



SUPPLIER INFORMATION SECURITY ADDENDUM

Introduction

Nomad offers financial and technology services in a digital environment, in which the protection of data, systems, and services depends on the security practices adopted not only by Nomad, but also by the suppliers, service providers, and partners that support its operations.

This Information Security Addendum for Suppliers ("Addendum") establishes the mandatory minimum information security and cybersecurity requirements for suppliers supporting Nomad Group services, including banking, payment, and investment activities, as well as other services provided.

This Addendum complements the public Information Security and Cybersecurity Policy of the Nomad Group and is shared strictly within a corporate (B2B) scope during supplier onboarding and contracting. It is a confidential document and must not be distributed to end customers or to any party outside the contracting relationship.

Scope and Applicability

This Addendum applies to any supplier, service provider, or subcontractor (collectively, "Supplier") that, in the context of

ADENDO DE SEGURANÇA DA INFORMAÇÃO PARA FORNECEDORES

Introdução

A Nomad oferece serviços financeiros e tecnológicos em ambiente digital, onde a segurança de dados, sistemas e serviços depende tanto das práticas internas quanto das adotadas por fornecedores, prestadores de serviço e parceiros que dão suporte às suas operações.

Este Adendo de Segurança da Informação para Fornecedores ("Adendo") estabelece os requisitos mínimos obrigatórios de segurança da informação e cibersegurança para fornecedores que suportam os serviços do Grupo Nomad, incluindo atividades bancárias, de pagamentos, de investimento e demais serviços prestados.

Este Adendo complementa a Política de Segurança da Informação e Cibersegurança pública do Grupo Nomad e é compartilhado estritamente em âmbito corporativo (B2B), durante o onboarding e a contratação de fornecedores. É documento confidencial e não deve ser distribuído a clientes finais ou a terceiros alheios à relação contratual.

Escopo e Aplicabilidade

Este Adendo aplica-se a qualquer fornecedor, prestador de serviço ou subcontratado (coletivamente, "Fornecedor")



services provided to the Nomad Group: (i) processes, stores, transmits, or accesses Nomad Data; (ii) accesses Nomad systems, networks, or technology environments; or (iii) supports services related to Nomad Group products, business lines, or activities, including the Nomad Banking Program, money transmission activities operated by Nomad Fintech, Inc., and investment services provided by Nomad Investment Services, Inc.

The application of this Addendum is proportionate to the risk of the relationship, considering the sensitivity of the data processed, the criticality of the services, and the level of access granted—the same factors that guide the definition of "Critical Supplier" below.

The requirements of this Addendum are minimum requirements and are in addition to—not in lieu of—the obligations under the service agreement entered into with the Supplier. Where there is a conflict between the agreement, applicable law, and external partner requirements, the strictest obligation prevails.

Each supplier's risk rating—assigned during onboarding and reviewed annually—is part of Nomad's internal third-party risk management process. For suppliers deemed relevant under internationally recognized compliance frameworks, the assessment may be based on current independent assurance reports (such as SOC 2 Type II and/or ISO/IEC 27001) or on information provided by the supplier—including standardized

que, no contexto dos serviços prestados ao Grupo Nomad: (i) trate, armazene, transmita ou acesse Dados Nomad; (ii) acesse sistemas, redes ou ambientes tecnológicos da Nomad; ou (iii) suporte serviços relacionados a produtos, linhas de negócio ou atividades do Grupo Nomad, incluindo o Nomad Banking Program e as atividades de transmissão de dinheiro operadas pela Nomad Fintech, Inc. e os serviços de investimento prestados pela Nomad Investment Services, Inc.

A aplicação deste Adendo é proporcional ao risco do relacionamento, considerando a sensibilidade dos dados tratados, a criticidade dos serviços e o nível de acesso concedido — os mesmos fatores que orientam a definição de "Fornecedor Crítico" abaixo.

Os requisitos deste Adendo são mínimos e se somam, sem substituir, às obrigações do contrato de prestação de serviços celebrado com o Fornecedor. Prevalece a obrigação mais rígida entre o contrato, a legislação aplicável e os requisitos de parceiros externos.

