Guides sur les risques liés aux fournisseurs de l'Union européenne et des États membres

Comment Cyber Crucible prend en charge les régimes à l'échelle de l'UE (GDPR, DORA, NIS2, l'AI Act) et les spécificités propres à chaque État membre (Allemagne, France, Irlande, Pays-Bas, Espagne, Italie, Pologne, Suède) du point de vue de la sélection des fournisseurs. Indique clairement ce que Cyber Crucible détient et ne détient pas, et ne fait aucune promesse de conformité au nom du client.

- Comment Cyber Crucible prend-il en charge les exigences de protection des données en Italie ?
- Comment Cyber Crucible prend-elle en charge les exigences de protection des données en Pologne ?
- Comment Cyber Crucible prend-elle en charge les exigences de protection des données en Suède et dans les pays nordiques ?

Quelles règles de l'UE influencent le choix d'un fournisseur de sécurité, au-delà du RGPD ?

Réponse courte : Au-delà du RGPD, trois régimes de l'UE façonnent de plus en plus la sélection des fournisseurs : DORA (résilience opérationnelle pour les entités financières et leurs prestataires TIC), NIS2 (obligations en matière de cybersécurité pour les entités essentielles et importantes, y compris la sécurité de la chaîne d'approvisionnement), et l'AI Act de l'UE (règles hiérarchisées selon le risque pour les systèmes d'IA). Chacun de ces régimes fait peser des obligations sur les fournisseurs. La conception de Cyber Crucible — aucun contenu client collecté, traitement local, option sur site — soutient les obligations du client au titre de chacun d'eux, sans que Cyber Crucible ne revendique une conformité au nom du client.

Le paysage en un coup d'œil

- **RGPD** — la référence de base pour le traitement des données personnelles dans toute l'UE. Consultez la page RGPD des Guides de conformité par pays.
- **DORA** — s'applique à partir du 17 janvier 2025 aux entités financières et, surtout, à leurs prestataires tiers de services TIC.
- **NIS2** — les États membres devaient la transposer avant octobre 2024 ; en 2026, la plupart l'ont fait, tandis que plusieurs finalisaient encore leur législation nationale.
- **AI Act de l'UE** — obligations hiérarchisées selon le risque, mises en œuvre progressivement jusqu'en 2026-2027.

Comment Cyber Crucible s'intègre

Le thème récurrent est le risque lié à la chaîne d'approvisionnement et aux tiers. Étant donné que Cyber Crucible ne collecte aucun contenu client, aucune information d'identification ni clé, et peut fonctionner entièrement à l'intérieur du périmètre du client, il réduit la surface que ces régimes visent à contrôler. Les pages de cet ouvrage traitent chaque régime et les principaux États membres. La documentation est disponible à l'adresse **dpo@cybercrucible.com**.

Comment Cyber Crucible accompagne-t-il les entités financières européennes dans le cadre de DORA ?

Réponse courte : Cyber Crucible est un prestataire tiers de services TIC au sens de DORA, et il accompagne les obligations DORA d'une entité financière — contrôles contractuels, informations sur les incidents et tests de résilience — tout en réduisant le risque tiers TIC, car il ne collecte jamais les données de l'entité. DORA s'applique à compter du 17 janvier 2025. Cyber Crucible ne prétend pas être « conforme à DORA » au nom d'un client ; la conformité relève de l'entité financière, et Cyber Crucible fournit le soutien et les preuves dont son programme a besoin.

Comment il soutient le programme DORA de l'entité

- **Réduction du risque TIC.** Aucun contenu client, identifiant ou clé n'est collecté, et la protection s'exécute localement — réduisant ainsi la surface d'attaque tierce que DORA vise.
- **Contrôles contractuels.** Cyber Crucible peut intégrer les dispositions contractuelles attendues par DORA pour les accords avec des prestataires tiers TIC (sécurité, coopération en cas d'incident, droits d'audit et d'information, transparence en matière de sous-traitance).
- **Coopération en cas d'incident.** Un processus documenté de réponse aux violations fournit des informations rapides et de qualité probante, et un délai de notification contractuel est disponible pour soutenir les obligations de signalement d'incidents de l'entité.
- **Résilience.** La protection des postes de travail continue de fonctionner en cas de panne du back-end de gestion, ce qui soutient les objectifs de résilience opérationnelle.

La limite en toute transparence

DORA permet également aux Autorités européennes de surveillance de désigner des prestataires tiers de services TIC **critiques** (CTPP) pour une surveillance directe au niveau de l'UE. Cyber

Crucible n'est pas désigné comme CTPP et ne se présente pas comme tel. Il soutient les obligations de l'entité financière ; il ne les assume pas.

Comment Cyber Crucible soutient-il les obligations NIS2 pour les entités essentielles et importantes ?

