Guides sur le risque fournisseur par État et par secteur aux États-Unis

Comment Cyber Crucible répond aux lois américaines sur la protection de la vie privée et la sécurité au niveau des États, ainsi qu'aux règles sectorielles, du point de vue de la sélection des fournisseurs — New York DFS, Californie, Texas, Virginie, Colorado, Massachusetts, Illinois et Pennsylvanie. Précise clairement ce que Cyber Crucible détient et ne détient pas.

- Comment Cyber Crucible prend-il en charge le Connecticut Data Privacy Act (CTDPA) ?
- Comment Cyber Crucible prend-il en charge le Consumer Privacy Act de l'Utah (UCPA) ?
- Comment Cyber Crucible prend-il en charge la loi de l'Oregon sur la protection de la vie privée des consommateurs (OCPA) ?
- Comment Cyber Crucible soutient-il le My Health My Data Act de l'État de Washington ?
- Comment Cyber Crucible prend-elle en charge les nouvelles lois de confidentialité des États américains 2025-2026 ?

Quelles lois étatiques américaines sur la confidentialité et la sécurité influencent la sélection d'un fournisseur de sécurité ?

Réponse brève : Un ensemble croissant et hétérogène de lois d'État américaines impose des obligations qui s'appliquent aux fournisseurs d'une entreprise — des lois globales sur la confidentialité (Californie, Virginie, Colorado, Texas, et d'autres), des règles sectorielles comme la New York DFS Part 500 pour les services financiers, des exigences de sécurité des données comme la Massachusetts 201 CMR 17.00, des lois biométriques comme l'Illinois BIPA, et des lois de notification de violation de données dans chaque État. Le point commun est qu'un acheteur doit confirmer que son fournisseur de sécurité minimise les données, contracte de manière appropriée, et sécurise tout ce qu'il touche.

Ce que ces lois exigent généralement d'un fournisseur

- Un contrat écrit (accord de traitement des données) limitant le fournisseur aux instructions du client.
- La minimisation des données et la limitation de la finalité.
- Des mesures de sécurité raisonnables et une notification rapide en cas de violation.
- Le soutien aux droits des consommateurs (accès, suppression) lorsque des données personnelles sont traitées.

Pourquoi Cyber Crucible répond à la plupart de ces exigences de manière structurelle

Étant donné que Cyber Crucible ne collecte jamais le contenu, les identifiants ou les clés des clients et effectue le traitement sur le poste (endpoint), les obligations les plus critiques ont peu de prise — il y a un minimum de données personnelles sous sa garde. Un accord de traitement des données ainsi que la documentation associée sont disponibles auprès de **dpo@cybercrucible.com**. Les pages de ce recueil traitent des règles étatiques spécifiques qu'un examinateur est le plus susceptible de citer.

Comment Cyber Crucible soutient-il les exigences de cybersécurité de la New York DFS Part 500 ?

Réponse courte : Pour une institution financière soumise à la New York DFS Part 500 (23 NYCRR 500), Cyber Crucible soutient plusieurs contrôles requis — authentification multifacteur, chiffrement, contrôles d'accès et réponse aux incidents — tout en réduisant le risque tiers, car il ne collecte jamais les informations non publiques que la réglementation protège. Cyber Crucible est un prestataire de services tiers au sens de la réglementation, et non une entité couverte elle-même.

Contrôles pris en charge

- **Contrôles d'accès et MFA** pour le tableau de bord de gestion, appuyés par une authentification forte.
- **Chiffrement** des données en transit et au repos.
- **Réponse aux incidents** dans le cadre d'un processus documenté de réponse aux violations, avec un délai de notification garanti disponible contractuellement — soutenant l'obligation de notification de 72 heures de la DFS pour l'entité couverte.
- **Réduction du risque tiers** grâce à la minimisation des données : aucune information non publique n'est collectée.

La limite en toute honnêteté

Les obligations de la Part 500 — désignation d'un CISO, évaluation des risques, certification annuelle — relèvent de la responsabilité de l'entité couverte. Cyber Crucible fournit des éléments de preuve de contrôle pour la politique de prestataires de services tiers de l'entité (500.11). Il ne s'agit pas d'une entité couverte et ne détient aucune « certification » Part 500. Les éléments de preuve sont fournis sous accord de confidentialité (NDA).

