MANUAL DE TRATAMENTO E COMUNICAÇÃO DOS DADOS PESSOAIS E SENSÍVEIS

IReS
INSPEÇÃO REGIONAL DE SAÚDE

MAIO 2022

PREÂMBULO

O Regulamento Geral sobre Proteção de Dados (doravante abreviadamente designado por RGPD), aprovado pelo Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, diretamente aplicável a partir de 25 de maio de 2018, revogou a Diretiva 95/46/CE, operando uma mudança de paradigma no modelo de tratamento de dados pessoais e de livre circulação dos mesmos, com vista à garantia do mercado único sem restrições em virtude do diferente enquadramento legal e salvaguarda do direito à proteção dos dados pessoais.

Assim, o RGPD definiu o novo regime jurídico de proteção de pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados, reforçando a proteção jurídica dos direitos dos titulares dos dados e criando novas obrigações e responsabilidades para todas as entidades públicas e privadas, constituindo a proteção de tais dados um direito fundamental.

Por outro lado, a Lei n.º 58/2019, de 8 de agosto assegurou, na ordem jurídica interna, a execução daquele regulamento, aplicando-se aos tratamentos de dados pessoais realizados no território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento, mesmo que o tratamento de dados pessoais seja efetuado em cumprimento de obrigações legais ou no âmbito da prossecução de missões de interesse público (cf. artigo 1.º e n.º 1 do artigo 2.º da citada Lei).

ÍNDICE

ENQUADRAMENTO DA IReS

A Inspeção Regional da Saúde (IReS) configura-se como um serviço da Secretaria Regional da Saúde e Desporto (SRSD), dotado de autonomia administrativa, estando incumbida de proceder ações de auditoria, fiscalização e controlo na área da saúde. A IReS desenvolve a sua ação em todo o território da Região Autónoma dos Açores, designadamente em todos os domínios da atividade e da prestação dos cuidados de saúde das entidades que integram o Serviço Regional de Saúde, bem como das entidades privadas, singulares ou coletivas, com ou sem fins lucrativos, que prestam cuidados de saúde ou exercem outras atividades no setor da saúde (cf. artigos 43.º e 44.º do DRR n.º 15/2021/A, de 6 de julho).

Este serviço de controlo, auditoria e fiscalização da SRSD tem por missão assegurar o cumprimento da legislação aplicável em vigor em todos os domínios de atividade, bem como na prestação de cuidados, no setor da saúde, visando o bom funcionamento e a qualidade dos serviços, a defesa dos legítimos interesses e bem-estar dos cidadãos, bem como a salvaguarda do interesse público (cf. n.º 1 do artigo 45.º do DRR n.º 15/2021/A, de 6 de julho).

A IReS desenvolve ações inspetivas de acordo com o respetivo plano de atividades previamente aprovado, que incidem sobre entidades do Serviço Regional de Saúde, bem como em relação às entidades privadas, singulares ou coletivas, com ou sem fins lucrativos que prestam cuidados de saúde ou exercem outras atividades neste setor.

Para o sucesso destas ações, que são desenvolvidas por inspetores, estão acometidos alguns poderes instrutórios: a IReS pode, assim, solicitar informações, esclarecimentos ou depoimentos que repute necessários para apuramento de matérias que se inscrevem nas suas competências, dirigindo-se diretamente às instituições do Serviço Regional de Saúde, bem como em relação às entidades privadas, singulares ou coletivas, com ou sem fins lucrativos, que prestam cuidados de saúde ou exercem outras atividades neste setor, tendo tais entidades o dever de colaboração para com a IReS (cf. n.ºs 1 e 2 dos artigos 52.º e 53.º do DRR n.º 15/2021/A, de 6 de julho). Os dirigentes e pessoal da inspeção podem aceder e requisitar para consulta ou junção aos autos, processos ou documentos

existentes nos arquivos clínicos das instituições e serviços, públicos ou privados, que atuem no Serviço Regional de Saúde (cf. n.º 3 artigo 53.º do DRR n.º 15/2021/A, de 6 de julho).

A IReS dispõe ainda de prerrogativa especial, podendo, no âmbito das suas competências e atribuições, conforme expressamente previsto no artigo 5.º do DLR n.º 40/2012/A, de 8 de outubro, aceder aos documentos e informação existentes nos arquivos clínicos das instituições e serviços, públicos ou privados, que atuem no Serviço Regional de Saúde.

Refira-se ainda que os trabalhadores integrados na carreira especial de inspeção encontram-se sujeitos ao dever especial de sigilo profissional, previsto no artigo 7.º do DL n.º 170/2009, de 3 de agosto.

QUADRO NORMATIVO E ORIENTAÇÕES APLICÁVEIS

Para além do RGPD, existe um conjunto de orientações e atos normativos que se mostram necessários ter em conta quando se fala em tratamento de dados pessoais e vicissitudes conexas.

