
Política de privacidade informação sobre o tratamento dos dados pessoais

Clientes e potenciais clientes (prospects)

A proteção dos seus dados pessoais é importante para a Nickel, constituindo uma das suas preocupações. A Financière des Paiements Électroniques SAS, Instituição de Pagamentos devidamente constituída de acordo com as leis de França considerada legalmente como Prestadora de Serviços de Pagamento pela ACPR (Autorité de Contrôle Prudentiel et de Résolution) sob o nº 16598, com sede em 1 Place des Marseillais- 94220 Charenton-le-Pont, matriculada no Registo do Comércio e das Sociedades de Créteil sob o nº B 753 886 092 e com o capital social de EUR 770 440, a operar em Portugal através da **Financière des Paiements Électroniques SAS - Sucursal em Portugal** com número Único de Pessoa Colectiva e Fiscal 980 712 050, com sede na Rua Galileu Galilei, nº2, 8º andar, Torre Ocidente, Centro Colombo, 1500-392 Lisboa, registada no Banco de Portugal com número de Instituição Financeira 5810 (doravante designada por **Nickel** ou «**Nós**»), é responsável pela recolha e tratamento dos seus dados pessoais, no que respeita às nossas atividades.

Nós pertencemos ao grupo BNP Paribas e o objectivo do presente documento de informação sobre o tratamento dos dados pessoais dos clientes e potenciais clientes, consiste em explicar como recolhemos e tratamos os seus dados pessoais e como os pode controlar e gerir.

Esta informação aplica-se, uniformemente, a todos os produtos e serviços da Nickel bem como à recolha e tratamento, se necessário, de informações complementares caso o cliente venha a subscrever outros produtos e serviços em particular que a Nickel oferece.

Este documento fornece respostas para as seguintes questões:

ÍNDICE

Está abrangido por esta informação sobre o tratamento dos dados pessoais?	3
Como pode controlar as nossas atividades de tratamento dos seus dados pessoais?	3
• Direito de acesso	3
• Direito de rectificação e actualização	3
• Direito ao apagamento/esquecimento	3
• Direito de oposição do tratamento com fundamento no interesse legítimo	4
• Direito de oposição ao tratamento com fundamento em prospecção comercial	4
• Direito de limitação do Tratamento	4
• Direito de não ficar sujeito a decisões individuais exclusivamente automatizadas com impacto na sua esfera jurídica	4
• Direito a retirar o seu consentimento	4
• Direito de portabilidade	4
Com que finalidade e com que fundamento jurídico usamos os seus dados pessoais?	4
• Estar em conformidade com as nossas obrigações legais e regulamentares	4
• Fins de combate ao branqueamento de capitais e ao financiamento do terrorismo	5
• Executar um contrato do qual seja parte ou medidas pré-contratuais a seu pedido	5
• Com base no nosso interesse legítimo ou no de terceiros	5
• Respeitando as suas escolhas e desde que tenha dado o seu consentimento específico	6
Que tipos de dados pessoais recolhemos?	7

De quem recolhemos dados pessoais?	8
Com quem partilhamos os seus dados pessoais e porquê?	8
• Com entidades do grupo BNP Paribas	8
• Com destinatários fora do Grupo BNP Paribas e subcontratantes	8
Transferências internacionais de dados pessoais	9
Por quanto tempo guardamos os seus dados pessoais?	9
Como pode acompanhar a evolução desta política de privacidade?	9
Como nos pode contactar?	9
Anexo I - Tratamento de dados pessoais no combate ao branqueamento de capitais e financiamento do terrorismo	10
Anexo 2 - Tempo de conservação dos dados pessoais	12

1. Está abrangido por esta informação sobre o tratamento dos dados pessoais?

Esta informação sobre dados pessoais aplica-se caso seja:

- um dos nossos clientes
- membro da família de um cliente Nickel. Os nossos clientes podem, ocasionalmente, partilhar connosco informações sobre a sua família, quando tal seja necessário, para lhes fornecer um produto ou prestar um serviço ou para os conhecer melhor;
- uma pessoa interessada nos nossos produtos ou serviços, que nos faculte os seus dados pessoais (num Agente Nickel, no nosso sítio da internet, na aplicação App Nickel, em eventos ou actividades de patrocínio) para que o possamos contactar.

Quando nos facultar dados pessoais relativos a outras pessoas, certifique-se de que as informa acerca da divulgação dos seus dados pessoais e convide-os a ler a presente Política de Privacidade constante no presente documento de informação sobre o tratamento dos dados pessoais dos clientes e prospects. Garantimos que faremos o mesmo, sempre que possível (por ex., se tivermos acesso aos contactos da pessoa em causa).

2. Como pode controlar as nossas atividades de tratamento dos seus dados pessoais?

Tem direitos que lhe permitem exercer um controle real sobre os seus dados pessoais e a forma como os tratamos.

Se pretender exercer os direitos enumerados em seguida, pode apresentar um pedido, enviando uma carta para o seguinte endereço dadospessoais@nickel.eu no nosso sítio da internet com uma digitalização/cópia do seu cartão de identificação, se solicitado.

