Condições Gerais Serviços de Meios de Comunicação à Distância

Clientes Particulares

1. Âmbito

1. As presentes Condições Gerais destinam-se a regular os termos e as condições de utilização dos meios de comunicação à distância.

2. Para efeitos do disposto no presente contrato, consideram-se meios de comunicação à distância entre o Banco e o Cliente, os seguintes canais de comunicação remota:

a) Canal Telefonia Vocal, mais adiante designado por Centro de Contactos quando envolva um serviço de call center – meio de comunicação por telefone estabelecido por iniciativa do Banco ou do Cliente, incluindo os contactos telefónicos estabelecidos através do Centro de Contactos (comunicações associadas aos números telefónicos 707502424 / 918272424 / 935222424 / 965992424 (chamada nacional) e +351707502424 / +351210052424 (chamada internacional) ou outros números que os venham a substituir e divulgados pelo Banco);

b) Canal Internet – meio de acesso do Cliente ao Banco através do sítio de Internet www.millenniumbcp.pt;

c) Canal Mobile - meio de acesso do Cliente ao Banco através de, App Millennium, App MTrader, Apple watch e outras extensões das Apps;

d) Millennium Teller Machine, adiante designada por MTM - meio de acesso do Cliente ao Banco através de máquina selfbanking (caixa automático) em que o Cliente pode efetuar consultas e realizar operações bancárias de tesouraria e adesão a produtos e serviços financeiros de forma autónoma ou assistida (presencial ou remota, sendo esta última realizada com Código de Autenticação).2.2. Os meios de comunicação à distância são canais de comunicação remota de acesso do Cliente aos serviços que em cada momento o Banco tenha disponíveis para oferecer nesses canais, para a outorga de atos ou negócios jurídicos no âmbito da relação bancária estabelecida com o Banco, na sua qualidade de instituição de crédito e de agente de seguros, permitindo o acesso à conta de depósitos à ordem para consulta, obtenção de informações e realização de operações, bem como a divulgação e comercialização pelo Banco, e contratação à distância, de produtos e serviços financeiros, incluindo os relativos a serviços de pagamento, valores mobiliários e seguros.

3. Os meios de comunicação à distância são canais de comunicação remota de acesso do Cliente aos serviços que em cada momento o Banco tenha disponíveis para oferecer nesses canais, para a outorga de atos ou negócios jurídicos no âmbito da relação bancária estabelecida com o Banco, na sua qualidade de instituição de crédito e de agente de seguros, permitindo o acesso à conta de depósitos à ordem para consulta, obtenção de informações e realização de operações, bem como a divulgação e comercialização pelo Banco, e contratação à distância, de produtos e serviços financeiros, incluindo os relativos a serviços de pagamento, valores mobiliários e seguros.

4. Para efeitos do disposto no número anterior, consideram-se atos ou negócios jurídicos outorgados no âmbito da relação bancária, todos os que respeitam aos processos de abertura, manutenção e encerramento de contas de depósitos à ordem, de serviços de pagamento, de crédito ou de registo ou depósito de instrumentos financeiros, à movimentação das referidas contas e aos processos de celebração e de execução de contratos de seguros do ramo Vida e Não Vida e a gestão de sinistros, incluindo, designadamente, a realização de operações sobre seguros, a emissão de procurações, a emissão de declarações relativas a dados pessoais, a apresentação de reclamações ou pedidos diversos, a apresentação de pedidos de declarações, de pedidos de informação, de pedidos de segundas vias de extratos ou de outros documentos, a passagem de recibos, a subscrição de contratos de utilização de instrumentos de pagamento, incluindo instrumentos de pagamento para transações seguras em comércio eletrónico e desmaterializadas baseados em cartão, a pedidos de códigos de acesso ou de utilização de serviços de Internet ou de instrumentos de pagamento, a celebração de contratos de acquiring e requisição de TPA's, a contratação de débitos diretos, a contratação de serviços de envio de fundos, a emissão e revogação de ordens de pagamento, incluindo de ordens permanentes ou periódicas, a emissão de ordens de aquisição, venda ou resgate sobre instrumentos financeiros, ainda que em Bolsa, a subscrição ou resgate de produtos de investimento de retalho e de produtos de investimento com base em seguros, a requisição de cheques, a compra e venda de moeda, a constituição, reforço ou liquidação de depósitos a prazo, a contratação e resolução de alugueres de cofres, a contratação ou gestão de operações de crédito, leasing, a emissão de garantias.

5. No âmbito das comunicações à distância, o Cliente aceita ser abordado por iniciativa do Banco. No caso do Canal Telefonia Vocal, os contactos serão realizados para os números de telefone indicados pelo Cliente.

6. Para efeitos do ponto anterior, o Cliente expressamente consente e solicita ao Banco que, através dos referidos canais de comunicação remota e, bem assim, do correio eletrónico, proceda à divulgação, preste informações e lhe apresente propostas concretas de celebração ou de alteração de contratos, subscrição de produtos e serviços e de execução de operações à distância de produtos e serviços financeiros, incluindo serviços bancários, de pagamentos, de crédito, de intermediação ou investimento em instrumentos financeiros, de adesão individual a fundos de pensões abertos, de seguros, mesmo que tais propostas impliquem um pedido de pagamento.

BANCO COMERCIAL PORTUGUÊS, S.A., Sociedade Aberta, com sede na Praça D. João I, n.º 28, Porto, o capital social de [UGD Custom], matriculada na Conservatória do Registo Comercial do Porto sob o número único de matrícula e de identificação fiscal 501 525 882

Mod. 10903229

7. O Cliente pode agregar ao serviço prestado através dos meios de comunicação à distância outras contas de depósitos à ordem de que seja titular no Banco (contas agregadas), mas no caso de conta coletiva de movimentação conjunta ou mista sem poderes de movimentação autónoma, aplica-se especialmente o disposto no número seguinte desta clausula e na clausula 8distª n.º 7, infra.

8. Sem prejuízo de outras medidas de restrição de acesso que o Banco pode estabelecer, no caso de a conta de depósitos à ordem ou outra conta agregada ser uma conta coletiva de movimentação conjunta ou mista sem poderes de movimentação autónoma por parte do Cliente, (i) o acesso aos canais Internet, Mobile e MTM fica limitado ao modo consulta e obtenção de informações, sem acesso à realização de operações, (ii) a utilização do canal Centro de Contactos para a realização de operações implica um procedimento de confirmação, nos termos do previsto infra na Cláusula 8ª n.º 7.

9. Pelos meios de comunicação à distância o Cliente pode solicitar a aquisição de produtos e serviços com terceiras entidades, nos termos do acordo celebrado entre estas e o Banco.

10. A prestação de serviços através de meios de comunicação à distância rege-se também, em tudo o que não se encontra aqui especificamente previsto, pelo disposto nas cláusulas do Capítulo A- Condições Gerais de Contas de Depósitos à Ordem e do Capitulo B-Condições Gerais de Prestação de Serviços de Pagamento das Condições Gerais de Conta – Pessoas Singulares, que aqui se dão por reproduzidas para todos os efeitos.

11. Todos os contratos celebrados através de meios de comunicação à distância ficam subordinados às presentes Condições Gerais e às condições gerais e particulares aplicáveis à contratação de cada produto ou serviço concretamente disponibilizado, assim como ao tarifário em vigor no preçário do Banco, legislação aplicável e usos bancários em geral.

2. Riscos associados aos meios de comunicação à distância

1. Os meios de comunicação à distância para acesso do Cliente ao Banco estão sujeitos a riscos de fraude, nomeadamente de "phishing", bem como, de consulta e realização de operações fraudulentas por terceiros não autorizados na conta do Cliente.

2. O phishing é uma fraude que consiste em substituir a identidade do Banco ou de qualquer outra entidade fidedigna, cuja finalidade é a obtenção de informações confidenciais do Cliente, nomeadamente dados bancários, dados pessoais ou códigos de acesso. Os ataques de "phishing" podem produzir-se através de mensagens de correio eletrónico, SMS ou chamadas telefónicas nas quais se pode imitar e substituir a identidade do Banco ou de qualquer outra entidade fidedigna. Essas mensagens de correio eletrónico ou SMS podem conter um ficheiro anexo que efetua a instalação de software malicioso (malware) no equipamento do Cliente ou reencaminhar para uma página web fraudulenta, que reproduz ou copia o aspeto da página original do Banco, e na qual é solicitado ao Cliente a introdução de dados pessoais e/ou códigos e credenciais de acesso, como por exemplo, o seu Código de Utilizador, algumas ou todas as posições do seu Código Multicanal, o Código de Autenticação, o seu número de telemóvel ou os números dos seus cartões bancários;

3. O Cliente deve estar atento, ser precavido e ter em conta que tanto a mensagem de correio eletrónico ou SMS, como a página web fraudulenta, podem ser muito complexas e sofisticadas. O Cliente tem de desconfiar e suspeitar, nomeadamente:

a) do tom de urgência de mensagens que o ameacem com a suspensão do acesso à conta, dos códigos de acesso ou do cartão se não fornecer os seus dados imediatamente;

b) do pedido de confirmação dos seus dados pessoais via correio eletrónico ou SMS, designadamente remetendo-o para o preenchimento on-line de formulários de informações pessoais e códigos de acesso;

c) de erros ortográficos/gramaticais e outros erros patentes na mensagem ou na página web fraudulenta, ou outros elementos que sugiram a origem diversa ou suspeita dos mesmos;

d) de mensagens de correio eletrónico ou SMS com links ou ficheiros em anexo;

e) da indicação de que, para simular operações, deve fornecer Código(s) de Autorização que o Banco lhe enviou por SMS ou gerados via Token;

4. O Cliente obriga-se a ler atentamente e dar cumprimento escrupuloso às recomendações e regras de segurança constantes do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra e faz parte integrante do presente Contrato, bem como, a ir consultar e ler, pelo menos uma vez em cada trimestre do ano civil, os avisos de segurança e os alertas periódicos que o Banco divulga no sítio de Internet www.millenniumbcp.pt, incluindo a descrição das fraudes praticadas em cada momento para a captura fraudulenta dos Código de Utilizador, Código Multicanal e demais credenciais personalizadas de acesso dos Clientes.