Comment Cyber Crucible répond-il aux obligations des fournisseurs en vertu du CCPA/CPRA de Californie ?

Réponse brève : Cyber Crucible agit en tant que prestataire de services au sens du CCPA/CPRA, tenu par contrat de ne traiter les données que selon les instructions du client, et ne vend ni ne partage d'informations personnelles. Étant donné qu'il ne collecte pratiquement aucune information personnelle en premier lieu, les obligations relatives aux droits des consommateurs et au traitement des données ont très peu de portée dans le cadre de sa garde.

Comment cela s'aligne

- **Rôle de prestataire de services** dans le cadre d'un contrat écrit interdisant tout usage secondaire.
- **Aucune vente ni partage** d'informations personnelles.
- **Soutient les droits des consommateurs** (accès, suppression) en ne détenant pas les informations personnelles qui devraient autrement faire l'objet de recherches ou de suppressions.

Notes relatives à la sélection des fournisseurs

Le California Privacy Rights Act a renforcé les conditions contractuelles applicables aux prestataires de services et ajouté des obligations concernant les informations personnelles sensibles ; Cyber Crucible ne collecte pas de données personnelles sensibles. Un accord de traitement des données conforme au CCPA est disponible sur demande.

Comment Cyber Crucible prend-il en charge le Texas Data Privacy and Security Act (TDPSA) ?

Réponse courte : En vertu du Texas Data Privacy and Security Act, Cyber Crucible agit en tant que sous-traitant lié par un accord de traitement des données, aidant le responsable du traitement dans le cadre des demandes liées à la sécurité et aux personnes concernées. Sa conception axée sur la minimisation des données — ne collectant aucun contenu client, aucune identifiant ni clé — signifie qu'il y a peu de données personnelles à traiter, ce qui simplifie les obligations du responsable du traitement.

Comment cela s'aligne

- **Rôle de sous-traitant** dans le cadre d'un accord de traitement des données conforme au TDPSA.
- **Assistance en matière de sécurité et de violations** auprès du responsable du traitement.
- **Empreinte minimale de données personnelles**, réduisant l'exposition et la charge de réponse.

Notes relatives à la sélection des fournisseurs

Le TDPSA s'applique largement aux entreprises opérant au Texas. Étant donné que Cyber Crucible ne traite essentiellement aucune donnée personnelle et peut être déployé sur site, il répond à la fois aux préférences en matière de sécurité et de résidence des données qu'un acheteur texan peut avoir. La documentation est disponible sur demande.

Comment Cyber Crucible prend-il en charge la Consumer Data Protection Act (VCDPA) de Virginie ?

Réponse courte : Cyber Crucible soutient les obligations d'un responsable du traitement au titre de la VCDPA en tant que sous-traitant opérant dans le cadre d'un accord de traitement des données, en contribuant aux obligations de sécurité des données et aux demandes relatives aux droits des consommateurs. Sa conception sans collecte de données signifie qu'il ne détient que peu ou pas de données personnelles, ce qui allège la charge de traitement et de réponse du responsable du traitement.

Comment cela s'aligne

- **Obligations du sous-traitant** — aide en matière de sécurité, de notification des violations de données et d'évaluations de la protection des données.
- **Minimisation des données** — aucun contenu client, identifiant ou clé n'est collecté.
- **Limitation de la finalité** — traitement effectué strictement selon les instructions du responsable du traitement.

Remarques concernant la sélection des fournisseurs

La VCDPA exige que les responsables du traitement lient contractuellement les sous-traitants et réalisent des évaluations pour les traitements à risque plus élevé ; l'empreinte minimale de données personnelles simplifie ces deux aspects. Un accord de traitement des données est disponible sur demande.

Comment Cyber Crucible prend-il en charge le Colorado Privacy Act (CPA) ?

