Código de Conduta para a Protecção de Dados Pessoais

O presente Código de Conduta da Cloud365, Lda. (doravante identificada como "Cloud365") para a Protecção de Dados Pessoais, foi elaborado no âmbito do art.º 40º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, Regulamento Geral sobre a Protecção de Dados (RGPD) e vincula todos os Trabalhadores da Cloud365 quanto à recolha, o tratamento e a utilização de dados pessoais respeitantes à Cloud365, aos próprios Trabalhadores, aos Clientes e a terceiros com os quais exista um relacionamento com a Cloud365.

O presente Código aplica-se também às relações da Cloud365 com todos os seus Colaboradores, Parceiros e Subcontratantes.

Artigo 1º

Definições

Para efeitos do presente Código são consideradas as seguintes definições estabelecidas no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016:

1) "Dados pessoais" - informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, directa ou indirectamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via electrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

2) "Tratamento" - uma operação ou um conjunto de operações efectuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

3) “Limitação do tratamento” - a inserção de uma marca nos dados pessoais conservados com o objectivo de limitar o seu tratamento no futuro;

4) “Definição de perfis” - qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;

5) “Pseudonimização” - o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;

6) “Ficheiro” - qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;

7) “Responsável pelo tratamento” - a pessoa singular ou colectiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;

8) “Subcontratante” - uma pessoa singular ou colectiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;

9) “Destinatário” - uma pessoa singular ou colectiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou dos Estados-Membros não são consideradas destinatários; o tratamento desses dados por

essas autoridades públicas deve cumprir as regras de protecção de dados aplicáveis em função das finalidades do tratamento;

10) "Terceiro" - a pessoa singular ou colectiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade directa do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais;

11) "Consentimento" do titular dos dados - uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou acto positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objecto de tratamento;

12) "Violação de dados pessoais" - uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;

13) "Dados sensíveis" – os dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas, a filiação sindical, os dados genéticos e os dados biométricos tratados simplesmente para identificar um ser humano, os dados relacionados com a saúde e os dados relativos à vida sexual ou orientação sexual da pessoa;

14) "Dados genéticos" - os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que dêem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa;

15) "Dados biométricos" - dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;

16) "Dados relativos à saúde" - dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde.

Artigo 2º

Recolha e tratamento de dados

1. A recolha de dados para tratamento deve processar-se nos termos da legislação em vigor, no estrito cumprimento dos direitos, liberdades e garantias previstos na Constituição da República Portuguesa e efectuar-se de forma lícita, legal e transparente.
2. A recolha de dados pessoais pela Cloud365 deve ser precedida do consentimento dos e da informação aos respectivos titulares sobre a finalidade que a determinou e processar-se em estrita adequação a esse consentimento e a essa finalidade.
3. A Cloud365 e os seus Trabalhadores, bem como os Subcontratantes devem impreterivelmente assegurar que:

   a) o titular dos dados deu previamente o seu consentimento e que o tratamento é efectuado apenas no âmbito das finalidades para as quais os mesmos foram recolhidos, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades;

   b) a recolha, utilização e conservação é realizada apenas sobre os dados pessoais mínimos, necessários e suficientes, para a finalidade respectiva;

   c) a conservação dos dados pessoais é efectuada apenas pelo período de tempo necessário para o cumprimento, quer da finalidade do tratamento que lhe deu origem, quer dos prazos legalmente estipulados para o efeito;

   d) não existe qualquer transmissão de dados pessoais para fins comerciais ou de publicidade, salvo a existência de consentimento expresso por parte dos seus titulares nesse sentido;

   e) o tratamento dos dados pessoais é realizado para fins legalmente previstos ou para a prossecução dos serviços legitimamente contratados;

   f) o tratamento é necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, excepto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a protecção dos dados pessoais, em especial se o titular for uma criança;

   g) os dados pessoais são sempre objecto de um tratamento lícito, leal e transparente em relação ao titular dos dados; e

h) os dados pessoais são tratados de uma forma que garanta a sua segurança, incluindo a protecção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adoptando as medidas técnicas ou organizativas adequadas.

Artigo 3°

Condições aplicáveis ao consentimento

1. O responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.
2. O pedido de consentimento deve ser apresentado de uma forma que o distinga claramente de outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples;
3. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efectuado com base no consentimento previamente dado.