5. O Banco é responsável por assegurar a fiabilidade da sua página de Internet e serviços de Mobile Banking e MTM, bem como a segurança dos seus servidores e componentes informáticos.

6. O Cliente é responsável pela segurança e fiabilidade do equipamento informático e de comunicação utilizado para acesso ao Banco através dos meios de comunicação à distância, nomeadamente dos computadores, tablets, telemóveis, números de telemóvel, e ligações à Internet de sua propriedade ou sob sua alçada, nos termos do disposto nos números seguintes e nas recomendações e regras de segurança constantes do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra.

7. O Cliente deverá dispor de equipamento informático e de comunicação com as características adequadas para poder aceder ao Banco através dos meios de comunicação à distância, sendo da sua responsabilidade a segurança, manutenção e introdução das modificações eventualmente necessárias para assegurar em permanência o acesso, por essa via, ao Banco, de acordo com as inovações e alterações tecnológicas que vierem a ser introduzidas e o cumprimento rigoroso das regras e recomendações de segurança constantes do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra, e, bem assim, dos alertas divulgados pelo Banco, em cada momento, no sítio de Internet www.millenniumbcp.pt.

8. As características mínimas, de equipamento e comunicações, em cada momento necessárias para a utilização de cada meio de comunicação à distância, encontram-se descritas no sítio de Internet www.millenniumbcp.pt, nos espaços informativos de cada canal, que o Cliente se obriga a ir consultar periodicamente, e a observar escrupulosamente.

3. Open Banking

Fica expressamente convencionado e aceite que, em conformidade com o disposto na Diretiva (UE) 2015/2366 de 25.03.2015 e nas disposições legais que a regulamentam e transpõem, o Banco, na sua qualidade de prestador de serviços de pagamento que gere a Conta de depósitos á ordem supra identificada está obrigado a disponibilizar o acesso à referida conta a terceiras partes (third parties payment services providers), sem que tenha que existir qualquer relação contratual entre estas e o Banco e desde que o Cliente ofereça o seu consentimento, para efeitos da prestação de serviços de agregação de contas, iniciação de pagamentos e confirmação de saldos, melhor descritos infra no ANEXO 2 – OPEN BANKING.

4. Códigos para Autenticação do Cliente

1. Ao Cliente que expressamente o solicite ao Banco pela página web no sítio de Internet www.millenniumbcp.pt, pelo canal Mobile, numa agência ou numa Caixa Automática da Marca Multibanco, poderá ser atribuído um Código Multicanal para acesso aos canais Centro de Contactos, Internet, Mobile e MTM.

2. O acesso aos canais Internet, Mobile e MTM requer que o Banco atribua, adicionalmente um Código de Utilizador, que o Cliente deverá alterar no primeiro acesso ao sítio de Internet www.millenniumbcp.pt.

3. Será ainda atribuído ao Cliente um código designado Chave de Confirmação para validação de operações no canal telefonia vocal ou centro de contactos.

4. O acesso através de Apple Watch à conta de depósitos à ordem e a outras contas agregadas está sujeito adicionalmente a processos de identificação e de reconhecimento definidos em cláusulas contratuais próprias.

5. O acesso ao canal MTM poderá ser efetuado alternativamente com um cartão bancário personalizado e introdução correta do respetivo PIN.

6. O Banco nunca solicita a introdução do Código Multicanal nem da Chave de Confirmação na totalidade.

7. Para a outorga de determinados atos ou negócios jurídicos nos meios de comunicação à distância, nomeadamente para a realização de operações de pagamento acima de certo montante realizadas por débito na conta de depósitos à ordem ou numa conta agregada ao serviço, pode ser exigível uma confirmação adicional através (i) de um sistema de Autenticação Forte do Cliente (AFC) – prévia confirmação da operação com um dado biométrico ou um código de utilização única gerado por Token ou enviado por SMS para o número de telemóvel do Cliente no momento da realização da mesma, ou (ii) da confirmação da operação com algumas posições aleatórias do Código Multicanal ou da Chave de Confirmação do Cliente,.

8. O Cliente, através dos serviços disponíveis, poderá, em cada momento, definir e gerir as operações de pagamento que designadamente possam acarretar diminuição do património, e/ou em função dos beneficiários envolvidos, não carecerão da utilização da AFC ou de uma Chave de Confirmação para a sua realização.

9. O Banco poderá, em cada momento, definir um conjunto de condições – designadamente relativas a beneficiários, montantes e/ou operações – cuja verificação poderá dispensar a utilização da AFC ou de uma Chave de Confirmação adicional para a execução das mesmas.

10. No sítio de Internet www.millenniumbcp.pt o Cliente pode alterar a qualquer momento o Código de Utilizador, bem como, o Código Multicanal. A Chave de Confirmação pode ser alterada no canal Centro de Contactos (apenas em atendimento automático – Voice Response System). O Código Multicanal pode também ser alterado através do canal Centro de Contactos (apenas em atendimento automático – Voice Response System) e do canal Mobile (área de segurança).

11. Para realização de algumas transações ou para alteração de dados pessoais poderão ser solicitadas informações adicionais de segurança (pessoais ou de relação com o Banco) através de um contacto telefónico personalizado do serviço Centro de Contactos.

5. Chave Móvel Digital

1. Nos Canais Internet e Mobile, exclusivamente para acesso e autenticação nos mesmos, o Cliente pode optar, em alternativa à utilização dos códigos previstos na cláusula anterior, à utilização do serviço de autenticação Chave Móvel Digital disponibilizado pelo Estado Português e subcontratado pelo Banco.

2. A Chave Móvel Digital é um meio de acesso e autenticação que permite a associação de um número de telemóvel ao número de identificação civil para um cidadão português ou o número de passaporte para um cidadão estrangeiro residente em Portugal. A Chave Móvel Digital permite ao utilizador autenticar-se através de:

a) Número de telemóvel;

b) PIN – Número de Identificação Pessoal intransmissível criado no registo da Chave Móvel Digital;

c) Código de segurança numérico único e temporário de 6 dígitos enviado por SMS para o número de telemóvel do Cliente ou obtido via App "Autenticação Gov".

3. Ao optar por algum destes métodos o Cliente tem a responsabilidade pela utilização segura do PIN bem como do telemóvel associados ao seu registo.

4. O acesso aos canais Internet e Mobile do Banco através de autenticação com Chave Móvel Digital carece de prévia adesão do Cliente no site de Internet autenticacao.gov.pt ou presencialmente nos Espaços Cidadão.

5. Ao escolher esta forma de autenticação o Cliente é redirecionado de forma segura para o serviço de Autenticação do Estado onde é informado da comunicação dos dados pessoais solicitados pelo Banco e concorda explicitamente com essa transmissão.

6. Fica expressamente convencionado que a autenticação do utilizador através da Chave Móvel Digital confere ao Banco legitimidade para conceder o acesso e a utilização do canal Internet ou Mobile escolhido e à(s) conta(s) de depósitos à ordem do Cliente.

6. Convenção sobre prova

1. O acesso e a utilização, pelo Cliente, dos Meios de Comunicação à Distância do Banco, designadamente para realização de operações de pagamento, transmissão de ordens e instruções, está sujeita à correta utilização, em conformidade ao prescrito nas presentes clausulas e no respetivo Anexo I – Riscos e Regras de Segurança, que aqui consta infra:

a) O Código de Utilizador, o Código Multicanal, a Chave de Confirmação e/ou cada código de utilização única que o Banco envie para o número de telemóvel do Cliente indicado ao Banco para a realização de operações à distância, ou gerado por Token; e

b) O telemóvel ou dispositivo móvel do Cliente com o número de telemóvel previamente fornecido ao Banco para realização de operações à distância e/ou no qual haja instalado uma App do Millennium bcp, ou a App MB Way associada a cartão de pagamento emitido pelo Banco; e

c) O endereço de correio eletrónico do Cliente indicado ao Banco para efeitos de troca de comunicações à distância e/ou para efeitos de autenticação perante o Banco.

2. Todos os Códigos e os demais elementos e dispositivos do Cliente indicados nas alíneas do número precedente, constituem credenciais de segurança personalizadas que permitem ao Banco verificar a identidade do Cliente, autenticar o respetivo acesso e uso de cada canal à distância, e estabelecer a autoria das ordens aí transmitidas, consubstanciando uma assinatura eletrónica objeto de um direito individual e exclusivo do Cliente, cuja utilização identifica e autentica o Cliente perante o Banco e lhe atribui a autoria das instruções e documentos eletrónicos assim transmitidos.

3. As partes aceitam a equiparação jurídica das sobreditas credenciais de segurança personalizadas do Cliente, bem como da Chave Móvel Digital, às assinaturas manuscritas do Cliente.

4. O Banco assumirá legitimamente qualquer acesso, pedido de informação, transmissão de ordens ou instruções, subscrição de contrato ou outorga de quaisquer atos ou negócios jurídicos mediante a utilização das sobreditas credenciais de segurança personalizadas , bem como da Chave Móvel Digital, nos termos ora convencionados, como sendo da autoria do Cliente, não lhe sendo exigível verificar a identidade do utilizador por qualquer outra via.

5. O referido no número anterior não pode ser interpretado como inibindo o Banco de obter a confirmação junto do Cliente das ordens ou instruções recebidas, incluindo uma confirmação por escrito, com assinatura autógrafa, nem prejudica a adoção de outra forma de contratualização das operações bancárias a pedido do Banco ou em resultado de disposição legal, ou limitar a aceitação de determinado tipo de instruções em função de montantes, número de ordens ou outro critério.

6. As ordens e instruções que o Banco recebe, bem como os atos de subscrição de contratos, ou outorga de quaisquer atos ou negócios jurídicos, desde que corretamente validados mediante a utilização das sobreditas credenciais de segurança personalizadas ou da Chave Móvel Digital, gozam de plenos efeitos jurídicos, ficando o Banco irrevogavelmente legitimado para cumpri-las ou executa-los e efetuar os débitos e créditos que deles decorram, entendendo-se, em qualquer caso, que o Banco atua em cumprimento das ordens e instruções recebidas e da vontade real do Cliente.