Se tiver alguma questão relativa ao uso dos seus dados pessoais, ao abrigo da presente Política de Privacidade constante no Documento de Informação sobre o Tratamento dos Dados Pessoais Clientes e Potenciais Clientes, pode contactar o nosso Encarregado da Protecção de Dados no seguinte endereço dadospessoais@nickel.eu

Além dos direitos acima referidos, pode apresentar uma reclamação junto da autoridade de supervisão competente, que é geralmente a do seu local de residência, a Comissão Nacional de Protecção de Dados em Portugal.

2.1. Direito de acesso

Tem o direito de saber se os dados pessoais da sua Conta Cliente são ou não tratados acedendo aos mesmos, diretamente, através do nosso sítio da internet ou através da aplicação móvel App Nickel.

Se pretender ter acesso aos seus dados pessoais, podemos facultar-lhe uma cópia dos dados pessoais que solicitou, bem como as informações relativas ao seu tratamento, através de um pedido expresso da sua parte.

O seu direito de acesso pode ser limitado se tal informação não puder ser prestada por razões de segurança, objectivamente fundamentadas ou se for proibida, por outras disposições legais aplicáveis, como é o caso do regulamento relativo ao combate ao branqueamento de capitais e ao financiamento do terrorismo, que nos proíbe de lhe facultar o acesso direto aos seus dados pessoais tratados para esta finalidade. Neste caso, deve exercer o seu direito de acesso junto da CNPD, que nos solicitará os dados pessoais em questão.

2.2. Direito de rectificação e actualização

Tem direito de obter a retificação dos seus dados pessoais quando estejam inexatos ou desatualizados.

2.3. Direito ao apagamento/esquecimento

Se desejar, pode solicitar a eliminação dos seus dados pessoais, na medida em que seja permitido por lei.

2.4. Direito de oposição do tratamento com fundamento no interesse legítimo

Se não concordar com o tratamento com fundamento no interesse legítimo, tem o direito de se opor, a qualquer momento, tendo em conta motivos relacionados com a sua situação particular, indicando-nos especificamente o tratamento ao qual se pretende opor e as respectivas razões.

Nestes casos, o Encarregado de Protecção de Dados cessa o tratamento, a menos que apresente razões imperiosas e legítimas que prevaleçam sobre os interesses, direitos e liberdades do titular, ou para efeitos de exercício de um direito num processo judicial.

Não trataremos mais os seus dados pessoais excepto se existirem motivos legítimos e imperiosos de os tratar ou por razões de serem necessários o seu tratamento para constatação, exercício e defesas de direitos na justiça.

2.5. Direito de oposição ao tratamento com fundamento em prospecção comercial

Se não concordar com o tratamento em fundamento na prospecção comercial, incluindo a criação de perfis no que diz respeito a essa prospecção, tem o direito de se opor, a qualquer momento, a esse tratamento.

2.6. Direito de limitação do Tratamento

Tem o direito de, durante um certo período de tempo, limitar o tratamento dos seus dados pessoais. Tem o direito de obter a limitação do tratamento dos dados sempre que conteste a exactidão dos mesmos e até o responsável pelo tratamento verificar a qualidade dos mesmos no seu pedido.

O seu pedido, que contesta a exactidão dos dados pessoais e onde se identifica devidamente, vai ser analisado devidamente e durante este período tem o direito de obter a limitação do tratamento dos seus dados até o responsável pelo tratamento verificar a qualidade dos mesmos.

2.7. Direito de não ficar sujeito a decisões individuais exclusivamente automatizadas com impacto na sua esfera jurídica

Por uma questão de princípio, tem o direito de não ficar sujeito a uma decisão tomada apenas com base num tratamento automatizado, definição de perfis ou outro, que produza efeitos na sua esfera jurídica ou o afete significativamente. No entanto, podemos automatizar essa decisão se for necessário para a celebração ou execução de um contrato conosco autorizado por lei ou se nos tiver dado consentimento.

Em qualquer caso, tem o direito de contestar a decisão, manifestar o seu ponto de vista e solicitar a intervenção de uma pessoa competente para analisar a decisão.

2.8. Direito a retirar o seu consentimento

Se deu consentimento para o tratamento dos seus dados pessoais, pode retirar esse consentimento a qualquer momento.

2.9. Direito de portabilidade

Tem o direito a receber do Responsável pelo tratamento os seus dados pessoais, num formato estruturado, de uso corrente e de leitura automática e o direito de os transmitir a outro responsável, apenas se o tratamento de dados em causa se basear no consentimento ou num contrato e for realizado por meios automatizados.

Tem o direito a que os seus dados sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.

3. Com que finalidade e com que fundamento jurídico usamos os seus dados pessoais?

O objectivo desta secção, é explicar por que motivo tratamos os seus dados pessoais e o fundamento jurídico para o fazer.

3.1. Estar em conformidade com as nossas obrigações legais e regulamentares

Os seus dados pessoais são tratados para cumprir as nossas várias obrigações legais e regulamentares, sempre que necessário, nomeadamente prestadores de serviços de pagamento.

