Guides de conformité par pays

Réponses juridiction par juridiction — ce que la loi de protection des données de chaque pays exige spécifiquement, et comment l'architecture de Cyber Crucible y répond. Golfe, Afrique, Europe et Royaume-Uni.

- Cyber Crucible est-il conforme à la loi PDPL de l'Arabie saoudite ?
- Cyber Crucible est-il conforme à la loi émiratie sur la protection des données ?
- Cyber Crucible est-il conforme à la loi de Bahreïn sur la protection des données ?
- Cyber Crucible est-il conforme à la loi qatarienne sur la protection des données ?
- Cyber Crucible respecte-t-il la loi omanaise sur la protection des données ?
- Le Koweït ne dispose pas d'une loi globale sur la protection des données — qu'est-ce que cela signifie pour la sélection des fournisseurs ?
- Cyber Crucible est-il conforme à la loi kenyane sur la protection des données ?
- Cyber Crucible respecte-t-il l'exigence de localisation des données du Nigéria ?
- Cyber Crucible est-il conforme à la loi POPIA d'Afrique du Sud ?
- Cyber Crucible est-il conforme à la loi égyptienne sur la protection des données ?
- Cyber Crucible est-il conforme à la loi ghanéenne sur la protection des données (Data Protection Act) ?
- Cyber Crucible répond-il à l'exigence de localisation des données de la Zambie ?
- Cyber Crucible est-il conforme à la loi rwandaise sur la protection des données ?
- Cyber Crucible respecte-t-elle la loi marocaine sur la protection des données ?
- Quelles sont les exigences en matière de protection des données en Libye ?
- Cyber Crucible est-il conforme au RGPD ?
- Cyber Crucible est-il conforme au RGPD britannique (UK GDPR) ?

Cyber Crucible est-il conforme à la loi PDPL de l'Arabie saoudite ?

Réponse courte : Cyber Crucible a examiné ses opérations au regard de la loi saoudienne sur la protection des données personnelles (PDPL), utilise des clauses contractuelles types (SCC) approuvées par la SDAIA pour tout transfert de données personnelles d'origine saoudienne, et peut être déployé entièrement à l'intérieur du Royaume sans aucun flux transfrontalier. Il ne collecte que des données de télémétrie système et de sécurité — jamais le contenu de fichiers, de documents, de courriels ou de communications.

Ce que la loi exige

La PDPL est entrée en vigueur le 14 septembre 2023, avec une période de grâce jusqu'au 14 septembre 2024. L'Arabie saoudite maintient l'une des préférences de localisation les plus strictes du Golfe, et la Saudi Data & AI Authority (SDAIA) en assure la supervision. Les transferts hors du Royaume nécessitent une garantie reconnue ainsi que, dans la plupart des cas, une évaluation des risques liés au transfert (Transfer Risk Assessment).

Ce qui s'applique spécifiquement ici

- **Des SCC pré-approuvées par la SDAIA** sont utilisées pour tout transfert de données personnelles d'origine saoudienne vers les États-Unis, adoptées sans modification hormis les champs requis, et étendues à tout sous-traitant ultérieur.
- **Une évaluation des risques liés au transfert** a été réalisée conformément aux directives structurées de la SDAIA — flux de données, régime juridique de destination, contrôles, risque résiduel, mesures d'atténuation documentées.
- **Rôle de sous-traitant** — Cyber Crucible agit normalement en tant que sous-traitant dans le cadre d'un accord de traitement des données (DPA) écrit ; le client saoudien est responsable du traitement.
- **Représentant local au titre de l'article 33** — en tant que sous-traitant, cette obligation incombe à vous, en tant que responsable du traitement.

La solution la plus simple

Compte tenu de la préférence pour la localisation, le déploiement entièrement sur site et isolé (air-gapped) constitue la réponse la plus solide : toute la gestion du backend s'effectue au sein de vos propres baies physiquement sécurisées, sans aucune télémétrie sortante. Là où rien ne traverse la frontière, les obligations liées au transfert ne s'appliquent pas.

> Les SCC et l'évaluation des risques liés au transfert (TRA) sont disponibles auprès de **dpo@cybercrucible.com**. Statut valable à la date de rédaction — veuillez confirmer les exigences en vigueur auprès de votre conseil juridique local.

Cyber Crucible est-il conforme à la loi émiratie sur la protection des données ?

Réponse courte : Oui, dans le cadre de la même architecture — collecte minimale, traitement local, et options de déploiement où les données ne quittent jamais le pays. Un point spécifique aux Émirats arabes unis mérite attention : si votre entité relève de la DIFC ou de l'ADGM, un régime différent s'applique par rapport à la loi fédérale.