7. Fica expressamente pactuado entre o Cliente e o Banco que, nos termos e para os efeitos do n.º 4 do art. 3º do Decreto-Lei nº 290-D/99, de 2 de agosto, a utilização das sobreditas credenciais de segurança personalizadas do Cliente, incluindo de cada um dos Códigos de Autenticação atribuídos ao Cliente, o telemóvel ou dispositivo móvel do Cliente com o número de telemóvel previamente indicado ao Banco para a realização de operações à distância, bem como da Chave Móvel Digital, nos termos ora estabelecidos, terão o mesmo valor jurídico e probatório da assinatura manuscrita do Cliente em papel.

8. O disposto nos números 4 e 5 e na presente cláusula aplica-se também à contratação de produtos e serviços com terceiras entidades, prevista na cláusula 1ª n.º 9, agindo o Banco, no âmbito desta disposição, em nome e em representação daquelas entidades.

7. Obrigações do Cliente relativas às suas credenciais de segurança personalizadas, número de telemóvel e endereço de correio eletrónico

1. O Cliente obriga-se a tomar todas as medidas de cuidado e de diligência razoáveis para preservar a segurança e a confidencialidade dos seus códigos e credenciais de segurança personalizadas indicados nos números 1 e 2 da cláusula 6ª (Convenção sobre prova) anterior , para efeitos de autenticação perante o Banco, e a não permitir nem facilitar o seu conhecimento nem a sua utilização por terceiros, ainda que seus mandatários, obrigando-se a manter sempre a respetiva confidencialidade, e a fazer uma utilização atenta, cuidadosa, reservada e exclusivamente pessoal dos mesmos.

2. O Cliente é responsável pela confidencialidade, guarda, utilização e manutenção corretas do Código de Utilizador, Código Multicanal, a Chave de Confirmação, bem como, dos demais elementos e credenciais de segurança personalizados referidos nos números 1 e 2 da cláusula 6ª (Convenção sobre prova) anterior.

3. Designadamente, o Cliente obriga-se a adotar todas as precauções adequadas para não tornar acessíveis ou percetíveis a terceiros o Código de Utilizador, Código Multicanal, a Chave de Confirmação os quais deverá memorizar destruindo o respetivo suporte de informação do(s) mesmo(s). Caso o Cliente pretenda guardar o(s) referido(s) códigos, nunca os deve deixar em lugar visível, acessível e/ou percetível a terceiros, e especialmente não os deve anotar em suporte facilmente acessível a outrem, nem no próprio telemóvel, dispositivo móvel ou computador, nem em qualquer outro documento ou suporte que tenha ou junto dos mesmos.

4. O Cliente deve estar atento, ser precavido e ter em conta que existe o risco de receber mensagens de correio eletrónico enganadoras, SMS ou até chamadas telefónicas nas quais se imita e substitui a identidade do Banco, a fim de, ardilosa e fraudulentamente obter do Cliente os seus dados, códigos pessoais e credenciais de acesso, como por exemplo, o seu Código de Utilizador, (todas) as posições do seu Código Multicanal, o seu número de telemóvel, os números do seu (s) cartões bancários e/ou de Crédito. Designadamente, o tom de urgência de mensagens que o ameacem, por exemplo, com a suspensão do acesso à conta ou do cartão se não fornece os seus dados imediatamente, ou o pedido de confirmação dos seus dados pessoais via correio eletrónico ou SMS, designadamente remetendo para o preenchimento on-line de formulários de informações pessoais,

solicitando o fornecimento de códigos e credenciais de acesso, ou e-mails ou SMS com links ou ficheiros para descarregar e instalar têm de fazer o Cliente suspeitar e desconfiar.

5. O Cliente obriga-se a ler atentamente e dar cumprimento escrupuloso às recomendações e regras de segurança constantes do ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA, que aqui consta infra e faz parte integrante do presente Contrato, bem como a ir consultar e ler, pelo menos uma vez em cada trimestre do ano civil, os avisos de segurança e os alertas periódicos que o Banco divulga no sítio de Internet www.millenniumbcp.pt, incluindo a descrição de concreto(s) procedimento(s) utilizados em cada momento para a captura fraudulenta dos Código de Utilizador, Código Multicanal e demais credenciais personalizadas de acesso, dos Clientes.

6. O Cliente não deve nunca, em circunstância nenhuma, introduzir todas as posições do seu Código Multicanal num mesmo momento ou para o mesmo ato. O Banco nunca solicita todas as posições do Código Multicanal.

7. O Cliente obriga-se ainda a tomar todas as medidas de cuidado e de diligência razoáveis para acautelar e preservar:

a) A posse, a segurança e a utilização exclusiva, reservada e confidencial em cada momento do seu telemóvel ou dispositivo móvel com o número de telemóvel previamente fornecido ao Banco para realização de operações à distância, e/ou no qual tenha instalado uma App do Millennium bcp ou a App MB Way associada a cartão de pagamento emitido pelo Banco;

b) A utilização exclusiva, reservada e confidencial em cada momento do endereço de correio eletrónico do Cliente indicado ao Banco para troca de comunicações à distância e/ou para efeitos de autenticação perante o Banco.

8. Se em algum momento, o Cliente:

a) Suspeitar que terceiros têm conhecimento, no todo ou em parte, do seu Código de Utilizador, e/ou Código Multicanal ou da Chave de Confirmação, ou em caso de extravio, furto ou roubo ou apropriação abusiva dos mesmos ou de algum deles, e/ou

b) Verificar o registo na conta de qualquer transação não consentida ou a existência de erros ou irregularidades na efetivação das operações, e/ou

c) Receber um Código de Autenticação para simulação de transação, e/ou

d) Receber um Código de Autenticação para confirmação de uma operação que o Cliente não tenha solicitado, e/ou

e) Suspeitar de acesso indevido de terceiro(s) ao seu endereço de correio eletrónico e/ou ao seu telemóvel, computador, ou dispositivo móvel, ou ao seu número de telemóvel, por qualquer forma,

Então deverá suspender o procedimento e, sem atraso injustificado , entrar de imediato em contacto com o Banco, por via telefónica para o telefone 707502424 / 918272424 / 935222424 / 965992424 (chamada nacional) ou +351707502424 / +351210052424 (chamada internacional), que é um serviço de atendimento permanente – 24 horas/dia, 365 dias/ano, a fim de dar o alerta e solicitar o respetivo bloqueio/impedimento de uso abusivo ou fraudulento perante o Millennium bcp. O Cliente deverá ainda confirmar ao Banco o sucedido, por escrito, num prazo não superior a 5 dias.

9. Todos os casos previstos nas alíneas a) a d) do número precedente deverão ser prontamente participados às autoridades policiais competentes, devendo o Cliente apresentar ao Banco a respetiva comprovação documental, com a cópia de teor da participação realizada.

10. No âmbito das comunicações telefónicas referidas no número 8 precedente desta cláusula, não é aplicável a utilização do Código de Utilizador nem do Código Multicanal; neste caso, o Cliente declara e aceita que o Banco o considere identificado e reconhecido logo que indique cumulativa e corretamente a resposta às questões colocadas pelo Banco sobre elementos do património financeiro do Cliente, das contas de depósitos da sua titularidade, ou outros factos que sejam de conhecimento do Banco em virtude da respetiva relação de clientela ou outras que tenham sido previamente combinadas entre as partes para o efeito; neste caso, o Banco não solicitará por telefone, SMS ou correio eletrónico, informações acerca dos Códigos de Utilizador e de Autenticação, nem da Chave de Confirmação do Cliente, nem os números do(s) seu(s) Cartões de Crédito, ou do seu telemóvel.

11. Após a comunicação do Cliente referida nos números precedentes desta cláusula, o Banco bloqueará o acesso às contas do Cliente através dos canais Centro de Contactos, Internet, Mobile e MTM.

12.1. Após ter procedido, sem atraso injustificado à notificação a que se refere o precedente numero 8, o Cliente não suporta quaisquer perdas relativas a operações de pagamento não autorizadas resultantes de quebra de confidencialidade dos seus códigos e credenciais de segurança personalizadas indicados nos números 1 e 2 da cláusula 6ª (Convenção sobre prova),

designadamente em caso de extravio, furto ou roubo ou apropriação abusiva dos mesmos ou de algum deles, salvo aquelas forem devidas a atuação fraudulenta do Cliente.

12.2. O Cliente suporta as perdas relativas a operações de pagamento não autorizadas, resultantes de quebra de confidencialidade dos códigos e credenciais de segurança personalizadas do Cliente indicados nos números 1 e 2 da cláusula 6ª (Convenção sobre prova), designadamente em caso de extravio, furto ou roubo ou apropriação abusiva dos mesmos ou de algum deles, que sejam realizadas antes da notificação a que se refere o precedente numero 8, de acordo com as seguintes regras:

a) O Cliente suporta todas as perdas resultantes de operações de pagamento não autorizadas se aquelas forem devidas a atuação fraudulenta ou ao incumprimento deliberado de uma ou mais das obrigações do Cliente previstas no presente Contrato, designadamente na presente clausula, e no Anexo I – Riscos e Regras de Segurança que aqui consta infra, e se em caso de suspeita de fraude o Banco comunicar por escrito esses motivos às autoridades judiciárias.

b) Havendo negligência grosseira do Cliente, este suporta as perdas resultantes de operações de pagamento não autorizadas até ao limite do saldo disponível ou da linha de crédito associada à conta, ainda que superiores a 50€.

c) Nos restantes casos, o Cliente suporta as perdas relativas às operações não autorizadas, no âmbito do saldo disponível ou da linha de crédito associada à conta, até ao limite máximo de 50€; esta responsabilidade do Cliente não se aplica se:

(i) A perda, extravio, roubo, furto, acesso indevido ou outra forma de apropriação abusiva dos códigos e credenciais de segurança personalizadas do Cliente indicados nos números 1 e 2 da cláusula 6ª (Convenção sobre prova), não pudesse ser detetada pelo Cliente antes da realização de um pagamento, exceto se o Cliente tiver atuado fraudulentamente; ou

(ii) A perda tiver sido causada por atos ou omissões de um trabalhador, de um agente ou de uma sucursal do prestador de serviços de pagamento, ou de uma entidade à qual as suas atividades tenham sido externalizadas.