Utilizamos os seus dados pessoais para :

- monitorizar operações e transações de forma a identificar aquelas que se desviam do padrão normal (por ex., quando levanta uma grande quantia de dinheiro num país que não seja o seu local de residência);

- gerir e comunicar riscos (riscos financeiros, jurídicos, reputacionais, de adequação com normas ou regulamentos aplicáveis, etc.) em que nós e o Grupo BNP Paribas possa incorrer no âmbito das suas atividades;
- detetar e prevenir a corrupção;
- auxiliar no combate à fraude fiscal e cumprir as obrigações de controlo e notificação fiscal;
- registar transações para fins contabilísticos;
- prevenir, detetar e comunicar riscos relacionados com a Responsabilidade Social Corporativa e desenvolvimento sustentável;
- cumprir as disposições aplicáveis aos prestadores de serviços de confiança que emitem certificados de assinatura eletrónica;
- trocar e comunicar diferentes operações, transações ou ordens ou responder a um pedido oficial de uma Autoridade Tributária, fiscal, administrativa, criminal ou judicial, árbitros ou mediadores, outras entidades responsáveis pela aplicação da lei, organismos públicos, locais ou estrangeiros, devidamente autorizados.

3.2. Fins de combate ao branqueamento de capitais e ao financiamento do terrorismo

Como parte de um grupo bancário, devemos ter um sistema robusto de combate ao branqueamento de capitais e ao financiamento do terrorismo (AML/TF) em cada uma das nossas entidades, gerido de forma centralizada, bem como um sistema para aplicar sanções locais, europeias e internacionais.

Neste contexto, somos responsáveis pelo tratamento dos dados, em conjunto com a BNP Paribas SA.

O processamento implementado para atender a essas obrigações legais está detalhado no **Anexo I**.

3.3. Executar um contrato do qual seja parte ou medidas pré-contratuais a seu pedido

Os seus dados pessoais são tratados, quando é necessário, para celebrar ou executar um contrato, de forma a:

- subscrever o contrato, nomeadamente por assinatura eletrónica, os produtos e serviços distribuídos pela Nickel;
- fornecer os produtos e serviços da Nickel em conformidade com as Condições Gerais-Contrato Cliente, nomeadamente, permitindo pagar e ser pago;
- responder aos seus pedidos e prestar-lhe assistência;
- garantir o procedimento sucessório;

3.4. Com base no nosso interesse legítimo ou no de terceiros

Quando uma atividade de tratamento tem por base um interesse legítimo nosso ou de terceiro, ponderamos esse interesse face aos seus interesses ou direitos e liberdades fundamentais para garantir que existe um equilíbrio justo entre eles. Se pretender mais informações sobre o interesse legítimo prosseguido no âmbito de uma determinada atividade de tratamento, contacte-nos através dos endereços constantes na secção 10 deste documento.

3.4.1. No decurso da nossa atividade como serviço de pagamento usamos os seus dados pessoais para:

- gerir os riscos aos quais estamos expostos:
 - o guardamos comprovativos das operações ou transações, incluindo provas eletrónicas;
 - o monitoramos as suas transações para gerir, prevenir e detectar fraudes;
 - o procedemos à cobrança de dívidas;
 - o tratamos de ações judiciais e defesa em caso de litígio judicial;
- aumentar a cibersegurança, gerir as nossas plataformas e sítio na internet, e garantir a continuidade das atividades;
- aumentar a automatização e eficiência dos nossos processos operacionais e serviços ao cliente (por ex., preenchimento automático de reclamações, acompanhamento dos seus pedidos e

melhoria da sua satisfação com base nos dados pessoais recolhidos durante as nossas interações consigo, como gravações de chamadas telefónicas, *e-mails* ou chats).

- acompanhar a gestão do seu orçamento de forma a categorizar automaticamente os dados das transacções;
- realizar estudos estatísticos e desenvolver modelos preditivos e descritivos para:
 - o fins comerciais: identificar os produtos e serviços que melhor possam atender às suas necessidades, criar novas ofertas ou identificar novas tendências entre os nossos clientes, desenvolver a nossa política comercial tendo em conta as preferências dos nossos clientes;
 - o fins de segurança: para prevenir potenciais incidentes e melhorar a gestão da segurança;
 - o fins de adequação com normas ou regulamentos aplicáveis (por ex., combate ao branqueamento de capitais e ao financiamento do terrorismo) e gestão do risco;
 - o fins de prevenção da corrupção e fraude;
- organizar concursos, sorteios, operações promocionais, realizar estudos de opinião e de satisfação dos clientes.

3.4.2. Tratamos os seus dados pessoais para realizar um modelo padrão de modo a personalizar os nossos produtos e propostas

De forma a melhorar a sua experiência e satisfação, precisamos de determinar a que grupo de clientes pertence. Para este efeito, criamos um perfil padrão que resulta dos dados relevantes que selecionamos a partir das seguintes informações:

- dados que nos comunicou diretamente nas nossas interações consigo ou quando subscreve um produto ou serviço;
- dados resultantes da utilização dos nossos produtos ou serviços, como os que estão relacionados com as suas contas, incluindo o saldo das contas, movimentos regulares ou atípicos, a utilização do seu cartão no estrangeiro, bem como a categorização automática dos dados das suas transacções (por ex., a distribuição das suas despesas e dos seus recebimentos por categoria, conforme se possa ver na sua área de cliente);
- dados recolhidos a partir do uso dos nossos vários canais: sítio e aplicações (por ex., se é conhecedor das tecnologias digitais, se prefere um percurso de cliente para subscrever um produto ou serviço com mais autonomia (autoatendimento) ou puramente digital.