A classificação de risco de cada Fornecedor — atribuída no onboarding e revisada anualmente — integra o processo interno de gestão de risco de terceiros da Nomad. Para fornecedores relevantes sob frameworks de conformidade reconhecidos internacionalmente, a avaliação pode se basear em relatórios de asseguração independentes vigentes (como SOC 2 Type II e/ou ISO/IEC 27001) ou em informações fornecidas pelo Fornecedor, incluindo



questionnaires and transparency portals—at Nomad’s discretion.

questionários padronizados e portais de transparência, a critério da Nomad.

Definitions

- "Nomad Data" means any data or information owned, controlled, or processed by the Nomad Group or on its behalf that the Supplier receives, accesses, or processes in the context of the services, including Non-Public Personal Information, transactional data, authentication data, and confidential business information.
- "Nonpublic Personal Information" or 'NPI' means personally identifiable financial information of customers provided to Nomad, generated through transactions or otherwise obtained, that is not lawfully available to the public, including personal and sensitive data protected under Brazil's General Data Protection Law (Law No. 13,709/2018), regardless of its financial nature.
- "Security Incident" means any event, or series of events, that causes or may cause a negative impact on technology assets, compromising the confidentiality, integrity, availability, or privacy of information, arising from or resulting from an operational failure.
- "Subcontractor" means any third party engaged by the Supplier to perform a portion of the services involving Nomad Data or access to its environments.

Definições

- "Dados Nomad" significa quaisquer dados ou informações de titularidade, sob controle ou tratados pelo Grupo Nomad ou em seu nome, que o Fornecedor receba, acesse ou trate no contexto dos serviços, incluindo Informações Pessoais Não Públicas, dados transacionais, dados de autenticação e informações confidenciais de negócio.
- "Informações Pessoais Não Públicas" ou NPI são informações financeiras identificáveis de clientes fornecidas à Nomad, geradas em transações ou obtidas por qualquer outro meio, que não estejam legalmente disponíveis ao público, incluindo dados pessoais e sensíveis protegidos pela LGPD (Lei nº 13.709/2018), independentemente de seu caráter financeiro.
- "Incidente de Segurança" significa qualquer evento, ou série de eventos, que gere impacto negativo, real ou potencial, sobre ativos tecnológicos, comprometendo a confidencialidade, integridade, disponibilidade ou privacidade das informações, com origem em falha operacional ou dela decorrente.
- "Subcontratado" significa qualquer terceiro contratado pelo Fornecedor para executar parte dos serviços que envolva



- "Critical Supplier" means a Supplier classified as such by Nomad—whether during onboarding or a periodic review—based on an internal third-party risk classification methodology that considers, among other factors: (i) the volume and sensitivity of the Nomad Data processed, including NPI; (ii) the criticality of the systems, networks, or environments to which the Supplier has access; (iii) the operational, financial, or regulatory impact of any failure, interruption, or unavailability of the services; and (iv) the availability of replacement alternatives within a timeframe compatible with the continuity of Nomad's services.

Regulatory Context

The Nomad Group—including the Nomad Banking Program (operated by Nomad Fintech, Inc.) and the investment services of Nomad Investment Services, Inc.—is subject to U.S. federal regulations applicable to its lines of business, its strategic partner, and the service providers that support them. The requirements of this Addendum reflect, among others, the following sources:

- Gramm-Leach-Bliley Act, Section 501(b) (15 U.S.C. § 6801), and the Interagency Guidelines Establishing Information Security Standards (12 CFR Part 30, Appendix B), which require financial institutions to oversee service providers

Dados Nomad ou acesso a seus ambientes.

- "Fornecedor Crítico" significa o Fornecedor assim classificado pela Nomad, no onboarding ou em revisão periódica, com base em metodologia interna de classificação de risco de terceiros que considera, entre outros fatores: (i) o volume e a sensibilidade dos Dados Nomad tratados, incluindo NPI; (ii) a criticidade dos sistemas, redes ou ambientes aos quais o Fornecedor tem acesso; (iii) o impacto operacional, financeiro ou regulatório de eventual falha, interrupção ou indisponibilidade dos serviços; e (iv) a existência de alternativas de substituição em prazo compatível com a continuidade dos serviços da Nomad.

