Guides internationaux sur les risques liés aux fournisseurs

Réponses aux risques fournisseurs pays par pays au-delà des guides existants pour le Golfe, l'Afrique et l'UE/le Royaume-Uni — Canada, Australie, Inde, Singapour, Japon, Brésil, Suisse, Nouvelle-Zélande, Corée du Sud et Turquie. Indique clairement ce que Cyber Crucible détient et comment l'architecture prend en charge chaque régime.

Cyber Crucible est-il conforme à la LPRPDE du Canada et à la Loi 25 du Québec ?

Réponse courte : Cyber Crucible soutient les obligations d'une organisation canadienne au titre de la LPRPDE et de la Loi 25 du Québec principalement en effectuant le traitement au niveau du point de terminaison et en ne collectant aucun contenu client, identifiant ou clé — il y a donc peu de renseignements personnels sous sa garde à protéger, divulguer ou transférer. Il agit en tant que fournisseur de services sous le contrôle de l'organisation, avec une entente de traitement des données disponible.

Comment cela s'aligne

- **Responsabilisation et mesures de sécurité.** Un chiffrement robuste, un contrôle d'accès et un traitement local appuient le principe de mesures de sécurité de la LPRPDE.
- **Spécificités de la Loi 25.** Les réformes progressives du Québec ont ajouté des obligations de déclaration des incidents de confidentialité, la protection des renseignements personnels par défaut, ainsi que des règles sur les transferts hors du Québec ; la conception sans collecte de données, pouvant fonctionner sur site, appuie les préférences de résidence des données et limite l'exposition liée aux transferts.
- **Soutien en cas d'atteinte.** La communication rapide des informations relatives à un incident aide l'organisation à respecter ses obligations de déclaration au titre de la LPRPDE et de la Loi 25.

La limite à préciser honnêtement

La conformité relève de l'organisation ; Cyber Crucible est un contrôle de soutien et un sous-traitant. Il ne détient aucune certification canadienne. Une entente de traitement des données et la documentation associée sont disponibles auprès de **dpo@cybercrucible.com**.

Cyber Crucible est-il conforme à la loi australienne sur la protection de la vie privée (Privacy Act) et aux APP ?

Réponse courte : Cyber Crucible soutient les obligations d'une entité australienne au titre du Privacy Act 1988 et des Australian Privacy Principles en minimisant les données — l'entreprise ne collecte aucun contenu client, aucune information d'identification, ni aucune clé — et en traitant les données localement sur le terminal. Cela répond directement à l'APP 11 (sécurité des informations personnelles) et limite l'exposition liée à la divulgation transfrontalière au titre de l'APP 8.

Comment cela s'aligne

- **Sécurité APP 11** — chiffrement, contrôle d'accès et protection autonome des terminaux.
- **Transfert transfrontalier APP 8** — le déploiement sur site conserve les informations personnelles en Australie lorsque cela est requis ; aucun contenu client n'est transféré à l'étranger pour le traitement de sécurité.
- **Assistance en cas de violation** — informations sur les incidents pour soutenir les obligations du dispositif Notifiable Data Breaches.

Remarques pour la sélection des fournisseurs

Le régime de sanctions australien pour les violations graves ou répétées de la vie privée a été considérablement renforcé, ce qui accroît la vigilance envers les fournisseurs. L'empreinte de données minimale maintient un faible niveau de risque du côté du fournisseur. La documentation est disponible sur demande.

Cyber Crucible est-il conforme à la loi indienne sur la protection des données personnelles numériques (DPDP) ?

Réponse courte : Cyber Crucible soutient les obligations d'un responsable de données (« data fiduciary ») en vertu de la loi indienne Digital Personal Data Protection Act en agissant comme un sous-traitant de données qui ne collecte pratiquement aucune donnée personnelle et traite les données au niveau du poste de travail (endpoint). Étant donné que le contenu client n'est jamais collecté, les obligations de consentement, de limitation de la finalité et d'effacement n'ont qu'une portée minimale dans le cadre de sa garde des données.

En quoi cela est conforme

- **Rôle de sous-traitant** dans le cadre d'un contrat avec le responsable de données.
- **Minimisation des données** — aucun contenu client, identifiant ou clé n'est collecté.
- **Mesures de sécurité et assistance en cas de violation** pour les obligations du responsable de données.

