CÓDIGO DE CONDUTA NO TRATAMENTO DE DADOS PESSOAIS

(ARTIGO 40.º DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS PESSOAIS)

Preâmbulo

O presente Código é elaborado nos termos e para os efeitos do artigo 40.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento sobre a Proteção de Dados), doravante designado por RGPD.

Considera-se que o tratamento dos dados pessoais deve ser concebido para servir as pessoas, sendo premente a aprovação de Código de Conduta pelo Conselho Diretivo do Instituto de Ação Social das Forças Armadas, I. P. (doravante designado por IASFA), destinado a contribuir para a correta aplicação do RGPD.

O artigo 24.º, n.º 3 do RGPD dispõe que o cumprimento de Código de Conduta, aprovado nos termos do artigo 40.º do RGPD, pode ser utilizado como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento.

É também o que sucede, relativamente ao subcontratante, para demonstração de que o subcontratante, a que recorre o responsável pelo tratamento, apresenta garantias suficientes de execução de medidas técnicas e organizativas adequadas para que o tratamento se faça em conformidade com o RGPD (artigo 28.º, n.º 5 do RGPD).

Também o cumprimento dos deveres estabelecidos em matéria de segurança no tratamento dos dados pessoais, a que se refere o artigo 32.º do RGPD, pode ser demonstrado pelo cumprimento de um Código de Conduta (artigo 32.º, n.º 3 do RGPD).

Constata-se deste modo a necessidade de execução de um Código de Conduta na Organização, considerando também que o direito à proteção de dados não é um direito absoluto, que se consubstancia em princípios de proporcionalidade, licitude, transparência, minimização de dados ou exatidão, por vezes de difícil deteção e que este Código de caráter normativo pretende implementar boas práticas e que todos beneficie.

Este Código abrange transversalmente toda a Organização, designadamente as metodologias de trabalho e processos que envolvam o tratamento de dados pessoais, bem como a utilização de materiais ou equipamentos, programas ou *softwares*, canais de comunicação e suportes em papel, aplicando-se tanto ao tratamento de dados automatizados ou manual, independentemente do modo como os dados pessoais são conservados.

É aprovado o Código de Conduta para tratamento de dados pessoais que se rege pelos presentes articulados, enquanto conjunto de princípios e orientações de atuação de todos os trabalhadores, funcionários e dirigentes do IASFA.

CAPÍTULO I
OBJETO E ÂMBITO

Artigo 1.º
Objeto

O presente Código consagra os princípios da atuação e as normas de ética e conduta profissional que devem ser observados pelo Instituto de Ação Social das Forças Armadas, I. P. (IASFA), e por todos os seus trabalhadores, no exercício das suas funções, cuja atividade envolva a recolha, consulta, utilização e qualquer outra forma de tratamento de dados pessoais, incluída no n.º 2 do artigo 4.º do Regulamento Geral de Proteção de Dados (RGPD), aprovado pelo Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.

Artigo 2.º
Âmbito

1- O presente Código aplica-se:

a) A todos os trabalhadores do IASFA, independentemente da natureza do seu vínculo laboral, no âmbito da recolha, do tratamento e da utilização de dados pessoais;

b) Às relações do IASFA, seja com os seus trabalhadores, com os fornecedores externos, com as empresas subcontratadas ou outras partes interessadas.