Ce que la loi exige

Le décret-loi fédéral n° 45 de 2021 des Émirats arabes unis établit le cadre fédéral de protection des données personnelles. Il autorise un éventail plus large de bases légales que les régimes du Golfe davantage centrés sur le consentement, et adopte une approche fondée sur les risques et les garanties en matière de transfert transfrontalier, plutôt qu'une localisation stricte. La mise en œuvre a dépendu des règlements d'application — un domaine qui a évolué, il convient donc de vérifier la position actuelle.

La question des zones franches

C'est un piège fréquent. Le DIFC (Dubai International Financial Centre) et l'ADGM (Abu Dhabi Global Market) disposent de leurs propres régimes de protection des données, distincts de la loi fédérale. Si votre entité est établie dans l'une ou l'autre de ces zones, les règles applicables et l'autorité de contrôle diffèrent.

Déterminez quel cadre vous régit avant d'évaluer tout fournisseur — la réponse détermine ce que vous devez être en mesure de démontrer.

Ce qui s'applique spécifiquement ici

- **Flexibilité de la base légale** — l'éventail plus large de bases signifie qu'un raisonnement de type « intérêt légitime » pour le traitement lié à la sécurité est généralement plus praticable que dans les régimes centrés sur le consentement.
- **Garanties relatives aux transferts** — la mise en zone régionale (staging) maintient le traitement au sein des Émirats arabes unis ; un déploiement en air gap élimine totalement

le transfert.
- **Rôle de sous-traitant** dans le cadre d'un DPA écrit, selon vos instructions documentées.

> Statut au moment de la rédaction — vérifiez les exigences actuelles, y compris les règlements d'application et l'applicabilité aux zones franches, auprès d'un conseil juridique local.

Cyber Crucible est-il conforme à la loi de Bahreïn sur la protection des données ?

Réponse courte : Oui. La loi de Bahreïn s'inspire fortement du RGPD avec une portée extraterritoriale, de sorte que les mêmes contrôles qui satisfont au RGPD s'appliquent — collecte minimale, rôle de sous-traitant documenté, mesures de sécurité solides et transfert contrôlé.

Ce que la loi exige

Bahreïn dispose d'une loi autonome sur la protection des données en vigueur depuis 2019. Elle est souvent citée comme l'une des plus claires et des plus abouties du Golfe, avec des droits solides pour les personnes concernées, des obligations de responsabilité explicites, et une **application extraterritoriale** — ce qui signifie qu'elle peut s'appliquer à des fournisseurs situés hors de Bahreïn traitant des données de résidents bahreïniens.

Ce qui s'applique spécifiquement ici

La portée extraterritoriale est le point à souligner. Cela signifie que la question ne porte pas seulement sur *votre* propre conformité, mais aussi sur celle de vos fournisseurs.

- **Responsabilité (accountability)** — la liste des données exclues (aucune clé, identifiant, jeton ou contenu) est explicite et documentée plutôt que décrite en termes généraux, ce qui correspond exactement à ce qu'exigent les obligations de responsabilité.
- **Droits des personnes concernées** — limités en pratique ici, car la télémétrie comportementale est pseudonymisée et le contenu n'est jamais collecté, de sorte que le volume de données personnelles soumises à des demandes d'exercice de droits est minime.
- **Transfert** — hébergement régional ou déploiement isolé (air-gapped).

Pourquoi l'alignement avec le RGPD est utile

Comme la loi de Bahreïn suit de près le RGPD, la cartographie RGPD s'applique presque directement. Si votre organisation a déjà réalisé un travail d'évaluation des fournisseurs conforme au RGPD, l'essentiel de ce travail reste valable.

> Statut au moment de la rédaction — à confirmer auprès d'un conseil juridique local.

Cyber Crucible est-il conforme à la loi qatarienne sur la protection des données ?

Réponse courte : Oui. Le régime du Qatar est plus centré sur le consentement que celui de ses voisins, ce qui rend la collecte minimale particulièrement précieuse — moins de données personnelles sont traitées, plus la charge liée au consentement est réduite.

Ce que la loi exige

Le Qatar dispose d'une loi autonome sur la protection des données en vigueur depuis 2017, ce qui en fait l'une des premières de la région. Il maintient un modèle plus strict, centré sur le consentement, par rapport à l'ensemble plus large de bases légales des Émirats arabes unis, ainsi qu'une approche fondée sur le risque pour les garanties relatives aux transferts.

