

Guias de Conformidade por País

Respostas por jurisdição — o que a lei de proteção de dados de cada país exige especificamente, e como a arquitetura da Cyber Crucible atende a isso. Golfo, África, Europa e Reino Unido.

- [A Cyber Crucible cumpre a PDPL da Arábia Saudita?](#)
- [A Cyber Crucible cumpre a lei de proteção de dados dos EAU?](#)
- [A Cyber Crucible está em conformidade com a lei de proteção de dados do Bahrein?](#)
- [A Cyber Crucible está em conformidade com a lei de proteção de dados do Catar?](#)
- [A Cyber Crucible está em conformidade com a lei de proteção de dados de Omã?](#)
- [O Kuwait não possui uma lei abrangente de proteção de dados — o que isso significa para a seleção de fornecedores?](#)
- [A Cyber Crucible cumpre a Lei de Proteção de Dados do Quênia?](#)
- [A Cyber Crucible atende ao requisito de localização de dados da Nigéria?](#)
- [A Cyber Crucible cumpre com a POPIA da África do Sul?](#)
- [A Cyber Crucible está em conformidade com a lei de proteção de dados do Egito?](#)
- [A Cyber Crucible está em conformidade com a Lei de Proteção de Dados de Gana?](#)
- [A Cyber Crucible atende ao requisito de localização de dados da Zâmbia?](#)
- [A Cyber Crucible está em conformidade com a lei de proteção de dados de Ruanda?](#)
- [A Cyber Crucible cumpre a lei de proteção de dados de Marrocos?](#)
- [Quais são os requisitos de proteção de dados na Líbia?](#)
- [A Cyber Crucible está em conformidade com o GDPR?](#)
- [A Cyber Crucible está em conformidade com o UK GDPR?](#)

A Cyber Crucible cumpre a PDPL da Arábia Saudita?

Resposta curta: A Cyber Crucible avaliou as suas operações em conformidade com a Lei de Proteção de Dados Pessoais da Arábia Saudita, utiliza Cláusulas Contratuais Padrão aprovadas pela SDAIA para qualquer transferência de dados pessoais de origem saudita e pode ser implementada integralmente dentro do Reino, sem qualquer fluxo transfronteiriço. Recolhe apenas telemetria de sistema e de segurança — nunca conteúdo de ficheiros, documentos, e-mail ou comunicações.

O que a lei exige

A PDPL entrou em vigor em 14 de setembro de 2023, com um período de tolerância até 14 de setembro de 2024. A Arábia Saudita mantém algumas das preferências de localização de dados mais rigorosas do Golfo, e a Autoridade Saudita de Dados e IA (SDAIA) supervisiona o cumprimento. As transferências para fora do Reino exigem uma salvaguarda reconhecida e, na maioria dos casos, uma Avaliação de Risco de Transferência.

O que se aplica especificamente aqui

- **CCPs pré-aprovadas pela SDAIA** são utilizadas para qualquer transferência de dados pessoais de origem saudita para os Estados Unidos, adotadas sem modificações além dos campos obrigatórios, e alargadas a qualquer subprocessador subsequente.
- **Uma Avaliação de Risco de Transferência** foi concluída seguindo as orientações estruturadas da SDAIA — fluxos de dados, regime jurídico de destino, controlos, risco residual, medidas de mitigação documentadas.
- **Função de subcontratante (processor)** — a Cyber Crucible atua normalmente como subcontratante nos termos de um Acordo de Processamento de Dados (DPA) escrito; o cliente saudita é o responsável pelo tratamento (controller).
- **Representante local nos termos do Artigo 33** — enquanto subcontratante, essa obrigação recai sobre si, na qualidade de responsável pelo tratamento.

A via mais direta

Dada a preferência pela localização de dados, a implementação totalmente no local (on-premises) e isolada (air-gapped) constitui a resposta mais robusta: toda a gestão de backend dentro das suas próprias infraestruturas fisicamente protegidas, sem qualquer telemetria de saída. Quando nada

atravessa a fronteira, não surgem obrigações de transferência.

“ As CCPs e a Avaliação de Risco de Transferência estão disponíveis através de **dpo@cybercrucible.com**. Situação válida à data de redação — confirme os requisitos atuais com aconselhamento jurídico local.

A Cyber Crucible cumpre a lei de proteção de dados dos EAU?

