MIRHOSTING.COM

MIRhosting B.V.
KVK (Registration ID) 63945630
BTW (VAT) ID NL855463600B01

Our commitment to compliance and network security

MIRhosting operates mission-critical infrastructure for customers who cannot afford downtime, data leaks or breaches of regulatory requirements. As a European infrastructure provider, we treat compliance and network security as core operational requirements.

We recognise our responsibility to ensure that our services are used lawfully and securely, and that our network is not misused in ways that could harm customers, third parties or the wider digital community. In this statement, we explain how we screen customers, monitor our infrastructure for abuse and comply with applicable sanctions regimes.

Robust onboarding and verification

Security starts before the first byte of data is transmitted. Every new MIRhosting customer goes through a structured Know Your Customer (KYC) procedure.

Initial screening

Each new customer is subject to an automated compliance check. We verify the company's legal status and key registration data, assess its ownership and beneficial ownership structure, screen against international sanctions lists and PEP lists, and take

into account any history of potential abuse of infrastructure. To do this, we rely on reputable European and international services in order to minimise the risk of unlawful or improper use of our network.

Enhanced due diligence

Customers with large service volumes, more complex infrastructure or other indicators of potentially elevated risk may be subject to enhanced due diligence. This may include additional identity verification and, where necessary, further checks tailored to the nature of the requested services and the customer's profile. In such cases we may engage external compliance specialists.

MIRhosting reserves the right to refuse to provide services or to discontinue them if the information obtained in the course of such checks gives rise to concerns that cannot be properly mitigated.

Ongoing monitoring and response to abuse

Our infrastructure must not be used for malicious or unlawful activities, including, among other things, the distribution of malware, hacking, DDoS attacks, fraud or other forms of abuse.

We apply technical and organisational measures designed to detect indicators of abuse or unlawful use of our services. When such indicators appear, we promptly review the situation. This may include an internal investigation, communication with the customer, and engagement with relevant third parties such as upstream providers, partners or competent authorities.

If we confirm that our services are being used unlawfully or in

breach of our terms and acceptable use policies, we may

suspend or terminate the relevant services, restrict access, or take other measures we consider necessary. Where required or appropriate, we also cooperate with law-enforcement and regulatory authorities.

Sanctions compliance and zero-tolerance policy

MIRhosting strictly complies with applicable European Union sanctions regimes and other relevant legal requirements.

When a potential sanctions risk is identified – at the onboarding stage, during periodic reviews or following the emergence of new information – our standard course of action is to:

- suspend or restrict the relevant services to the extent necessary,

- preserve records and technical logs relating to the case, and

- carry out additional review and analysis of information about the customer, beneficial owners and the nature of the use of services.

In complex or borderline cases we engage external experts in sanctions regulation and compliance to obtain specialised advice and ensure that our actions are aligned with applicable law and regulatory expectations.

We apply a zero-tolerance policy to confirmed breaches of sanctions legislation and reserve the right to refuse to provide services, or to suspend or terminate them, where this is necessary to comply with legal requirements and to protect the integrity of our network.

Continuous improvement and transparency

We continue to invest in safeguards, internal procedures and staff training aimed at preventing abuse of our infrastructure and ensuring an effective response to incidents. Our internal policies are periodically reviewed and updated in light of legal changes, regulatory guidance and industry practice.

We adhere to the principles of transparency and open communication regarding our approach to compliance and security so that customers, partners and regulators understand how we operate and how seriously we take these responsibilities.

This statement has been prepared with the support of qualified legal counsel and reflects MIRhosting's current practices in the area of compliance and network security. It does not limit any rights or obligations arising under applicable law, our general terms and conditions or individual service agreements.