Artigo 4°

Arquivos Físicos

1. A decisão de criação de arquivos físicos só deve ser tomada depois de esgotadas todas as alternativas viáveis de criação dos mesmos arquivos em suporte informático.
2. No caso de ser necessária a criação de arquivos físicos, todos os Trabalhadores da Cloud365 devem respeitar e promover as práticas de salvaguarda e segurança do arquivo por aquela definidas, bem como zelar para que os necessários acessos e níveis de controlo sobre os mesmos sigam critérios coincidentes com o objectivo deste Código e com as instruções da Cloud365, nomeadamente:

   a) Atentar no cuidado com a localização segura, controlada e preferencialmente condicionada ao acesso dos documentos físicos que contenham dados pessoais (papel, suportes informáticos, etc.);

b) Inibir-se de guardar dados pessoais no computador do seu local de trabalho, salvo instruções em contrário dadas por escrito pela Cloud365 e, neste caso, assegurando as medidas de restrição de acesso a esses dados estabelecidas por aquela;

c) Transportar ou transferir fisicamente documentos em suporte papel ou informático, que contenham dados pessoais, unicamente quando tal for estritamente necessário à realização da tarefa em causa e apenas pelo tempo que a mesma perdurar;

d) Cumprir com as orientações internas em matéria de criação, manutenção e destruição das versões de trabalho e cópias dos documentos que contenham dados pessoais.

Artigo 5º

Direito à informação e acesso

A Cloud365 obriga-se a informar os titulares dos dados que recolhe, bem como sobre a respectiva finalidade e a identificar o responsável pelo tratamento

Sempre que solicitado por titulares de dados, e desde que legalmente permitido, a Cloud365 procede à rectificação e actualização dos dados pessoais constantes dos seus ficheiros e bases de dados no prazo máximo de 7 (sete) dias.

Artigo 6º

Eliminação de dados pessoais

Quando um titular dos dados solicitar a eliminação dos mesmos, e desde que legalmente permitido, a Cloud365 dará cumprimento a esse pedido no prazo máximo de 7 (sete) dias a contar do termo legalmente estipulado para o efeito, considerando sempre o maior prazo imposto por lei para a sua conservação.

Artigo 7º

Dados sensíveis

Os dados sensíveis que a Cloud365 tiver, por lei ou por contrato, de recolher, serão guardados sigilosamente e só os Trabalhadores estritamente necessários é que poderão saber da sua existência e ter acesso aos mesmos.

Artigo 8º

Equipamento de segurança

1. A Cloud365 salvaguarda a segurança no tratamento dos dados pessoais, impedindo a consulta, modificação, destruição ou introdução de dados por pessoa não autorizada a fazê-lo.

2. A Cloud365, na prossecução das suas actividades, utiliza um conjunto de procedimentos e tecnologias de segurança destinados à protecção dos dados pessoais, protegendo o acesso ou divulgação não autorizados, nomeadamente através de:

a) Medidas de segurança física, como o controlo de acessos físicos às suas instalações, medidas de segurança contra incêndios, alojamento de equipamentos em centros de dados dedicados, com procedimentos de acesso restritos, e utilização de aplicações online (Software-as-a-Service) cujos prestadores atestem o cumprimento do RGPD;

b) Medidas de segurança lógica:

i) na componente de acessos a sistemas e postos de trabalho através de mecanismos de gestão de identidades, autenticação, privilégios, controlo e registo de acessos;

ii) na componente de rede, o uso de firewalls e segregação de redes (interna, externa, zona desmilitarizada), bem como utilização de canais de comunicação seguros, nomeadamente através da encriptação de informação.

iii) protecção dos dispositivos móveis (computadores portáteis, 'smartphones') com software de proteção contra actividades maliciosas (anti-malware), incluindo antivírus, anti-phishing e firewall.

Artigo 9º

Utilização de recursos informáticos e tecnologias de informação

1. Os Trabalhadores da Cloud365 devem utilizar unicamente o material e os recursos informáticos que lhes são disponibilizados pela mesma, exclusivamente para fins profissionais e de forma diligente, sendo proibida a troca de periféricos, a realização de back ups em suportes não autorizados pela Cloud365 ou a abertura de equipamentos informáticos sem autorização prévia e escrita da Cloud365.
2. A Cloud365 possui um sistema central de directório para gestão das contas e estações de trabalho dos seus Trabalhadores, sendo atribuído a cada um deles uma conta de utilizador e uma palavra-passe, para acesso ao posto de trabalho e demais recursos informáticos da rede interna, de acordo com o respectivo perfil de acesso.
3. É da responsabilidade de cada utilizador a manutenção segura das suas palavras passe que são impreterivelmente pessoais e intransmissíveis.
4. Sempre que possível, será implementado um terceiro factor de autenticação para acesso a Sistemas que alojem dados pessoais.
5. A atribuição ou alteração de acessos à rede e aplicações informáticas da Cloud365 deverá seguir os respectivos procedimentos internos em vigor a cada momento.
6. A detecção de anomalias no funcionamento de equipamentos e aplicações ou suspeitas de malware devem ser de imediato comunicadas à Cloud365.