A menos que se oponha, procederemos a essa personalização com base na criação de perfis padrão. Para melhor atender às suas necessidades poderemos ir mais além, se consentir, realizando uma personalização por medida, conforme descrito abaixo.

3.5. Respeitando as suas escolhas e desde que tenha dado o seu consentimento específico

Em relação a algumas atividades de tratamento de dados pessoais, daremos informações específicas e pediremos o seu consentimento. Relembramos que pode retirar o seu consentimento a qualquer momento.

Em particular, pedimos o seu consentimento para:

- personalização das nossas propostas e produtos ou serviços, com base em perfis mais sofisticados para antecipar as suas necessidades e comportamentos;
- qualquer proposta eletrónica de produtos e serviços que não seja semelhante àqueles que subscreveu ou de produtos e serviços dos nossos parceiros de confiança;
- utilização dos seus dados de navegação (*cookies*) para fins comerciais ou para melhorar o conhecimento do seu perfil.

Outros pedidos de consentimento podem ser solicitados para tratar os seus dados pessoais, quando necessário e em determinadas situações.

4. Que tipos de dados pessoais recolhemos?

Recolha directa

Recolhemos e utilizamos os seus dados pessoais, ou seja, qualquer informação que o identifique ou que permita identificá-lo.

Dependendo, nomeadamente, do tipo de produto ou serviço que lhe disponibilizamos e das interações que temos consigo, recolhemos vários tipos de dados pessoais sobre si, incluindo:

- **Dados de identificação:** por ex., nome completo, género, local e data de nascimento, nacionalidade, número do cartão de cidadão, número do passaporte, fotografia, assinatura;
- **Dados de contacto:** endereço postal, endereço de *e-mail*, número de telefone fixo ou telemóvel (particulares ou profissionais);
- **Informações relativas à sua situação financeira e familiar:** por ex., estado civil, regime de bens, número de filhos e idade;
- **Informações financeiras e fiscais:** por ex. Número de contribuinte (NIF), morada de residência fiscal, morada de residência, salário e outros rendimentos;
- **Informações relativas à educação e emprego:** por ex. categoria profissional, sector profissional, nível de estudos;
- **Informações ligadas à sua conta de pagamento:** por ex. número do cartão, transferências e levantamentos dados dos beneficiários, incidentes de pagamentos;
- **Dados de transações:** por ex. movimentos e saldos de contas, transações incluindo os dados dos beneficiários, como nomes completos, endereços e dados de contacto, bem como os dados das transações bancárias, montante, data, hora e tipo de transação (cartão de pagamento, transferência, cheque, débito direto);
- **Dados relativos aos seus hábitos e preferências relacionados com o uso dos nossos produtos e serviços;**
- **Dados recolhidos nas nossas interações consigo:** por ex., os seus comentários, sugestões, necessidades recolhidas durante as nossas interações consigo pessoalmente nos Agentes Nickel, em comunicações telefónicas (conversas), por *e-mail*, chat, trocas nas nossas páginas de redes sociais e as suas reclamações mais recentes. A sua ligação e dados de rastreamento, como *cookies* e rastreadores para fins não publicitários ou analíticos nos nosso sítio da internet, serviços online, aplicações, páginas de redes sociais;
- **Dados de geolocalização:** por ex. localizações de levantamentos ou pagamentos por motivos de segurança, ou para identificar a localização da agência ou prestador de serviço que lhe esteja mais próximo;
- **Dados sobre os seus dispositivos (telemóvel, computador, tablet, etc.):** endereço IP, especificações técnicas e dados de identificação exclusiva;
- **Credenciais de login personalizadas ou distintivos de segurança** utilizados para aceder ao sítio da internet e aplicação App Nickel.

Podemos recolher dados sensíveis, como dados de saúde, dados biométricos ou dados relativos a infrações criminais, sujeito ao cumprimento das condições estritas estabelecidas no RGPD e na lei de execução do mesmo (Lei 59/2019, de 8 de agosto).

Recolha indirecta

Podemos recolher igualmente dados pessoais de forma indirecta, mesmo que não seja um cliente Nickel, nomeadamente:

- Dados de identificação, de contacto e actividades numéricas de prospecção,
- Dados de identificação e de contacto de representantes legais e membros da família, herdeiros, devedores(por ex. em caso de processos de insolvência e sobreendividamento) mandatários sociais.

5. De quem recolhemos dados pessoais?

Recolhemos dados pessoais diretamente de si, enquanto nosso Cliente; no entanto, podemos também recolher dados pessoais de outras fontes.

Por vezes, recolhemos dados de fontes públicas:

- publicações/bases de dados disponibilizadas por autoridades oficiais ou terceiros (por ex., Diário da República, Registo Comercial, bases de dados geridas pelas autoridades de supervisão, como seja o Banco de Portugal;
- *websites*/páginas de redes sociais de pessoas coletivas ou clientes comerciais que contenham as

- informações sobre si que tenha divulgado (por ex., o seu próprio site ou página de redes sociais);
- informações públicas, como as que foram publicadas nos meios de comunicação social.