Contexto Regulatório

O Grupo Nomad — incluindo o Nomad Banking Program (operado pela Nomad Fintech, Inc.) e os serviços de investimento da Nomad Investment Services, Inc. — está sujeito à regulação federal norte-americana aplicável a suas linhas de negócio, a seu parceiro estratégico e aos prestadores de serviço que os suportam. Os requisitos deste Adendo refletem, entre outras, as seguintes fontes:

- Gramm-Leach-Bliley Act, Seção 501(b) (15 U.S.C. § 6801), e as Interagency Guidelines Establishing Information Security Standards (12 CFR Part 30, Apêndice B), que exigem que instituições financeiras supervisionam seus



and to require them, by contract, to implement appropriate safeguards;

- Computer-Security Incident Notification Rule (12 CFR Part 53), which establishes incident notification obligations for banking organizations and their bank service providers;
- Interagency Guidance on Third-Party Relationships: Risk Management (June 2023), applicable to the oversight of the full third-party life cycle;
- FFIEC Information Technology Examination Handbook, as a reference for expected controls; and
- SEC Regulation S-P (17 CFR Part 248) and SEC Regulation S-ID (Identity Theft Red Flags Rule), applicable to Nomad Investment Services, Inc. as a registered broker-dealer, requiring due diligence and contractual oversight of service providers regarding the protection of customer information;
- FINRA Rules 3110 (Supervision) and 4370 (Business Continuity), applicable to Nomad Investment Services, Inc. as a member of the Financial Industry Regulatory Authority.
- Additionally, regarding activities carried out in Brazil by the Nomad Group, this Addendum observes Brazil's General Data Protection Law – Law No. 13,709/2018 ("LGPD"), as well as best practices for cybersecurity and the contracting of data processing and cloud computing services set forth in CMN Resolution No. 4.893/2021 and BCB Resolution No. 85/2021.

prestadores de serviço e exijam deles, contratualmente, a implementação de salvaguardas adequadas;

- Computer-Security Incident Notification Rule (12 CFR Part 53), que estabelece obrigações de notificação de incidentes para organizações bancárias e seus prestadores de serviços bancários;
- Interagency Guidance on Third-Party Relationships: Risk Management (junho de 2023), aplicável à supervisão de todo o ciclo de vida de terceiros;
- FFIEC Information Technology Examination Handbook, como referência de controles esperados;
- SEC Regulation S-P (17 CFR Part 248) e SEC Regulation S-ID (Identity Theft Red Flags Rule), aplicáveis à Nomad Investment Services, Inc. como corretora de valores mobiliários (broker-dealer) registrada, exigindo due diligence e supervisão contratual de prestadores de serviço quanto à proteção de informações de clientes;
- FINRA Rules 3110 (Supervision) e 4370 (Business Continuity), aplicáveis à Nomad Investment Services, Inc. como membro da Financial Industry Regulatory Authority.
- Adicionalmente, no que se refere a atividades desenvolvidas no Brasil pelo Grupo Nomad, este Adendo observa a Lei Geral de Proteção de Dados – Lei nº 13.709/2018 ("LGPD"), bem como as melhores práticas de segurança cibernética e de contratação de serviços de processamento de dados e computação em nuvem previstas na



Resolução CMN nº 4.893/2021 e na Resolução BCB nº 85/2021.

Suppliers classified as critical risk may be subject to examination by U.S. federal banking regulators (OCC, FDIC) under the Bank Service Company Act (12 U.S.C. § 1867(c)) and, where they support investment services, to the oversight exercised by the SEC and FINRA over Nomad Investment Services, Inc. In any event, they must demonstrate the compliance of their programs with these requirements upon Nomad's request.

Information Security Program

The Supplier must maintain a written information security program appropriate to its size, complexity, and the nature and scope of its activities, designed to protect the confidentiality, integrity, and availability of Nomad Data. The program must be aligned with a recognized framework, such as NIST Cybersecurity Framework, ISO/IEC 27001, or an equivalent standard.