Pourquoi la centralité du consentement favorise cette architecture

Dans un régime centré sur le consentement, chaque catégorie de données personnelles que vous traitez est une catégorie pour laquelle vous pourriez avoir besoin d'une base légale. Cela rend le fait de *ne pas collecter* nettement plus précieux que le fait de bien protéger.

Cyber Crucible ne collecte jamais de clés de chiffrement, d'identifiants, de jetons de session ni de contenu de fichiers. La télémétrie comportementale est pseudonymisée lorsqu'elle pourrait identifier une personne, et les sources de télémétrie sont configurables afin que vous puissiez restreindre davantage la collecte.

Le résultat est que la surface de consentement pour l'outil de sécurité lui-même est exceptionnellement réduite.

Transfert

Le staging régional maintient le traitement à proximité ou à l'intérieur de la juridiction ; le déploiement en air-gapped élimine entièrement les flux transfrontaliers.

> Statut au moment de la rédaction — à confirmer auprès d'un conseiller juridique local.

Cyber Crucible respecte-t-il la loi omanaise sur la protection des données ?

Réponse courte : Oui — et Oman est actuellement la juridiction la plus sensible au facteur temps dans le Golfe. La loi omanaise sur la protection des données personnelles entre pleinement en vigueur le **5 février 2026**, à l'issue d'une période de grâce de deux ans, de sorte que les solutions fournisseurs qui étaient conformes par défaut entrent désormais dans le champ d'application.

Ce qu'exige la loi

La loi omanaise reprend étroitement les principes du RGPD tout en intégrant des exigences locales concernant le consentement et le traitement des données. La période de grâce de deux ans se termine le 5 février 2026, date à laquelle une conformité totale est attendue.

Pourquoi cela importe pour la sélection des fournisseurs dès maintenant

Les périodes de grâce créent un schéma prévisible : les organisations reportent l'examen de leurs fournisseurs jusqu'à l'approche de l'échéance, puis découvrent qu'un outil de sécurité exportant en continu la télémétrie des terminaux vers une autre juridiction est difficile à justifier dans le cadre du nouveau régime.

Si vous examinez votre pile technologique en vue de l'échéance de février 2026, voici les questions à poser à tout fournisseur de solutions de protection des terminaux :

1. Quelles données personnelles collecte-t-il, de manière précise et énumérée ?
2. Où ces données sont-elles traitées, et peuvent-elles être conservées à Oman ?
3. Quel est le mécanisme de transfert si elles quittent le pays ?
4. Peut-il fonctionner sans aucune télémétrie sortante ?

Les réponses de Cyber Crucible sont les suivantes : exclusions énumérées (aucune clé, identifiant, jeton ou contenu) ; le traitement est local à l'appareil terminal ; une mise en attente régionale (staging) est disponible ; et oui — le déploiement en air gap ne produit aucune télémétrie sortante.

> Statut au moment de la rédaction — veuillez confirmer la position actuelle et toute prolongation éventuelle auprès d'un conseiller juridique local.

Le Koweït ne dispose pas d'une loi globale sur la protection des données — qu'est-ce que cela signifie pour la sélection des fournisseurs ?

Réponse courte : Le Koweït a adopté une approche sectorielle ciblée plutôt que de promulguer une loi nationale globale sur la protection des données, la réglementation de la CITRA encadrant la manière dont les secteurs des télécommunications et des technologies de l'information traitent le contenu des utilisateurs. Cela fait de la souveraineté des données une décision commerciale et sécuritaire plutôt qu'une obligation de conformité — mais la décision n'en demeure pas moins importante.

La situation actuelle

Le Koweït demeure l'exception notable parmi les principaux États du Golfe en ne disposant d'aucune loi nationale globale sur la protection des données personnelles. À la place, la réglementation de la CITRA traite spécifiquement du traitement du contenu des utilisateurs dans les télécommunications et les technologies de l'information.

Pourquoi « absence de loi » ne signifie pas « absence de risque »

Trois raisons pour lesquelles les organisations au Koweït pèsent encore cette question avec attention :

1. **Les règles sectorielles s'appliquent toujours.** Si vous opérez dans les télécommunications ou les technologies de l'information, les exigences de la CITRA constituent des obligations effectives.
2. **Les contreparties imposent des conditions.** Les partenaires multinationaux, les assureurs et les clients exigent fréquemment, par voie contractuelle, un traitement

équivalent au GDPR, indépendamment de la loi locale.
3. **La réglementation finit généralement par arriver.** Tous les autres États du CCG ont désormais promulgué une loi globale. Choisir des fournisseurs qui satisfont déjà à des régimes plus stricts permet d'éviter une migration forcée par la suite.