12.3 Se a operação de pagamento tiver sido iniciada através de um prestador do serviço de iniciação do pagamento, recai sobre este último o ónus de provar que, no âmbito da sua esfera de competências, a operação de pagamento foi autenticada e devidamente registada, e não foi afetada por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento por si prestado.

12.4. Concluídas as diligências de prova previstas nos números anteriores, se se concluir que o Banco ou um prestador de serviços de iniciação de pagamento é responsável pelas perdas de operações não autorizadas, o Banco assegurará o reembolso imediatamente e, em todo o caso, o mais tardar até ao final do primeiro dia útil seguinte do montante da operação de pagamento não autorizada e, se for caso disso, reporá a conta do Cliente na situação em que estaria se a operação de pagamento não autorizada não tivesse sido executada, com data-valor não posterior à data em que o montante foi debitado.

8. Tratamento das instruções do Cliente

1. Sem prejuízo do disposto quanto a menores no número 1 da cláusula décima primeira infra, o Cliente pode dar instruções ao Banco através dos meios de comunicação à distância a qualquer hora do dia, todos os dias do ano, e presencialmente no âmbito dos horários de funcionamento das Agências do Banco.

2. A execução das ordens transmitidas pelo Cliente será efetuada de acordo com as condições aplicáveis ao tipo de canal remoto em causa, serviço ou produto solicitado.

3. O Banco poderá abster-se de executar ordens transmitidas pelo Cliente, quando estas não respeitarem as disposições legais aplicáveis ou colidirem com os usos bancários, quando a conta a movimentar não se encontre provisionada para a operação pretendida, ou ainda quando não for cumprida qualquer disposição constante do presente Contrato e das cláusulas do Capítulo A- Condições Gerais de Contas de Depósitos à Ordem e do Capitulo B-Condições Gerais de Prestação de Serviços de Pagamento das Condições Gerais de Conta – Pessoas Singulares, designadamente em virtude de alguma irregularidade no processo de transmissão e/ou autorização da ordem em causa que não seja devidamente sanada no prazo de 72 horas.

4. Uma vez autorizadas e enviadas ao Banco para processamento imediato não é possível efetuar alterações, nem cancelar as ordens transmitidas através dos meios de comunicação à distância, sem prejuízo do disposto no Capítulo B-Condições Gerais de Prestação de Serviços de Pagamento das Condições Gerais de Conta – Pessoas Singulares.

5. Considerando que os serviços ou operações disponibilizados pelo Banco através dos meios de comunicação à distância estão sujeitos a interferências, interrupções, desconexões ou outras anomalias, designadamente em consequência de avarias, sobrecargas, cargas de linha, faltas de energia, o Cliente reconhece expressamente que o Banco não será responsável pelos danos, potenciais ou atuais, incluindo lucros cessantes, que, direta ou indiretamente, possam resultar para o Cliente por força da ocorrência de tais eventos, na medida em que as referidas interferências, interrupções, desconexões ou anomalias tenham

origem em atos ou omissões de terceiros, nestes incluindo as entidades fornecedoras ou licenciadoras de serviços ao Banco, e em serviços cuja detenção e controlo lhes pertença.

6. A função "Banco Mail" do canal Internet não obriga o Banco à execução de ordens, salvo acordo expresso para o efeito.

7. Apenas para o canal Centro de Contactos, e no caso de contas coletivas de movimentação conjunta ou mistas sem poderes de movimentação autónoma por parte do Cliente, a execução de qualquer operação depende da prévia receção pelo Banco da confirmação, através de documento escrito, de todos os cotitulares que obrigam a conta, o que deverá acontecer no prazo máximo das 48 horas seguintes à respetiva transmissão. O Cliente aceita que, nestes casos, a confirmação constitua meio bastante de prova das operações a que respeita.

8. No canal centro de contactos, com a resposta correta às questões que sejam colocadas ao Cliente em cada contacto telefónico, em conformidade com os procedimentos de identificação e de reconhecimento dos Clientes vigentes, e segundo o previsto na cláusula 4ª n.º 3 supra, e a manifestação do acordo do mesmo às concretas propostas que venham a ser formuladas pelo Banco, fica desde já o Banco autorizado a debitar o valor e os custos associados à transação respetiva.

9. Por razões de segurança e como meio de prova, o Cliente autoriza o Banco a proceder à gravação de todas as conversações mantidas entre ambos por Telefonia Vocal, reconhecendo a validade de tais registos como meio probatório pleno da vontade negocial manifestada por qualquer das partes por essa via, nomeadamente das informações, esclarecimentos ou aconselhamentos prestados pelo Banco, das ordens e instruções transmitidas pelo Cliente, ou da subscrição ou adesão por este a serviços comercializados pelo Banco.

9. Registo das operações

1. O Cliente e o Banco acordam que o registo informático das operações realizadas ao abrigo do presente Contrato, o qual poderá ser visualizado em terminal e/ou impresso em papel, constitui prova adequada das ordens dadas pelo Cliente.

2. O Banco compromete-se manter permanentemente atualizada a informação que disponibiliza ao Cliente através dos canais Internet, Mobile e MTM. Todavia, sobre esta prevalecerão sempre os registos contabilísticos próprios do Banco.

10. Suspensão, bloqueio do acesso, alterações contratuais, denuncia e resolução do Contrato

1. O Banco poderá inibir e bloquear temporária ou definitivamente, o(s) acesso(s) aos meios de comunicação á distância pelo Cliente e/ou de alguma das suas facilidades ou serviços, por motivos objetivamente fundamentados que se relacionem com:

a) Por razões de segurança, nomeadamente se o Banco for informado ou tiver conhecimento de que ocorreu quebra de confidencialidade do(s) códigos e credenciais de segurança personalizadas do Cliente indicados nos números 1 e 2 da cláusula 6ª (Convenção sobre prova), designadamente em caso de extravio, furto ou roubo ou apropriação abusiva dos mesmos, ou suspeita de utilização não autorizada ou fraudulenta, ou de perda ou extravio, furto ou roubo ou falsificação de Cartão de débito ou de crédito emitido pelo Banco e de que o Cliente seja Titular;

b) A suspeita de utilização não autorizada ou fraudulenta de qualquer irregularidade de que possa resultar um prejuízo sério para o Banco, para o Cliente ou para o Sistema de Pagamentos nomeadamente quando tal lhe seja solicitado pela entidade gestora do Sistema de Pagamentos por motivos de segurança ou de utilização abusiva, indevida ou não autorizada;

c) Se o Cliente realizar transações ilegais de qualquer natureza;

d) Se o presente Contrato cessar, por qualquer forma, os seus efeitos;

e) Se for declarada falência, insolvência, ou declaração judicial de acompanhamento de maior do Cliente, se o saldo da(s) conta(s) do Cliente se mostrar indisponível na sequência de ordem judicial de penhora, arrolamento, arresto, ou qualquer outra forma de apreensão judicial, ou outras ordens de bloqueio ou análogas decretadas por autoridades judiciais, judiciárias ou de supervisão.

2. Nos casos referidos no número 1 precedente desta cláusula, o Banco deve informar o Cliente do bloqueio do(s) o(s) acesso(s) aos meios de comunicação á distância pelo Cliente, e da respetiva justificação por SMS para o telemóvel do Cliente, se possível antes de efetuar o bloqueio ou, o mais tardar, imediatamente após o bloqueio, salvo se tal informação não puder ser prestada por razões de segurança objetivamente fundamentadas ou for proibida por outras disposições legais aplicáveis.

3. Logo que deixem de se verificar os motivos que levaram ao bloqueio, o Banco deve desbloquear o(s) acesso(s) aos meios de comunicação á distância pelo Cliente.

4. Além dos casos referidos no número 1 precedente desta cláusula, fica bem entendido que por questões de segurança o Cliente ficará inibido de aceder aos meios de comunicação á distância do Banco através do Centro de Contactos, Internet, Mobile e MTM caso ocorram três falhas consecutivas no uso do Código de Utilizador, do Código Multicanal ou da Chave de Confirmação. Neste caso, a reativação do Código de Utilizador, do Código Multicanal ou da Chave de Confirmação poderá ser obtida através de contato presencial numa Agência do Banco ou contato telefónico através do canal Centro de Contactos. Não sendo possível reativar os códigos originais, nos termos do número anterior, deverão ser obtidos novos códigos através dos meios disponíveis para esse efeito, como sejam as Agências do Banco, o sítio da Internet www.millenniumbcp.pt ou as caixas automáticas Multibanco.

5. O presente Contrato terá duração indeterminada.

6.1. O presente Contrato poderá ser denunciado, sem invocação de qualquer fundamento ou motivo:

a) A qualquer momento, pelo Cliente, mediante instrução escrita e devidamente assinada pelo Cliente presencialmente numa Sucursal do Banco;

b) Pelo Banco, neste caso mediante um pré-aviso escrito de sessenta dias sobre a data em que a denúncia haja de produzir efeitos, remetido ao Cliente nos termos previstos nas disposições da clausula 13ª (Disposições Complementares) infra.

6.2. A denúncia do Contrato implica o cancelamento dos acessos aos meios de comunicação á distância pelo Cliente.

7. O Banco pode, mediante comunicação escrita enviada ao Cliente segundo o previsto na clausula 13ª (Disposições Complementares) infra, resolver o presente Contrato com efeitos imediatos, cancelando imediatamente os acessos aos meios de comunicação á distância pelo Cliente nos seguintes casos:

a) Quando tenha sido declarada falência, insolvência, ou o Banco tenha conhecimento da declaração judicial de acompanhamento de maior do Cliente.

b) Quando o Cliente revogue ilegitimamente ordens de pagamento que tenha dado através dos meios de comunicação á distância do Banco;

c)) Quando se verifique que o Cliente, por negligência grave ou dolo grosseiro, tenha provocado dano ao Banco ou a qualquer outro operador ou interveniente nas operações de pagamento ou crédito através dos meios de comunicação á distância do Banco.

d) Se o saldo da(s) conta(s) do Cliente ou de qualquer outra conta de depósito da titularidade ou co-titularidade do Cliente junto do Banco se mostrar indisponível na sequência de ordem judicial de penhora, arrolamento, arresto, ou qualquer outra forma de apreensão judicial, ou outras ordens de bloqueio ou análogas decretadas por autoridades judiciais, judiciárias ou de supervisão.