Suppliers classified as critical must make information security policies and controls available, conduct risk assessments at least annually, and update them whenever there is a significant change in their environment, the threat landscape, or the services provided to the Nomad Group.

Fornecedores classificados como risco crítico podem estar sujeitos ao exame dos reguladores bancários federais dos EUA (OCC, FDIC), nos termos do Bank Service Company Act (12 U.S.C. § 1867(c)) e, quando suportarem serviços de investimento, à supervisão da SEC e da FINRA sobre a Nomad Investment Services, Inc. Em qualquer caso, deverão evidenciar a conformidade de seus programas com essas exigências, mediante solicitação da Nomad.

Programa de Segurança da Informação

O Fornecedor deve manter programa formal e documentado de segurança da informação, proporcional ao risco e adequado a seu porte, complexidade, natureza e escopo de atividades, destinado a proteger a confidencialidade, integridade e disponibilidade dos Dados Nomad. O programa deve seguir framework reconhecido, como NIST Cybersecurity Framework, ISO/IEC 27001 ou padrão equivalente.

Fornecedores classificados como críticos devem disponibilizar políticas e controles de segurança da informação, realizar avaliações de risco ao menos anualmente, e atualizá-los sempre que houver mudança relevante em seu ambiente, no cenário de ameaças ou nos serviços prestados ao Grupo Nomad.



Personnel Security and Training

The Supplier must maintain a documented personnel security program for professionals with access to Nomad Data, covering: (i) background checks prior to granting access, including for privileged accounts, to the extent permitted by applicable law; (ii) written confidentiality obligations for all individuals with access to Nomad Data; (iii) security awareness training upon hiring and, at a minimum, annually; and (iv) a documented disciplinary process for violations, applied consistently and including, where appropriate, the revocation of access and removal from services provided to Nomad.

Segurança de Pessoal e Treinamento

O Fornecedor deve manter programa documentado de segurança de pessoal para profissionais com acesso a Dados Nomad, contemplando: (i) verificação de antecedentes antes da concessão de acesso, incluindo perfis privilegiados, na medida permitida pela legislação aplicável; (ii) obrigações escritas de confidencialidade para todos com acesso a Dados Nomad; (iii) treinamento de conscientização em segurança na contratação e, no mínimo, anualmente; e (iv) processo disciplinar documentado para violações, aplicado de forma consistente e incluindo, quando cabível, revogação de acessos e afastamento dos serviços prestados à Nomad.

Access Control

- Access to Nomad Data and Nomad environments must observe the principles of least privilege and need-to-know.
- Access profiles must observe segregation of duties, so that no individual concentrates incompatible activities — such as requesting, approving, executing, and auditing the same operation — to the extent the organizational structure permits.
- Each user must have individual and unique credentials; shared or generic accounts are prohibited for access to Nomad Data.
- The Supplier must adopt strong authentication, including multi-factor

Controle de Acesso

- O acesso a Dados Nomad e a ambientes da Nomad deve observar os princípios de menor privilégio e need-to-know.
- Os perfis de acesso devem observar segregação de funções, de modo que nenhum indivíduo concentre atividades incompatíveis — como solicitar, aprovar, executar e auditar a mesma operação —, na medida em que a estrutura organizacional permitir.
- Cada usuário deve ter credenciais individuais e únicas; contas compartilhadas ou genéricas são proibidas para acesso a Dados Nomad.



authentication (MFA), proportional to the criticality of the systems and the sensitivity of the Nomad Data involved.

- Access rights must be reviewed periodically — including upon changes in function — and revoked when the professional is terminated.
- Privileged access must be restricted and have additional layers of security.

- O Fornecedor deve adotar autenticação forte, incluindo multifator (MFA), proporcional à criticidade dos sistemas e à sensibilidade dos Dados Nomad envolvidos.
- Os direitos de acesso devem ser revisados periodicamente — inclusive em mudanças de função — e revogados quando o profissional for desligado.
- Acessos privilegiados devem ser restritos e ter camadas adicionais de segurança.