La position pratique

Étant donné que Cyber Crucible ne collecte jamais de clés, d'identifiants, de jetons ou de contenu, et peut être déployé de manière entièrement isolée du réseau (air-gapped), il satisfait aux régimes les plus stricts de la région. Le choisir au Koweït, c'est choisir de ne pas avoir ce problème lorsque la loi changera.

> Situation au moment de la rédaction — confirmez les exigences sectorielles actuelles auprès d'un conseiller juridique local.

Cyber Crucible est-il conforme à la loi kenyane sur la protection des données ?

Réponse courte : Oui. La loi kenyane de 2019 sur la protection des données (Data Protection Act 2019) restreint le transfert transfrontalier vers des pays dotés de garanties appropriées, et applique une règle plus stricte aux données personnelles sensibles. Cyber Crucible ne collecte aucune donnée personnelle sensible, et peut être déployé de manière à ce qu'aucune donnée ne quitte le Kenya.

Ce qu'exige la loi

Les articles 48 et 49 de la Data Protection Act 2019 interdisent le transfert de données personnelles vers un pays ne disposant pas de garanties appropriées en matière de sécurité des données, avec plusieurs bases autorisées, dont l'adéquation.

La règle plus stricte qui compte : le transfert de données personnelles *sensibles* n'est autorisé que lorsque la personne concernée a donné son consentement **et** que des garanties appropriées existent. Les deux conditions, pas l'une ou l'autre.

Pourquoi la règle sur les données sensibles est le point clé

Cette double exigence est difficile à satisfaire sur le plan opérationnel — obtenir et prouver le consentement individuel de chaque personne concernée, de manière continue, pour un outil de sécurité.

Cyber Crucible contourne ce problème : **aucune donnée personnelle sensible n'est collectée.** Ni données biométriques, de santé ou génétiques ; ni données révélant l'origine raciale ou ethnique, les convictions religieuses ou les opinions politiques. Les données de télémétrie décrivent le comportement du système et les événements de sécurité, et non des attributs personnels.

Lorsque des données de télémétrie comportementale pourraient indirectement identifier une personne, les identifiants sont pseudonymisés ou masqués.

Transfert

Le stockage intermédiaire régional maintient le traitement à l'intérieur du Kenya. Le déploiement en air-gap ne produit aucune télémétrie sortante, de sorte que les articles 48 à 49 ne s'appliquent pas.

> Statut au moment de la rédaction — à confirmer auprès d'un conseil juridique local.

Cyber Crucible respecte-t-il l'exigence de localisation des données du Nigéria ?

Réponse courte : Oui — et c'est la juridiction où l'architecture importe le plus. La Nigeria Data Protection Act de 2023 impose une exigence de localisation des données : les données personnelles des citoyens nigérians doivent être stockées à l'intérieur du Nigéria. Le déploiement sur site de Cyber Crucible conserve tout au sein de votre propre infrastructure, dans le pays, sans aucune télémétrie sortante.

Ce qu'exige la loi

Les articles 41 à 43 de la Nigeria Data Protection Act de 2023 fixent des conditions pour le transfert transfrontalier, notamment des garanties dans le pays de destination et le consentement de la personne concernée. Au-delà de ces conditions, **le Nigéria impose une exigence de localisation** — les données personnelles des citoyens nigérians doivent être stockées à l'intérieur du Nigéria. Des règles sectorielles dans les services financiers ajoutent des obligations de localisation supplémentaires.

Pourquoi la plupart des fournisseurs de sécurité peinent sur ce point

C'est l'exemple le plus clair d'une règle qu'une sécurité des postes de travail dépendante du cloud ne peut pas satisfaire par conception. Un outil dont l'architecture consiste à « collecter la télémétrie sur le poste de travail, l'envoyer vers notre cloud pour analyse » déplace, structurellement, des données personnelles hors du Nigéria comme condition de son fonctionnement. Des garanties contractuelles ne résolvent pas une exigence relative au lieu de stockage.

Pourquoi cette architecture y satisfait

- **L'analyse est locale.** L'évaluation des menaces et leur interdiction se déroulent sur le poste de travail, généralement en moins de 200 millisecondes. Aucun aller-retour vers le

cloud n'est requis pour la protection.

- **Le backend peut être entièrement dans le pays.** Le modèle sur site exécute tous les logiciels de gestion au sein de vos propres racks physiquement sécurisés.
- **Zéro télémétrie sortante** dans la configuration en air gap — rien ne sort, donc rien n'est stocké à l'étranger.
- **Moins de données à localiser de toute façon** — les clés, identifiants, jetons et contenus de fichiers ne sont jamais collectés en premier lieu.