Notes pour la sélection des fournisseurs

L'Inde a notifié les DPDP Rules, 2025 en novembre 2025, les obligations substantielles entrant progressivement en vigueur sur environ les 18 mois suivants ; les détails opérationnels (gestion du consentement, signalement des violations, mécanismes de transfert transfrontalier) sont donc encore en cours de mise en application. En attendant, le déploiement sur site (on-premises) permet de répondre aux préférences en matière de résidence des données. Cyber Crucible ne détient aucune certification indienne et soutient, plutôt qu'il n'assume, les obligations du responsable de données. La documentation est disponible sur demande.

Cyber Crucible est-il conforme à la PDPA de Singapour ?

Réponse courte : Cyber Crucible soutient les obligations d'une organisation au titre de la Personal Data Protection Act de Singapour en tant qu'intermédiaire de données qui effectue le traitement au niveau du poste de travail et ne collecte aucun contenu client, identifiant ou clé. Les obligations de protection et de limitation des transferts ont peu de prise, car très peu de données personnelles sont en sa possession.

Comment cela s'aligne

- **Rôle d'intermédiaire de données** dans le cadre d'un contrat écrit.
- **Obligation de protection** — chiffrement, contrôle d'accès et prévention au niveau du poste de travail.
- **Limitation des transferts** — déploiement sur site et absence de transfert offshore du contenu client à des fins de traitement de sécurité.

Remarques pour la sélection des fournisseurs

La PDPA de Singapour comprend un régime obligatoire de notification des violations de données ; la communication rapide d'informations sur les incidents y contribue. Un accord de traitement des données est disponible sur demande.

Cyber Crucible est-il conforme à la loi APPI du Japon ?

Réponse courte : Cyber Crucible soutient les obligations d'un opérateur commercial en vertu de la loi japonaise sur la protection des informations personnelles (APPI) en minimisant les données et en traitant localement. Il ne collecte aucun contenu client, identifiant ou clé, de sorte que les règles relatives au traitement, à la fourniture à des tiers et aux transferts transfrontaliers ont une portée minimale dans sa garde.

Comment cela s'aligne

- **Traitement sécurisé** — chiffrement, contrôle d'accès et protection des terminaux.
- **Transfert transfrontalier** — le déploiement sur site permet de conserver les données personnelles au Japon ; aucun contenu client n'est transféré à l'étranger pour le traitement de sécurité.
- **Support en cas de violation** — informations sur les incidents pour appuyer les attentes de signalement de l'APPI.

Notes pour la sélection des fournisseurs

Les amendements à l'APPI ont renforcé les règles de signalement des violations et les règles transfrontalières ; l'empreinte de données minimale allège les obligations des fournisseurs. La documentation est disponible sur demande.

Cyber Crucible est-elle conforme à la LGPD du Brésil ?

Réponse courte : Cyber Crucible soutient les obligations d'un responsable du traitement en vertu de la Lei Geral de Proteção de Dados (LGPD) du Brésil en tant qu'opérateur (sous-traitant) qui traite les données au niveau du point de terminaison (endpoint) et ne collecte aucun contenu client, identifiant ou clé. La plupart des obligations de la LGPD — base légale, droits des personnes concernées, règles de transfert — ont une surface d'exposition minimale, car peu de données personnelles sont sous sa garde.

Comment cela s'aligne

- **Rôle d'opérateur** sous contrat, traitant les données selon les instructions du responsable du traitement.
- **Mesures de sécurité** — chiffrement, contrôle d'accès et prévention autonome au niveau du point de terminaison.
- **Soutien en cas de violation** pour les obligations de notification du responsable du traitement auprès de l'ANPD.

Remarques sur la sélection des fournisseurs

L'ANPD a été de plus en plus active en matière d'application et de directives sur les transferts ; le déploiement sur site soutient les préférences en matière de résidence des données. Cyber Crucible ne détient aucune certification brésilienne et soutient les obligations du responsable du traitement. La documentation est disponible sur demande.

Cyber Crucible est-il conforme à la LPD suisse révisée ?

Réponse courte : Cyber Crucible soutient les obligations d'une organisation suisse au titre de la Loi fédérale sur la protection des données révisée (LPD révisée) en minimisant les données et le traitement localement sur le point de terminaison. Étant donné qu'il ne collecte aucun contenu client, aucune information d'identification ni aucune clé, les obligations relatives à la sécurité, au registre des activités de traitement et aux transferts n'ont qu'une portée minimale dans le cadre de sa garde.