Resposta curta: Sim, sob a mesma arquitetura — recolha mínima, processamento local e opções de implementação em que os dados nunca saem do país. Um ponto específico dos EAU é importante: se a sua entidade estiver sediada no DIFC ou na ADGM, aplica-se um regime diferente do da lei federal.

O que a lei exige

O Decreto-Lei Federal n.º 45 de 2021 dos EAU estabelece o quadro federal de proteção de dados pessoais. Permite uma gama mais ampla de bases legais do que os regimes do Golfo mais centrados no consentimento, e adota uma abordagem baseada no risco e orientada para salvaguardas relativamente à transferência transfronteiriça, em vez de uma localização estrita. A implementação tem dependido dos Regulamentos de Execução — uma área que tem evoluído, pelo que deve confirmar a posição atual.

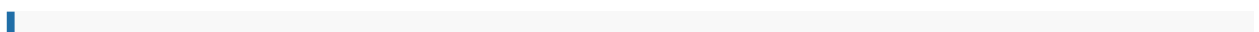
A questão das zonas francas

Isto apanha muita gente desprevenida. O DIFC (Dubai International Financial Centre) e a ADGM (Abu Dhabi Global Market) operam os seus próprios regimes de proteção de dados, separados da lei federal. Se a sua entidade estiver estabelecida em qualquer um deles, as regras aplicáveis e a autoridade de supervisão são diferentes.

Determine qual o quadro que o rege antes de avaliar qualquer fornecedor — a resposta altera o que precisa de comprovar.

O que se aplica especificamente aqui

- **Flexibilidade da base legal** — a gama mais ampla de bases significa que o raciocínio ao estilo de interesse legítimo para o processamento relacionado com segurança é, em geral, mais viável do que em regimes centrados no consentimento.
- **Salvaguardas de transferência** — o alojamento regional mantém o processamento dentro dos EAU; a implementação com air-gap elimina completamente a transferência.
- **Função de subcontratante (processor)** ao abrigo de um DPA escrito, segundo as suas instruções documentadas.



Situação à data de redação — confirme os requisitos atuais, incluindo os Regulamentos de Execução e a aplicabilidade nas zonas francas, junto de consultores jurídicos locais.

A Cyber Crucible está em conformidade com a lei de proteção de dados do Bahrein?

Resposta curta: Sim. A lei do Bahrein é fortemente inspirada no GDPR, com alcance extraterritorial, pelo que os mesmos controlos que satisfazem o GDPR se aplicam — recolha mínima, papel de subcontratante documentado, salvaguardas de segurança robustas e transferência controlada.

O que a lei exige

O Bahrein possui uma lei de proteção de dados autónoma em vigor desde 2019. É frequentemente citada como uma das mais claras e maduras do Golfo, com direitos sólidos dos titulares dos dados, obrigações explícitas de responsabilização e **aplicação extraterritorial** — o que significa que pode abranger fornecedores fora do Bahrein que processem dados de residentes bareinitas.

O que se aplica especificamente aqui

O alcance extraterritorial é o ponto que merece destaque. Significa que a questão não é apenas saber se você cumpre, mas se os seus fornecedores também cumprem.

- **Responsabilização** — a lista de dados excluídos (sem chaves, credenciais, tokens ou conteúdo) é explícita e documentada, em vez de descrita em termos genéricos, o que é exatamente o que as obrigações de responsabilização exigem.
- **Direitos dos titulares dos dados** — na prática, restritos aqui, porque a telemetria comportamental é pseudonimizada e o conteúdo nunca é recolhido, pelo que o volume de dados pessoais sujeitos a pedidos de exercício de direitos é mínimo.
- **Transferência** — armazenamento regional temporário ou implementação isolada (air-gapped).

Por que o alinhamento com o GDPR ajuda

Como a lei do Bahrein acompanha de perto o GDPR, o mapeamento do GDPR aplica-se de forma quase direta. Se a sua organização já realizou o trabalho de avaliação de fornecedores para o GDPR, a maior parte desse trabalho é reaproveitável.

“ Situação no momento da redação — confirme com o departamento jurídico local.

A Cyber Crucible está em conformidade com a lei de proteção de dados do Catar?

Resposta curta: Sim. O regime do Catar é mais centrado no consentimento do que o dos seus vizinhos, o que torna a coleta mínima especialmente valiosa — quanto menos dados pessoais forem processados, menor o encargo de consentimento.