> Statut au moment de la rédaction — vérifiez les exigences actuelles, y compris les règles sectorielles financières, auprès d'un conseil juridique local.

Cyber Crucible est-il conforme à la loi POPIA d'Afrique du Sud ?

Réponse courte : Oui. La POPIA restreint les transferts transfrontaliers, sauf si la destination offre une protection substantiellement similaire ou si la personne concernée y consent. Cyber Crucible minimise dès le départ ce qui est traité, et peut être déployé de manière à ce qu'aucun transfert n'ait lieu.

Ce qu'exige la loi

La loi sud-africaine sur la protection des informations personnelles (Protection of Personal Information Act, 2013) interdit le transfert d'informations personnelles hors du pays sans le consentement de la personne concernée, sauf si la juridiction destinataire est soumise à une loi offrant une protection substantiellement similaire.

Ce qui s'applique spécifiquement ici

Le critère de « protection substantiellement similaire » constitue une évaluation que vous devez pouvoir justifier. Deux éléments simplifient cette évaluation :

1. **La portée est réduite.** Les clés de chiffrement, les identifiants, les jetons de session et le contenu des fichiers ne sont jamais collectés. Ce qui reste est constitué de télémétrie comportementale, pseudonymisée lorsqu'elle pourrait permettre d'identifier une personne.
2. **Protections contractuelles** — le traitement s'effectue dans le cadre d'un DPA écrit comprenant des clauses de sécurité, de confidentialité et de notification des violations, étendues à tout sous-traitant.

Ou éviter entièrement ce test

Le staging régional maintient le traitement en Afrique du Sud. Le déploiement en isolation complète (air-gapped) ne génère aucun flux sortant, auquel cas les dispositions relatives au transfert ne s'appliquent tout simplement pas — une voie généralement plus rapide que de démontrer l'adéquation.

> Statut au moment de la rédaction — à confirmer auprès d'un conseil juridique local.

Cyber Crucible est-il conforme à la loi égyptienne sur la protection des données ?

Réponse courte : Oui. L'Égypte exige une autorisation préalable pour les transferts transfrontaliers de données personnelles — une exigence sensiblement plus élevée que de simples garanties contractuelles. Cyber Crucible peut être déployé de manière à ce qu'aucun transfert n'ait lieu, supprimant ainsi l'exigence d'autorisation plutôt que d'avoir à la satisfaire.

Ce qu'exige la loi

Le cadre égyptien de protection des données exige une **autorisation préalable** pour les transferts de données personnelles hors du pays. Il s'agit d'un modèle fondé sur la permission plutôt que sur les garanties : on ne peut pas simplement mettre en place des protections contractuelles et procéder.

Pourquoi ce modèle d'autorisation change la sélection des fournisseurs

Dans un modèle fondé sur les garanties, un fournisseur disposant de solides clauses contractuelles est viable. Dans un modèle fondé sur l'autorisation, chaque flux transfrontalier constitue une procédure administrative comportant des délais, un pouvoir discrétionnaire et un risque de renouvellement.

Un outil de sécurité qui exporte en continu des données de télémétrie crée un flux permanent nécessitant que cette autorisation reste valide. Si l'autorisation expire ou si les conditions changent, le fonctionnement normal de l'outil devient un problème de conformité.

La réponse simple

Le déploiement sur site en environnement isolé (air-gapped) ne génère aucune télémétrie sortante — rien n'est transféré, donc aucune autorisation n'est requise. Le pré-positionnement régional permet de conserver le traitement au niveau local lorsqu'un modèle hybride est privilégié.

Les catégories les plus susceptibles d'attirer l'attention des régulateurs — clés, identifiants, jetons, contenu des fichiers — ne sont jamais collectées, quel que soit le mode de déploiement.

> Statut au moment de la rédaction — confirmez les exigences actuelles et la procédure d'autorisation auprès d'un conseiller juridique local.

Cyber Crucible est-il conforme à la loi ghanéenne sur la protection des données (Data Protection Act) ?

Réponse courte : Oui, et le Ghana constitue un cas comparativement simple. Le Ghana se distingue parmi les juridictions africaines par le fait qu'il **n'impose pas** d'exigences supplémentaires en matière de transfert transfrontalier au-delà de ses obligations générales de protection des données — les contrôles standards s'appliquent donc sans régime de transfert spécifique.