Data Protection

- The Supplier must encrypt Nomad Data in transit and at rest using market-recognized, up-to-date algorithms and protocols that are commensurate with the information classification and applicable regulatory and contractual requirements.
- Nomad Data must be logically segregated from the data of the Supplier's other clients and used exclusively for the contracted services; any other purpose requires prior written authorization from Nomad.
- Nomad Data must be stored and processed in Brazil, the United States, or another jurisdiction with compatible data protection, subject to prior notice to Nomad regarding the location; outside the United States [or other jurisdictions approved in writing by Nomad], prior written authorization is also required.
- Production Nomad Data may not be used in development or testing environments unless anonymized or protected by

Proteção de Dados

- O Fornecedor deve criptografar os Dados Nomad em trânsito e em repouso, com algoritmos e protocolos reconhecidos pelo mercado, atualizados e proporcionais à classificação da informação e aos requisitos regulatórios e contratuais aplicáveis.
- Os Dados Nomad devem ser logicamente segregados dos dados de outros clientes do Fornecedor e usados exclusivamente para os serviços contratados; qualquer outra finalidade requer autorização prévia e por escrito da Nomad.
- Os Dados Nomad devem ser armazenados e tratados no Brasil, nos Estados Unidos ou em outra jurisdição com proteção de dados compatível, mediante aviso prévio à Nomad sobre a localização; fora dos Estados Unidos [ou de outras jurisdições aprovadas por escrito pela Nomad], é exigida também autorização prévia e por escrito.
- Dados Nomad de produção não podem ser usados em ambientes de



controls equivalent to those used in production.

- Records, including personal data, must be retained only for the time necessary to fulfill the defined purposes and applicable legal requirements, and must be securely deleted at the end of that period.

desenvolvimento ou teste, salvo se anonimizados ou protegidos por controles equivalentes aos de produção.

- Os registros, incluindo dados pessoais, devem ser retidos apenas pelo tempo necessário às finalidades definidas e aos requisitos legais aplicáveis, e eliminados de forma segura ao fim desse prazo.

Network, Infrastructure, and Operations Security

- Systems that process Nomad Data must be hardened according to industry benchmarks, protected by firewalls and intrusion detection or prevention mechanisms, and covered by anti-malware controls kept up to date.
- Security patches must be applied within risk-based timelines, with critical vulnerabilities remediated within [15] days of vendor release or of identification.
- Security events on systems that process Nomad Data must be logged. Logs must be time-synchronized, protected against tampering, monitored, and retained for at least [12] months.
- Changes to production environments must follow a documented change management process.

Segurança de Rede, Infraestrutura e Operações

- Sistemas que tratam Dados Nomad devem receber hardening conforme benchmarks de mercado, ser protegidos por firewalls e mecanismos de detecção/prevenção de intrusão, e contar com controles antimalware atualizados.
- Patches de segurança devem seguir prazos baseados em risco, com vulnerabilidades críticas corrigidas em até 15 dias da liberação ou da identificação.
- Eventos de segurança devem ser registrados em log, com sincronização de horário, proteção contra adulteração, monitoramento e retenção mínima de 12 meses.
- Mudanças em produção devem seguir processo documentado de gestão de mudanças.

Secure Development and Vulnerability Management

- Software developed or maintained by the Supplier in connection with the services must follow a secure development life

Desenvolvimento Seguro e Gestão de Vulnerabilidades

- Softwares desenvolvidos ou mantidos pelo Fornecedor no contexto dos serviços devem seguir um ciclo de



cycle, with segregation between development, test, and production environments.

- The Supplier must run vulnerability scans on systems that process Nomad Data at least quarterly and after material changes.
- The Supplier must engage a qualified independent party to perform penetration testing at least annually, and must remediate findings within timelines proportional to severity [critical: 15 days; high: 30 days; medium: 90 days].
- Upon request, the Supplier must share with Nomad an executive summary of the most recent penetration test and the status of open findings.

desenvolvimento seguro, com segregação entre ambientes de desenvolvimento, teste e produção.