Artigo 3.º
Definições

1. Para efeitos do presente Código, as definições são as que expressamente constam no RGPD e que se reproduzem:

a) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada,

direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização (como seja o endereço de uma residência), identificadores por via eletrónica (como seja um endereço de correio eletrónico pessoal, dados de localização de um telemóvel [1], endereço de IP ou *cookies*), ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

b) «Tratamento», uma operação ou um conjunto de operações efetuadas 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 interconexação, a limitação, o apagamento ou a destruição;

c) «Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

d) «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;

e) «Dados genéticos», os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem 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;

f) «Dados biométricos», os 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;

g) «Dados relativos à saúde», os 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;

h) «Categorias especiais de dados especiais», os dados pessoais que estão sujeitos a condições de tratamento específicas, concretamente: dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; filiação sindical; dados genéticos,

[1] Importa salientar que, em alguns casos, existe legislação setorial específica que regula, por exemplo, a utilização de dados de localização ou a utilização de *cookies* - Diretiva relativa à privacidade e às comunicações eletrónicas (Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002 e Regulamento (CE) n.º 2006/2004 do Parlamento Europeu e do Conselho, de 27 de outubro de 2004.

dados biométricos tratado simplesmente para identificar um ser humano; dados relacionados com a saúde; dados relativos à vida sexual ou orientação sexual da pessoa; dados relativos a condenações em processos contraordenacionais ou criminais ou ainda suspeita de atividade ilícita; dados de menores (sem consentimento dos titulares das responsabilidades parentais);

i) «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou 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;

j) «Subcontratante», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate de dados pessoais por conta do responsável pelo tratamento destes.

Artigo 4.º
Objetivos

1. O presente Código tem por objetivos:

a) Clarificar e harmonizar os padrões de referência no exercício da atividade de tratamento de dados pessoais;

b) Harmonizar valores, princípios de atuação e normas de conduta que balizem o relacionamento do IASFA com os seus trabalhadores, com os fornecedores externos, com as empresas subcontratadas e com outras partes interessadas em matéria de tratamento de dados pessoais;

c) Promover a cultura organizacional do cumprimento da lei e de conformidade com os valores e procedimentos de auditoria, bem como para a implementação das práticas de conduta ética;

d) O alinhamento com o preconizado para os Códigos de Conduta do RGPD.

Artigo 5.º
Natureza

1. O presente Código de Conduta é parte integrante dos procedimentos internos do IASFA.

2. A observância das regras do presente Código não dispensa os trabalhadores do IASFA do conhecimento e do cumprimento das restantes normas internas, das disposições legais e dos regulamentos em vigor.

CAPÍTULO II

PRINCÍPIOS GERAIS

Artigo 6.º
Princípios gerais

1. Os trabalhadores do IASFA desenvolvem a sua atividade e executam as suas funções em observância dos princípios éticos da Administração Pública, cumprindo e fazendo cumprir as obrigações legais, regulamentares e de conduta a que estão subordinados, nomeadamente o Código de Conduta do IASFA, aprovado por deliberação do Conselho Diretivo em 25 de julho de 2022, instrumento orientador para a atuação quotidiana de todos os trabalhadores, consubstanciando os princípios, as regras e as normas de caráter ético e deontológico, com entrada em vigor na data de 26 de julho de 2022.

2. Os trabalhadores do IASFA no exercício das suas funções devem observar os princípios relativos ao tratamento de dados pessoais constantes no RGPD, nomeadamente os princípios da confidencialidade e do cumprimento dos deveres legais estabelecidos em matéria de tratamento de dados pessoais.

Artigo 7.º
Deveres dos trabalhadores no âmbito da proteção de dados pessoais

1. Os trabalhadores do IASFA, no exercício das suas funções:

a) Atuam de forma idêntica, independentemente da raça, género, saúde, deficiência, convicções políticas ou ideológicas, ou outros princípios consagrados na Constituição da República Portuguesa como direitos fundamentais;

b) Devem garantir aos seus clientes ou beneficiários, aos fornecedores externos, às empresas subcontratadas e a outras partes interessadas, ressalvado o dever de sigilo, uma resposta rigorosa e em tempo às solicitações por estas apresentadas;

c) Devem atuar de boa-fé, com isenção, responsabilidade e rigor;

d) Devem guardar, proteger e conservar sob rigoroso sigilo, todos os dados pessoais de terceiros a que tenham tido acesso no desempenho das suas funções, em particular no que diz respeito a dados pessoais sensíveis;