8. O Contrato cessa ainda a sua vigência, extinguindo-se imediatamente o direito de acessos aos meios de comunicação á distância do Banco em caso de morte do Cliente.

9.1. O Banco pode propor modificações do clausulado do presente Contrato, que decorram de exigências legais ou relacionadas com sistemas internacionais e regras de segurança, ou ainda quando o entenda conveniente.

9.2. Essa(s) modificação(ões) será(ão) comunicada(s) ao Cliente através de pré-aviso escrito enviado nas disposições da clausula 13ª (Disposições Complementares) infra, com antecedência não inferior a sessenta dias sobre a data da sua aplicação.

9.3. Fica expressamente convencionado que, perante o silêncio subsequente do Cliente se considera que este aceita tacitamente a(s) alteração(ões) assim proposta(s) pelo Banco, exceto se, antes da entrada em vigor dessa proposta, o Cliente notificar o Banco de que não a(s) aceita.

9.4. Discordando dessa(s) modificação(ões) proposta(s), o Cliente poderá resolver e pôr termo imediato ao presente Contrato, desde que o comunique ao Banco, por correio registado com aviso de receção ou outro meio do qual fique registo escrito comprovativo.

11. Cliente menor, titular de conta de depósito à ordem, com idade igual ou superior a 14 anos

1. Relativamente à conta de depósitos à ordem, titulada por Cliente menor, com idade compreendida entre os 14 e os 17 anos, o(s) respetivo(s) representante(s) legal(ais), considerando a natural capacidade do menor decorrente da sua idade, poderá(ão) segundo o seu exclusivo critério, solicitar ao Banco, através de pedido expresso por escrito, a atribuição, a esse Cliente menor de um Código Multicanal para os canais Centro de Contactos, Internet, Mobile e MTM, assim como, para estes dois últimos canais, o respetivo Código de Utilizador, reconhecendo-se ao Banco a liberdade de aceitar ou não a atribuição dos referidos Códigos.

2. O Código Multicanal permitirá ao Cliente menor realizar unicamente operações de consulta - de saldos e de movimentos - da conta de depósitos à ordem. Não é permitida a realização de quaisquer outras operações ou quaisquer transações.

3. O Código Multicanal e o Código de Utilizador são pessoais e intransmissíveis e serão entregues exclusivamente ao menor, que deverá utilizá-los de forma cuidadosa, reservada e exclusivamente pessoal, e tomar todas as medidas de cuidado e de diligência razoáveis para preservar a posse, a segurança e a utilização reservada e confidencial em cada momento do seu telemóvel ou dispositivo móvel, e do seu número de telemóvel previamente fornecido ao Banco, nos termos previstos nas cláusulas6ª e 8ª supra, e responsabilizando-se o(s) seu(s) representante(s) legal(is), perante o Banco, pela sua utilização adequada e responsável, nos termos estabelecidos nestas cláusulas.

12. Informação financeira

1. A informação financeira disponível através dos canais Internet e Mobile, nomeadamente cotações, índices, notícias, estudos ou outra, é disponibilizada pelo Banco com um intuito meramente informativo e é elaborada por terceiros, que autorizam o Banco a difundir tal informação aos Clientes.

2. Apesar de o Banco selecionar criteriosamente as fontes de informação, podem escapar à sua análise erros ou omissões, não podendo por isso garantir a exatidão ou completude da informação difundida nem ser por tal responsabilizado, ou responsabilizado pela má interpretação ou utilização da mesma.

3. O Cliente utilizará a informação financeira difundida por sua conta e risco, sendo o Cliente exclusivamente responsável pelas decisões de investimento tomadas com base na referida informação.

13. Disposições complementares

1. Na vigência do presente Contrato, o Cliente tem o direito de receber a seu pedido, a todo o tempo, os termos do contrato em vigor em cada momento, em formato digital (ficheiro informático) disponibilizado para o endereço eletrónico fornecido pelo Cliente ou para consulta no canal Internet do Banco, mediante acesso à conta em www.millenniumbcp.pt. nos termos aqui previstos. Em alternativa, se o Cliente assim o requerer presencialmente em qualquer balcão do Banco, os termos do Contrato ser-lhe-ão facultados em suporte de papel.

2. Na vigência do presente Contrato, as comunicações do Banco ao Cliente serão realizadas preferencialmente por e-mail remetido para o endereço eletrónico do Cliente fornecido ao Banco, e/ou, se aplicável e possível, por SMS para o respetivo número de telemóvel, ou, em ultimo recurso serão enviadas para o seu endereço postal, fornecidos ao Banco em cada momento, segundo o disposto nos números seguintes desta clausula .

3. Em caso de alteração do respetivo endereço eletrónico e/ou do respetivo número de telemóvel, fornecidos ao Banco o Cliente obriga-se a informar sempre e prontamente o Banco dessa alteração e a fornecer o seu endereço eletrónico e número de telemóvel atualizados, em cada momento, para contactos e comunicações com o Banco.

4. Fica ainda expressamente convencionado que compete exclusivamente ao Cliente zelar pela consulta assídua e permanente atualização e bom funcionamento do respetivo endereço eletrónico e número de telemóvel indicados ao Banco para contactos e comunicações.

5. Ao presente contrato e às comunicações entre as partes é aplicável a língua portuguesa.

6. As comunicações escritas que o Cliente pretenda dirigir ao Banco no âmbito do presente Contrato podem ser remetidas para a Agência onde tenha relações preferenciais, à escolha do Cliente, ou para a sede do Banco.

7. Os contactos de iniciativa do Banco não implicam custos para o Cliente, sem prejuízo do preço e encargos devidos pelo serviço financeiro que venha a ser contratado na sequência de cada contacto.

Mod. 10903229 BANCO COMERCIAL PORTUGUÊS, S.A. Sociedade Aberta, com sede na Praça D.João I, 28, Porto, o Capital Social de [UGD Custom], matriculada na Conservatória do Registo Comercial do Porto sob o número único de matrícula e de identificação fiscal 501 525 882

8. O pagamento de todos os produtos e serviços financeiros e seguros que venham a ser adquiridos pelo Cliente no âmbito da utilização dos meios de comunicação à distância previstos nas presentes Condições Gerais poderá ser efetuado por débito de qualquer conta individual ou solidária de que o Cliente seja ou venha a ser titular junto do Banco.

9. O Banco Comercial Português, S.A. está sujeito à supervisão do Banco Central Europeu, com sede em Sonnemannstrasse 22, 60314 Frankfurt, Alemanha e do Banco de Portugal, o qual tem sede na Rua do Ouro, 27, 1100-150 Lisboa, no âmbito do Mecanismo Único de Supervisão.

10.1. O Cliente pode apresentar reclamações ou queixas por ações ou omissões dos órgãos e colaboradores do Banco ao Provedor do Cliente, que as aprecia após as necessárias diligências de instrução, podendo este emitir recomendações à Comissão Executiva do Banco. As recomendações do Provedor do Cliente são vinculativas para os órgãos e serviços, após aprovação da referida Comissão. As questões devem ser colocadas por escrito ao cuidado do Provedor do Cliente, utilizando para o efeito o endereço divulgado em www.millenniumbcp.pt.

10.2. O Cliente poderá igualmente apresentar as suas reclamações ao Banco de Portugal. Para esse efeito, pode optar pela utilização do Livro de Reclamações disponível nos balcões do Banco, sendo este disponibilizado logo que o Cliente o solicite, ou pela utilização do Livro de Reclamações Eletrónico disponível em www.livroreclamacoes.pt seguindo as instruções aí divulgadas para o efeito, ou pelo acesso em linha ao Portal do Cliente Bancário onde pode preencher o formulário de reclamação online ou imprimir e preencher o referido formulário de reclamação e enviá-lo pelo correio para a morada do Banco de Portugal, seguindo as instruções ali constantes para o efeito.

10.3. Os litígios de valor igual ou inferior à alçada dos tribunais de 1ª instância poderão, em alternativa aos meios judiciais competentes, ser submetidos às seguintes entidades extrajudiciais de resolução de litígios: Centro de Arbitragem de Conflitos de Consumo de Lisboa (www.centroarbitragemlisboa.pt) e Centro de Informação de Consumo e Arbitragem do Porto (www.cicap.pt).

10.4. O Cliente pode submeter a resolução extrajudicial os litígios respeitantes a produtos ou serviços contratados online, utilizando a plataforma de RLL – resolução de litígios em linha, também designada plataforma ODR – online dispute resolution (https://webgate.ec.europa.eu/odr/main/?event=main.home.show), criada à escala da União Europeia ao abrigo do Regulamento (UE) n.º 524/2013, do Parlamento Europeu e do Conselho, de 21 de maio de 2013.

10.5. Informa-se que o Banco disponibiliza um serviço para receção e tratamento extrajudicial de qualquer reclamação que os Clientes entendam ser de efetuar. Para o efeito, as reclamações deverão ser dirigidas a: Centro de Atenção ao Cliente, através do número 707 502 424 e/ou por correio eletrónico para o endereço www.millenniumbcp.pt e/ou por escrito, devendo, neste caso, a reclamação ser endereçada para Av. Prof. Dr. Cavaco Silva, Tagus Park Edf. 3, Piso 0, Ala C, 2744-002 Porto Salvo.

11. Para julgar todas as questões dele emergentes, fixam-se como competentes os foros da comarca de Lisboa, do Porto e do domicílio do Titular em Portugal, com expressa renúncia a qualquer outro.

ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA

1. Regras gerais para o acesso/uso de todos os Meios de Comunicação à Distância do Banco

1. O Cliente obriga-se a ler atentamente e dar cumprimento escrupuloso às presentes recomendações e regras de segurança aqui constantes, bem como, a ir consultar e ler, pelo menos uma vez em cada trimestre do ano civil, todos os avisos de segurança e os alertas periódicos que o Banco divulga no sítio de Internet www.millenniumbcp.pt, incluindo a descrição de concretos procedimentos fraudulentos utilizados em cada momento para a captura fraudulenta dos Código de Utilizador, Código Multicanal e demais credenciais personalizadas de acesso dos Clientes aos meios de comunicação á distância do Banco.