Réponse courte : Cyber Crucible agit en tant que sous-traitant dans le cadre du Colorado Privacy Act, lié par un accord de traitement des données pour suivre les instructions du responsable du traitement, contribuer à la sécurité et soutenir les droits des consommateurs. Comme il ne collecte pratiquement aucune donnée personnelle, la plupart des obligations du CPA n'ont qu'une portée minimale sur les données qu'il détient.

Comment cela s'aligne

- **Rôle de sous-traitant** avec un traitement contractuellement limité.
- **Assistance en matière de sécurité** et soutien en cas de violation auprès du responsable du traitement.
- **Soutien des droits des consommateurs** en ne détenant pas les données personnelles qui seraient autrement concernées.

Remarques pour la sélection des fournisseurs

Le CPA exige des évaluations de protection des données pour les traitements à risque plus élevé, ainsi que le respect des mécanismes universels de retrait au niveau du responsable du traitement ; l'empreinte minimale simplifie la situation du côté du fournisseur. La documentation est disponible sur demande.

Comment Cyber Crucible prend-il en charge la réglementation Massachusetts 201 CMR 17.00 (WISP) ?

Réponse courte : La réglementation Massachusetts 201 CMR 17.00 exige que toute organisation détenant des informations personnelles concernant un résident du Massachusetts maintienne un Written Information Security Program (programme écrit de sécurité de l'information) comportant des mesures de protection spécifiques. Cyber Crucible soutient le WISP du client grâce au chiffrement, au contrôle d'accès et à la surveillance — et réduit l'exposition propre du client, car Cyber Crucible ne détient pratiquement aucune information personnelle.

Comment cela s'aligne

- **Mesures de protection techniques** — le chiffrement en transit et au repos, l'authentification forte et le contrôle d'accès correspondent aux exigences de la réglementation relatives aux systèmes informatiques.
- **La protection des terminaux et la surveillance** soutiennent l'exigence de logiciels de sécurité « raisonnablement à jour ».
- **Empreinte de données minimale** — les obligations de la réglementation s'appliquent aux informations personnelles ; Cyber Crucible n'en collecte pas.

Notes relatives à la sélection des fournisseurs

La réglementation 201 CMR 17.00 exige également la supervision contractuelle des prestataires de services tiers. Un accord de traitement des données ainsi qu'une documentation des contrôles sont disponibles sur demande.

Comment Cyber Crucible répond-il aux préoccupations liées au BIPA de l'Illinois et aux données biométriques ?

Réponse courte : Cyber Crucible ne collecte, ne stocke ni ne traite d'identifiants biométriques ou d'informations biométriques ; il ne crée donc pas l'exposition que la loi Biometric Information Privacy Act (BIPA) de l'Illinois vise à traiter. Aucune donnée biométrique n'est en sa possession pour laquelle un consentement, une conservation ou une destruction serait requis en vertu de la loi.

Pourquoi il n'y a pas d'exposition au BIPA

- **Aucune collecte biométrique.** Cyber Crucible analyse le comportement des processus et de la mémoire, et non les visages, les empreintes digitales ou d'autres identifiants biométriques.
- **Aucune donnée personnelle sensible.** Plus largement, Cyber Crucible ne collecte pas de données biométriques, de santé ou d'autres catégories particulières de données.

Remarques pour la sélection des fournisseurs

Le BIPA est notable pour son droit d'action privé et ses dommages-intérêts statutaires, ce qui fait des fournisseurs de données biométriques une cible d'examen approfondi ; Cyber Crucible n'entre tout simplement pas dans cette catégorie. Cela peut être confirmé dans la documentation de gouvernance des données disponible sur demande.

Comment Cyber Crucible prend-elle en charge la loi de Pennsylvanie sur la notification des violations de données ?

Réponse brève : La loi de Pennsylvanie sur la notification des violations concernant les informations personnelles (Breach of Personal Information Notification Act, 73 P.S. §2301, telle que modifiée par l'Act 151 de 2022) exige la notification des résidents concernés — et, pour les violations plus importantes, du Procureur général — après une violation touchant des informations personnelles couvertes. Cyber Crucible aide une organisation de Pennsylvanie à remplir ses obligations en ne détenant elle-même aucune information personnelle et en fournissant rapidement des informations d'incident de qualité probante, afin que l'organisation puisse respecter ses délais légaux. Cyber Crucible a son siège social à Pittsburgh, en Pennsylvanie.

