l'enregistrement des clients, la connexion, l'authentification de base, l'authentification unique, le contrôle d'accès au périmètre, la gestion des préférences et des autorisations, ainsi que de nombreuses autres fonctionnalités nécessaires pour collecter, gérer et sécuriser les données personnelles.

Identity Cloud offre les fonctionnalités suivantes pour aider les entreprises à respecter les réglementations de conformité en matière de confidentialité :

- Mécanismes de consentement par case à cocher pour consentement explicite
- Gouvernance centralisée pour le contrôle des accès
- Autorisation, enregistrement et profilage progressifs
- Mécanismes d'accès aux enregistrements de données simples
- Mécanismes de correction et d'intégrité des données
- Portabilité des données
- Effacement/suppression des données
- Accès étendu pour les utilisateurs et les intégrations
- Pseudonymisation des données
- Filtrage selon l'âge

En exécutant Identity Cloud, les entreprises et les organisations peuvent mettre en œuvre une gestion des identités de qualité professionnelle, de manière rapide et flexible. Conçue à partir d'une architecture cloud, cette solution s'adapte intelligemment aux besoins de capacité pour faire face aux pics de trafic et offrir des expériences performantes à des millions d'utilisateurs. Akamai Identity Cloud est conçu pour aider les entreprises à se conformer aux réglementations internationales en matière de confidentialité, à renforcer la confiance dans leur marque, à gérer les données clients et à limiter les risques en rendant les données disponibles en toute sécurité dans toutes les régions et applications.

Pour en savoir plus sur Akamai Identity Cloud, rendez-vous sur akamai.com/identitycloud.

Conclusion

La conformité au RGPD, au CCPA et aux autres législations associées en matière de confidentialité, ainsi que l'assurance de la sécurité, sont des facteurs essentiels pour toute entreprise ou organisation qui souhaite développer et conserver des relations de confiance avec ses clients. Les utilisateurs attendent de la transparence et exigent que leurs données personnelles restent privées et sécurisées. Les violations de données récentes, les usurpations d'identité et les événements mondiaux associés soulignent la nécessité pour les entreprises d'être reconnues comme les gardiens fidèles des informations à caractère personnel.

Lorsque les clients autorisent la collecte et le stockage de leurs informations privées auprès d'une entreprise, ils concluent essentiellement un contrat de confiance. Si cette confiance est rompue, il devient très difficile de la restaurer. L'obtention et le stockage des données des utilisateurs, ainsi que le traitement des informations d'identification et des informations personnelles des clients, sont des devoirs de diligence que les entreprises actuelles ne peuvent se permettre d'enfreindre ou de compromettre. Si la confiance est rompue, cela peut facilement mettre en danger la réputation de la marque, la fidélité de la clientèle et, en définitive, le chiffre d'affaires continu et la réussite de l'entreprise.

Annexe : Présentation des exigences réglementaires en matière de confidentialité

Cette annexe présente un aperçu des types généraux d'exigences qui se trouve dans le RGPD, le CCPA, ainsi que de nombreuses réglementations majeures en matière de protection des données et de confidentialité dans le monde entier : consentement, droit de s'opposer, droit d'accès, droit à l'oubli, portabilité des données, sécurité et notification de violation. La mise en œuvre de ces droits varie en fonction des différentes lois en vigueur en matière de protection des données et de la vie privée. Vous devez donc consulter votre conseiller juridique pour déterminer la manière dont les différentes lois s'appliquent à vous.

Pour en savoir plus sur la manière dont Akamai Identity Cloud peut vous aider à répondre à ces exigences en matière de conformité réglementaire, veuillez lire notre article de blog.

Consentement	Les entreprises doivent souvent obtenir le consentement des utilisateurs finaux avant de collecter et de traiter leurs données personnelles à certaines fins. Les conditions requises pour obtenir un consentement valide et le moment où un tel consentement est requis varient selon les réglementations en vigueur.
Droit de s'opposer	Les conditions permettent à la personne concernée de s'opposer à l'utilisation de ses données personnelles pour certains types de traitement de données, tels que le marketing direct ou l'analyse statistique.
Droit d'accès	De nombreuses lois donnent à la personne concernée le droit d'accéder, d'examiner et de corriger ces données personnelles et, dans certains cas, de rechercher des informations supplémentaires sur leur utilisation et leur divulgation.

Droit d'effacer ou de supprimer des données personnelles	De nombreuses lois incluent le « droit à l'oubli » pour que les utilisateurs demandent à ce que leurs données personnelles soient effacées et ne soient plus diffusées à des tiers ou exposées à des traitements tiers.
Portabilité des données	Les entreprises sont tenues de fournir aux personnes concernées des copies de leurs données dans un format couramment utilisé et lisible par machine, ce qui permet aux utilisateurs de transférer leurs données vers une autre organisation sans obstacle.
Sécurité	Les entreprises doivent mettre en œuvre des mesures de sécurité des données appropriées au risque afin de s'assurer que les données ne sont pas consultées, modifiées, perdues, détruites ou divulguées par inadvertance.
Notification de violation	Les entreprises doivent informer les utilisateurs finaux de toute violation de données dans un délai donné après avoir pris connaissance de la situation.

SOURCES

1) https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
2) https://www.cnet.com/news/british-airways-faces-record-breaking-230m-gdpr-fine-for-2018-data-breach/
3) https://www.zdnet.com/article/marriott-faces-123-million-gdpr-fine-in-the-uk-for-last-years-data-breach/
4) https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375
5) https://www.caprivacy.org/
6) https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou
7) https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf
8) https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
9) https://www.capitol.hawaii.gov/measure_indiv.aspx?billtype=SB&billnumber=418&year=2019
10) http://mgaleg.maryland.gov/webmga/frmMain.aspx?pid=billpage&stab=01&id=sb0613&tab=subject3&ys=2019rs
11) https://malegislature.gov/Bills/191/SD341
12) http://billstatus.ls.state.ms.us/documents/2019/html/HB/1200-1299/HB1253IN.htm
13) https://www.nmlegis.gov/Legislation/Legislation?chamber=S&legType=B&legNo=176&year=19
14) https://assembly.state.ny.us/leg/?default_fld=&bn=S00224&term=2019&Summary=Y&Actions=Y&Text=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y
15) https://www.legis.nd.gov/assembly/66-2019/bill-index/bi1485.html
16) http://webserver.rilin.state.ri.us/billtext19/senatetext19/S0234.htm
17) https://capitol.texas.gov/tlodocs/86R/billtext/html/HB04518I.htm
18) https://pd.rkn.gov.ru/authority/p146/p164/
19) https://pd.rkn.gov.ru/authority/p146/p164/
20) https://www.tc260.org.cn/front/postDetail.html?id=20190201173320
21) https://meity.gov.in/content/personal-data-protection-bill-2018
22) https://www.ppc.go.jp/en/
23) https://www.ibm.com/security/data-breach