Réponse courte : Pour une organisation classée comme entité essentielle ou importante au titre de NIS2, Cyber Crucible soutient les mesures de gestion des risques requises — protection des postes de travail, contrôle des accès, chiffrement et gestion des incidents — et soutient les exigences de la directive en matière de sécurité de la chaîne d'approvisionnement, car il ne collecte aucune donnée client et peut fonctionner à l'intérieur du périmètre de l'entité. Cyber Crucible soutient ces obligations ; il ne les certifie ni ne les assume.

Comment il soutient les mesures NIS2

- **Mesures de gestion des risques de cybersécurité.** La prévention autonome des postes de travail, l'accès sécurisé par MFA et le chiffrement correspondent à plusieurs des mesures de référence de la directive.
- **Sécurité de la chaîne d'approvisionnement.** En tant que fournisseur qui ne collecte aucun contenu client et propose un déploiement sur site, Cyber Crucible réduit plutôt qu'il n'ajoute au risque de chaîne d'approvisionnement que NIS2 demande aux entités de gérer.
- **Soutien à la gestion et au signalement des incidents.** Un processus documenté de réponse aux violations aide l'entité à respecter les délais d'alerte précoce et de notification imposés par NIS2.

La limite honnête

Les obligations NIS2 incombent à l'entité essentielle ou importante, et non à un outil de sécurité individuel. La transposition par les États membres a varié : d'ici 2026, la plupart des États avaient transposé la directive dans leur droit national, tandis que plusieurs — dont la France, l'Irlande, les Pays-Bas et l'Espagne — étaient encore en train de la finaliser. Cyber Crucible ne détient aucune « certification » NIS2 ; il fournit des éléments de preuve à l'appui des contrôles sous accord de confidentialité (NDA).

Quel est le lien entre Cyber Crucible et l'AI Act de l'UE ?

Réponse courte : Cyber Crucible n'utilise l'IA que pendant la phase de développement (ses travaux de découverte par IA génétique) et exécute des heuristiques déterministes et fixes en temps d'exécution — il n'y a aucun modèle d'IA en direct prenant des décisions sur le terminal du client. Cyber Crucible n'introduit donc pas de système d'IA à haut risque ou à usage général dans l'environnement du client. Le client reste responsable de l'évaluation de ses propres obligations au titre de l'AI Act de l'UE, dont les exigences entrent en vigueur progressivement jusqu'en 2026-2027.

Pourquoi l'architecture importe ici

- **Aucun système d'IA en temps d'exécution déployé chez le client.** Le terminal exécute des heuristiques noyau déterministes, et non un modèle en direct — il n'existe donc aucun système d'IA embarqué que le client devrait classifier et gouverner au titre du règlement.
- **Uniquement en phase de développement.** Les travaux d'IA se déroulent dans l'environnement de développement interne de Cyber Crucible, sur des jeux de données de recherche internes ; aucun contenu, identifiant ou clé du client n'est utilisé pour entraîner, alimenter ou ajuster un modèle.
- **Transparence.** Comme le comportement en temps d'exécution est déterministe et testable plutôt que probabiliste, il est simple à décrire et à documenter.

La limite en toute honnêteté

Cyber Crucible n'affirme pas que le produit est « conforme à l'AI Act de l'UE », et ne procède pas à cette détermination pour le compte d'un client. Cette page décrit le fonctionnement du produit afin que l'évaluation de l'AI Act réalisée par le client puisse en tenir compte avec précision. Ceci ne constitue pas un conseil juridique.

Comment Cyber Crucible soutient-il les exigences en matière de protection des données et de sécurité en Allemagne ?

Réponse courte : En Allemagne, Cyber Crucible soutient les obligations d'une organisation au titre du RGPD et de la loi fédérale sur la protection des données (BDSG) en ne collectant aucun contenu client, identifiant ou clé, et en traitant les données au niveau du terminal. Pour les organisations relevant du régime de cybersécurité allemand (le cadre de la loi BSI, dans le cadre de sa transposition de NIS2), la conception permettant un traitement local et un déploiement sur site soutient leurs obligations en matière de sécurité et de chaîne d'approvisionnement.

Comment cela s'aligne

- **RGPD + BDSG.** La minimisation des données, le chiffrement et le contrôle des accès soutiennent le socle allemand de protection des données ; un accord de traitement des données est disponible.
- **Résidence des données.** Le déploiement sur site conserve les données personnelles en Allemagne lorsque cela est requis ; aucun contenu client n'est transféré à l'étranger pour le traitement de sécurité.
- **Régime de cybersécurité.** L'Allemagne a transposé progressivement NIS2 dans le cadre de sa loi BSI ; Cyber Crucible soutient les mesures de gestion des risques et de sécurité de la chaîne d'approvisionnement des entités concernées.