Desde logo, importa não olvidar o Manual de Boas Práticas e a Recomendação n.º 1/2019, ambas do Grupo de Trabalho para o RGPD do Governo Regional dos Açores, criado pela Orientação n.º 1/2018, de 21 de fevereiro. Estes dois instrumentos contêm um conjunto de diretrizes que visam a salvaguarda dos dados pessoais, nas suas múltiplas aceções (recolha, tratamento, etc.), com vista a atingir o desiderato pretendido pela União Europeia com o recurso ao RGPD.

Por outro lado, a Lei n.º 58/2019, de 8 de agosto, assegurou, na ordem jurídica interna, a execução do RGPD, aplicando-se tal ato normativo aos tratamentos de dados pessoais realizados no território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento dos dados. No que tange especificamente ao tratamento de dados de saúde e dados genéticos, o n.º 1 do artigo 29.º deste diploma consagra o *princípio da necessidade*, ao prescrever que nos tratamentos de dados de saúde e de dados genéticos, o acesso a dados pessoais deve nortear-se pela estrita necessidade de conhecer a informação. Nos termos dos números 4 e 5 do mesmo artigo, os titulares dos órgãos, trabalhadores e prestadores de serviços do responsável pelo tratamento de dados de saúde e de dados genéticos, o encarregado de proteção de dados, os estudantes e investigadores na área da saúde e da genética e todos os profissionais de saúde que tenham acesso a dados relativos à saúde, estão obrigados a um dever de sigilo, sendo tal dever igualmente aplicável a todos os titulares de órgãos e trabalhadores que, no contexto do acompanhamento, financiamento ou fiscalização da atividade de prestação de cuidados de saúde, tenham acesso a dados relativos à saúde.

Já a Lei n.º 59/2019, de 8 de agosto, estabelece as regras relativas à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, transpondo para a ordem jurídica interna a Diretiva (UE)

2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Este ato normativo aplica-se ao tratamento de dados pessoais para os efeitos acima referidos, nos termos da lei processual penal e demais legislação aplicável, seja por meios total ou parcialmente automatizados, bem como ao tratamento de dados pessoais contidos num ficheiro ou a ele destinados por meios não automatizados.

ENCARREGADO DE PROTEÇÃO DE DADOS

Uma das principais novidades introduzidas pelo RGPD foi a figura do Encarregado de Proteção de Dados (EPD), o *Data Protection Officer* (DPO). Não sendo uma novidade para diversos países da União Europeia, cuja legislação já contemplava uma figura similar, a imposição de nomeação de um EPD em Portugal assume um especial relevo, pelo papel que este desempenha junto do responsável pelo tratamento dos dados.

O EPD tem o seu regime previsto nos artigos 37.º a 39.º do RGPD, bem como nos artigos 9.º a 13.º da já citada Lei n.º 58/2019, de 8 de agosto. De nomeação obrigatória nas entidades públicas, o EPD assume as vestes de responsável formal pelo cumprimento do RGPD.

O EPD desempenha um papel fulcral, na medida em que lhe compete garantir que a organização, *in casu* a SRS, cumpre todas as obrigações legais do RGPD, sendo o ponto de contacto com a autoridade de controlo nacional – a Comissão Nacional de Proteção de Dados – e funcionando como mediador junto do titular dos dados.

Nos termos do RGPD e da Lei n.º 58/2019, de 8 de agosto, o encarregado de proteção de dados deve:

i. Informar e aconselhar o responsável pelo tratamento, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações no âmbito da proteção de dados pessoais;
ii. Controlar a conformidade com o RGPD e demais disposições de proteção de dados aplicáveis. No âmbito desta função, o EPD deve recolher informações para identificar as atividades de tratamento; analisar e verificar a conformidade das atividades de tratamento; prestar informações e aconselhamento e formular recomendações ao responsável pelo tratamento;
iii. Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto obre a proteção de dados e controlar a sua realização;
iv. Assegurar a realização de auditorias, quer periódicas, quer não programadas;

v. Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança;
vi. Assegurar as relações com os titulares dos dados nas matérias abrangidas pelo RGPD e pela legislação nacional em matéria de proteção de dados.

Assim, ao EPD é atribuída a responsabilidade formal de assegurar que o organismo está devidamente *compliant* com as regras de proteção de dados. Prescreve o RGPD que o EPD deve ser designado com base nas suas competências profissionais, entre as quais se considera essencial um adequado conhecimento da legislação e práticas nacionais e europeias de proteção de dados, conhecimento das operações de processamento realizadas e conhecimento das tecnologias de informação e de segurança dos dados, por forma a promover uma cultura de proteção de dados.