e) Devem fomentar no IASFA uma política de mesa limpa (*clean desk policy*), por forma a que os dados pessoais não sejam partilhados em sistemas de e-mail, partilha em rede, *smartphones*, plataformas partilhadas, ficheiros locais ou computadores, devendo os documentos em suporte papel, que contenham dados pessoais, ser guardados em espaços fechados (armários, gavetas ou módulos de arquivo), e não devem ser expostos em cima de secretárias quando os

trabalhadores não estão a trabalhar nelas, bem como as salas de arquivo devem encontrar-se fechadas enquanto não estão a ser utilizadas;

f) Devem auditar internamente os processos do IASFA, com proposta de melhoria(s), dever de recomendar, com implementação de um regime baseado no risco;

g) Devem respeitar o princípio da privacidade, assegurando que o tratamento de dados pessoais se enquadra nos fundamentos de licitude estabelecidos e que os direitos dos titulares dos dados são devidamente respeitados, não devendo ser divulgados dados sobre, por exemplo, estado civil, contactos pessoais, moradas, agregado familiar, entre outros;

h) Sempre que, no exercício das suas funções, um trabalhador, funcionário ou dirigente do IASFA colabora no desenvolvimento de qualquer processo ou procedimento que implique o tratamento de dados pessoais, deve ter em conta os princípios de proteção de dados e incluir as garantias necessárias para que o tratamento a efetuar cumpra os requisitos do RGPD e proteja os direitos dos titulares dos dados.

Artigo 8.º
Diligência no tratamento de orientações e reclamações

O IASFA garante que todas as reclamações recebidas de clientes ou beneficiários, de fornecedores externos, de empresas subcontratadas e de outras partes interessadas, referentes a qualquer operação de recolha, tratamento e arquivo de dados pessoais efetuado pelos seus trabalhadores são imediatamente encaminhadas para o Encarregado de Proteção de Dados, para apreciação, decisão e resposta ao reclamante. Procedimento idêntico deve ser adotado para as orientações emitidas pela Autoridade de Controlo nacional.

CAPÍTULO III
REGRAS ESPECÍFICAS

Artigo 9.º
Recolha de dados

1. A recolha de dados pessoais para tratamento pode decorrer de uma obrigação legal, no âmbito da execução de um contrato onde o titular dos dados seja parte ou decorrente do consentimento do seu titular, devendo processar-se no cumprimento da legislação em vigor, bem como no estrito cumprimento dos direitos, liberdades e garantias dos cidadãos.

2. A recolha de dados pessoais e o seu tratamento deve ser efetuada de forma informada, lícita, leal e transparente em relação ao titular dos dados.

3. Sempre que a recolha de dados seja fundamentada no consentimento do seu titular, o IASFA deve garantir que o consentimento foi dado por escrito, podendo ser manifestado via eletrónica ou em suporte papel.

4. O consentimento do titular dos dados deve consubstanciar uma vontade livre, específica, informada e explícita.

5. A recolha de dados pessoais pelo IASFA, como pelas empresas contratadas, junto dos respetivos titulares, é limitada aos dados necessários para cumprimento das finalidades a que se destinam.

6. A recolha referida no número anterior é precedida de informação aos titulares dos mesmos, relativamente à finalidade a que se destinam e de que serão processados de forma adequada e pertinente a essa finalidade.