Também recolhemos dados pessoais junto de terceiros:

- de outras entidades do Grupo BNP Paribas;
- dos nossos clientes;
- dos nossos parceiros comerciais;
- dos prestadores de serviços de iniciação de pagamento e agregadores de contas (prestadores de serviços de informações de contas).

6. Com quem partilhamos os seus dados pessoais e porquê?

6.1. Com entidades do grupo BNP Paribas

Como entidade do grupo BNP Paribas trabalhamos em estreita colaboração com outras empresas do Grupo. Os seus dados pessoais podem ser partilhados com entidades do Grupo BNP Paribas, sempre que seja necessário para:

- cumprir as várias obrigações legais e regulamentares acima descritas,
- realizar os nossos interesses legítimos que são gerir, prevenir e detectar fraudes.
- ao dar o seu consentimento permite-nos oferecer-lhe o acesso a todos os produtos e serviços do Grupo BNP Paribas respondendo melhor aos seus desejos e necessidades;

6.2. Com destinatários fora do Grupo BNP Paribas e subcontratantes

A fim de cumprir algumas das finalidades descritas nesta Política de Privacidade, podemos, quando necessário, partilhar os seus dados pessoais com:

- subcontratantes que prestem serviços em nossa representação (por ex., serviços informáticos, logística, serviços de impressão, telecomunicações, cobrança de dívidas, consultoria, distribuição e marketing);
- parceiros bancários e comerciais, agentes independentes, intermediários ou corretores, instituições financeiras, contrapartes, bancos, bancos correspondentes, seguradoras, operadores de sistemas de pagamento, emissores ou intermediários de cartões de pagamentos;
- autoridades financeiras, fiscais, administrativas, criminais e judiciais locais ou estrangeiras, árbitros ou mediadores, autoridades ou instituições públicas (por ex., o Banco de Portugal, Banque de France, Caisse des dépôts et des Consignations), aos quais nós, ou qualquer elemento do Grupo BNP Paribas, sejamos obrigados a divulgar para:
 - atender o seu pedido;
 - exercer a nossa defesa, ação ou processo;
 - cumprir um regulamento ou recomendação emitida por uma autoridade competente que se aplique a nós ou a qualquer membro do Grupo BNP Paribas;
- prestadores de serviços de pagamento de terceiros (informações sobre as suas contas bancárias), com o objetivo de prestar um serviço de iniciação de pagamento ou de informação sobre contas, caso tenha consentido a transferência dos seus dados pessoais a esse terceiro;
- profissionais de certas profissões regulamentadas, como advogados, notários ou auditores, quando necessário em circunstâncias específicas (contencioso, auditoria, etc.), bem como para as nossas seguradoras ou para a um comprador, real ou potencial, das empresas ou negócios do Grupo BNP Paribas.

7. Transferências internacionais de dados pessoais

Os seus dados pessoais podem também ser abrangidos por transferências internacionais com origem no Espaço Económico Europeu (EEE) para um país não pertencente ao EEE. Nas situações em que a Comissão Europeia

reconhece que um país não pertencente ao EEE fornece um nível adequado de proteção de dados pessoais, os seus dados pessoais podem ser transferidos com esse fundamento.

Para transferências para países não pertencentes ao EEE, em que o nível de proteção não foi reconhecido como adequado pela Comissão Europeia, iremos utilizar numa derrogação aplicável à situação específica (por ex., se a transferência for necessária para cumprir o contrato que temos consigo, como quando efetua um pagamento internacional) ou implementar uma das seguintes garantias adequadas para garantir a proteção dos seus dados pessoais:

- cláusulas-tipo de proteção de dados aprovadas pela Comissão Europeia;
- regras vinculativas aplicáveis às empresas.

Para obter uma cópia das garantias adequadas adotadas, ou informações sobre onde estão disponíveis, pode enviar-nos um pedido por escrito para o endereço de contacto constante na secção 10.

8. Por quanto tempo guardamos os seus dados pessoais?

Para mais informações sobre os prazos de conservação, pode consultar o **Anexo II**.

9. Como pode acompanhar a evolução desta política de privacidade?

Num mundo em que as tecnologias estão constantemente a evoluir, iremos rever regularmente esta Política de Privacidade e atualizá-la sempre que necessário. Pode encontrar este Aviso Legal e a sua última versão *online*, no nosso sítio na internet, (www.nickel.eu) na rubrica «Documentos Legais» ou através dos nossos canais de comunicação habituais.

10. Como nos pode contactar?

Se já é nosso cliente, qualquer questão relacionada com o tratamento dos seus dados pessoais ou exercício de direitos pode, de forma autónoma, contactar o Encarregado de Protecção de Dados através dos seguintes contactos: enviando um email para dadospessoais@nickel.eu.

Os seguintes artigos da Área de Cliente explicam como exercitá-los:

Como solicito a exportação dos meus dados pessoais?

Como posso modificar as minhas informações pessoais (sobrenome, nome, endereço de e-mail, telefone, endereço postal)?

Como posso limitar o tratamento dos meus dados pessoais?