Artigo 10º

Relações entre a Cloud365 e os subcontratantes na transmissão de dados

1. A Cloud365 apenas transmitirá dados pessoais a terceiros quando for obrigada por lei ou por contrato ou se o seu titular o autorize ou solicite.
2. Sempre que a Cloud365 transmita ou ceda dados pessoais a um subcontratante tem de assegurar que os mesmos sejam utilizados de acordo com a finalidade previamente estabelecida e que as condições de transmissão ou cedência são reduzidas a escrito, designadamente quanto à sua utilização e finalidade.

Artigo 10º

Relações institucionais com a autoridade nacional de controlo

A Cloud365 tem o dever de colaborar com a autoridade nacional de controlo facultando-lhes as informações, sempre que solicitado, e demais documentação relativa à recolha, tratamento automatizado e transmissão.

Artigo 11º

Segredo Profissional

1. Todos os Colaboradores da Cloud365, independentemente do tipo de vínculo existente, bem como os prestadores de serviços e fornecedores, que tratem dados pessoais, estão obrigados ao sigilo profissional sobre os mesmos, nomeadamente de não poder revelar ou utilizar esses dados, excepto nos casos em que a lei o obrigue, nomeadamente quando as entidades públicas devidamente credenciadas para o efeito exijam a transmissão dos dados.
2. O dever de confidencialidade e de sigilo que impende sobre todos os Colaboradores da Cloud365, bem como sobre os prestadores de serviços e fornecedores, não cessa com o termo das funções ou dos serviços prestados.

Artigo 12º

Responsabilidade

1. Todos os Trabalhadores da Cloud365 são responsáveis individualmente pela violação ou transmissão ilegal dos dados pessoais que a Cloud365 possua na sua base de dados ou a que tenha acesso por via contratual, podendo incorrer disciplinarmente pela violação ou transmissão dos dados pessoais a que tenham acesso, devido ou indevido.
2. Esta responsabilidade será aferida de acordo com a gravidade da situação em causa.
3. Os restantes Colaboradores, fornecedores ou prestadores de serviços são responsáveis nos termos contratuais e legalmente estabelecidos.

Artigo 13º

Recepção e tratamento das reclamações

1. Segundo o nº 1 do artigo 33º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente.

Artigo 14º

Violação de dados pessoais

1. Caso o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, susceptível de implicar um risco para os direitos e liberdades das pessoas singulares, deve notificá-la à autoridade nacional de controlo, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma.
2. Não sendo possível cumprir o prazo referido no número anterior, a notificação deve ser acompanhada dos motivos do atraso, podendo as informações serem fornecidas por fases e sem demora devidamente injustificada.
3. Quando se verifique uma situação de violação, deve a Cloud365 abrir um processo de averiguações interno para apurar as causas dessa mesma violação.
4. É dever de todos os Trabalhadores que tenham conhecimento de qualquer situação que possa implicar uma violação de dados pessoais comunicá-la, com carácter de urgência, à Cloud365, através do endereço electrónico admin@cloud365.global ou através de qualquer outro meio mais expedito.
5. Os interessados que pretendam reclamar pela violação dos seus dados, devem fazê-lo directamente à Cloud365 para o endereço electrónico: admin@cloud365.global ou através do 'web site' da Cloud365, se essa facilidade estiver disponível.

Artigo 15°

Esclarecimentos e aplicação do código

Os pedidos de esclarecimento de dúvidas na interpretação ou aplicação do presente Código de Conduta deverão ser dirigidos à Cloud365 para: admin@cloud365.global.

Artigo 16°

Preenchimento de lacunas

A todas as omissões, ao previsto no presente Código de Conduta, será aplicado o estipulado no Regulamento Geral de Protecção de Dados, na Lei n.° 58/2019, de 08 de Agosto, bem como na demais legislação nacional em vigor sobre este assunto.

Artigo 17°

Entrada em vigor

O presente Código de Conduta entrará em vigor no dia 1 de Novembro de 2022.