Ce que la loi exige

Le Ghana dispose d'un cadre de protection des données établi, doté d'une autorité de contrôle. L'analyse des juridictions africaines identifie systématiquement le Ghana comme l'exception : contrairement à la plupart de ses voisins, il n'ajoute pas de conditions supplémentaires spécifiquement au partage transfrontalier de données.

Cela ne signifie pas que le transfert n'est pas réglementé — les obligations générales relatives au traitement licite, à la sécurité et aux droits des personnes concernées s'appliquent toujours. Cela signifie qu'il n'existe pas d'approbation distincte ou d'obstacle d'adéquation à franchir.

Ce qui s'applique spécifiquement ici

Avec la question du transfert simplifiée, l'évaluation se réduit aux questions habituelles :

- **Que collecte-t-on ?** Uniquement la télémétrie système et de sécurité. Aucune clé, identifiant, jeton ou contenu.
- **Comment est-ce sécurisé ?** TLS 1.3 en transit, chiffrement des charges utiles JWE par agent, chiffrement au repos, contrôle d'accès basé sur les rôles.
- **Qui est responsable ?** Cyber Crucible agit en tant que sous-traitant dans le cadre d'un accord de traitement des données (DPA) écrit, selon vos instructions documentées.

La souveraineté reste néanmoins à considérer

Même en l'absence de restriction de transfert, un déploiement dans le pays ou en environnement isolé (air-gapped) reste disponible — et les organisations desservant des clients régionaux le préfèrent souvent, car les juridictions voisines sont considérablement plus strictes.

> Statut au moment de la rédaction — à confirmer auprès d'un conseil juridique local.

Cyber Crucible répond-il à l'exigence de localisation des données de la Zambie ?

Réponse courte : Oui. La loi zambienne sur la protection des données (Data Protection Act) exige que les responsables du traitement traitent et stockent les données personnelles et les données personnelles sensibles dans un centre de données ou sur un serveur **situé en Zambie**. Le déploiement sur site (on-premises) de Cyber Crucible satisfait directement à cette exigence — le backend s'exécute au sein de votre propre infrastructure, dans le pays.

Ce que la loi exige

La partie X de la loi zambienne sur la protection des données réglemente les transferts transfrontaliers, et l'article 70 oblige un responsable du traitement à traiter et stocker les données personnelles et les données personnelles sensibles dans un centre de données ou sur un serveur situé en Zambie.

Il s'agit d'une **obligation relative à l'emplacement de stockage**, et non d'un critère de garanties. Les protections contractuelles ne suffisent pas à y satisfaire.

Pourquoi cela élimine la plupart des outils de sécurité basés sur le cloud

Un fournisseur dont le produit nécessite l'envoi de la télémétrie des terminaux vers une région cloud située en dehors de la Zambie ne peut pas se conformer à l'article 70 en améliorant simplement ses contrats ou son chiffrement. L'exigence porte sur *l'endroit où les données se trouvent physiquement*.

Pourquoi cette architecture y satisfait

- **Backend sur site** — l'ensemble du logiciel de gestion s'exécute sur des serveurs que vous contrôlez, en Zambie.

- **Analyse locale** — l'évaluation des menaces et leur interdiction se produisent sur le terminal lui-même, de sorte que la protection ne dépend jamais d'un service situé hors du pays.
- **Zéro télémétrie sortante** dans la configuration en air gap.
- **Périmètre minimal** — les clés, identifiants, jetons et contenus ne sont jamais collectés, de sorte que le volume de données personnelles soumises à l'article 70 est de toute façon restreint.

> Statut valable à la date de rédaction — à confirmer auprès d'un conseil juridique local, y compris pour toute règle spécifique à un secteur donné.

Cyber Crucible est-il conforme à la loi rwandaise sur la protection des données ?

Réponse courte : Oui. La loi rwandaise sur la protection des données est supervisée par la National Cyber Security Authority, et des règles sectorielles spécifiques ajoutent des obligations de localisation — notamment pour les banques agréées, qui doivent conserver leurs données primaires au Rwanda. Le déploiement sur site (on-premises) satisfait ces deux exigences.

Ce que la loi exige

Le Rwanda a promulgué une loi sur la protection des données désignant la **National Cyber Security Authority (NCSA)** comme autorité de supervision ; son bureau de protection des données a été lancé en mars 2022.

Parallèlement à la loi générale, une réglementation sectorielle ajoute une obligation de localisation : la réglementation en matière de cybersécurité impose aux banques agréées par la Banque centrale de conserver leurs données primaires sur le territoire rwandais.