La limite honnête

La conformité relève de la responsabilité de l'organisation et, le cas échéant, de son délégué à la protection des données et de l'autorité de contrôle compétente. Cyber Crucible ne détient aucune certification allemande et soutient ces obligations sans s'y substituer. La documentation est disponible sur demande.

Comment Cyber Crucible prend-elle en charge les exigences de protection des données en France ?

Réponse courte : En France, Cyber Crucible soutient les obligations d'une organisation au titre du GDPR et de la Loi Informatique et Libertés (appliquée par la CNIL) en minimisant les données et en traitant localement. Comme elle ne collecte aucun contenu client, identifiant ou clé, la plupart des obligations que la CNIL fait appliquer présentent une surface d'exposition minimale dans sa garde.

Comment cela s'aligne

- **GDPR + droit national.** Le chiffrement, le contrôle d'accès et la minimisation des données soutiennent le socle français ; un accord de traitement des données est disponible.
- **Résidence des données.** Le déploiement sur site permet de conserver les données personnelles en France lorsque cela est requis.
- **Régime de cybersécurité.** La transposition de NIS2 en France était encore en cours d'examen législatif en 2026 ; Cyber Crucible soutient les mesures de sécurité et de chaîne d'approvisionnement des entités concernées dans le cadre du dispositif tel qu'adopté.

La limite honnête

La CNIL est une autorité de contrôle active ; la conformité relève de l'organisation, et Cyber Crucible la soutient sans revendiquer de certification française. La documentation est disponible sur demande.

Comment Cyber Crucible prend-il en charge les exigences de protection des données en Irlande ?

Réponse courte : En Irlande, Cyber Crucible soutient les obligations d'une organisation au titre du GDPR et du Data Protection Act 2018 (appliqué par la Data Protection Commission) en ne collectant aucun contenu client, identifiant ou clé, et en effectuant le traitement sur le poste. L'Irlande est l'autorité de contrôle chef de file pour de nombreuses multinationales, ce qui relève le niveau d'exigence de l'examen des fournisseurs ; l'empreinte de données minimale maintient un risque faible du côté du fournisseur.

Comment cela s'aligne

- **GDPR + DPA 2018.** La minimisation des données, le chiffrement et le contrôle d'accès soutiennent la base irlandaise ; un accord de traitement des données est disponible.
- **Résidence des données.** Le déploiement sur site permet de conserver les données personnelles en Irlande lorsque cela est requis.
- **Régime de cybersécurité.** La transposition de NIS2 par l'Irlande était encore en cours de finalisation en 2026 ; Cyber Crucible soutient les mesures des entités concernées dans le cadre adopté.

La limite honnête

La Data Protection Commission est une autorité chef de file de premier plan au sein de l'UE ; la conformité relève de l'organisation. Cyber Crucible ne détient aucune certification irlandaise et soutient ces obligations. La documentation est disponible sur demande.

Comment Cyber Crucible facilite-t-il le respect des exigences en matière de protection des données aux Pays-Bas ?

Réponse courte : Aux Pays-Bas, Cyber Crucible facilite le respect des obligations d'une organisation au titre du RGPD et de la loi néerlandaise de mise en œuvre du RGPD (Dutch GDPR Implementation Act, appliquée par l'Autoriteit Persoonsgegevens) en minimisant les données et le traitement au niveau du poste de travail (endpoint). Il ne collecte aucun contenu client, identifiant ou clé, si bien que la plupart des obligations n'ont que peu de portée dans le cadre de sa garde.

Comment cela s'articule

- **RGPD + mise en œuvre nationale.** Le chiffrement, le contrôle d'accès et la minimisation des données soutiennent le socle néerlandais ; un accord de traitement des données (data processing agreement) est disponible.
- **Résidence des données.** Le déploiement sur site permet de conserver les données personnelles aux Pays-Bas lorsque cela est requis.
- **Régime de cybersécurité.** La transposition néerlandaise de la directive NIS2 (la Cyberbeveiligingswet) était encore en cours de finalisation en 2026 ; Cyber Crucible soutient les mesures des entités concernées dans le cadre du dispositif tel qu'il sera adopté.

Les limites, en toute transparence

La conformité relève de la responsabilité de l'organisation et, le cas échéant, de l'Autoriteit Persoonsgegevens. Cyber Crucible ne détient aucune certification néerlandaise et facilite le respect de ces obligations. La documentation est disponible sur demande.

Comment Cyber Crucible prend-il en charge les exigences de protection des données en Espagne ?

Réponse courte : En Espagne, Cyber Crucible soutient les obligations d'une organisation au titre du RGPD et de la Loi organique sur la protection des données (LOPDGDD, appliquée par l'AEPD) en ne collectant aucun contenu client, identifiant ou clé, et en traitant les données localement. Comme le nombre de données personnelles en sa possession est minimal, la plupart des obligations que l'AEPD fait respecter ont peu de matière à s'appliquer.