2. O Cliente deve estar atento e ser precavido contra tentativas de fraude por terceiros não autorizados. Designadamente, o Cliente tem de suspeitar e de desconfiar de, nomeadamente:

a) do tom de urgência de mensagens que o ameacem com a suspensão do acesso à conta, dos códigos de acesso ou do cartão se não fornecer os seus dados imediatamente;

b) do pedido de confirmação dos seus dados pessoais via correio eletrónico ou SMS, designadamente remetendo-o para o preenchimento on-line de formulários de informações pessoais e códigos de acesso;

c) de erros ortográficos/gramaticais e outros erros patentes na mensagem ou na página web fraudulenta, ou outros elementos que sugiram a origem diversa ou suspeita dos mesmos;

d) de mensagens de correio eletrónico ou SMS com links ou ficheiros em anexo;

e) da indicação de que, para simular operações, deve fornecer Código(s) de Autorização que o Banco lhe enviou por SMS ou gerados via Token,

3. O Millennium bcp não envia mensagens de correio eletrónico ou SMS com links e nunca solicita a confirmação dos seus dados pessoais ou dados de acesso a contas bancárias por estas vias de comunicação, designadamente remetendo para o preenchimento on-line de formulários de informações pessoais e fornecimento de credenciais de acesso e nem solicitando ao Cliente que ligue para certo numero de telefone. Se tal vier a suceder, o Cliente deve considerar que se pode tratar de uma tentativa de fraude.

4. O Cliente deve analisar as mensagens de correio eletrónico que recebe antes de abrir, confirmando sempre a origem e o assunto da mesma e, se continuar com dúvidas, confirme previamente junto da entidade emitente. O Cliente não deve aceitar a execução de ficheiros/ programas cujo download se ative sem o ter solicitado.

5. O Banco não simula transações com Clientes. Se em algum momento o Cliente receber um Código de Autenticação para simulação de transação ou para confirmação de uma operação que o Cliente não tenha solicitado, o Cliente deve abster-se de introduzir ou divulgar esse código e deve de imediato reportar o facto sem demora para o(s) número telefónico 707502424 / 918272424 / 935222424 / 965992424 (chamada nacional) ou +351707502424 / +351210052424 (chamada internacional) que é um serviço de atendimento permanente – 24 horas/dia, 365 dias/ano, a fim de dar o alerta e solicitar o respetivo bloqueio/impedimento de uso abusivo ou fraudulento perante o Millennium bcp.

6. O Cliente não deve nunca facultar o(s) Código(s) de Autenticação a terceiros, sob nenhum pretexto, obrigando-se a fazer uma utilização atenta, prudente, e exclusivamente pessoal do mesmo, e assumindo todos os riscos e consequências inerentes à sua divulgação indevida.

7. Se verificar em algum momento que o seu telemóvel se encontra inativo ou que o número de telemóvel não funciona corretamente, o Cliente deverá contactar de imediato a sua operadora de telecomunicações e garantir o correto funcionamento do cartão SIM relativo ao seu número de telemóvel indicado ao Banco.

8. Se em algum momento, o Cliente:

a) Suspeitar que terceiros têm conhecimento, no todo ou em parte, do seu Código de Utilizador, e/ou Código Multicanal ou da Chave de Confirmação, ou em caso de extravio, furto ou roubo ou apropriação abusiva dos mesmos ou de algum deles, e/ou

b) Verificar o registo na conta de qualquer transação não consentida ou a existência de erros ou irregularidades na efetivação das operações, e/ou

c) Receber um Código de Autenticação para simulação de transação, e/ou

d) Receber um Código de Autenticação para confirmação de uma operação que o Cliente não tenha solicitado, e/ou

e) Suspeitar de acesso indevido de terceiro(s) ao seu endereço de correio eletrónico e/ou ao seu telemóvel ou dispositivo móvel, ou ao seu número de telemóvel, por qualquer forma,

Então deverá, suspender o procedimento e sem atraso injustificado entrar de imediato em contacto com o Banco, por via telefónica para o telefone 707502424 / 918272424 / 935222424 / 965992424 (chamada nacional) ou +351707502424 / +351210052424 (chamada internacional), que é um serviço de atendimento permanente – 24 horas/dia, 365 dias/ano, a fim de dar o alerta e solicitar o respetivo bloqueio/impedimento de uso abusivo ou fraudulento perante o Millennium bcp. O Cliente deverá ainda confirmar ao Banco o sucedido, por escrito, num prazo não superior a 5 dias.

9. Quando o Cliente pretender ver algum tema de segurança abordado na nossa newsletter, ou necessite de esclarecimentos, deve contactar-nos através do correio eletrónico particulares@millenniumbcp.pt ou através do telefone 707502424 / 918272424 / 935222424 / 965992424 (chamada nacional) ou +351707502424 / +351210052424 (chamada internacional) que é um serviço de atendimento permanente – 24 horas/dia, 365 dias/ano.

Regras Adicionais para o sítio de Internet www.millenniumbcp.pt:

1. Sempre que aceder às suas contas bancárias, através do sítio do Millennium bcp, verifique se o endereço é apresentado da seguinte forma, conforme o browser utilizado:

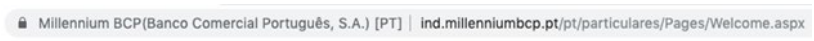
IE

Edge

Firefox

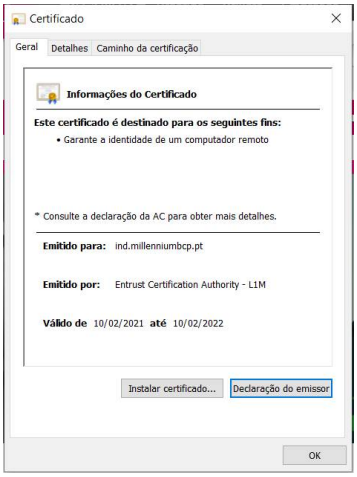
Chrome

Safari

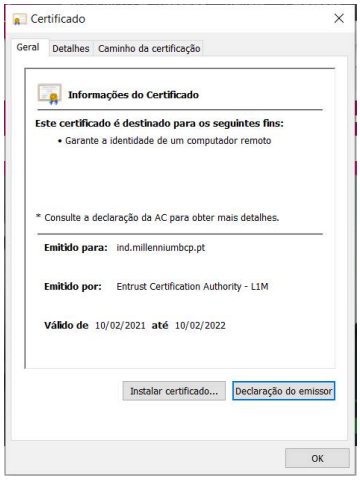


Em caso de dúvida, confirme a origem do certificado digital - efetuando clique sobre o cadeado - e verifique se corresponde, efetivamente, ao Millennium bcp:

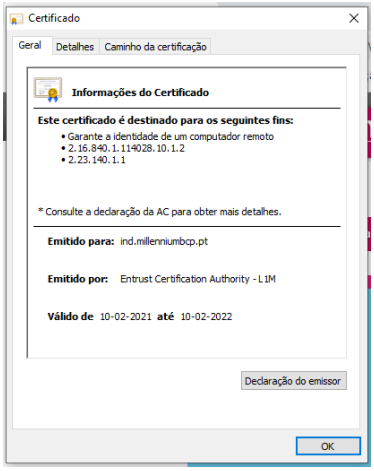
IE



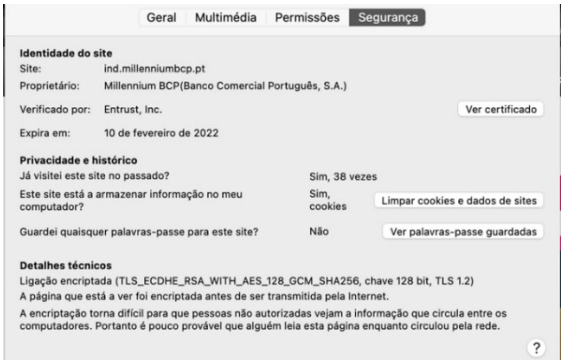
Edge



Chrome



Firefox



Safari

2. No acesso ao sítio de Internet www.millenniumbcp.pt **o Banco nunca solicita o número de telemóvel nem a instalação de software/programas de segurança.**

3. Caso seja um Utilizador exclusivo do sítio de Internet www.millenniumbcp.pt, será solicitado no primeiro acesso, e a cada 90 dias, a identificação do Código de Utilizador, três (3) dígitos aleatórios do Código Multicanal e um Código de Autenticação gerado via Token ou enviado por SMS para o número de telemóvel do Cliente, registado no Banco. Nos restantes acessos será solicitada apenas a identificação do Código de Utilizador e três (3) dígitos aleatórios do Código Multicanal. Serão solicitados sempre os mesmos 3 dígitos até que o acesso seja efetuado com sucesso. Tudo o que for solicitado para além do referido constitui uma tentativa de fraude que deverá reportar imediatamente, sem atraso injustificado, para o(s) número telefónico 707502424 / 918272424 / 935222424 / 965992424 (chamada nacional) ou +351707502424 / +351210052424 (chamada internacional) que é um serviço de atendimento permanente – 24 horas/dia, 365 dias/ano, a fim de dar o alerta e solicitar o respetivo bloqueio/impedimento de uso abusivo ou fraudulento perante o Millennium bcp.

4. Para consultar os movimentos da(s) conta(s) ou extratos bancários com antiguidade superior a 90 dias, será solicitado um Código de Autenticação, sempre que no acesso ao sítio de Internet www.millenniumbcp.pt não tenha sido solicitado o Código de Autenticação, gerado via Token ou enviado por SMS para o número de telemóvel do Cliente, registado no Banco, para além dos três (3) dígitos aleatórios do Código Multicanal.

5. Na realização e confirmação de transações será solicitado um Código de Autenticação gerado via Token ou enviado por SMS para o número de telemóvel do Cliente, registado no Banco, no momento da realização da mesma.

6. Na realização de operações de pagamento por débito na conta de depósitos à ordem ou numa conta agregada ao serviço, pode ser exigível uma confirmação adicional através de um sistema de Autenticação Forte do Cliente (AFC) – nesse caso, será solicitado ao Cliente a introdução de um Código de Autenticação gerado via Token ou enviado por SMS para o número de telemóvel do Cliente, registado no Banco, no momento da realização da mesma.