Comment cela s'aligne

- **Aucune information personnelle détenue** — l'organisation conserve le contrôle de toute détermination de violation et de notification ; il n'existe aucun ensemble de données côté fournisseur susceptible d'être perdu.
- **Informations d'incident rapides** — le processus de réponse aux violations est conçu pour fournir à l'organisation les faits dont elle a besoin pour notifier dans le délai requis.
- **Définitions élargies prises en compte** — l'amendement de 2022 a élargi la notion d'informations personnelles couvertes (y compris les informations médicales et certaines combinaisons d'identifiants) ; la conception sans collecte de données maintient Cyber Crucible en dehors de ces catégories.

Notes relatives à la sélection du fournisseur

Pour les violations touchant plus de 500 résidents de Pennsylvanie, l'amendement ajoute une obligation de notification au Procureur général ; le rôle de Cyber Crucible est d'appuyer cette obligation, non de la déterminer. Les détails relatifs à la gestion des incidents sont disponibles sous accord de non-divulgation (NDA).

Comment Cyber Crucible prend-il en charge le Connecticut Data Privacy Act (CTDPA) ?

Réponse courte : Cyber Crucible agit en tant que sous-traitant au sens du Connecticut Data Privacy Act, lié par un accord de traitement des données l'obligeant à agir selon les instructions du responsable du traitement et à l'assister dans le traitement des demandes de sécurité et des personnes concernées. Étant donné qu'il ne collecte aucun contenu client, identifiant ou clé, la plupart des obligations du CTDPA n'ont que peu de portée dans le cadre de sa garde.

Comment cela s'aligne

- **Rôle de sous-traitant** avec un traitement contractuellement limité et une obligation d'assistance envers le responsable du traitement.
- **Minimisation des données** — aucun contenu client, identifiant ou clé n'est collecté.
- **Assistance en matière de sécurité et en cas de violation de données** fournie au responsable du traitement.

Remarques pour la sélection des fournisseurs

Le CTDPA exige que les responsables du traitement lient les sous-traitants par contrat, respectent les signaux universels de refus (opt-out) et réalisent des évaluations pour les traitements à risque plus élevé ; l'empreinte minimale en matière de données personnelles simplifie considérablement le volet fournisseur. Un accord de traitement des données est disponible à l'adresse **dpo@cybercrucible.com**.

Comment Cyber Crucible prend-il en charge le Consumer Privacy Act de l'Utah (UCPA) ?

Réponse courte : Cyber Crucible agit en tant que sous-traitant dans le cadre de l'Utah Consumer Privacy Act, en suivant les instructions documentées du responsable du traitement dans le cadre d'un accord de traitement des données. Sa conception sans collecte de données signifie qu'il y a peu de données personnelles en sa possession pour que les règles de traitement et de divulgation de l'UCPA s'appliquent.

Comment cela s'aligne

- **Rôle de sous-traitant** dans le cadre d'un contrat avec le responsable du traitement.
- **Minimisation des données** — aucun contenu client, identifiant ou clé n'est collecté.
- **Mesures de sécurité** — chiffrement, contrôle d'accès et prévention au niveau des terminaux.

Notes pour la sélection des fournisseurs

L'UCPA est généralement considéré comme plus orienté vers les entreprises que certaines lois d'autres États, mais il exige néanmoins des contrats de sous-traitance et une sécurité raisonnable ; l'empreinte minimale répond à ces deux exigences. La documentation est disponible sur demande.

Comment Cyber Crucible prend-il en charge la loi de l'Oregon sur la protection de la vie privée des consommateurs (OCPA) ?

Réponse courte : Cyber Crucible agit en tant que sous-traitant au titre de l'Oregon Consumer Privacy Act, tenu par contrat de ne traiter les données que sur instruction du responsable du traitement et d'apporter son concours en matière de sécurité et de demandes relatives aux droits des consommateurs. Étant donné qu'il ne collecte pratiquement aucune donnée personnelle, la plupart des obligations de l'OCPA n'ont qu'une portée minimale dans le cadre de sa garde des données.