- O Fornecedor deve executar varreduras de vulnerabilidade nos sistemas que tratem Dados Nomad ao menos trimestralmente e após mudanças relevantes.
- O Fornecedor deve contratar terceiro independente e qualificado para realizar testes de intrusão ao menos anualmente, corrigindo os apontamentos em prazos proporcionais à severidade [crítico: 15 dias; alto: 30 dias; médio: 90 dias].
- Mediante solicitação, o Fornecedor deve compartilhar com a Nomad um sumário executivo do teste de intrusão mais recente e o status dos apontamentos em aberto.

Artificial intelligence

The use of generative artificial intelligence tools or third-party AI assistants to process Nomad Data—including, without limitation, for development, analysis, or support related to the contracted services—is subject to Nomad’s prior written approval, even if it does not involve model training.

Prior to adopting any artificial intelligence tool that processes Nomad Data, the Supplier must inform Nomad of: (i) the tool and the underlying provider; (ii) the purpose of use; and (iii) the measures adopted to prevent the underlying provider from retaining, reusing, or training models using Nomad Data.

Inteligência Artificial

O uso de ferramentas de inteligência artificial generativa ou de assistentes de IA de terceiros para o processamento de Dados Nomad — incluindo, sem limitação, para desenvolvimento, análise ou suporte relacionados aos serviços contratados — está sujeito a aprovação prévia e por escrito da Nomad, ainda que não envolva o treinamento de modelos.

Previamente à adoção de qualquer ferramenta de inteligência artificial que processe Dados Nomad, o Fornecedor deve informar à Nomad: (i) a ferramenta e o provedor subjacente; (ii) a finalidade do uso; e (iii) as medidas adotadas para impedir que o



The use of Nomad Data for training, fine-tuning, or enhancing artificial intelligence models—whether proprietary or third-party—is prohibited without Nomad’s prior written authorization.

Any unauthorized use of Nomad Data by artificial intelligence tools, or any leakage, exposure, or improper processing of Nomad Data through such tools, constitutes a Security Incident for the purposes of this Addendum and is subject to the notification obligations set forth in the "Incident Response and Notification" section.

provedor subjacente retenha, reaproveite ou treine modelos com Dados Nomad.

É proibido o uso de Dados Nomad para o treinamento, o ajuste (fine-tuning) ou o aprimoramento de modelos de inteligência artificial, próprios ou de terceiros, sem autorização prévia e por escrito da Nomad.

Qualquer uso não autorizado de Dados Nomad por ferramentas de inteligência artificial, ou qualquer vazamento, exposição ou tratamento indevido de Dados Nomad por meio dessas ferramentas, constitui Incidente de Segurança para os fins deste Adendo, sujeito às obrigações de notificação previstas na seção "Resposta e Notificação de Incidentes".

Incident Response and Notification

The Supplier must maintain incident response policies, procedures, and a plan — covering detection, containment, eradication, recovery, and communication — with a scope proportional to the Supplier's risk classification.

The Supplier must notify Nomad of any Security Incident in a timely manner and, in any event, within 24 hours of its discovery, via the channels defined by Nomad (e.g., health dashboard, security center, or equivalents).

For material incidents, the notification must describe, to the extent known, the

Resposta e Notificação de Incidentes

O Fornecedor deve manter políticas, procedimentos e plano de resposta a incidentes — cobrindo detecção, contenção, erradicação, recuperação e comunicação —, com abrangência proporcional à classificação de risco do Fornecedor.

O Fornecedor deve notificar a Nomad sobre qualquer Incidente de Segurança tempestivamente e, em qualquer caso, em até 24 horas após sua descoberta, pelos canais definidos pela Nomad (ex.: health dashboard, security center ou equivalentes).

Para incidentes relevantes, a notificação deve descrever, na medida do conhecido, a



nature and scope of the incident, the affected Nomad Data, the containment and remediation measures adopted, and a point of contact—information necessary for Nomad to comply with regulatory obligations and deadlines. The Supplier must also preserve relevant evidence and refrain from making public statements regarding Nomad or its partners without prior written approval, unless required by law.

Business Continuity and Disaster Recovery

The Supplier must keep Nomad constantly informed of any limitations, restrictions, or events that may affect the services or compliance with applicable legislation, even if they do not, in isolation, constitute a Security Incident or trigger a continuity plan.