7. O Cliente deve ler sempre atentamente todo o conteúdo do SMS recebido com o Código de Autenticação, pois os dados da operação são identificados no texto da mensagem.

8. O Código de Autenticação não será solicitado caso execute um pagamento:
- para um dos seus beneficiários/favoritos previamente definidos como confiáveis;
- para contas da sua titularidade no Millennium bcp;
- de baixo valor, até atingir um valor acumulado definido pelo Banco.

9. O Millennium bcp envia sempre correio eletrónico e SMS sem links.

10. Nunca aceda ao sítio do Millennium bcp através de links de mensagens, motores de pesquisa ou, mesmo, através da opção "Favoritos". Digite sempre o endereço completo www.millenniumbcp.pt para evitar o acesso a páginas fraudulentas e muito idênticas à do sítio do Millennium bcp, bem como, para evitar a instalação de software malicioso no equipamento utilizado para acesso ao sítio do Millennium bcp.

11. O Millennium bcp nunca solicita elementos de caráter pessoal e/ou confidencial, como por exemplo Código Multicanal completo, Chave de Confirmação, número de telemóvel, alteração de dados, etc. no acesso ao sítio de Internet www.millenniumbcp.pt, por correio eletrónico, SMS ou por qualquer outro meio.

12. Não utilize um Código Multicanal óbvio (números sequenciais, números iguais, dados pessoais como por exemplo a data de nascimento, número telemóvel, etc.) para o acesso ao sítio de Internet www.millenniumbcp.pt. Periodicamente, pelo menos semestralmente, altere o seu Código Multicanal na opção "Personalizar", do menu "Área M".

13. Defina códigos de acesso únicos para o sítio de Internet www.millenniumbcp.pt e não os utilize em outros sítios.

14. O acesso a www.millenniumbcp.pt pode, igualmente, ser efetuado através do serviço de autenticação Chave Móvel Digital disponibilizado pelo Estado Português.

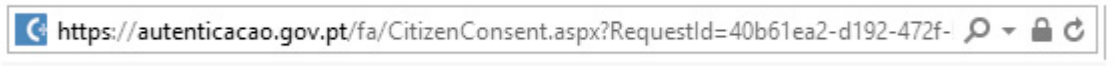
15. A Chave Móvel Digital permite autenticar-se através de:

a) Número de telemóvel;

b) PIN – Número de Identificação Pessoal intransmissível criado no registo da Chave Móvel Digital;

c) Código de segurança numérico único e temporário de 6 dígitos enviado por SMS para o número de telemóvel.

16. Ao escolher esta forma de autenticação será redirecionado de forma segura para o serviço de autenticação do Estado, em:



sendo informado dos dados pessoais solicitados pelo Banco e concorda explicitamente com essa transmissão, conforme:

17. Nunca forneça a terceiros quaisquer elementos pessoais de identificação que possam ser utilizados para certificação junto das operadoras móveis, nem os Códigos de Utilizador e de Acesso Multicanal ou outros, nomeadamente os Códigos de Autenticação recebidos por SMS ou obtidos via Token.

18. Deve igualmente ser impedido o acesso de terceiros aos equipamentos utilizados para confirmar operações bancárias bem como aos seus componentes, como sejam o(s) cartão(ões) SIM do número de telemóvel do Cliente indicado ao Banco.

19. O Cliente deve manter o seu computador protegido, obrigando-se nomeadamente a:

- Instalar um bom antivírus, mantendo-o permanentemente atualizado:

- Utilizar uma firewall para filtrar o tráfego da Internet que entra e sai do computador;

- Estar atento às atualizações de segurança que os fornecedores credíveis de software disponibilizam, aplicando-as de acordo com as instruções fornecidas;

- Utilizar sempre versões atualizadas dos navegadores e sistemas operativos;

- Desativar as opções guardar palavra-passe e preenchimento automático do seu navegador;

- Se se tratar de computador partilhado com outrem, deverá ter em atenção e aplicar sempre as medidas de proteção básicas: desconectar e terminar sempre cada sessão, e apagar a memória cache;

- Não deve abrir as mensagens eletrónicas de origem desconhecida, e sobretudo não deve clicar ou abrir anexos ou links constantes das mesmas.

- Não deve abrir ficheiros provenientes de remetentes desconhecidos;

- Deve manter-se informado sobre a segurança geral quanto à utilização da internet.

- Ter em atenção que as redes Wi-Fi gratuitas facilitam o acesso de terceiros ao seu computador e aos dados e comunicações do mesmo. Não deve utilizar redes Wi-Fi públicas para aceder ao canal internet ou mobile do Banco e nem para aceder a sites que requeiram a introdução de informações sensíveis, compras online e homebanking. Para este tipo de acessos utilize sempre e só a sua própria rede de dados;

Regras adicionais para o acesso ao Serviço do Centro de Contactos

1. O acesso ao serviço telefónico do Banco efetua-se através dos números 707 50 24 24 / 918 27 24 24 / 935 22 24 24 / 965 99 24 24 ou a partir do estrangeiro +351 707 50 24 24 / +351 210 05 24 24, por duas formas distintas:

- Atendimento automático - VRS (Voice Response System) é solicitado o número de conta à ordem e as 4 primeiras posições do Código Multicanal;

- Atendimento personalizado é solicitado o número de conta à ordem e 3 posições aleatórias do Código Multicanal.

2. Para validar as operações é necessário ter a Chave de Confirmação, sendo solicitadas 3 posições aleatórias da mesma.

Regras adicionais para o acesso ao Serviço Mobile

1- O Cliente deve:

a) Ativar uma forma de bloqueio automático do seu equipamento móvel e de desbloqueio por código secreto ou dado biométrico do Cliente;

b) Proteger o seu smartphone/tablet com um bom antivírus, mantendo-o sempre atualizado e operacional.

c) Estar atento às atualizações de segurança que os fornecedores credíveis de software disponibilizam e aplicá-las de acordo com as instruções que são fornecidas.

d) Desativar a opção de instalação de aplicações de origem desconhecida nas definições de segurança do seu equipamento;

e) Recorrer sempre aos sites/stores oficiais quando necessitar de instalar qualquer aplicação, e ser cauteloso: antes de efetuar o download de uma aplicação, leia a opinião de outros utilizadores e verifique a que funcionalidades e permissões terá de dar acesso no seu equipamento (ex: leitura e envio de sms, acesso aos seus contactos, localização). É muito importante que esteja atento às permissões que concede às aplicações que instala no dispositivo móvel;

f) Ao usar o correio eletrónico no seu equipamento móvel, o Cliente deve certificar-se que nunca acede a mensagens que não reconhece, principalmente a anexos ou links constantes das mesmas. No caso de receber algum correio eletrónico suspeito aparentemente proveniente do Banco, não o abra, e deve reportar o facto ao Banco, sem demora, numa Sucursal ou por via telefónica para o telefone 707502424 / 918272424 / 935222424 / 965992424 (chamada nacional) ou +351707502424 / +351210052424 (chamada internacional), que é um serviço de atendimento permanente – 24 horas/dia, 365 dias/ano, a fim de dar o alerta.

g) Recordar que o Millennium bcp NUNCA envia correio eletrónico e SMS com links.

h) Ter em atenção que as redes Wi-Fi gratuitas facilitam o acesso de terceiros ao seu telemóvel e aos dados e comunicações do mesmo. Não deve utilizar redes Wi-Fi públicas para aceder ao canal internet ou mobile do Banco e nem para aceder a sites que requeiram a introdução de informações sensíveis, compras online e homebanking. Para este tipo de acessos utilize sempre e só a rede de dados do equipamento móvel;

i) Desativar o Bluetooth quando não precisar porquanto o telemóvel ficará menos vulnerável a ciberataques.

j) Manter o seu smartphone seguro fisicamente, e sob vigilância permanente.

App Millennium

1. As aplicações do Millennium bcp para instalação e utilização no telemóvel estão disponíveis para equipamentos Apple e Android TM.

2. Instale as aplicações a partir das lojas de aplicações oficiais das marcas (Apple Store e Play Store). Nunca o faça utilizando links que lhe sejam facultados por terceiros, nomeadamente por correio eletrónico ou por SMS.

3. Registo na App Millennium:

a) Depois de instalada a App Millennium, defina o Código de Acesso Único (PIN) constituído por 4 algarismos, para o acesso à App Millennium e não o utilize noutras aplicações;

b) De seguida, introduza o Código de Utilizador e três (3) posições aleatórias do Código Multicanal para validar o envio do Código de Autenticação por SMS, indispensável ao registo da aplicação;

c) Por último, introduza o Código de Autenticação que recebeu por SMS.

4. Acesso à App Millennium:

4.1. O acesso à App Millennium é efetuado através do PIN constituído por 4 algarismos, definido no processo do registo;

4.2. Em alternativa à utilização do Código de Acesso Único (PIN), o acesso pode efetuar-se através de impressão digital ou reconhecimento facial do Cliente, desde que o equipamento contemple estas tecnologias. Na página de login, poderá sempre optar pelo acesso com impressão digital, reconhecimento facial ou através do PIN. Para ativar/desativar o acesso à App Millennium por impressão digital ou reconhecimento facial, basta aceder à área de "Configurações".

4.3. Não utilize um PIN óbvio (1234, 1111, ano de nascimento, código postal, etc.) para o acesso às aplicações do Millennium bcp. Periodicamente, altere o seu PIN no ícone do perfil (canto superior direito), disponível após acesso à App Millennium. Em seguida selecione Segurança » alterar PIN.

4.4. Atingindo as três falhas consecutivas de PIN, tem de proceder a um novo registo da App Millennium conforme descrito no ponto 3 precedente para definir novo PIN.

5. Para realizar operações a App Millennium pode solicitar:

- Três (3) dígitos aleatórios do Código Multicanal; ou,

- Um Código de Autenticação enviado por SMS para o número de telemóvel registado no Banco; ou,

- Um dado biométrico (impressão digital ou reconhecimento facial).

Tudo o que for solicitado para além do referido, constitui uma tentativa de fraude e deverá reportar sem demora para o 707502424 / 918272424 / 935222424 / 965992424 (chamada nacional) ou +351707502424 / +351210052424 (chamada internacional) que é um serviço de atendimento permanente – 24 horas/dia, 365 dias/ano.