Em suma, o EPD deve ter a capacidade para informar, aconselhar e orientar a organização, bem como os seus trabalhadores, a respeito das obrigações constantes do RGPD, assim como as outras disposições de proteção de dados em vigor da União Europeia ou noutros estados membros.

RGPD: CONCEITOS GERAIS E PRINCÍPIOS

Cumpre dar nota dos conceitos gerais e princípios relativos ao tratamento de dados pessoais. Assim, cabe-nos iniciar pelos conceitos, nomeadamente:

i. ***Dados pessoais*:** toda a informação relativa à identificação ou que possa levar à identificação do seu titular, de forma direta ou indireta; é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, por referencia a um identificador, como por exemplo um nome, número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

ii. ***Tratamento*:** operação ou conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não, 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;

iii. ***Responsável pelo tratamento de dados*:** a pessoa singular ou coletiva, autoridade pública, instituição ou outro organismo que determina as finalidades e os meios de tratamento de dados pessoais e aplica as medidas técnicas e organizativas adequadas para assegurar e comprovar que o tratamento é realizado em conformidade com o regulamento;

iv. ***Consentimento*:** uma manifestação do titular dos dados, livre, específica, informada e explícita, pelo qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

v. ***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;

vi. ***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.

Em relação aos princípios relativos ao tratamento de dados pessoais, há que ter em consideração, designadamente, os seguintes:

i. ***Licitude, lealdade e transparência*:** os dados pessoais são objeto de tratamento lícito, leal e transparente em relação ao titular dos dados;
ii. ***Limitação das finalidades*:** os dados pessoais são recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades;
iii. ***Minimização de dados:*** os dados pessoais recolhidos são adequados, pertinentes e limitados ao que é necessário relativamente à finalidade do tratamento;
iv. ***Exatidão***: os dados pessoais devem ser exatos e atualizados sempre que necessário;
v. ***Limite da conservação***: os dados pessoais serão conservados apenas durante o tempo necessário para as finalidades que foram recolhidos;
vi. ***Integridade e confidencialidade***: os dados pessoais devem ser tratados de forma que garanta a sua segurança e proteção, incluindo proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental;
vii. ***Responsabilidade***: o responsável pelo tratamento de dados pessoais tem a obrigação de garantir os princípios colocados e deve poder comprovar esta garantia.

DIREITOS DOS TITULARES DOS DADOS

O RGPD tem como objetivo primordial garantir o funcionamento do mercado único para o qual os distintos regimes de proteção de dados pessoais se configuravam como um verdadeiro obstáculo. Assim, o RGPD dedica a sua parte inicial – todo o Capítulo III – à consagração dos direitos fundamentais dos titulares dos dados.

Neste sentido, os titulares dos dados pessoais têm o direito à informação (finalidades, responsável do tratamento, prazo de conservação, etc.), o direito ao acesso, retificação, ao esquecimento, à portabilidade dos dados, a limitar ou opor-se ao tratamento dos seus dados pessoais, bem como a apresentar reclamação junto à autoridade de controlo e a recorrer jurisdicionalmente.

A IReS deverá assegurar os direitos dos titulares em matéria de proteção de dados pessoais e facilitar o exercício dos mesmos, nomeadamente, dispondo de minutas para o efeito. Assim, mostra-se necessário que se tomem medidas no sentido de garantir que a pessoa que pretende exercer os seus direitos sobre os dados é, realmente, o titular dos mesmos. Neste sentido, se a IReS tiver dúvidas razoáveis quanto à identidade da pessoa que apresenta o pedido, poderá solicitar as informações adicionais necessárias para confirmar a sua identidade.

DIREITO À INFORMAÇÃO

Um dos direitos mais importantes dos titulares dos dados é o direito à informação, direito que permite que o titular dos dados seja informado quanto a todos os dados relevantes sobre o tratamento de dados – quem é o responsável de tratamento, o encarregado de proteção de dados e os seus contactos (DPO), a finalidade do tratamento e prazo de conservação, bem como os seus direitos e a forma como pode exercê-los – devendo tais informações serem prestadas no momento da recolha dos dados junto do seu titular, através da *minuta n.º 2*, em anexo ao presente manual, da qual faz parte integrante, que deverá conter informação condensada sobre:

a) Identidade e contactos do responsável pelo tratamento;
b) As finalidades do tratamento e o respetivo fundamento jurídico;
c) Os destinatários ou categorias de destinatários dos dados pessoais;
d) O prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
e) Os direitos que goza o titular dos dados e como poderá exercê-los;
f) O direito de apresentar reclamação a uma autoridade de controlo.