7. Os trabalhadores do IASFA, e as empresas subcontratadas, devem assegurar:

a) A recolha, a utilização e conservação dos dados, recai apenas sobre os dados pessoais necessários, suficientes e mínimos para a finalidade a que se destinam;

b) O tratamento dos dados realiza-se para os fins legalmente previstos ou para a prossecução de serviços a pedido do titular dos dados, e apenas no âmbito das finalidades para os quais os dados foram recolhidos;

c) A conservação dos dados pessoais efetua-se pelo período de tempo estritamente necessário para o cumprimento da finalidade do tratamento que lhe deu origem;

d) A não existência de qualquer transmissão de dados pessoais para fins comerciais ou de publicidade;

e) O tratamento dos dados pessoais é realizado para fins legalmente previstos ou para a prossecução de serviços *online* a seu pedido;

f) Em caso de partilha de dados, que são utilizados meios que permitam uma rastreabilidade dos acessos;

g) Os dados que não sejam estritamente necessários são apagados;

h) A manutenção dos dados o mais centralizados possível para poder cumprir com os direitos dos titulares de forma ágil;

i) O armazenamento, em local seguro e confidencial, de todos e quaisquer documentos e suportes físicos com dados pessoais;

j) O controlo dos acessos aos documentos com dados pessoais.

Artigo 10.º
Categorias especiais de dados pessoais

1. O IASFA através dos seus trabalhadores compromete-se, a não recolher, conservar ou utilizar, sem prejuízo dos casos em que o tratamento esteja expressamente previsto na lei ou por via contratual, as seguintes categorias de dados pessoais:

a) De menores, sem consentimento dos titulares das responsabilidades parentais;

b) Quando revelem origem racial e étnica;

c) Genéticos, biométricos e médicos;

d) Relativos a condenações em processos contraordenacionais ou criminais ou ainda suspeita de atividade ilícita.

Artigo 11.º
Direito à informação e acesso aos dados

1. O IASFA obriga-se a informar os titulares de dados, sobre a existência de dados pessoais que lhes respeitem, a respetiva finalidade, bem como quaisquer informações obrigatórias decorrentes de lei, sempre que solicitada por escrito, devendo estas solicitações ser encaminhadas para o Encarregado de Proteção de Dados.

2. O IASFA não utiliza bases de dados de clientes ou beneficiários, de fornecedores externos, de empresas subcontratadas e de outras partes interessadas, relativamente às quais não tenha sido previamente autorizada por escrito. Quando autorizada, o seu acesso e utilização serão limitados ao estritamente necessário para cumprir as obrigações contratuais e legais delas decorrentes.

Artigo 12.º
Retificação, atualização e portabilidade de dados

1. Sempre que solicitado por escrito pelo titular dos dados, o IASFA compromete-se a retificar, atualizar, disponibilizar e eliminar os dados constantes dos seus ficheiros, bases de dados e plataformas a eles respeitantes, quando legalmente permitido e sem demora justificada.

2. O pedido de retificação e de atualização de dados deve ser imediatamente encaminhada para o Encarregado de Proteção de Dados e respondido em prazo razoável, não devendo ultrapassar os 60 (sessenta) dias, sendo qualquer atraso objeto de justificação.

Artigo 13.º
Direito ao apagamento de dados

1. Sempre que solicitado por escrito pelo titular dos dados, o IASFA compromete-se a eliminar os dados constantes dos seus ficheiros, bases de dados e plataformas a ele respeitantes, quando legalmente permitido, e sem demora injustificada.

2. Sempre que seja requerida uma limitação do tratamento de dados, não prevista em disposição legal, ou quando a sua eliminação não se enquadre em nenhuma das situações previstas no n.º 1 do artigo 17.º do RGPD, o titular dos dados deve ser notificado das causas de indeferimento do pedido.

Artigo 14.º
Equipamentos e segurança dos dados

1. O IASFA, na prossecução das suas atividades, observa um conjunto de tecnologias e procedimentos de segurança adequados à proteção de dados pessoais, no intuito de preservar e proteger o acesso ou divulgação não autorizados, que se elencam:

a) Medidas de segurança física, como o controlo de acessos físicos de trabalhadores e visitantes às instalações, sistema de videovigilância, medidas de segurança contra incêndios e alojamento de equipamentos em centro de dados dedicado, com procedimentos de acesso restritos;

b) Medidas de segurança lógica, na componente de acessos a sistemas e postos de trabalho através de mecanismos de gestão de identidades, autenticação, privilégios, controlo e registo de acessos; na componente de rede, o uso de *firewalls* e segregação de redes (interna, externa);

c) Cláusulas de garantia de sigilo: em relação a eventuais consultas de dados pessoais na gestão de contratos, em cujo âmbito possa, de forma direta ou indireta, ter acesso aos referidos dados; no cômputo das suas atividades de manutenção corretiva e/ou evolutiva aplicacional ou de infraestruturas, ou de gestão de outros recursos e ativos tangíveis e intangíveis.