Comment cela s'aligne

- **Rôle de sous-traitant** dans le cadre d'un accord de traitement des données.
- **Sécurité dès la conception** — le chiffrement, le contrôle d'accès et la prévention au niveau du point de terminaison soutiennent l'obligation de sécurité des données de la LPD révisée.
- **Transfert transfrontalier** — le déploiement sur site permet de conserver les données personnelles en Suisse lorsque cela est requis ; des Clauses Contractuelles Types sont disponibles pour les transferts.

Notes pour la sélection des fournisseurs

La LPD révisée s'aligne étroitement sur le RGPD, de sorte qu'une grande partie du support GDPR de Cyber Crucible s'applique également. La documentation, y compris les CCT, est disponible sur demande.

Cyber Crucible est-il conforme à la loi néo-zélandaise sur la protection de la vie privée de 2020 (Privacy Act 2020) ?

Réponse courte : Cyber Crucible soutient les obligations d'un organisme néo-zélandais au titre du Privacy Act 2020 en ne collectant aucun contenu client, aucune information d'identification ni aucune clé, et en effectuant le traitement au niveau du poste (endpoint). Les principes de protection des informations (Information Privacy Principles) — en particulier le stockage et la sécurité (IPP 5) et la divulgation transfrontalière (IPP 12) — présentent une surface d'exposition minimale, car peu d'informations personnelles sont sous sa garde.

Comment cela s'aligne

- **Sécurité (IPP 5)** — chiffrement, contrôle d'accès et protection autonome des postes de travail.
- **Transfert transfrontalier (IPP 12)** — le déploiement sur site conserve les informations personnelles en Nouvelle-Zélande ; aucun contenu client n'est transféré à l'étranger pour le traitement de sécurité.
- **Assistance en cas de violation** pour les obligations de l'organisme en matière de notification des violations de la vie privée devant être signalées.

Notes pour la sélection des fournisseurs

Le Privacy Act 2020 a introduit une notification obligatoire des violations et des avis de conformité ; la transmission rapide des informations sur les incidents soutient les deux. La documentation est disponible sur demande.

Cyber Crucible prend-il en charge la loi PIPA de Corée du Sud ?

Réponse courte : Cyber Crucible facilite le respect des obligations d'une organisation au titre de la loi PIPA (Personal Information Protection Act) de Corée du Sud — l'un des régimes les plus stricts au monde — en minimisant les données et le traitement sur le point de terminaison. Il ne collecte aucun contenu client, aucun identifiant ni aucune clé, de sorte que les obligations relatives au consentement, au traitement et aux transferts transfrontaliers présentent une surface minimale au sein de sa garde.

Comment cela s'aligne

- **Rôle de sous-traitant** sous contrat, selon les instructions du responsable du traitement.
- **Garanties solides** — le chiffrement, le contrôle d'accès et la prévention au niveau du point de terminaison répondent aux exigences de sécurité rigoureuses de la PIPA.
- **Transfert transfrontalier** — le déploiement sur site permet de conserver les informations personnelles en Corée ; aucun contenu client n'est transféré à l'étranger pour le traitement de sécurité.

Remarques pour la sélection des fournisseurs

La PIPA prévoit des sanctions importantes et des exigences de sécurité détaillées ; l'empreinte minimale des données et l'option de déploiement sur site maintiennent un faible niveau de risque du côté du fournisseur. La documentation est disponible sur demande.

Cyber Crucible est-il conforme à la loi turque KVKK ?

Réponse courte : Cyber Crucible soutient les obligations d'un responsable du traitement au titre de la loi turque sur la protection des données personnelles (KVKK) en ne collectant aucun contenu client, identifiant ou clé, et en traitant les données au niveau du terminal (endpoint). Les obligations d'enregistrement, de sécurité et de transfert présentent une surface minimale, car il y a peu de données personnelles sous sa garde.

Conformité

- **Rôle de sous-traitant** dans le cadre du contrat.
- **Mesures de sécurité** — le chiffrement, le contrôle d'accès et la prévention au niveau des terminaux appuient l'exigence de mesures techniques de la KVKK.
- **Transfert transfrontalier** — le déploiement sur site favorise les préférences de résidence des données dans le cadre des règles de transfert turques.

Remarques pour la sélection des fournisseurs

Le régime de transfert de la KVKK et les obligations d'enregistrement VERBIS incombent au responsable du traitement ; Cyber Crucible soutient ces obligations, sans les assumer. La documentation est disponible sur demande.