DIREITO DE ACESSO

A qualquer momento, o titular dos dados tem o direito de obter da IReS a confirmação de que os dados pessoais que lhe dizem respeito são ou não objeto de tratamento e, se for esse o caso, tem o direito de aceder aos seus dados e às informações abaixo elencadas, devendo utilizar a *minuta n.º 1*, em anexo ao presente manual, da qual faz parte integrante:

a) As finalidades do tratamento dos dados;
b) As categorias dos dados pessoais em questão;
c) Os destinatários ou categorias de destinatários dos dados pessoais;
d) O prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
e) Os direitos que são conferidos ao titular dos dados ao abrigo do RGPD;
f) O direito de apresentar reclamação a uma autoridade de controlo;
g) A origem dos dados pessoais, caso a recolha não se tenha verificado junto do titular.

Estas informações podem ser fornecidas por escrito, eletronicamente ou, se assim solicitado, prestadas oralmente.

DIREITO DE RETIFICAÇÃO

O titular dos dados tem o direito de obter da IReS, sem demora injustificada, a retificação dos dados pessoais inexatos que lhe digam respeito, bem como o direito a que os seus dados incompletos sejam completados, devendo a IReS facultar a *minuta n.º 1*, em anexo ao presente manual, da qual faz parte integrante.

A IReS deve comunicar a retificação a entidades terceiras a quem os dados pessoais foram transmitidos, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado. Caso o titular dos dados assim o solicite, o responsável pelo tratamento fornece-lhe informações sobre os referidos destinatários.

DIREITO DE PORTABILIDADE DOS DADOS

A IReS deverá assegurar que quando o tratamento dos dados pessoais se basear no consentimento do titular e se realizar por meios automatizados, o titular tem direito, utilizando para o efeito a *minuta n.º 1*, em anexo ao presente manual, da qual faz parte integrante, a:

a) Receber os seus dados pessoais que foram objeto de tratamento e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e leitura automática;
b) Transmitir esses dados a outro responsável pelo tratamento, sem que o responsável a quem os dados foram fornecidos o possa impedir.

DIREITO À OPOSIÇÃO

O titular dos dados tem direito, a qualquer momento, de se opor ao tratamento dos seus dados por motivos relacionados com a sua situação particular, devendo para o efeito ser utilizada a *minuta n.º 1*, em anexo ao presente manual, da qual faz parte integrante.

DIREITO AO ESQUECIMENTO/APAGAMENTO

O titular dos dados pode solicitar que os seus dados possam ser totalmente apagados, sem demora injustificada e, neste sentido, a IReS deverá proceder ao apagamento dos mesmos, devendo ser utilizada para o efeito a *minuta n.º 1*, em anexo ao presente manual, da qual faz parte integrante.

Este direito apenas poderá ser concedido ao titular nas seguintes situações:

a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha e tratamento;

b) O titular dos dados pessoais retirou o consentimento no qual se baseia o tratamento dos dados pessoais, não existindo qualquer outro fundamento jurídico que justifique o tratamento dos mesmos;
c) O titular exerce o direito de oposição ao tratamento dos seus dados pessoais, por motivos relacionados com a sua situação particular;
d) Existe uma obrigação jurídica para o apagamento dos dados pessoais;
e) Quando tiver sido ultrapassado o período de conservação definido para os dados.

DIREITO À LIMITAÇÃO DO TRATAMENTO

Associado ao direito de apagamento e precisamente para dar resposta aos casos de impossibilidade de proceder ao apagamento dos dados, o titular dos dados tem o direito de solicitar à IReS a limitação do tratamento dos seus dados pessoais, através da *minuta n.º 1*, em anexo ao presente manual, da qual faz parte integrante, quando se verifiquem as seguintes situações:

a) Quando o titular contestar a exatidão dos seus dados, aplicando-se a aplicação do tratamento durante o período necessário à verificação, pelo responsável, daquela exatidão;
b) O tratamento dos dados for ilícito e o titular dos dados se opuser ao seu apagamento, solicitando antes a limitação do tratamento;
c) Quando os dados pessoais já não sejam necessários para fins de tratamento, mas sejam requeridos pelo titular dos dados para efeitos de declaração, exercício ou defesa de um direito num processo judicial;
d) Quando o titular se tiver oposto ao tratamento dos seus dados pessoais, este deverá ser limitado até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

BOAS PRÁTICAS

Por forma a dar cumprimento às exigências do RGPD importa que os colaboradores da IReS adotem um conjunto de boas práticas no exercício das suas funções. Neste sentido, todos os trabalhadores devem garantir a confidencialidade e a segurança do tratamento dos dados pessoais no decorrer das suas atividades profissionais, de modo a prevenir-se, igualmente, contra acessos ou divulgações não autorizadas, consulta, alteração, cópia ou eliminação de dados pessoais de forma indevida ou ilícita. Cada trabalhador é individualmente responsável por respeitar as políticas de privacidade e segurança preconizadas, devendo adotar as seguintes práticas[1]:

RESPONSABILIZAÇÃO E COMPROMISSO

De modo a assegurar a adoção das medidas propostas neste manual, é necessária uma responsabilização clara, firme e eficaz a este objetivo e ao seu cumprimento, que envolva diretamente o dirigente máximo do serviço. Assim, a implementação das medidas propostas depende do compromisso e da assunção de responsabilidades de cada elemento envolvido por parte de todos os trabalhadores que procedam ao tratamento de dados pessoais.