Artigo 15.º
Relação com terceiros na transmissão de dados pessoais

1. Desde que não resulte de uma obrigação legal, e o terceiro seja uma entidade pública ou equiparada, o IASFA através dos seus trabalhadores e antes de transmitir qualquer listagem a terceiros, deve assegurar que a mesma apenas diz respeito a dados:

a) Cuja eliminação não lhe tenha sido pedida, ou tendo sido pedida, a mesma tenha sido objeto de indeferimento devidamente fundamentado;

b) Em relação aos quais não tenha sido exercido o direito de oposição à sua transmissão;

c) Quando haja garantia do transmissário relativamente à utilização dos dados no estrito respeito dos fins que determinam a sua recolha, vertida em contrato ou em declaração do titular dos dados;

2. Quando os dados pessoais sejam colocados à disposição ou transmitidos a terceiros, compete ao IASFA estabelecer as condições da sua utilização, mediante acordo escrito ou acordo de confidencialidade, garantindo que se cumprem as obrigações decorrentes do RGPD.

CAPÍTULO IV

RESPONSABILIDADES

Artigo 16.º
Confidencialidade / segredo profissional

1. Os trabalhadores do IASFA, independentemente do tipo de vínculo existente, bem como os fornecedores externos, as empresas subcontratadas e outras partes interessadas que tratem de dados pessoais, estão obrigados a manter sigilo sobre os mesmos, nomeadamente de não poder revelar ou utilizar esses dados, salvo obrigação legal ou decisão judiciária.

2. O dever de confidencialidade e de sigilo que impende sobre os trabalhadores do IASFA, independentemente do tipo de vínculo existente, bem como os fornecedores externos, as empresas subcontratadas e outras partes interessadas que tratem de dados pessoais, não cessa com o termo das funções ou dos serviços prestados, mantendo-se pelo tempo necessário estipulado legalmente ou contratualmente.

3. É expressamente proibida a utilização, disponibilização ou permitido o acesso por qualquer meio, ainda que temporário, a dados pessoais a pessoal não autorizado ou que não necessite deles para uma finalidade definida e no exercício das funções atribuídas.

Artigo 17.º
Responsabilidade

1. Os trabalhadores do IASFA são responsáveis disciplinarmente pela violação ou transmissão ilegal dos dados pessoais a que tenham acesso, devido ou indevido, assim como das orientações constantes do presente Código.

2. Os clientes e beneficiários, os fornecedores externos, as empresas subcontratadas e outras partes interessadas, são responsáveis nos termos contratuais e legalmente estabelecidos.

Artigo 18.º
Violação de dados pessoais

1. Considera-se violação de dados pessoais uma quebra de segurança que provoca, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, de dados pessoais.

2. Quando o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, suscetível de implicar um risco para os direitos e liberdades do titular dos dados, deve notificar a Autoridade de Controlo, sem demora injustificada e, sempre que possível, no prazo máximo de 72 (setenta e duas) horas após conhecimento do ocorrido.

3. No caso de incumprimento do prazo referido no número anterior, a notificação à Autoridade de Controlo deve ser acompanhada dos motivos para o atraso, podendo as informações ser fornecidas por fases e sem demora injustificada.

4. O responsável pela articulação com a Autoridade de Controlo, para estes efeitos, é o Encarregado da Proteção de Dados.