6. O Código de Autenticação não será solicitado caso execute um pagamento:

- para um dos seus beneficiários/favoritos previamente definidos como confiáveis;

- para contas da sua titularidade no Millennium bcp;

- de baixo valor, até atingir um valor acumulado definido pelo Banco.

Extensão da App Millennium para Apple Watch

1. A aplicação para Apple Watch é uma extensão da App Millennium e é ativada a partir da mesma, pelo que pressupõe a prévia adesão do utilizador à referida aplicação nos termos estabelecidos supra.

2. Para utilização desta aplicação é necessário parametrizar na App Millennium quais as contas/cartões que pretende visualizar através do Apple Watch.

3. As operações de consulta de informação bancária proporcionadas pela aplicação para Apple Watch não requerem a introdução de quaisquer códigos pessoais secretos. Contudo, a informação bancária apenas estará disponível quando o Apple Watch estiver próximo do iPhone do Cliente, constituindo esta circunstância uma medida de segurança que o utilizador deverá ter sempre presente, para salvaguarda da confidencialidade da informação que lhe diz diretamente respeito.

Regras adicionais para o acesso à MTM

1. O acesso à MTM efetua-se através de cartão bancário ou de três (3) dígitos aleatórios do Código Multicanal. Serão solicitados sempre os mesmos 3 dígitos até que o login seja efetuado com sucesso, pelo que, tudo o que for solicitado para além do referido (ex. Código de Acesso completo, número de telemóvel) constitui uma tentativa de fraude e deverá reportar para o 707502424 / 918272424 / 935222424 / 965992424 (chamada nacional) ou +351707502424 / +351210052424 (chamada internacional).

2. Nunca forneça a terceiros quaisquer elementos pessoais de identificação nem os Códigos de Utilizador ou de Acesso Multicanal, ou outros.

Riscos

A utilização dos meios de comunicação à distância com incumprimento das regras e recomendações acima transmitidas, pode acarretar riscos para o Cliente, incluindo:

- Acesso de terceiros a dados pessoais e confidenciais;

- Realização de transações por terceiros que implicam movimentação do património da conta e perdas financeiras para o Cliente

ANEXO 2 – OPEN BANKING

1. Compete ao Cliente avaliar se quer ou não partilhar os seus dados bancários. O Open Banking dá ao Cliente a possibilidade de compartilhar com terceiras entidades saldos e movimentos das contas detidas junto do Banco, mas apenas se o Cliente nisso consentir expressamente.

2.1. Se o Cliente considerar adequado que determinadas instituições ou operadores de serviços de pagamento, sem qualquer relação contratual com o Banco (third parties payment services providers - TPPs) tenham acesso eletrónico ao saldo da conta de pagamento de que é titular no Banco, bem como a outras informações financeiras da conta, ou que iniciem pagamentos diretamente na conta, poderá contratar com essas instituições ou operadores alguns dos seguintes serviços de Open Banking:

- Serviços de iniciação de pagamentos;

- Serviços de informação sobre contas;

- Serviços de confirmação de saldos.

Os serviços de iniciação de pagamentos permitem a um TPP iniciar uma ordem de pagamento na conta de que o Cliente é titular no Banco (ex., um pagamento online diretamente da conta do cliente para a conta do TPP).

Os serviços de informação sobre contas permitem a um TPP agregar no seu sítio de Internet informação financeira de várias contas, incluindo os saldos e movimentos da conta detida pelo Cliente junto do Banco (instituições financeiras ou entidades que gerem sites de comparação de preços estarão entre as empresas que prestarão esse tipo de serviço).

Os serviços de confirmação de saldos permitem a um TPP que emite instrumentos de pagamento baseados em cartões, no momento em que o Cliente realiza um pagamento com o cartão, confirmar que a conta detida junto do Banco tem saldo suficiente para realizar o pagamento.

2.2. A possibilidade de um TPP prestar os serviços atrás referidos requer que a conta detida junto do Banco esteja acessível nos canais digitais do Banco e, consequentemente, a prévia adesão do Cliente ao presente Contrato de Utilização dos Meios de Comunicação à Distância.

2.3. O consentimento do Cliente para a prestação de serviços de iniciação de pagamento ou de serviços de informação sobre contas ou de confirmação de saldos deve ser conferido diretamente aos respetivos prestadores de serviços de iniciação de pagamento ou de serviços de informação sobre contas ou de confirmação de saldos. A prestação desses serviços requer que a conta do Cliente esteja acessível em linha através do sítio www.millenniumbcp.pt, que o (s) prestador(es) de serviços estejam devidamente autorizados ou registados pelas autoridades competentes para prestar os respetivos serviços, que os mesmos se autentiquem junto do Banco de forma adequada e comuniquem de forma segura, de acordo com as normas aplicáveis em cada momento.

2.4. Para efeitos do disposto no número anterior, está na disponibilidade do Cliente autorizar diretamente um prestador de serviços de iniciação de pagamento a aceder a informações sobre a conta e a transmitir ao Banco ordens de pagamento sobre a conta e/ou autorizar um prestador de serviços de pagamento a aceder a informações sobre a conta e os respetivos saldos.

2.5. Fica expressamente convencionado que o Banco fica legitimado a prestar as informações e a executar as ordens de pagamento no âmbito dos serviços de iniciação de pagamento e de informação sobre contas quando os respetivos prestadores entrem em contacto com o Banco solicitando tais informações e transmitindo tais ordens de pagamento desde que se verifiquem todos os requisitos indicados em 2.3. supra e o Banco logre obter com sucesso a autenticação forte do Cliente.

2.6. A verificação das circunstâncias previstas no número precedente corresponde ao consentimento expresso do Cliente para a prestação dos respetivos serviços, nesses casos, o Banco deve considerar qualquer pedido de informação ou ordem ou instrução recebida por parte do prestador de serviços respetivo como sendo um pedido de informação ou ordem ou instrução dada pelo próprio Cliente ao Banco. Cabe ao Cliente certificar-se de que o prestador de serviços de pagamento por si utilizado tem a sua expressa autorização para aceder à conta junto do Banco, sendo responsável pelas consequências de fornecer códigos de autenticação e credenciais de segurança personalizadas através de meios de comunicação á distância a terceiros não autorizados, designadamente sendo responsável pelas perdas que daí resultem.

2.7. O Banco fica obrigado a disponibilizar ao TPP o IBAN da conta detida pelo Cliente junto do Banco e, conforme os casos, o respetivo saldo ou o saldo e movimentos da conta, ou a aceitar a operação de pagamento por aquele iniciada, não sendo requerido ao TPP identificar o Cliente nem fazer prova do contrato que com ele celebrou para prestar os serviços de Open Banking e aceder diretamente ao Banco.

3. É responsabilidade do Cliente, uma vez redirecionado para a página web/app do Millennium bcp, confirmar a autorização dada a um TPP para que este possa prestar determinado serviço de Open Banking e aceder diretamente ao Banco, devendo para o efeito, no sítio de Internet www.millenniumbcp.pt, introduzir corretamente o Código de Utilizador, três posições aleatórias do Código Multicanal e um Código de Autenticação enviado por SMS para o número de telemóvel registado no Banco ou obtido por Token, ou, na App Millennium, introduzir corretamente o PIN de Segurança constituído por quatro dígitos numéricos e um Código de Autenticação enviado por SMS para o número de telemóvel registado no Banco. Tudo o que for solicitado para além do referido supra constitui uma tentativa de fraude e deverá reportar para o 707 50 24 24. Para chamadas a partir do estrangeiro, ligue para +351 210 05 24 24.

4. O Código de Utilizador, o Código Multicanal e o PIN, indicados no ANEXO 1 - RISCOS E REGRAS DE SEGURANÇA destas Condições Gerais, são elementos de autenticação pessoais, confidenciais e intransmissíveis, pelo que o Cliente não pode permitir a sua utilização por terceiros, fazendo uma utilização rigorosa, exclusivamente pessoal dos mesmos.

5. Antes de decidir compartilhar com terceiras entidades saldos e movimentos das contas detidas junto do Banco, o Cliente deve tomar as medidas necessárias para confirmar que o TPP é uma entidade legítima, verificando designadamente tratar-se de uma entidade registada junto do Banco de Portugal ou junto da National Competent Authority do país de origem.

6. Constitui obrigação do TPP prestar informações claras e objetivas sobre a sua identidade e contactos, finalidade e fundamento do tratamento da informação que diz respeito ao Cliente, os destinatários dos dados se os houver, o facto de tencionar transferir dados para um país terceiro, se for o caso.

7. O Cliente deve ter em consideração que se decidir conferir a um TPP o seu acordo para que este tenha acesso aos seus dados bancários e se, além disso, confirmar na página web/app do Millennium bcp a autorização dada a um TPP para que este possa prestar determinado serviço de Open Banking e aceder diretamente ao Banco, o Banco não pode garantir a forma nem as finalidades com que a informação será tratada por aquele, e tratando-se de um serviço de iniciação de pagamentos a operação considera-se assim autorizada, não podendo o consentimento para a sua execução ser então retirado. Não obstante, obtido o consentimento do Cliente, nos termos suprarreferidos, e tendo acedido aos dados bancários que lhe dizem respeito, o TPP é única e exclusivamente responsável pela segurança dos dados assim obtidos.

8. O Cliente deve ter presente que pode a qualquer momento gerir e retirar na página web/App do Millennium bcp as autorizações para serviços de Open Banking conferidas a TPP´s, devendo para o efeito aceder ao menu Área M ao sítio de Internet www.millenniumbcp.pt. Pode igualmente ligar para a linha de apoio do Millennium bcp.

9. Em qualquer caso, nos termos da lei, o Banco tem a prerrogativa de recusar o acesso de um TPP aos dados bancários do Cliente se considerar que há risco de fraude.

Mod. **10903229** BANCO COMERCIAL PORTUGUÊS, S.A. Sociedade Aberta, com sede na Praça D.João I, 28, Porto, o Capital Social de [UGD Custom], matriculada na Conservatória do Registo Comercial do Porto sob o número único de matrícula e de identificação fiscal 501 525 882