Ademais, reveste especial atenção o pessoal informático da SRSD que presta apoio à IReS, na medida em que pelo exercício das suas funções poderão tomar contacto com dados pessoais e/ou sensíveis, designadamente dados de saúde. Para o efeito, deverão os colaboradores informáticos, enquanto elementos externos à IReS, subscrever uma declaração de compromisso de confidencialidade nos termos da *minuta n.º 4*, em anexo ao presente manual, da qual faz parte integrante.

Os trabalhadores envolvidos na adoção das medidas propostas neste manual, devem ter um comportamento proativo na identificação de situações ou processos envolvendo operações de tratamento de dados pessoais que possam não estar conformes, bem como

[1] Cf. *Manual de Boas Práticas* e *Recomendação n.º 1/2019*, ambos do Grupo de Trabalho para o RGPD do Governo Regional dos Açores, criado através da Orientação n.º 1/2018, do Presidente do Governo dos Açores, de 21 de fevereiro de 2018.

sugerir medidas no âmbito da sua atividade que promovam a correção das situações identificadas.

CONTROLO DE ACESSOS FÍSICOS ÀS INSTALAÇÕES

a) Aquando do acesso de visitantes deve ser efetuado o registo na portaria (entrada principal do Solar dos Remédios), bem como a confirmação da visita/reunião com o respetivo destinatário interno.
b) Devem existir zonas neutras de acesso, tais como salas de espera e de reuniões de trabalho com elementos externos à IReS.

SEGURANÇA FÍSICA DOS PROCESSOS

a) Todos os processos, *dossiers*, capas e documentos contendo dados pessoais devem ser arquivados em armários fechados com chave.
b) Todos os processos devem ser guardados num local seguro, que assegure a sua integridade, confidencialidade, fiabilidade e autenticidade, garantindo ao nível da segurança a prova de invulnerabilidades, perda, furto e destruição.
c) Todos os trabalhadores da IReS devem adotar uma política de secretária limpa, devendo o posto de trabalhar estar organizado, por forma a que não haja impressos ou suportes digitais móveis (*ex.: pen*, CD-ROM, *etc.*), com dados pessoais, chaves de arquivos físicos ou senhas de acesso a sistemas informáticos que possam ser alvo de acesso indevido por terceiros.
d) Cada trabalhador é responsável pelos documentos/processos que lhe são confiados, pelo que não os podem deixar em cima da secretária sem qualquer vigilância, ou em outro local onde não consiga garantir o sigilo.
e) Não podem ser utilizadas fotocópias que contenham dados pessoais como folhas de rascunho ou para outras finalidades, pois pode ocorrer a sua dispersão e o acesso ser facilitado a terceiros.
f) As impressões e/ou cópias de documentos contendo dados pessoais devem ser limitadas ao estritamente necessário.
g) Todos os trabalhadores da IReS devem garantir que nenhuma impressão e/ou cópia fica esquecida na impressora/fotocopiadora.

h) Devem ser destruídos e sempre que possível triturados, os documentos contendo dados pessoais que não sejam necessários arquivar, incluindo as fotocópias utilizadas apenas como instrumento de trabalho que contenham dados pessoais.
i) A transmissão, transferência e transporte de documentos contendo dados pessoais, quer entre diferentes serviços dentro de um mesmo edifício quer entre diferentes instalações, quando realizado em suporte físico, deve ser devidamente protegida, em envelope apropriado para o efeito e identificado como confidencial (se possível com uma caracterização específica) de modo a impedir o acesso não autorizado ao seu conteúdo.
j) A informação que contenha dados pessoais em suporte de papel deve ser remetida por protocolo ou por correio registado ou por correio registado com aviso de receção, sendo estas as três formas de garantir a segurança dos dados.
k) Na distribuição e transporte realizado por colaboradores internos, os envelopes que contenham documentos com dados pessoais devem estar permanentemente sob o controlo da pessoa que os transporta, devendo ser evitada a circulação desnecessária dos processos e documentos que contenham dados pessoais.