O que a lei exige

O Catar possui uma lei de proteção de dados independente em vigor desde 2017, tornando-se uma das primeiras da região. Mantém um modelo mais rigoroso, centrado no consentimento, em comparação com o conjunto mais amplo de bases legais dos Emirados Árabes Unidos, além de uma abordagem baseada em risco para as salvaguardas de transferência.

Por que a centralidade no consentimento favorece esta arquitetura

Num regime centrado no consentimento, cada categoria de dados pessoais que você processa é uma categoria para a qual pode ser necessária uma base legal de processamento. Isso torna *não coletar* materialmente mais valioso do que proteger bem.

A Cyber Crucible nunca coleta chaves de criptografia, credenciais, tokens de sessão ou conteúdo de arquivos. A telemetria comportamental é pseudonimizada quando poderia identificar um indivíduo, e as fontes de telemetria são configuráveis, permitindo restringir ainda mais a coleta.

O resultado é que a superfície de consentimento para a própria ferramenta de segurança é excepcionalmente pequena.

Transferência

O staging regional mantém o processamento próximo ou dentro da jurisdição; a implantação com air-gap elimina completamente o fluxo transfronteiriço.

“ Situação no momento da redação — confirme com o departamento jurídico local.

A Cyber Crucible está em conformidade com a lei de proteção de dados de Omã?

Resposta curta: Sim — e Omã é, neste momento, a jurisdição mais sensível ao tempo no Golfo. A lei de proteção de dados pessoais de Omã entra em pleno vigor em **5 de fevereiro de 2026**, após um período de carência de dois anos, pelo que as pilhas de fornecedores que eram compatíveis por padrão passam agora a estar no âmbito de aplicação.

O que a lei exige

A lei de Omã reflete de perto os princípios do GDPR, incorporando ao mesmo tempo requisitos locais relativos ao consentimento e ao tratamento de dados. O período de carência de dois anos termina em 5 de fevereiro de 2026, altura em que se espera a conformidade total.

Por que isto é relevante para a seleção de fornecedores agora

Os períodos de carência criam um padrão previsível: as organizações adiam a revisão dos fornecedores até se aproximar o prazo e, então, descobrem que uma ferramenta de segurança que exporta continuamente telemetria de endpoint para outra jurisdição é difícil de justificar ao abrigo do novo regime.

Se está a rever a sua pilha tecnológica tendo em conta a data de fevereiro de 2026, as perguntas que vale a pena colocar a qualquer fornecedor de endpoint são:

1. Que dados pessoais recolhe, de forma específica e enumerada?
2. Onde são processados esses dados, e podem ser mantidos em Omã?
3. Qual é o mecanismo de transferência, caso os dados saiam do país?
4. Pode operar sem qualquer telemetria de saída?

As respostas da Cyber Crucible são: exclusões enumeradas (sem chaves, credenciais, tokens ou conteúdo); o processamento é local ao endpoint; está disponível preparação regional (staging); e sim — a implementação isolada (air-gapped) não produz qualquer telemetria de saída.

Situação à data de redação — confirme a posição atual e qualquer prorrogação junto de aconselhamento jurídico local.

O Kuwait não possui uma lei abrangente de proteção de dados — o que isso significa para a seleção de fornecedores?

Resposta curta: O Kuwait adotou uma abordagem setorial direcionada, em vez de promulgar uma lei nacional abrangente de proteção de dados, com a regulamentação da CITRA a reger a forma como os setores de telecomunicações e TI tratam o conteúdo dos utilizadores. Isso torna a soberania dos dados uma decisão comercial e de segurança, em vez de uma obrigação de conformidade — mas a decisão continua a ser importante.

A posição atual

O Kuwait continua a ser a exceção notável entre os principais estados do Golfo por não possuir uma lei nacional abrangente de proteção de dados pessoais. Em vez disso, a regulamentação da CITRA aborda especificamente o tratamento de conteúdo de utilizadores nos setores de telecomunicações e TI.