Como faço para apagar os meus dados pessoais?

Anexo I - Tratamento de dados pessoais no combate ao branqueamento de capitais e financiamento do terrorismo

Nós fazemos parte de um Grupo bancário que deve adotar e manter um programa robusto de combate ao branqueamento de capitais e ao financiamento do terrorismo (CBC/FT) para todas as sociedades que o integram, gerido a nível central, um programa de combate à corrupção, bem como um mecanismo para garantir a conformidade com Sanções internacionais (i.e., sanções económicas ou comerciais, incluindo as leis, regulamentos, medidas restritivas e embargos associados, e medidas de congelamento de ativos que sejam aprovadas, administradas, impostas ou aplicadas pela República Francesa, a União Europeia, o Gabinete de Controlo de Ativos Estrangeiros do Departamento do Tesouro dos E.U.A., e qualquer autoridade competente nos territórios onde o Grupo BNP Paribas opera).

Neste contexto, atuamos enquanto responsável pelo tratamento de dados em conjunto com o BNP Paribas SA, a sociedade-mãe do Grupo BNP Paribas (portanto, o termo “nós” utilizado neste anexo também abrange o BNP Paribas SA).

De forma a cumprir com as obrigações de CBC/FT e com as Sanções internacionais, nós realizamos as seguintes operações de tratamento de dados, de forma a observar as nossas obrigações legais:

- Um programa “*Conheça o Seu Cliente*” (*Know Your Customer, KYC*) concebido de modo razoável para identificar, verificar e atualizar a identidade dos nossos clientes, incluindo, se for o caso, os seus respetivos beneficiários efetivos e procuradores;
- *Due diligence* reforçada para clientes de alto risco, Pessoas Politicamente Expostas ou “PPE” (PPE são as pessoas definidas pelos regulamentos que, devido às suas funções ou cargo (político, judicial ou administrativo), estejam mais expostas a estes riscos), e para situações de risco acrescido;
- Políticas, procedimentos e controlos escritos, concebidos de modo razoável, para garantir que o Banco não estabelece ou mantém relações com bancos fictícios;
- Uma política, baseada na avaliação interna dos riscos e da situação económica, de geralmente não tratar, nem de outra forma se envolver, independentemente da moeda, em atividades ou negócios:
 - o para, em nome de, ou em benefício de qualquer pessoa singular, coletiva ou organização sujeita a Sanções da República Francesa, da União Europeia, dos Estados Unidos, das Nações Unidas ou, em certos casos, outras sanções locais em territórios onde o Grupo opera;
 - o que envolvam, direta ou indiretamente, territórios sancionados, incluindo a Crimeia/Sevastopol, Cuba, Irão, Coreia do Norte ou Síria;
 - o que envolvam instituições financeiras ou territórios que possam estar relacionados com, ou controlados por organizações terroristas, reconhecidas como tal pelas autoridades competentes de França, da União Europeia, dos E.U.A. e das Nações Unidas.
- Análise da base de dados de clientes e filtragem de transações, concebidas de forma razoável para garantir a conformidade com a legislação aplicável;
- Sistemas e procedimentos concebidos para detetar e denunciar atividade suspeita às autoridades regulatórias competentes;
- Um programa de *compliance* concebido para prevenir e detetar subornos, corrupção e influência ilícita nos termos da Lei Francesa “*Sapin II*”, da FCPA dos E.U.A., e da Lei do Suborno (*Bribery Act*) do Reino Unido.

Neste contexto, nós temos de recorrer:

- o a serviços prestados por prestadores externos que mantêm listas atualizadas de PPE, como a Dow Jones Factiva (disponibilizada pela Dow Jones & Company, Inc.) e o serviço World-Check (disponibilizado pela REFINITIV, REFINITIV US LLC e London Bank of Exchanges);
- o a informações públicas disponíveis na imprensa sobre factos relacionados com branqueamento de capitais, financiamento do terrorismo ou corrupção;
- o à identificação de comportamentos ou situações de risco (existência de uma denúncia de transação suspeita ou equivalente) que possa ocorrer ao nível do Grupo BNP Paribas.

Nós realizamos essas verificações, tanto sobre o próprio cliente como sobre as transações que este realiza, quando o cliente inicia uma relação connosco, mas também ao longo da nossa relação com o cliente. No final da relação, e caso o cliente tenha sido alvo de um alerta, estas informações serão guardadas para o identificar e adaptar os nossos controlos caso o cliente entre numa nova relação com uma entidade do Grupo BNP Paribas, ou no contexto de uma transação na qual seja parte.



Para cumprir as nossas obrigações legais, nós trocamos informações recolhidas para fins de CBC/FT, anticorrupção ou Sanções internacionais entre entidades do Grupo BNP Paribas. Quando os dados do cliente são partilhados com países fora do Espaço Económico Europeu que não proporcionem um nível adequado de proteção, as transferências são reguladas pelas cláusulas contratuais-tipo da Comissão Europeia. Quando são recolhidos e partilhados dados adicionais para cumprir a legislação de países fora da UE, este tratamento é necessário para o nosso interesse legítimo, que é permitir que o Grupo BNP Paribas e as suas sociedades cumpram as suas obrigações legais e evitem sanções locais.