CONTROLO DE ACESSO À REDE INFORMÁTICA

a) Cada trabalhador deve tomar as precauções necessárias para evitar o acesso de terceiros aos sistemas.
b) As redes *wi-fi* disponibilizadas nas instalações que possibilitem a ligação à RAGRA devem usar encriptação forte e autenticação centralizada e individual.
c) As credenciais únicas de acesso aos sistemas (*username* e *password*) não podem ser partilhadas, nem definidas de forma facilmente identificável.
d) Não podem ser utilizadas as mesmas credenciais de acesso ao GRA em *sites* ou serviços externos.
e) Para garantir a segurança das credenciais de acesso, deve proceder-se à alteração das mesmas com regularidade, ou quando a alteração for exigida e/ou quando se suspeite do comprometimento das mesmas.
f) Devem ser tomadas precauções no início de sessão dos sistemas em aplicações ou base de dados, devendo o trabalhador certificar-se, por exemplo, de que não há pessoas próximas que consigam visualizar as credenciais utilizadas.

g) Nas situações em que é necessário abandonar a estação de trabalho, deve ser ativado manualmente o bloqueio de ecrã e, no final do dia, encerrada a sessão de trabalho.
h) O acesso remoto às aplicações do GRA não deve ser efetuado a partir de equipamentos e/ou redes de acesso público.
i) O trabalhador não pode tentar aceder a aplicações informáticas e outros recursos cujas permissões não lhe tenham sido previamente atribuídas.
j) Relativamente a pessoas não autorizadas, é proibido proporcionar o acesso ou revelar informação não só sobre os dados pessoais tratados, mas também relativa aos procedimentos de tratamentos de dados e às tecnologias de informação.
k) Não devem ser ignorados os alertas de segurança do sistema, nem podem ser instalados *softwares* ou executadas aplicações de origem desconhecida, com o objetivo de se evitarem códigos maliciosos.
l) Os trabalhadores não devem ter privilégios de administração do posto de trabalho.
m) Não podem ser efetuadas configurações de *hardware* e/ou *software* do sistema sem autorização prévia.
n) Os trabalhadores que utilizem equipamentos portáteis são responsáveis por salvaguardar o acesso de terceiros aos mesmos e devem notificar de imediato os serviços de informática em caso de perda ou roubo.
o) Os trabalhadores que utilizem equipamentos portáteis devem evitar que os mesmos se conectem a redes *wi-fi* não seguras (abertas), devendo ser implementados, sempre que possível, sistemas de encriptação nos equipamentos portáteis da IReS/GRA.
p) A transmissão e transferência de dados em suporte digital móvel, quer entre diferentes serviços de um mesmo edifício quer entre diferentes instalações, deve ser efetuada em dispositivos eletrónicos de armazenamento (*ex.:* CD, USB Flash Drives, Hard Disks, SSD) com cifragem e autenticação. Os dados pessoais devem estar permanentemente sob o controlo das pessoas que os transporta.

CONTROLO DE ACESSO APLICACIONAL

a) Documentos referentes a processos de recursos humanos que contenham dados pessoais – concursos, requerimentos, documentos de identificação, *curriculum*

vitae, atestados médicos, licenças, férias, justificação de faltas, horas extraordinárias, ações disciplinares, contencioso, entre outros – devem ser tramitados em papel ou por correio eletrónico. Caso sejam enviados por correio eletrónico, devem ser integrados no processo físico e o correio eletrónico eliminado.

b) No que concerne à utilização do correio eletrónico, não utilizar o correio eletrónico profissional para tratar de assuntos particulares, nem de forma contrária às orientações e mecanismos de segurança do organismo.
c) O envio de correio eletrónico de âmbito geral (ex.: *newsletters*, convocatórias, informações de carácter geral) para múltiplos endereços de correio eletrónico deve ser efetuado utilizando o campo BCC, por forma a não expor todos os destinatários.
d) Sempre que possível, a tramitação por correio eletrónico de processos que envolvam dados pessoais deve ser evitada. Nos casos em que seja necessário, o correio eletrónico deve ser dirigido a um único destinatário, que após processamento do seu conteúdo deve eliminá-lo.
e) Não podem ser abertos anexos de correio eletrónico executáveis nem devem ser exploradas hiperligações ou anexos desconhecidos.
f) Correio eletrónico que redirecione para *sites* externos ao GRA, solicitando autenticação com credenciais do GRA, deve ser reencaminhado para os serviços de informática, devendo também ser reencaminhado o correio eletrónico potencialmente malicioso.
g) Sempre que haja acesso remoto ao correio eletrónico do GRA, o trabalhador deve verificar que terminou com sucesso a sessão remota.
h) O acesso (incluindo o remoto) às máquinas da IReS pelos responsáveis da informática deverá ser realizado com prévio consentimento do trabalhador em causa e preferencialmente na presença do mesmo.
i) O acesso à caixa de correio eletrónico, com fundamento em ausência, apenas deve ocorrer por razões imperiosas e tem de ser claramente explicitado, e previamente comunicado ao trabalhador.
j) A disponibilização pública, nomeadamente em portais e páginas *online*, de informação, conteúdos ou documentos contendo dados pessoais que possibilitam

a identificação dos titulares (incluindo fotografias) deve ser realizada em respeito para com o disposto no RGPD e demais legislação aplicável.

k) Tal disponibilização pública deve ter fundamento jurídico, ser devidamente justificada, evidenciando a licitude do tratamento e se necessário salvaguardar a obtenção de eventuais autorizações.