Por que "sem lei" não é o mesmo que "sem risco"

Três razões pelas quais as organizações no Kuwait ainda ponderam isto cuidadosamente:

1. **As regras setoriais continuam a aplicar-se.** Se opera nos setores de telecomunicações ou TI, os requisitos da CITRA são obrigações vigentes.
2. **As contrapartes impõem termos.** Parceiros multinacionais, seguradoras e clientes frequentemente exigem, contratualmente, um tratamento equivalente ao RGPD, independentemente da legislação local.
3. **A regulamentação tende a chegar.** Todos os outros estados do CCG já promulgaram uma lei abrangente. Selecionar fornecedores que já cumprem regimes mais rigorosos evita uma migração forçada mais tarde.

A posição prática

Como a Cyber Crucible nunca recolhe chaves, credenciais, tokens ou conteúdo, e pode ser implementada de forma totalmente isolada (air-gapped), satisfaz os regimes mais rigorosos da região. Escolhê-la no Kuwait é optar por não ter este problema quando a lei mudar.

“ Estado no momento da redação — confirme os requisitos setoriais atuais com aconselhamento jurídico local.

A Cyber Crucible cumpre a Lei de Proteção de Dados do Quênia?

Resposta curta: Sim. A Lei de Proteção de Dados do Quênia de 2019 restringe a transferência transfronteiriça para países com salvaguardas apropriadas e aplica uma regra mais rigorosa aos dados pessoais sensíveis. A Cyber Crucible não recolhe quaisquer dados pessoais sensíveis e pode ser implementada de forma a que nenhum dado saia do Quênia.

O que a lei exige

As secções 48 e 49 da Lei de Proteção de Dados de 2019 proíbem a transferência de dados pessoais para um país que não disponha de salvaguardas de segurança de dados apropriadas, com várias bases permitidas, incluindo a adequação.

A regra mais rigorosa que importa: a transferência de dados pessoais *sensíveis* só é permitida quando o titular dos dados tiver consentido e existirem salvaguardas apropriadas. Ambas as condições, não apenas uma.

Por que a regra sobre dados sensíveis é o ponto-chave

Esse requisito duplo é difícil de satisfazer operacionalmente — obter e comprovar o consentimento individual de cada titular de dados afetado, de forma contínua, para uma ferramenta de segurança.

A Cyber Crucible contorna essa questão: **não é recolhido qualquer dado pessoal sensível.** Nem dados biométricos, de saúde ou genéticos; nem dados que revelem origem racial ou étnica, crença religiosa ou opinião política. A telemetria descreve o comportamento do sistema e eventos de segurança, não atributos pessoais.

Quando a telemetria comportamental puder identificar indiretamente um indivíduo, os identificadores são pseudonimizados ou mascarados.

Transferência

O staging regional mantém o processamento dentro do Quênia. A implementação com air-gap não produz qualquer telemetria de saída, pelo que as secções 48-49 não são aplicáveis.

“ Situação à data de redação — confirme com o consultor jurídico local.

A Cyber Crucible atende ao requisito de localização de dados da Nigéria?

Resposta curta: Sim — e esta é a jurisdição em que a arquitetura mais importa. A Lei de Proteção de Dados da Nigéria de 2023 impõe um requisito de localização de dados: os dados pessoais de cidadãos nigerianos devem ser armazenados dentro da Nigéria. A implementação on-premises da Cyber Crucible mantém tudo dentro da sua própria infraestrutura, no país, com zero telemetria de saída.

O que a lei exige

As Seções 41–43 da Lei de Proteção de Dados da Nigéria de 2023 estabelecem condições para a transferência transfronteiriça, incluindo salvaguardas do país de destino e o consentimento do titular dos dados. Além dessas condições, **a Nigéria impõe um requisito de localização** — os dados pessoais de cidadãos nigerianos devem ser armazenados dentro da Nigéria. Regras setoriais no setor de serviços financeiros acrescentam obrigações adicionais de localização.

Por que a maioria dos fornecedores de segurança tem dificuldades aqui

Este é o exemplo mais claro de uma regra que a segurança de endpoint dependente de nuvem não consegue satisfazer por design. Uma ferramenta cuja arquitetura consiste em "coletar telemetria no endpoint, enviá-la para a nossa nuvem para análise" está, estruturalmente, transferindo dados pessoais para fora da Nigéria como condição para funcionar. Salvaguardas contratuais não resolvem um requisito de localização de armazenamento.

Por que esta arquitetura realmente atende a esse requisito

- **A análise é local.** A avaliação de ameaças e a interdição ocorrem no endpoint em normalmente menos de 200 milissegundos. Nenhuma ida e volta à nuvem é necessária

para a proteção.

