REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

CÓDIGO DE CONDUTA.

VISEU, 04 DE DEZEMBRO DE 2023

APCV – Associação de Paralisia Cerebral de Viseu

CÓDIGO DE CONDUTA

1. Proteção dos dados pessoais

A proteção conferida pelo Regulamento Geral de Proteção de Dados, de ora em diante RGPD, "aplica-se ao tratamento de dados efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente do tratamento ocorrer dentro ou fora da União."

Esta proteção deve ser garantida, não só pelas Autoridades Nacionais, mas também por um responsável em cada empresa e/ou Instituição, que deverá garantir a efetividade dos direitos dos titulares dos dados pessoais, e o cumprimento escrupuloso do RGPD.

A defesa dos direitos e liberdades dos titulares dos dados exige uma repartição das responsabilidades dentro das empresas e/ou Instituições.

O tratamento de dados pessoais deve ser feito de forma lícita e equitativa, na medida do estritamente necessário, de forma a garantir a segurança da rede e das informações.

É nesta medida que cumpre à APCV – Associação de Paralisia Cerebral de Viseu, de ora em diante APCV, a elaboração do presente Código de Conduta, relativamente à Proteção de Dados Pessoais que visa definir as linhas orientadoras da APCV e os princípios que devem reger a atuação de todos os trabalhadores/colaboradores.

A APCV adota políticas e procedimentos consistentes com os valores que defende, e de acordo com os padrões e estratégias que tem vindo a assumir.

2. Âmbito e Objetivos

O Código de Conduta elaborado no âmbito do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 - Regulamento Geral sobre a Proteção de Dados (RGPD), visa consagrar e estabelecer procedimentos e normas de conduta profissional a respeitar no exercício das atividades de recolha, tratamento, conservação e eliminação dos dados pessoais.

O presente Código estabelece os princípios deontológicos e profissionais a observar por todos os trabalhadores/colaboradores da APCV, no desempenho das suas funções profissionais e contratuais, dentro da Instituição e/ou em representação da mesma.

- O Código pretende ainda comprovar que todas as medidas tomadas dentro da APCV e todas as políticas já adotadas, garantem um nível de Proteção de Dados exigido pelo

RGPD.

- As regras e condutas a adotar, estabelecidas no presente Código, têm carater geral e obrigatório, e o seu incumprimento poderá constituir infração passível de procedimento disciplinar no interior da APCV.

3. Regras e Procedimentos

- Consideram-se trabalhadores/colaboradores, para efeitos do presente Código, todos os que tenham com a APCV uma relação de trabalho, estágio, prestação de serviço, voluntariado ou outra equiparável.
- Todos os trabalhadores/colaboradores da APCV, que tratem dados pessoais, são individualmente responsáveis pelo cumprimento das disposições legais e regulamentares aplicáveis, nomeadamente, no que toca ao cumprimento das obrigações previstas no RGPD.
- Os membros da Direção, e dos restantes Corpos Sociais da APCV, além de estarem obrigados ao cumprimento das regras e procedimentos relativos à Proteção de Dados, têm a responsabilidade de implementar estruturas e garantir recursos adequados ao bom funcionamento e respeito pelas normas do RGPD.
- Os Responsáveis de cada Departamento, Resposta Social e Serviço da APCV, devem garantir que os procedimentos desenvolvidos no âmbito das suas atividades cumprem as regras do RGPD, e ter um papel ativo e dinâmico junto dos seus trabalhadores/colaboradores, para incentivar o cumprimento do mesmo.
- Os trabalhadores/colaboradores têm obrigação de garantir a confidencialidade dos dados, como parte indissociável das suas funções previstas no contrato de trabalho e no respetivo conteúdo funcional. Devem proceder em conformidade com toda a informação e formação recebida e cumprir todas as orientações definidas no Regulamento. O não cumprimento destas obrigações pode ter consequências disciplinares.
- Os trabalhadores/colaboradores devem estar sensibilizados para o tema em questão e devem cooperar ativamente para o cumprimento do RGPD.
- Todas as falhas no âmbito do RGPD devem ser reportadas ao DPO.
- Mediante aprovação da Direção, o DPO pode, no âmbito das suas funções, determinar a implementação de novas medidas, em qualquer área da APCV, devendo para este fim

dispor de controlos e acessos adequados, e do apoio de todas as áreas envolvidas.