ATENDIMENTO TELEFÓNICO

a) Não devem ser transmitidas informações sobre os trabalhadores da IReS limitando-se apenas à respetiva disponibilidade. No caso de indisponibilidade deve ser solicitado que se deixe recado e não deverá ser prestada nenhuma informação sobre a localização do trabalhador ou a sua ausência do edifício.
b) Todos os registos em suporte de papel, dos contactos telefónicos recebidos pelo serviço de atendimento telefónico têm de ser triturados após a conclusão da finalidade da recolha.

RECOLHA DE REGISTO DE ÁUDIO

a) Deverá ser facultada a informação relativa à finalidade do recurso a dispositivo de registo áudio ao titular dos dados, no âmbito dos processos, designadamente através da *minuta n.º 2*, em anexo ao presente manual, da qual faz parte integrante.
b) Quando cessar a finalidade que motivou o registo e tratamento da informação de dados, o responsável pelo processo, na presença de trabalhador da IReS e do próprio titular dos dados se assim o solicitar deverá proceder à destruição do registo, através da *minuta n.º 3*, em anexo ao presente manual, da qual faz parte integrante.

VIOLAÇÃO DAS MEDIDAS DE PROTEÇÃO DE DADOS PESSOAIS

a) Deve ser garantida a integridade e a confidencialidade dos dados pessoais, devendo ser comunicado de imediato ao dirigente máximo do serviço qualquer situação ou erro que as viole, com vista à sua imediata correção.

b) Deve ser imediatamente reportado ao dirigente máximo do serviço qualquer comportamento suspeito ou violação de segurança, incluindo pessoal, *hardware*, *software* e aplicações, comunicações, documentos ou segurança física.
c) Caso se verifiquem fugas de informação ou quebras de segurança de dados pessoais, estas devem ser reportadas de imediato ao dirigente máximo do serviço, o qual deve solicitar o envolvimento do Encarregado de Proteção de Dados.

BIBLIOGRAFIA

MAGALHÃES, FILIPA MATIAS/ PEREIRA, MARIA LEITÃO, *Regulamento Geral de Proteção de Dados. Manual Prático*, Vida Económica, 2.ª ed., revista e ampliada, 2018

SALDANHA, NUNO, *Novo Regulamento Geral de Proteção de Dados*, FCA-Editora de Informática, 2018

DOCUMENTOS DE RELEVO

Manual de Boas Práticas e *Recomendação n.º 1/2019*, ambos do Grupo de Trabalho para o RGPD do Governo Regional dos Açores, criado através da Orientação n.º 1/2018, de Sua Excelência o Presidente do Governo dos Açores, de 21 de fevereiro de 2018.

ANEXOS

- *Minuta n.º 1* – Requerimento para Exercício dos Direitos do Titular dos Dados;
- *Minuta n.º 2* – Declaração de Consentimento Tratamento de Dados Pessoais na IReS;
- *Minuta n.º 3* – Auto Destruição Ficheiro Áudio;
- *Minuta n.º 4* – Declaração de compromisso de confidencialidade.

Minuta n.º 1

GOVERNO DOS AÇORES

Requerimento para Exercício dos Direitos do Titular dos Dados

Nos termos Regulamento Geral sobre a Proteção de Dados (RGPD)

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho da União Europeia, de 27 de abril de 2016

Eu, _____, titular do documento de identificação nº_____, considerando os meus dados pessoais recolhidos e sujeitos a tratamento pela V/ Entidade, venho por este meio, nos termos dos arts. 12.º a 22.º do Regulamento Geral sobre a Proteção de Dados, exercer o seguinte direito (assinalar com X):

O direito a ser informado	
O direito de acesso aos seus dados	
O direito à retificação dos seus dados	
O direito ao esquecimento/apagamento	
O direito à limitação do tratamento	
O direito à oposição	
O direito à portabilidade dos dados	
Direitos de oposição a decisões individuais automatizadas, incluindo a definição de perfis	

Pretendo que o direito seja exercido da seguinte forma:

_____

_____

_____

Para dar cumprimento ao direito por mim exercido dou expressamente consentimento para utilização do meu e-mail_____ para posterior notificação ou qualquer outra informação relacionada com este formulário e autorizo a conservação da cópia digitalizada do mesmo pela V/ Entidade, nos prazos legais definidos, e para efeitos do cumprimento do disposto no RGPD.