- **O backend pode ser totalmente mantido no país.** O modelo on-premises executa todo o software de gestão dentro dos seus próprios racks fisicamente protegidos.
- **Zero telemetria de saída** na configuração com air gap — nada sai, portanto nada é armazenado no exterior.
- **Há menos itens a localizar de qualquer forma** — chaves, credenciais, tokens e conteúdos de arquivos nunca são coletados em primeiro lugar.

“ Situação no momento da redação — confirme os requisitos atuais, incluindo as regras do setor financeiro, junto a advogados locais.

A Cyber Crucible cumpre com a POPIA da África do Sul?

Resposta curta: Sim. A POPIA restringe a transferência transfronteiriça, a menos que o destino ofereça uma proteção substancialmente semelhante ou o titular dos dados dê o seu consentimento. A Cyber Crucible minimiza o que é processado desde o início e pode ser implementada de forma que não ocorra qualquer transferência.

O que a lei exige

A Lei de Proteção de Informações Pessoais da África do Sul (2013) proíbe a transferência de informações pessoais para fora do país sem o consentimento do titular dos dados, ou a menos que a jurisdição destinatária esteja sujeita a uma lei que ofereça uma proteção substancialmente semelhante.

O que se aplica especificamente aqui

O teste de "proteção substancialmente semelhante" é uma avaliação que deve ser comprovável. Dois fatores tornam essa avaliação mais simples:

1. **O âmbito é reduzido.** Chaves de encriptação, credenciais, tokens de sessão e conteúdos de ficheiros nunca são recolhidos. O que resta é telemetria comportamental, pseudonimizada nos casos em que poderia identificar um indivíduo.
2. **Proteções contratuais** — o processamento ocorre ao abrigo de um DPA escrito com termos de segurança, confidencialidade e notificação de violação de dados, estendidos a qualquer subprocessador.

Ou evite completamente o teste

O alojamento regional mantém o processamento na África do Sul. A implementação com isolamento físico (air-gapped) não produz qualquer fluxo de saída, caso em que as disposições de transferência simplesmente não se aplicam — geralmente um caminho mais rápido do que comprovar a adequação.



Situação no momento da redação — confirme com o departamento jurídico local.

A Cyber Crucible está em conformidade com a lei de proteção de dados do Egito?

Resposta curta: Sim. O Egito exige aprovação prévia para transferências transfronteiriças de dados pessoais — um patamar substancialmente mais elevado do que salvaguardas contratuais. A Cyber Crucible pode ser implementada de forma que nenhuma transferência ocorra, eliminando a exigência de aprovação em vez de tentar contorná-la.

O que a lei exige

O regime de proteção de dados do Egito exige **aprovação prévia** para transferências de dados pessoais para fora do país. Trata-se de um modelo baseado em permissão, e não em salvaguardas: não é possível simplesmente implementar proteções contratuais e prosseguir.

Por que o modelo de aprovação altera a seleção de fornecedores

Em um modelo de salvaguardas, um fornecedor com cláusulas contratuais robustas é viável. Em um modelo de aprovação, cada fluxo transfronteiriço constitui um processo administrativo, sujeito a prazos, discricionariedade e risco de renovação.

Uma ferramenta de segurança que exporta telemetria continuamente cria um fluxo contínuo que exige que essa aprovação permaneça válida. Se a aprovação expirar ou as condições mudarem, o funcionamento normal da ferramenta se transforma em um problema de conformidade.

A resposta direta

A implementação local com isolamento físico (air-gapped) não gera nenhuma telemetria de saída — nada é transferido, portanto nenhuma aprovação é necessária. O staging regional mantém o processamento local, quando um modelo híbrido é preferido.

As categorias com maior probabilidade de atrair atenção regulatória — chaves, credenciais, tokens, conteúdo de arquivos — nunca são coletadas, independentemente da forma de implementação.

“ Situação no momento da redação — confirme os requisitos atuais e o procedimento de aprovação com assessoria jurídica local.

A Cyber Crucible está em conformidade com a Lei de Proteção de Dados de Gana?

Resposta curta: Sim, e Gana é comparativamente simples. Gana destaca-se entre as jurisdições africanas por **não** impor requisitos adicionais à transferência transfronteiriça além das suas obrigações gerais de proteção de dados — pelo que os controlos padrão se aplicam sem um regime especial de transferência.