Pourquoi la règle sectorielle est la plus importante

Pour les services financiers au Rwanda, l'exigence de localisation bancaire constitue généralement la contrainte contraignante — plus stricte et plus spécifique que les dispositions générales relatives à la protection des données. Un produit de sécurité déployé sur les postes de travail d'une banque traite des données qui en relèvent.

Ce qui s'applique spécifiquement ici

- **Le déploiement sur site (on-premises)** conserve les données primaires au Rwanda, satisfaisant directement l'exigence de localisation.
- **L'analyse locale** signifie que la protection ne dépend d'aucun service situé hors du pays.

- **L'alignement avec l'autorité de supervision** — la NCSA étant à la fois l'autorité de cybersécurité et de protection des données, la capacité à démontrer *ce que* collecte un outil de sécurité, en termes énumérés, s'avère particulièrement utile.

> Statut au moment de la rédaction — veuillez confirmer les exigences générales et sectorielles actuelles auprès d'un conseil juridique local.

Cyber Crucible respecte-t-elle la loi marocaine sur la protection des données ?

Réponse courte : Oui. La loi n° 09-08 du Maroc et son décret d'application régissent le traitement des données personnelles, sous la supervision de la CNDP. Les mêmes contrôles s'appliquent — collecte minimale, rôle de sous-traitant documenté, garanties solides et déploiement dans le pays ou en environnement isolé (air-gapped) lorsque cela est préféré.

Ce que la loi exige

Le cadre juridique marocain repose sur la **loi n° 09-08** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que sur le **décret n° 2-09-165** portant application de cette loi. La **CNDP** (Commission Nationale de contrôle de la protection des Données à caractère Personnel) est l'autorité de contrôle, et elle est active dans la coopération internationale sur les enjeux émergents, notamment l'IA.

Ce qui s'applique spécifiquement ici

Le régime marocain figure parmi les plus établis d'Afrique du Nord, avec une autorité opérationnelle et des procédures de notification/autorisation qui varient selon le type de traitement. Implications pratiques pour l'évaluation d'un fournisseur :

- **Énumérer ce qui est collecté.** La liste des données exclues de Cyber Crucible est explicite — aucune clé, identifiant, jeton ou contenu — ce qui favorise l'exactitude des notifications.
- **Rôle de sous-traitant** dans le cadre d'un DPA écrit, sur instructions documentées.
- **Transfert** — hébergement régional ou déploiement en environnement isolé (air-gapped) ; ce dernier élimine la question.

Pour les organisations opérant à travers le Maghreb

Les exigences diffèrent considérablement entre le Maroc, la Tunisie, l'Algérie et la Libye. Choisir un fournisseur qui satisfait au régime applicable le plus strict — plutôt que d'évaluer chaque pays séparément — représente généralement la solution demandant le moins d'efforts.

> Statut au moment de la rédaction — à confirmer auprès d'un conseiller juridique local.

Quelles sont les exigences en matière de protection des données en Libye ?

Réponse courte : La Libye n'a pas encore élaboré de réglementation complète en matière de protection des données. Cela fait de la souveraineté des données une décision commerciale, sécuritaire et liée à la contrepartie plutôt qu'une obligation de conformité locale — mais pour les organisations gérant des opérations sensibles, cela reste une décision qu'il vaut la peine de prendre de manière délibérée.

La situation actuelle

La Libye n'a pas encore adopté de cadre complet de protection des données. Il n'existe pas d'équivalent à la PDPL saoudienne, à la loi 09-08 marocaine ou à la NDPA nigériane.

Pourquoi la souveraineté demeure importante en l'absence de loi locale

1. Les contreparties imposent des exigences. Les partenaires internationaux, les assureurs, les clients multinationaux et les bailleurs de fonds exigent régulièrement, par contrat, un traitement équivalent au RGPD, indépendamment du droit local. Respecter la norme la plus stricte permet d'éviter de devoir renégocier plus tard.

2. Les secteurs sensibles comportent leurs propres risques. L'énergie, les télécommunications, la finance et les opérations gouvernementales attirent l'attention indépendamment de toute législation sur la protection de la vie privée. L'endroit où un outil de sécurité envoie sa télémétrie — et qui peut y exiger l'accès — constitue une véritable question opérationnelle.

3. La réglementation tend à suivre. Les juridictions voisines d'Afrique du Nord ont adopté ou mis à jour leurs cadres réglementaires. Les décisions relatives aux fournisseurs prises aujourd'hui resteront valables lorsque la position de la Libye évoluera.