Anexo 2 - Tempo de conservação dos dados pessoais

Retention periods' update: December 2024

FIELD OF ACTIVITY	PROCESSING	RETENTION PERIOD
MARKETING & COMMUNICATION		
	Communicate regulatory information to customers (e.g. GTCs, KYC recertification, etc.) and carry out specific transactional communications related to SEPA regulations	Duration of the contractual relationship
	Communication on fraud prevention	Duration of the contractual relationship
	Global information and other transactional communications	Duration of the contractual relationship
	Collect customer and prospect opinions via surveys and telephone interviews about their Nickel experience	3 years from collection for customers and prospects
	Communicate with customers on overall account management, referral campaigns or existing/new products/services/offers to increase customer sales Communicate with prospects or closed customers to guide them through the (re)subscription process	Duration of the contractual relationship (for customers) 3 years from collection (for prospects)
	Send personalized communications to customers based on their usage or consumption habits in order to promote Nickel offers and services	Duration of the contractual relationship
	Communication on our partners' offers and services	Duration of the contractual relationship 1 year from organization
	Manage contests for customers and prospects	1 month from end of competition
	Monitor and moderate social networks to preserve Nickel's brand image	Duration of the contractual relationship
CUSTOMER SERVICE		

	Processing customer requests from social networks via our ZenDesk ticket management tool	Until 5 years
	Processing of external requests with removal of banking secrecy and seizure of the customer's account	All the individual's identity data and bank details: 5 years from the closing of an account Information relating to operations 5 years from their execution
	Management of special situations and customer account management during the contractual relationship	All the individual's identity data and bank details: 5 years from the closing of an account Information relating to operations 5 years from their execution
	Managing relations with social and legal bodies	All the individual's identity data and bank details: 5 years from the closing of an account Information relating to operations 5 years from their execution
	Processing GDPR requests coming from customers in order to meet their needs or support them in their procedures	Telephone records: 3 months ; Legal period: all the individual's identity data and bank details: 5 years from the closing of an account Information relating to operations 5 years from their execution
	Contacting customers about any KYC inconsistencies identified	Telephone records: 3 months ; Legal period: all the individual's identity data and bank details: 5 years from the closing of an account Information relating to operations 5 years from their execution
	Processing anti-money laundering and terrorist financing alerts	All the individual's identity data and bank details: 5 years from the closing of an account Information relating to operations 5 years from their execution
IT DEPARTMENT		

	Checks, controls and analyses of SEPA flows and accounting disparities to ensure proper execution of transactions and combat fraud	10 years after the date of execution of the operation
	Analysis of customer complaints and customer service requests	10 years after the date of execution of the operation
	Contact with fellow banks to analyze certain requests	10 years after the date of execution of the operation
	Analysis of survey requests received from other banks	10 years after the date of execution of the operation
	Monitoring of accounts and transactions to fight against cyberfraud	Until 5 years
LEGAL		
	Clients' dispute processing by receipting of mails, processing of requests with the support of relevant internal departments, reply by mail to the applicant	Depending on the cases: - 5 years by default - as long as the individual is a Nickel client + legal limitation period in terms of civil liability
	Internal reporting and communication with Group Legal	Until 5 years
ACCOUNTING OBLIGATIONS		
	Analysis of the age of customer accounts receivable to determine provisions or write-offs	10 years from the end of the accounting year
	Access to legal files on customer disputes (FPE) to estimate amounts and prepare accounting documents	10 years from the end of the accounting year
	Collection of required tax data (surname, first name, ID, card, etc.) for all transactions subject to VAT	10 years from the end of the accounting year
	(Except in Portugal and Germany) Regulatory Report	10 years from the end of the accounting year
	(Portugal Only) Tax Reports : Stamp Duty Report (DMIS) / SAFT to PTA / Invoice to the customer	10 years from the end of the accounting year
OTHER OFFERS AND SERVICES		
	Collection of consent to transmit the personal data required to access our RIA partner's offer	Until consent is withdrawn

CUSTOMER DATA MANAGEMENT		
	Data collection, recording, organization, structuring, adaptation, modification, extraction, reconciliation, analysis from internal of partner data sources to make it ready for internal use by the Business Units	Until 10 years
	Deletion or destruction of customer and prospects data based on GDPR requirements	Until 10 years after account closure for customers 3 years for prospects
	Algorithm creation and implementation of machine learning for the purpose of optimizing business lines' and functions' processes	Until 10 years
	Collect data from Nickel's SAAS services to monitor performance and produce follow-up dashboards and reports	Until 10 years
	Storage of cookies data (customers and prospects) based on consent collection to improve functionalities and customer experience. Read the cookies policy for more information: https://nickel.eu/fr/politique-utilisation-des-cookies	Until 13 months
COMPLIANCE		
	Internal alerts processing through detection of an alert via an algorithm, account analysis, investigation, discussion with the client and collection of client's supporting documents	Portugal: 7 years of duty of conserving after client's identification or after the termination of business relationship (Notice BoP 2/2018, articles 17/4 and 40 and article 51 of Law 83/2017) In any event, the records and documents must be destroyed upon expiry of a period of 10 years at the latest.