4. Entidade Responsável pelo Tratamento

- A entidade responsável pelo tratamento dos dados que nos confia é:

  APCV – Associação de Paralisia Cerebral de Viseu
  Quinta de Belém, Lote 24 – Vildemoinhos
  3510-779 Viseu
  Telefone: 232 410 020
  E-mail: info@apcviseu.org.pt

5. O Encarregado de Proteção de Dados

- De forma a garantir o Regulamento Geral sobre a Proteção de Dados, a APCV designou um Encarregado de Proteção de Dados (DPO).
- O Encarregado de Proteção de Dados pode ser contactado para esclarecimento de qualquer questão relacionada com tratamento de dados pessoais através do endereço de e-mail privacidade@apcviseu.org.pt
- O DPO é uma figura autónoma e independente que propicia a eficácia das respostas às solicitações e reclamações que possam ser apresentadas pelos titulares dos dados, bem como, uma maior eficácia na resposta a dúvidas e necessidades operacionais dos trabalhadores/colaboradores, no desempenho da sua função.

6. Princípios Fundamentais

Os destinatários do presente Código devem desenvolver a sua atividade no respeito pelos seguintes princípios:

- **LEGALIDADE** – todos os procedimentos adotados dentro da APCV têm de estar em conformidade com o RGPD;
- **BOA FÉ** – as relações dentro da APCV baseiam-se na confiança e na atuação correta e leal, com adequado sentido de cooperação;
- **LEALDADE E TRANSPARÊNCIA** – Os dados devem ser objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados;
- **LIMITAÇÃO DAS FINALIDADES –** Os dados pessoais são recolhidos para finalidades especificas e legitimas, não podendo ser tratados posteriormente de forma incompatível ou que exceda essas finalidades;

- **MINIMIZAÇÃO DOS DADOS –** A quantidade dos dados recolhidos deve ser adequada e limitada às finalidades em causa;
- **EXATIDÃO –** Os dados recolhidos devem ser exatos e atualizados sempre que necessário;
- **LIMITAÇÃO DE CONSERVAÇÃO –** Os dados pessoais recolhidos devem ser conservados apenas durante o período necessário para o cumprimento das finalidades para os quais são tratados, e de acordo com as exigências legais;
- **INTEGRIDADE E CONFIDENCIALIDADE –** Todos os dados recolhidos são conservados de forma segura, de modo a garantir que não existem acessos e tratamentos de dados não autorizados ou ilícitos, e para evitar a sua destruição ou danificação acidentais;
- **RESPONSABILIDADE –** O Responsável pelo tratamento deve assegurar o cumprimento do RGPD e tem o dever de comprovar o cumprimento do mesmo, por parte de toda a Organização e Serviços da Instituição.

7. Definições

Para efeitos do presente Código de Conduta, são consideradas as seguintes definições conforme previstas no artigo 4º do 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, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um 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;

2) 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 interconexão, a limitação, o apagamento ou a destruição;

3) Limitação do tratamento: a inserção de uma marca nos dados pessoais conservados com o objetivo 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 aspetos pessoais de uma

pessoa singular, nomeadamente para analisar ou prever aspetos 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 coletiva, 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 coletiva, 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 coletiva, 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 proteção de dados aplicáveis em função das finalidades do tratamento;

10) Terceiro: a pessoa singular ou coletiva, 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 direta 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 ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto 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 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;

14) 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

15) 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.

16) Autoridade de Controlo: uma autoridade pública independente criada por um Estado-Membro para fiscalizar a aplicação do RGPD, a fim de defender os direitos, liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União

8. Tratamento de Dados Pessoais

A informação pessoal deve ser tratada de acordo com algumas regras, nomeadamente:

- Tendo em conta uma finalidade determinada e legítima;
- Com base numa relação contratual e confidencial com a pessoa em causa;
- Com o consentimento por escrito dos titulares do Dados Pessoais;

Qualquer alteração ao método de recolha e tratamento de Dados Pessoais, relativamente ao já implementado, deve ser comunicado ao DPO para verificação da viabilidade e conformidade com a normas aplicáveis, e para que o titular dos Dados Pessoais seja devidamente informado da alteração.

A recolha de dados deve ser efetuada tendo em conta uma determinada finalidade e estar limitada à informação necessária para o processo em causa, não podendo incidir sobre dados de categorias especiais, salvo por trabalhador autorizado. Os dados pessoais podem

ser utilizados para fins diferentes dos que motivam a sua recolha, desde que o titular dos dados tenha sido, comprovadamente, informado e tenha dado consentimento explícito para tal tratamento.

É condição de legitimidade de tratamento que o titular dos dados esteja devidamente informado da finalidade do tratamento.