The Supplier must maintain business continuity and disaster recovery plans appropriate to the nature and criticality of the services, with RTO and RPO values compatible with the service levels agreed upon with Nomad.

Critical Suppliers must test these plans at least annually and make the results available to Nomad upon request, notifying Nomad whenever the activation of a plan affects the services provided.

Subcontracting

natureza e o alcance do incidente, os Dados Nomad afetados, as medidas de contenção e remediação adotadas e um ponto de contato — informações necessárias ao cumprimento das obrigações regulatórias e prazos da Nomad. O Fornecedor deve ainda preservar evidências relevantes e abster-se de manifestações públicas sobre a Nomad ou seus parceiros sem aprovação prévia e por escrito, salvo exigência legal.

Continuidade de Negócios e Recuperação de Desastres

O Fornecedor deve manter a Nomad permanentemente informada sobre limitações, restrições ou eventos que possam afetar os serviços ou o cumprimento da legislação aplicável, mesmo que não configurem, isoladamente, Incidente de Segurança ou acionamento de plano de continuidade.

O Fornecedor deve manter planos de continuidade de negócios e recuperação de desastres adequados à natureza e criticidade dos serviços, com RTO e RPO compatíveis com os níveis de serviço acordados com a Nomad.

Fornecedores Críticos devem testar esses planos ao menos anualmente e disponibilizar os resultados à Nomad mediante solicitação, notificando-a sempre que a ativação de um plano afetar os serviços prestados.

Subcontratação



The Supplier may not engage Subcontractors for services related to Nomad without Nomad's prior consent, detailing the scope and risks involved, and must conduct prior technical due diligence to ensure that the Subcontractor's controls and policies meet the information security, data protection, and privacy standards set forth in this Addendum — remaining fully responsible for the acts and omissions of its Subcontractors.

O Fornecedor não pode contratar Subcontratados para serviços relacionados à Nomad sem consentimento prévio desta, com detalhamento do escopo e dos riscos envolvidos, e deve realizar diligência técnica prévia para assegurar que os controles e políticas do Subcontratado atendam aos padrões de segurança da informação, proteção de dados e privacidade deste Adendo — permanecendo integralmente responsável por seus atos e omissões.

Oversight, Audits, and Assessments

- The Supplier must respond to Nomad's due diligence and periodic security questionnaires within the requested timelines.
- Critical Suppliers must provide Nomad, at least annually, with an independent assurance report demonstrating the effectiveness of their security controls, such as SOC 2 Type II, and/or ISO/IEC 27001 certification, or a PCI DSS Report on Compliance where payment card data is handled.
- The Supplier must permit Nomad, and their internal and external auditors to audit, inspect, and examine the facilities, records, and systems related to the services, upon reasonable notice, including onsite where justified by risk.
- The Supplier acknowledges that the services provided to the Nomad Banking Program are subject to examination and supervision by U.S. federal banking regulators, including the Office of the Comptroller of the Currency (OCC) and

Supervisão, Auditorias e Avaliações

- O Fornecedor deve responder aos questionários de due diligence e de segurança da Nomad nos prazos solicitados.
- Fornecedores Críticos devem fornecer à Nomad, ao menos anualmente, relatório de asseguaração independente que demonstre a eficácia de seus controles de segurança — como SOC 2 Type II, certificação ISO/IEC 27001 ou Report on Compliance PCI DSS, quando houver tratamento de dados de cartões.
- O Fornecedor deve permitir que a Nomad e seus auditores internos e externos auditem, inspecionem e examinem instalações, registros e sistemas relacionados aos serviços, mediante aviso razoável, inclusive presencialmente quando o risco justificar.
- O Fornecedor reconhece que os serviços prestados ao Nomad Banking Program estão sujeitos a exame e supervisão dos reguladores bancários federais dos EUA



the Federal Deposit Insurance Corporation (FDIC), under the Bank Service Company Act.

- The Supplier must remediate audit and assessment findings within timelines agreed with Nomad, proportional to the risk.