	External alerts processing by collecting, verifying and targeting client's concerned personal data.	Portugal: 7 years of duty of conserving after client's identification or after the termination of business relationship (Notice BoP 2/2018, articles 17/4 and 40 and article 51 of Law 83/2017)
	BNPP intra-group exchanges by sending of emails / phone exchanges of our clients personal data , of any type, with other banks in the context of investigations / financial security	Portugal: 7 years of duty of conserving after client's identification or after the termination of business relationship (Notice BoP 2/2018, articles 17/4 and 40 and article 51 of Law 83/2017)
	Information transfer with third-parties / institutions in the context of investigations (outside BNPP group)	Portugal: 7 years of duty of conserving after client's identification or after the termination of business relationship (Notice BoP 2/2018, articles 17/4 and 40 and article 51 of Law 83/2017)
	External exchanges by sending of the summary sheet (KYC Flux + supporting documents) along with an investigation report	Portugal: 7 years of duty of conserving after client's identification or after the termination of business relationship (Notice BoP 2/2018, articles 17/4 and 40 and article 51 of Law 83/2017)
	Compliance Permanent Control : review of alerts treatment by Compliance acting	Portugal: 7 years of duty of conserving after client's identification or after the termination of business relationship (Notice BoP 2/2018, articles 17/4 and 40 and article 51 of Law 83/2017)

	Complaints handling by receiving and processing customer complaints in order to provide an appropriate response within a reasonable timeframe	Portugal: 7 years of duty of conserving after client's identification or after the termination of business relationship (Notice BoP 2/2018, articles 17/4 and 40 and article 51 of Law 83/2017)
	Use of the Call for vigilance lists in screening algos and conservation of the list 6 months after the end of the vigilance call	Portugal: 7 years of duty of conserving after client's identification or after the termination of business relationship (Notice BoP 2/2018, articles 17/4 and 40 and article 51 of Law 83/2017)
	Transmission of fraudsters' data (description of the data management)	Portugal: 7 years of duty of conserving after client's identification or after the termination of business relationship (Notice BoP 2/2018, articles 17/4 and 40 and article 51 of Law 83/2017)
FRAUD AND REGULATORY		
	Fraud management: internal and external investigations and monitoring by collection and cross-checking of the data about suffered fraud or committed fraud of our customers	Until 5 years
	Regulatory projects : by collecting and cross checking the data in order to steer regulatory projects	Until 10 years
	Regulatory reporting to local regulation authorities (OTESI, ATRUVIA...)	10 to 30 years (depend on the applicable local regulation)
PAYMENT ACTIVITY		
	Wallet Enrolment for Apple	Until 7 years
	Wallet Enrolment for Google	Until 7 years
	Wallet Enrolment for Mastercard for Merchants, Click to Pay	Until 7 years

	Regular checking of wallet eligibility and display of information for all wallets	Duration of the contractual relationship
	Card Management (ordering, offer, lifecycle, PIN...)	Until 10 years (except card lifecycle: 7 years)
	Management of the card insurance	Until 10 years
	Card Payment Management	Until 10 years
	SEPA Management (Direct Debit Management, Credit Transfer Management, Instant Transfer Management)	Until 10 years
	Top Up Management : process to credit the Nickel account using another bank credit card	Until 10 years
	Rewards Management by rewarding clients/tobacconist that did great results by boosting their commission rates or giving them one time bonuses	Until 10 years
	Internal process to perform payment, withdrawal and deposit using the Nickel POS	Until 10 years
	Having fraud rules implemented on the payment system based on risk analysis to refuse transaction	Until 10 years
	Bank Account Management through account creation for customer, manage the accounting flow, manage the lifecycle of an account	Until 10 years
	Payment Limit Management : defines the payment limits per customer, the pricing and fees	Until 10 years
	Pricing & Fees Management by defining the pricing for each products and services and through planification, fee taking, cancellation, refund	Until 10 years
	Tax Management by managing the applicable taxes specific to Portuguese regulatory	Until 10 years
CUSTOMER EXPERIENCE		
	Customer authentication for validation of sensitive transactions	Until 10 years
	Operations management by displaying user interface operations	Until 5 years
	KYC management by displaying KYC on user interfaces and processing KYC	Until 10 years
	Displaying card data on user interfaces	Until 10 years (except card lifecycle: 7 years)

	Executing transactions on user interfaces	Until 5 years
	Communication management for customers	Duration of the contractual relationship
	Handling any type of customer request	Until 5 years except for telephone records: 3 months
CUSTOMER ACQUISITION		
	Acquisition of new customers through a full online process	Duration of the contractual relationship
	Management of customer acquisition through the use of advertising platforms	3 years from collection
	Management of customer acquisition through the use of affiliation platform	3 years from collection
	Sending hashed email to Google Ads to improve conversions and enrich algorithms (enhanced conversion)	20 days
	Management of customer acquisition and budget allocation through the use of advertising platforms Retargeting of Nickel website visitors to send personalised communication to prospects (current test)	3 to 6 months for cookie storage
	Enhancement of the current acquisition framework by testing the solution of several external providers	Until the end of the test
	Biometric consistency check at the time the relationship is established by analysing and comparing identity documents	Duration of the contractual relationship