O que a lei exige

Gana possui um quadro estabelecido de proteção de dados com uma autoridade de supervisão. A análise das jurisdições africanas identifica consistentemente Gana como a exceção: ao contrário da maioria dos seus vizinhos, não impõe condições adicionais especificamente à partilha transfronteiriça de dados.

Isto não significa que a transferência não seja regulada — as obrigações gerais relativas ao processamento lícito, segurança e direitos dos titulares dos dados continuam a aplicar-se. Significa que não existe um obstáculo separado de aprovação ou de adequação a superar.

O que se aplica especificamente aqui

Com a questão da transferência simplificada, a avaliação reduz-se às questões habituais:

- **O que é recolhido?** Apenas telemetria de sistema e de segurança. Sem chaves, credenciais, tokens ou conteúdo.
- **Como é protegido?** TLS 1.3 em trânsito, encriptação de payload JWE por agente, encriptação em repouso, controlo de acesso baseado em funções.
- **Quem é responsável?** A Cyber Crucible atua como subcontratante (processor) ao abrigo de um DPA escrito, seguindo as suas instruções documentadas.

Ainda vale a pena considerar a soberania

Mesmo sem uma restrição de transferência, a implementação no país ou em ambiente isolado (air-gapped) continua disponível — e as organizações que servem clientes regionais frequentemente preferem-na, uma vez que as jurisdições vizinhas são consideravelmente mais rigorosas.

“ Situação à data de redação — confirme com aconselhamento jurídico local.

A Cyber Crucible atende ao requisito de localização de dados da Zâmbia?

Resposta curta: Sim. A Lei de Proteção de Dados da Zâmbia exige que os controladores processem e armazenem dados pessoais e dados pessoais sensíveis em um centro de dados ou servidor **dentro da Zâmbia**. A implantação on-premises da Cyber Crucible satisfaz isso diretamente — o backend é executado dentro da sua própria infraestrutura, no país.

O que a lei exige

A Parte X da Lei de Proteção de Dados da Zâmbia regula a transferência transfronteiriça, e a Seção 70 obriga um controlador de dados a processar e armazenar dados pessoais e dados pessoais sensíveis em um centro de dados ou servidor localizado dentro da Zâmbia.

Trata-se de um **mandato de localização de armazenamento**, não de um teste de salvaguardas. Proteções contratuais não satisfazem esse requisito.

Por que isso elimina a maioria das ferramentas de segurança baseadas em nuvem

Um fornecedor cujo produto exija o envio de telemetria de endpoint para uma região de nuvem fora da Zâmbia não pode atender à Seção 70 melhorando seus contratos ou sua criptografia. O requisito diz respeito a *onde os dados estão fisicamente localizados*.

Por que esta arquitetura a satisfaz

- **Backend on-premises** — todo o software de gerenciamento é executado em servidores que você controla, dentro da Zâmbia.
- **Análise local** — a avaliação de ameaças e a interdição ocorrem no próprio endpoint, de modo que a proteção nunca depende de um serviço fora do país.

- **Zero telemetria de saída** na configuração isolada (air-gapped).
- **Escopo mínimo** — chaves, credenciais, tokens e conteúdo nunca são coletados, de modo que o volume de dados pessoais sujeitos à Seção 70 já é pequeno desde o início.

“ Situação no momento da redação — confirme com assessoria jurídica local, incluindo quaisquer regras específicas do setor.

A Cyber Crucible está em conformidade com a lei de proteção de dados de Ruanda?

Resposta curta: Sim. A lei de proteção de dados de Ruanda é supervisionada pela Autoridade Nacional de Segurança Cibernética, e as regras específicas do setor acrescentam obrigações de localização — nomeadamente para bancos licenciados, que devem manter os dados primários dentro de Ruanda. A implementação local (on-premises) satisfaz ambas as exigências.

O que a lei exige

Ruanda promulgou uma lei de proteção de dados com a **Autoridade Nacional de Segurança Cibernética (NCSA)** designada como autoridade supervisora; o seu gabinete de proteção de dados foi lançado em março de 2022.

Para além da lei geral, a regulamentação setorial acrescenta a localização: a regulamentação de segurança cibernética exige que os bancos licenciados pelo Banco Central mantenham os dados primários dentro do território ruandês.