Comment cela s'aligne

- **Obligations du sous-traitant** — apporter son concours en matière de sécurité, de réponse aux violations de données et d'évaluations de protection des données.
- **Minimisation des données** — aucun contenu client, identifiant ou clé n'est collecté.
- **Limitation de la finalité** — traitement effectué strictement sur instruction du responsable du traitement.

Remarques pour la sélection des fournisseurs

La loi de l'Oregon se distingue par une définition plus large des données personnelles et par des droits spécifiques accordés aux consommateurs concernant des tiers nommément désignés ; l'empreinte minimale maintient un risque faible côté fournisseur. Un accord de traitement des données est disponible sur demande.

Comment Cyber Crucible soutient-il le My Health My Data Act de l'État de Washington ?

Réponse courte : Le My Health My Data Act de l'État de Washington réglemente largement les « données de santé des consommateurs » et prévoit un droit d'action privé, ce qui expose réellement les fournisseurs qui manipulent ce type de données. Cyber Crucible ne collecte pas de données de santé des consommateurs — il analyse le comportement des processus et de la mémoire sur le poste de travail et n'ingère jamais le contenu des clients — il ne crée donc pas la surface de collecte et de consentement que la loi vise à encadrer.

Pourquoi la surface d'exposition est réduite

- **Aucune donnée de santé des consommateurs collectée.** Cyber Crucible ne recueille ni contenu, ni identifiants, ni inférences liés à la santé.
- **Traitement local.** L'analyse reste sur l'appareil ; il n'existe aucun ensemble de données de santé détenu par le fournisseur.
- **Aucune vente ni partage** d'informations personnelles, quelles qu'elles soient.

Remarques pour la sélection des fournisseurs

Le droit d'action privé prévu par la loi place les fournisseurs de données de santé au centre de l'examen ; Cyber Crucible ne relève tout simplement pas de cette catégorie. Cela peut être confirmé dans la documentation de gouvernance des données disponible sur demande. Ceci ne constitue pas un conseil juridique — une entité couvrée devrait évaluer ses propres obligations avec l'aide d'un conseiller juridique.

Comment Cyber Crucible prend-elle en charge les nouvelles lois de confidentialité des États américains 2025-2026 ?

Réponse courte : Une vague de lois complètes sur la confidentialité des États est entrée en vigueur en 2025 et 2026 — notamment dans le New Jersey, le Delaware, l'Iowa, le Nebraska, le New Hampshire, le Tennessee, le Minnesota, le Maryland, et, en 2026, l'Indiana, le Kentucky et le Rhode Island. Elles partagent une structure commune, et le rôle de sous-traitant de Cyber Crucible ainsi que sa conception sans collecte les prennent en charge de la même manière : peu de données personnelles en dépôt, traitement contractuellement limité, et sécurité raisonnable.

La structure commune de ces lois

- Un contrat de sous-traitance obligatoire limitant le fournisseur aux instructions du responsable du traitement.
- Des obligations de minimisation des données et de limitation des finalités.
- Des droits des consommateurs (accès, suppression, opt-out), avec de plus en plus de signaux d'opt-out universels.
- Des mesures de sécurité raisonnables et une notification en cas de violation.

Pourquoi une seule réponse couvre l'ensemble

Étant donné que Cyber Crucible ne collecte jamais le contenu, les identifiants ou les clés des clients et effectue le traitement sur le point de terminaison (endpoint), les obligations qui varient d'un État à l'autre — essentiellement liées au traitement et à la divulgation des données personnelles — ont très peu de matière à laquelle s'appliquer. Un accord de traitement des données unique et cohérent prend en charge l'ensemble. La loi du Maryland mérite d'être mentionnée pour sa norme de minimisation des données plus stricte, que la conception sans collecte prend bien en charge.

La limite honnête

Les seuils et dates d'entrée en vigueur des États évoluent, et ceci ne constitue pas un avis juridique ; un responsable du traitement doit confirmer quelles lois s'appliquent à lui. Cyber Crucible ne détient aucune « certification » d'État — elle appuie les obligations du responsable du traitement. La documentation est disponible à l'adresse **dpo@cybercrucible.com**.