_____ , ☐☐☐☐ / ☐☐ / ☐☐

_____

Assinatura
(Conforme B.I./Cartão de Cidadão)

A PREENCHER PELO SERVIÇO

Identificação do Serviço _____ Local_____

Rececionei o presente requerimento e comprovei a identidade do titular dos dados através do respectivo documento de identificação, conforme disposto no Regulamento Geral sobre a Proteção de Dados.

(O funcionário)

_____

Minuta n.º 2

DECLARAÇÃO DE CONSENTIMENTO

TRATAMENTO DE DADOS PESSOAIS NA IReS

Eu, _____, autorizo a Inspeção Regional da Saúde (IReS) a proceder à recolha, utilização, registo e tratamento dos meus dados pessoais, no âmbito do processo de _____ n.º _____ – _____*(assunto)* – nos termos do Regulamento Geral sobre Proteção de Dados (RGPD).

Declaro, ainda, que fui informado das seguintes questões:

1. **Que dados são recolhidos e tratados**

Os dados recolhidos no âmbito do processo de _____ (*inquérito/auditoria/inspeção/…*) são os estritamente necessários ao desenvolvimento do mesmo.

2. **Finalidades da recolha dos dados**

Os dados pessoais são utilizados e tratados apenas para a finalidade do processo de _____ n.º _____ – _____*(assunto)*, bem como para efeitos de eventual participação às ordens profissionais visadas no processo e Ministério Público.

2.1 Finalidades da recolha de registo áudio

O eventual recurso a dispositivo de gravação de áudio, no âmbito das inquirições, tem a única finalidade de posterior transcrição para suporte escrito – *Auto de Inquirição de Testemunha*. Uma vez o auto assinado, o respetivo ficheiro de áudio será eliminado pelo responsável do processo na presença de trabalhador da IReS e do próprio declarante se assim o solicitar.

3. **Direitos do titular dos dados pessoais**

O titular dos dados tem o direito de, a todo o tempo, exercer o direito de acesso, retificação, atualização e apagamento dos seus dados pessoais (direito a ser esquecido), podendo ainda opor-se ao tratamento dos mesmos, mediante pedido escrito dirigido à IReS.

4. Conservação dos seus dados pessoais

Os dados pessoais recolhidos pela IReS são armazenados pelo período necessário ao cumprimento das finalidades previstas no ponto 2, da presente declaração.

Para os devidos efeitos, declaro que a informação que forneço é correta e verdadeira, autorizando o tratamento dos dados e aceito o acesso aos mesmos pelos trabalhadores da IReS que desenvolvam quaisquer atividades necessárias para os fins relacionados com o processo de _____ n.º _____ – _____*(assunto)*.

Por ser verdade, dato e assino a presente declaração.

Angra do Heroísmo, __ de _____ de 20__

_____

Minuta n.º 3

AUTO DESTRUIÇÃO FICHEIRO ÁUDIO

Aos ____ dias do mês de _____ de dois mil e _____, procedeu-se à eliminação do ficheiro áudio "_____", do gravador da IReS (equipamento inventariado sob o número _____), considerando a assinatura do *Auto de Inquirição de Testemunha* pelo declarante _____ e pelo instrutor/responsável pelo processo de _____ n.º _____ – _____*(assunto)*, nos termos do ponto 2.1 da *Declaração de Consentimento Tratamento de Dados Pessoais na IReS*.

Angra do Heroísmo, __ de _____ de 20__

O instrutor,

_____

A trabalhadora,

_____

Minuta n.º 4

DECLARAÇÃO DE COMPROMISSO DE CONFIDENCIALIDADE

(Identificação completa, cargo, função, tarefa), no âmbito da colaboração técnica com a IReS, declara ter pleno conhecimento dos deveres a que se encontra adstrito, designadamente no que tange ao acesso e/ou divulgação de dados informáticos – via Sistema de Gestão de Correspondência (SGC), correio eletrónico, acesso (inclusive o remoto) às máquinas da IReS, e outras aplicações do domínio informático – no âmbito dos processos deste serviço inspetivo, nos termos do n.º 1, do artigo 21.º do Decreto-Lei n.º 276/2007, de 31 de julho, na sua redação atual, e aplicado na Região Autónoma dos Açores por força do Decreto Legislativo Regional n.º 40/2012/A, de 8 de outubro, comprometendo-se, em conformidade, a guardar absoluto sigilo sobre as matérias de que tiverem conhecimento no exercício das suas funções ou por causa delas, não podendo divulgar ou utilizar em proveito próprio ou alheio, diretamente ou por interposta pessoa, o conhecimento assim adquirido, mesmo após a cessação das funções.

A violação do sigilo profissional pode implicar a aplicação de sanções disciplinares, determináveis em função da sua gravidade, sem prejuízo da responsabilidade civil ou criminal que dela possa resultar.

Local

Data

Assinatura