Por que a regra setorial é a mais relevante

Para os serviços financeiros em Ruanda, o requisito de localização bancária é normalmente a restrição vinculativa — mais rigorosa e específica do que as disposições gerais de proteção de dados. Um produto de segurança implementado nos endpoints de um banco processa dados que se enquadram nesse requisito.

O que se aplica especificamente aqui

- **Implementação local (on-premises)** mantém os dados primários dentro de Ruanda, satisfazendo diretamente o requisito de localização.
- **Análise local** significa que a proteção não depende de nenhum serviço fora do país.

- **Alinhamento com a supervisão** — com a NCSA como autoridade tanto de segurança cibernética como de proteção de dados, ser capaz de demonstrar *o que* uma ferramenta de segurança recolhe, em termos enumerados, é particularmente útil.

“ Situação no momento da redação — confirme os requisitos gerais e setoriais atuais junto de consultoria jurídica local.

A Cyber Crucible cumpre a lei de proteção de dados de Marrocos?

Resposta curta: Sim. A Lei nº 09-08 de Marrocos e o respetivo decreto de execução regem o tratamento de dados pessoais, sob supervisão da CNDP. Aplicam-se os mesmos controlos — recolha mínima, papel de subcontratante documentado, salvaguardas robustas e implementação no país ou isolada de rede (air-gapped), conforme preferido.

O que a lei exige

O quadro legal de Marrocos assenta na **Lei nº 09-08**, relativa à proteção das pessoas singulares no que respeita ao tratamento de dados pessoais, em conjunto com o **Decreto nº 2-09-165** de execução. A **CNDP** (Commission Nationale de contrôle de la protection des Données à caractère Personnel) é a autoridade de supervisão e participa ativamente na cooperação internacional sobre questões emergentes, incluindo a IA.

O que se aplica especificamente aqui

O regime de Marrocos é dos mais consolidados no Norte de África, com uma autoridade em funcionamento e procedimentos de notificação/autorização que variam consoante o tipo de tratamento. Implicações práticas para a avaliação de fornecedores:

- **Enumerar o que é recolhido.** A lista de dados excluídos da Cyber Crucible é explícita — sem chaves, credenciais, tokens ou conteúdo — o que apoia a exatidão da notificação.
- **Papel de subcontratante** ao abrigo de um acordo de tratamento de dados (DPA) escrito, sob instruções documentadas.
- **Transferência** — armazenamento regional intermédio ou implementação isolada de rede (air-gapped); esta última elimina a questão.

Para organizações que operam em todo o Magrebe

Os requisitos diferem consideravelmente entre Marrocos, Tunísia, Argélia e Líbia. Selecionar um fornecedor que cumpra o regime aplicável mais rigoroso — em vez de avaliar cada um separadamente — é, geralmente, a via de menor esforço.

“ Situação à data de redação — confirme com aconselhamento jurídico local.

Quais são os requisitos de proteção de dados na Líbia?

Resposta curta: A Líbia ainda não desenvolveu regulamentações abrangentes de proteção de dados. Isso faz da soberania dos dados uma decisão comercial, de segurança e de contraparte, e não uma obrigação de conformidade local — mas, para organizações que lidam com operações sensíveis, continua a ser uma decisão que vale a pena tomar de forma deliberada.

A posição atual

A Líbia ainda não promulgou uma estrutura abrangente de proteção de dados. Não existe um equivalente à PDPL da Arábia Saudita, à Lei 09-08 de Marrocos ou à NDPA da Nigéria.

Por que a soberania continua importante mesmo sem uma lei local

- 1. As contrapartes impõem requisitos.** Parceiros internacionais, seguradoras, clientes multinacionais e financiadores exigem rotineiramente, por contrato, um tratamento equivalente ao GDPR, independentemente da lei local. Atender ao padrão mais rigoroso evita renegociações posteriores.
- 2. Setores sensíveis carregam seus próprios riscos.** Operações de energia, telecomunicações, finanças e governo atraem atenção independentemente da legislação de privacidade. Para onde uma ferramenta de segurança envia telemetria — e quem pode obrigar o acesso a esses dados ali — é uma questão operacional genuína.
- 3. A regulamentação tende a seguir.** Jurisdições vizinhas no Norte da África promulgaram ou atualizaram estruturas regulatórias. As decisões de fornecedores tomadas agora ainda estarão em vigor quando a posição da Líbia mudar.