Comment cela s'aligne

- **RGPD + LOPDGDD.** La minimisation des données, le chiffrement et le contrôle d'accès soutiennent le socle espagnol ; un accord de traitement des données est disponible.
- **Résidence des données.** Le déploiement sur site conserve les données personnelles en Espagne lorsque cela est requis.
- **Régime de cybersécurité.** La transposition de la directive NIS2 en Espagne était encore en cours de processus législatif en 2026 ; Cyber Crucible soutient les mesures des entités concernées dans le cadre du dispositif tel qu'adopté.

La limite honnête

L'AEPD est l'une des autorités de contrôle les plus actives de l'UE ; la conformité relève de la responsabilité de l'organisation. Cyber Crucible ne détient aucune certification espagnole et soutient ces obligations. La documentation est disponible sur demande.

Comment Cyber Crucible prend-il en charge les exigences de protection des données en Italie ?

Réponse courte : En Italie, Cyber Crucible soutient les obligations d'une organisation en vertu du RGPD et du Code italien de la protection des données personnelles (appliqué par le Garante) en minimisant les données et le traitement au niveau du poste de travail. Il ne collecte aucun contenu client, identifiant ou clé, de sorte que la plupart des obligations n'ont qu'une surface minimale relevant de sa responsabilité.

Comment cela s'aligne

- **RGPD + Code de la protection des données personnelles.** Le chiffrement, le contrôle d'accès et la minimisation des données soutiennent le socle italien ; un accord de traitement des données est disponible.
- **Résidence des données.** Le déploiement sur site permet de conserver les données personnelles en Italie lorsque cela est requis.
- **Régime de cybersécurité.** L'Italie a fait partie des premiers États membres à transposer NIS2 dans le droit national ; Cyber Crucible soutient les entités concernées dans leurs mesures de gestion des risques et de la chaîne d'approvisionnement.

La limite en toute honnêteté

Le Garante est une autorité de contrôle active ; la conformité relève de la responsabilité de l'organisation. Cyber Crucible ne détient aucune certification italienne et vient en soutien de ces obligations. La documentation est disponible sur demande.

Comment Cyber Crucible prend-elle en charge les exigences de protection des données en Pologne ?

Réponse courte : En Pologne, Cyber Crucible appuie les obligations d'une organisation au titre du RGPD et de la loi polonaise sur la protection des données à caractère personnel (appliquée par l'UODO) en ne collectant aucun contenu client, identifiant ou clé, et en effectuant le traitement au niveau du point de terminaison (endpoint). Cette empreinte de données minimale réduit la surface de la plupart des obligations.

Comment cela s'aligne

- **RGPD + droit national.** La minimisation des données, le chiffrement et le contrôle d'accès viennent appuyer les exigences de base polonaises ; un accord de traitement des données (DPA) est disponible.
- **Résidence des données.** Le déploiement sur site permet de conserver les données personnelles en Pologne lorsque cela est requis.
- **Régime de cybersécurité.** La Pologne a mis à jour son cadre du Système national de cybersécurité (KSC) pour refléter la directive NIS2 ; Cyber Crucible appuie les mesures des entités concernées dans le cadre adopté.

La limite en toute transparence

La conformité relève de la responsabilité de l'organisation et, le cas échéant, de l'UODO. Cyber Crucible ne détient aucune certification polonaise et vient en appui de ces obligations. La documentation est disponible sur demande.

Comment Cyber Crucible prend-elle en charge les exigences de protection des données en Suède et dans les pays nordiques ?

Réponse courte : En Suède et dans l'ensemble de la région nordique, Cyber Crucible prend en charge les obligations d'une organisation au titre du GDPR et des lois nationales de transposition (en Suède, appliquées par l'IMY) en minimisant les données et le traitement au niveau du terminal. Comme elle ne collecte aucun contenu client, identifiant ou clé, la plupart des obligations n'ont que peu de portée sur ce qu'elle détient.

Comment cela s'aligne

- **GDPR + transposition nationale.** Le chiffrement, le contrôle d'accès et la minimisation des données soutiennent le socle nordique ; un accord de traitement des données est disponible.
- **Résidence des données.** Le déploiement sur site conserve les données personnelles dans le pays lorsque cela est requis.
- **Régime de cybersécurité.** Les États membres nordiques transposent NIS2 en droit national selon leurs propres calendriers ; Cyber Crucible prend en charge les mesures des entités concernées dans le cadre tel qu'adopté.

La limite en toute honnêteté

La conformité relève de l'organisation et de l'autorité de surveillance nationale compétente. Cyber Crucible ne détient aucune certification nationale dans un pays nordique et soutient ces obligations sans s'y substituer. La documentation est disponible sur demande.