– OCC e FDIC –, nos termos do Bank Service Company Act.

- O Fornecedor deve remediar apontamentos de auditorias e avaliações nos prazos acordados com a Nomad, proporcionais ao risco.

Termination, Return, and Destruction of Data

Upon termination or expiration of the services, or at Nomad's request, the Provider must return all Nomad Data in its possession or under its control—including copies held by Subcontractors—within the timeframes agreed upon in the contract and in a structured, commonly used format that enables reading and migration by Nomad or a new service provider. Once Nomad confirms, in writing, the integrity and availability of the received data, the Provider must securely and permanently delete such data from all environments under its possession or control, including those of Subcontractors, and certify the deletion in writing within 30 days of such confirmation. Where retention is required by law, the protections set forth in this Addendum remain in effect for as long as the data is retained, even beyond the aforementioned timeframes. Confidentiality obligations survive termination.

Non-Compliance

Non-compliance with this Addendum may result, at Nomad's discretion and in proportion to the risk, in the requirement of a

Término, Devolução e Destruição de Dados

No término ou expiração dos serviços, ou mediante solicitação da Nomad, o Fornecedor deve devolver todos os Dados Nomad em sua posse ou sob seu controle — incluindo cópias de Subcontratados —, nos prazos acordados em contrato e em formato estruturado e de uso comum que permita a leitura e migração pela Nomad ou por novo prestador. Após a Nomad confirmar, por escrito, a integridade e disponibilidade dos dados recebidos, o Fornecedor deve excluí-los de forma segura e definitiva de todos os ambientes sob sua posse ou controle, incluindo os de Subcontratados, e certificar a exclusão por escrito em até 30 dias dessa confirmação. Quando a lei exigir retenção, as proteções deste Adendo permanecem enquanto os dados forem retidos, mesmo após esses prazos. As obrigações de confidencialidade sobrevivem ao término.

Descumprimento

O descumprimento deste Adendo pode resultar, a critério da Nomad e proporcionalmente ao risco, na exigência de



remediation plan with defined timelines, suspension of the Supplier's access to Nomad Data and environments, or termination of the services agreement, without prejudice to other contractual and legal remedies. Nomad may report material breaches to its external partners when required.

plano de remediação com prazos definidos, na suspensão do acesso do Fornecedor a Dados Nomad e ambientes, ou na rescisão do contrato – sem prejuízo de outras medidas contratuais e legais. A Nomad pode reportar descumprimentos relevantes a seus parceiros externos, quando exigido.

Confidentiality of this Addendum

This Addendum is shared exclusively within a corporate (B2B) scope during supplier onboarding and contracting. It must not be published, distributed to end customers, or disclosed to any third party without prior written consent from Nomad, except as required by law or regulation.

Confidencialidade deste Adendo

Este Adendo é compartilhado exclusivamente em âmbito corporativo (B2B), durante o onboarding e a contratação de fornecedores, e não deve ser publicado, distribuído a clientes finais nem divulgado a terceiros sem consentimento prévio e por escrito da Nomad, salvo exigência legal ou regulatória.

Final Provisions

This Addendum may be reviewed and updated periodically to reflect changes in the regulatory, technological, operational environment, or in the threat landscape. Nomad will communicate material updates to Suppliers, which must implement the corresponding adjustments within the timelines indicated.

This Addendum complements the services agreement executed with the Supplier and the other documents governing the relationship. In case of conflict, the provision that offers the higher level of protection to Nomad Data prevails.

Disposições Finais

Este Adendo pode ser revisado e atualizado periodicamente para refletir mudanças no ambiente regulatório, tecnológico ou operacional, ou no cenário de ameaças. A Nomad comunicará atualizações relevantes aos Fornecedores, que deverão implementar os ajustes nos prazos indicados.

Este Adendo complementa o contrato de prestação de serviços celebrado com o Fornecedor e os demais documentos que regem o relacionamento. Em caso de conflito, prevalece a disposição que ofereça o maior nível de proteção aos dados da Nomad.



This addendum was last updated in
September 2026.

Este adendo foi atualizado pela última vez
em Setembro de 2026.