A posição prática

Como a Cyber Crucible nunca coleta chaves, credenciais, tokens ou conteúdo, e pode operar totalmente isolada (air-gapped) com telemetria de saída zero, ela satisfaz os regimes mais rigorosos da região. Na Líbia, isso é uma escolha, e não uma obrigação — mas é uma escolha que

envelhece bem.

“ Situação no momento da redação — confirme a posição legislativa atual com um consultor jurídico local antes de se basear nela.

A Cyber Crucible está em conformidade com o GDPR?

Resposta curta: Sim, por concepção e não apenas por política. Conteúdo, credenciais, chaves de encriptação e tokens de sessão nunca são recolhidos; a análise ocorre no endpoint; a Cyber Crucible atua como subcontratante ao abrigo de um DPA escrito; e as opções de implementação mantêm os dados pessoais dentro da UE — ou dentro das suas próprias instalações.

Correspondência com os princípios do GDPR

- **Minimização de dados (Art. 5.º)** — a lista de dados excluídos é enumerada, não descrita em termos genéricos. A telemetria é limitada ao que é necessário para a deteção de ameaças e é configurável.
- **Integridade e confidencialidade (Art. 5.º, 32.º)** — TLS 1.3 em trânsito, encriptação de payload JWE por agente, encriptação em repouso, controlo de acesso baseado em funções, rotação de chaves, registo de auditoria.
- **Obrigações do subcontratante (Art. 28.º)** — DPA escrito que especifica o âmbito; processamento apenas mediante instruções documentadas; subcontratantes sujeitos a termos equivalentes.
- **Transferências (Capítulo V)** — preparação regional na UE, ou implementação isolada (air-gapped) que elimina completamente a transferência.
- **Proteção de dados desde a conceção (Art. 25.º)** — a alegação mais sólida possível: as categorias de maior risco não são protegidas por política, simplesmente nunca são recolhidas.

Pseudonimização

Nos casos em que a telemetria comportamental possa identificar indiretamente um indivíduo, os identificadores são pseudonimizados ou mascarados — uma salvaguarda expressamente reconhecida pelo GDPR.

O que isto não faz

Isto não torna a sua organização conforme com o GDPR. As suas obrigações dependem das suas próprias finalidades de processamento, bases legais, avisos e registos. O que isto elimina é uma dificuldade comum: um fornecedor de segurança a exportar continuamente dados pessoais para um país terceiro.

A Cyber Crucible está em conformidade com o UK GDPR?

Resposta curta: Sim. O UK GDPR e o Data Protection Act 2018 acompanham de perto o RGPD da UE, pelo que se aplica o mesmo mapeamento — recolha mínima, papel de subcontratante ao abrigo de um DPA escrito, salvaguardas técnicas robustas e opções de implementação que mantêm os dados no Reino Unido ou inteiramente nas suas instalações.

O que se aplica

Após a saída do Reino Unido da UE, o UK GDPR opera em conjunto com o Data Protection Act 2018, sob a supervisão do Information Commissioner's Office (ICO). Os princípios, as bases legais e as obrigações do subcontratante refletem de perto o RGPD da UE.

Onde as organizações devem prestar atenção

- **Transferências internacionais** utilizam os mecanismos próprios do Reino Unido — o International Data Transfer Agreement (IDTA) ou o UK Addendum às SCCs da UE, em vez de apenas as SCCs da UE.
- **Conformidade dupla** — as organizações que operam tanto no Reino Unido como na UE devem cumprir ambos os regimes, embora os controlos práticos se sobreponham quase inteiramente.

O que se aplica especificamente aqui

A avaliação é a mesma que para o RGPD da UE, e as respostas são as mesmas:

- Chaves, credenciais, tokens e conteúdos de ficheiros nunca são recolhidos.
- A análise ocorre no endpoint; a proteção não requer a movimentação de dados.
- Preparação regional no Reino Unido, ou implementação com air-gap que elimina totalmente a transferência.
- Papel de subcontratante ao abrigo de um DPA escrito, com subcontratantes vinculados a termos equivalentes.

Para o instrumento de transferência adequado às suas circunstâncias, contacte **dpo@cybercrucible.com**. Situação à data de redação — confirme as orientações atuais do ICO com o seu departamento jurídico.