La position pratique

Étant donné que Cyber Crucible ne collecte jamais de clés, d'identifiants, de jetons ou de contenu, et peut fonctionner entièrement en air gap avec une télémétrie sortante nulle, il satisfait aux régimes les plus stricts de la région. En Libye, il s'agit d'un choix plutôt que d'une obligation — mais c'est un choix qui résiste bien à l'épreuve du temps.

> Situation au moment de la rédaction — veuillez confirmer la position législative actuelle auprès d'un conseiller juridique local avant de vous y fier.

Cyber Crucible est-il conforme au RGPD ?

Réponse courte : Oui, par conception plutôt que par politique. Le contenu, les identifiants, les clés de chiffrement et les jetons de session ne sont jamais collectés ; l'analyse s'effectue sur le poste (endpoint) ; Cyber Crucible agit en tant que sous-traitant dans le cadre d'un DPA écrit ; et les options de déploiement conservent les données personnelles au sein de l'UE — ou au sein de votre propre bâtiment.

Correspondance avec les principes du RGPD

- **Minimisation des données (Art. 5)** — la liste des données exclues est énumérée, et non décrite en termes généraux. La télémétrie se limite à ce qui est nécessaire à la détection des menaces et est configurable.
- **Intégrité et confidentialité (Art. 5, 32)** — TLS 1.3 en transit, chiffrement des charges utiles JWE par agent, chiffrement au repos, contrôle d'accès basé sur les rôles, rotation des clés, journalisation d'audit.
- **Obligations du sous-traitant (Art. 28)** — DPA écrit précisant le périmètre ; traitement uniquement sur instructions documentées ; sous-traitants liés par des conditions équivalentes.
- **Transferts (Chapitre V)** — hébergement intermédiaire régional dans l'UE, ou déploiement isolé du réseau (air-gapped) qui élimine tout transfert.
- **Protection des données dès la conception (Art. 25)** — l'affirmation la plus forte possible : les catégories à plus haut risque ne sont pas protégées par une politique, elles ne sont tout simplement jamais collectées.

Pseudonymisation

Lorsque la télémétrie comportementale pourrait indirectement identifier une personne, les identifiants sont pseudonymisés ou masqués — une mesure de protection expressément reconnue par le RGPD.

Ce que cela ne fait pas

Cela ne rend pas votre organisation conforme au RGPD. Vos obligations dépendent de vos propres finalités de traitement, bases légales, mentions d'information et registres. Ce que cela supprime, c'est une difficulté courante : un fournisseur de sécurité exportant en continu des données personnelles vers un pays tiers.

Cyber Crucible est-il conforme au RGPD britannique (UK GDPR) ?

Réponse courte : Oui. Le UK GDPR et le Data Protection Act 2018 suivent de près le RGPD de l'UE, de sorte que la même correspondance s'applique — collecte minimale, rôle de sous-traitant dans le cadre d'un DPA écrit, protections techniques solides, et options de déploiement qui conservent les données au Royaume-Uni ou entièrement sur vos locaux.

Ce qui s'applique

Suite au départ du Royaume-Uni de l'UE, le UK GDPR fonctionne aux côtés du Data Protection Act 2018, sous la supervision de l'Information Commissioner's Office (ICO). Les principes, bases légales et obligations des sous-traitants reflètent étroitement le RGPD de l'UE.

Points d'attention pour les organisations

- **Transferts internationaux** utilisant les mécanismes propres au Royaume-Uni — l'International Data Transfer Agreement (IDTA) ou l'UK Addendum aux clauses contractuelles types (SCC) de l'UE, plutôt que les SCC de l'UE seules.
- **Double conformité** — les organisations opérant à la fois au Royaume-Uni et dans l'UE doivent satisfaire aux deux régimes, bien que les contrôles pratiques se recoupent presque entièrement.

Ce qui s'applique spécifiquement ici

L'évaluation est la même que pour le RGPD de l'UE, et les réponses sont identiques :

- Les clés, identifiants, jetons et contenus de fichiers ne sont jamais collectés.
- L'analyse s'effectue sur le poste de travail (endpoint) ; la protection ne nécessite pas de déplacement des données.
- Hébergement régional au Royaume-Uni, ou déploiement en air-gap qui supprime entièrement le transfert.
- Rôle de sous-traitant dans le cadre d'un DPA écrit, avec des sous-traitants ultérieurs liés par des conditions équivalentes.

> Pour connaître l'instrument de transfert approprié à votre situation, contactez **dpo@cybercrucible.com**. Statut valable au moment de la rédaction — veuillez confirmer les directives actuelles de l'ICO avec votre conseil juridique.