5. Sempre que se verifiquem situações de violação de dados pessoais, deve o IASFA abrir um processo de averiguações interno para apurar as causas que originaram essa situação, sendo o Encarregado de Proteção de Dados atempadamente envolvido e notificado, sempre que haja conhecimento de uma violação de dados pessoais, potencial ou efetiva.

6. É dever de todos os trabalhadores que tenham conhecimento de qualquer situação que possa implicar uma violação de dados pessoais comunicá-la, com caráter de urgência, ao Encarregado de Proteção de Dados, através do endereço eletrónico epd@iasfa.pt, ou qualquer outro meio mais expedito.

7. Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o IASFA deve comunicá-la, sem demora justificada, ao titular dos dados.

8. Todos os trabalhadores, funcionários e dirigentes são responsáveis disciplinarmente pela violação ou transmissão ilegal dos dados pessoais tratados pelo IASFA, sem prejuízo da responsabilidade civil e criminal a que haja lugar.

CAPÍTULO V
AUTORIDADE DE CONTROLO E ENCARREGADO DE PROTEÇÃO DE DADOS

Artigo 19.º
Autoridade de controlo

O IASFA através do seu Encarregado de Proteção de Dados coopera com a Autoridade de Controlo nacional, disponibilizando-lhe informações sempre que solicitado.

Artigo 20.º
Nomeação e competências do Encarregado de Proteção de Dados

1. O Encarregado de Proteção de Dados é nomeado pelo Concelho Diretivo do IASFA, tendo como principais funções:

a) Informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações;

b) Controlar a conformidade nos tratamentos efetuados ao abrigo do RGPD, com outras disposições de proteção de dados da União ou nacionais, e com políticas, do responsável pelo tratamento ou do subcontratante, relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

c) Prestar aconselhamento, quando lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controlar a sua realização;

d) Colaborar com a Autoridades de Controlo.

Artigo 21.º

Posição no IASFA do Encarregado de Proteção de Dados

O IASFA assegura que o Encarregado de Proteção de Dados é envolvido, de forma adequada e em tempo útil, em todas as questões relacionadas com a proteção de dados pessoais.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Artigo 22.º

Esclarecimentos, dúvidas, aplicação e divulgação do Código de Conduta

1. Os pedidos de esclarecimento, dúvidas de interpretação ou de aplicação do presente Código de Conduta, deverão ser dirigidos ao Encarregado de Proteção de Dados, por escrito, através do endereço eletrónico epd@iasfa.pt, ou outras vias, que em função da matéria, responderá ou reencaminhará para resposta à unidade orgânica correspondente.

2- O Encarregado de Proteção de Dados promoverá a divulgação do presente Código de Conduta através da sua inclusão nas páginas e lugares do estilo do IASFA, nomeadamente através dos canais internos e externos, a todos os trabalhadores do Instituto e aos demais interessados, como seja através de *newsletter* interna e externa, redes sociais, *site* do IASFA na internet e intranet.

3. No âmbito da aplicação do presente Código deverá ser promovida a formação dos trabalhadores, o acompanhamento da sua aplicação e a respetiva avaliação, em colaboração com a unidade orgânica que se considerar adequada.

4. Para os trabalhadores com acesso regular a dados pessoais, o IASFA tem por obrigação providenciar sessões periódicas de sensibilização e segurança informáticas.

Artigo 23.º
Direito subsidiário e omissões

1. São subsidariamente aplicáveis ao presente Código de Conduta as disposições no RGPD e a legislação nacional em vigor aplicável.

2. Todas as omissões ao previsto no presente Código de Conduta, aplica-se o estipulado no RGPD, bem como na legislação nacional em vigor.

Artigo 24.º
Entrada em vigor

O presente Código de Conduta entra em vigor na data da sua aprovação pelo Conselho Diretivo e após a sua divulgação nos termos do artigo 22.º, n.º 2 deste Código.