Os dados pessoais recolhidos devem ser exatos e atualizados se necessário, devendo ser tomadas as medidas adequadas para que sejam apagados ou retificados os dados inexatos ou incompletos.

No caso de haver necessidade de transferência de informação pessoal e/ou dos respetivos suportes são tomadas medidas especiais de segurança, por forma a assegurar a confidencialidade e acesso aos Dados Pessoais, somente por elementos autorizados.

A APCV cumpre as exigências da legislação laboral, nomeadamente da Lei n.º 7/2009, de 12 de fevereiro, assim como as exigências do Regulamento Geral de Proteção de Dados e da Lei n.º 58/2019 de 8 de agosto, no âmbito da Gestão e tratamento dos dados pessoais dos colaboradores.

O tratamento de dados pessoais só é permitido se os dados tratados forem necessários, adequados e proporcionais aos objetivos a atingir pela entidade empregadora. Os dados pessoais dos trabalhadores/colaboradores são assim tratados não só nos termos da legislação em vigor, mas também de acordo com o que é definido no respetivo contrato de trabalho.

Juntamente com a assinatura do contrato de trabalho, a APCV pede ao colaborador o seu consentimento expresso para:

- Proceder à recolha e utilização de imagem no âmbito do desempenho da sua atividade profissional e/ou voluntária da APCV, para divulgação da Instituição e das suas atividades com utentes/clientes;

Tem de ser obtido um consentimento autónomo para cada finalidade extracontratual, estando a APCV dotada de medidas e mecanismos para questões de prova de legitimidade.

Durante a vida laboral, os dados dos trabalhadores/colaboradores são recolhidos e tratados para efeitos de gestão contratual, gestão salarial, processos de formação, ausências, procedimentos disciplinares, seguros de trabalho, controlo de assiduidade, entre outros procedimentos inerentes à execução de contrato de trabalho ou prestação de serviços.

São igualmente tratados dados de categorias especiais, mas apenas no âmbito do cumprimento de obrigações contratuais, como é o caso da medicina no trabalho, da segurança no trabalho e no processamento de assiduidade e salários. Estes dados são tratados com a máxima confidencialidade pelas empresas prestadoras e contratualizadas, as quais fazem prova prévia de cumprimento através de mecanismos adequados, da confidencialidade e sigilo.

A recolha de dados pessoais feita pela APCV, e pelos seus subcontratantes, junto dos respetivos titulares, de forma direta e/ou indireta, é sempre precedida de informação aos mesmos sobre a finalidade que determinou a recolha e tratamento e processa-se em estrita adequação a essa finalidade.

A APCV assegura-se perante os seus trabalhadores/colaboradores:

- Que o tratamento é efetuado apenas no âmbito das finalidades para as quais os mesmos foram recolhidos;
- Que a recolha, utilização e conservação é realizada apenas sobre os dados pessoais mínimos, necessários e suficientes para a finalidade respetiva;
- Que a conservação dos dados pessoais é efetuada, apenas, pelo período de tempo necessário para o cumprimento da finalidade do tratamento que lhe deu origem;
- Que não existe qualquer transmissão de dados pessoais para fins não contratuais;
- Que o tratamento de dados pessoais é realizado para fins legalmente previstos.

9. Consentimento livre e esclarecido

O consentimento é um dos fundamentos mais importante que temos em conta nas relações estabelecidas entre a APCV e os seus utentes/clientes e a APCV e os seus trabalhadores/colaboradores.

Este consentimento limita a atuação de todos os serviços/departamentos da APCV, de forma a respeitar em primeiro lugar, os direitos e vontades dos titulares dos dados, neste âmbito. Para este consentimento ser válido tem de ser dado de forma livre e esclarecida, e tem de ser possível demonstrá-lo.

O consentimento esclarecido e válido pressupõe que foram fornecidas todas as informações necessárias ao titular dos dados para a formação da sua vontade, nomeadamente o fundamento e finalidade do tratamento; os dados que vão ser tratados;

a entidade que irá tratar os dados pessoais, e o prazo de conservação desses mesmos dados.

O consentimento pode ser retirado pelo seu titular a qualquer momento.

10. Direitos dos Titulares dos Dados Pessoais

1) Direito de Informação: O titular dos dados pessoais tem o direito a ser informado sobre os termos e condições do tratamento dos seus dados pessoais no momento da sua recolha ou, se os dados não forem recolhidos junto do próprio titular, a ser informado num prazo razoável após a sua obtenção dos dados pessoais, salvo exceções prevista no Regulamento Geral de Proteção de Dados.

2) Direito de Acesso: O titular dos dados pessoais tem o direito a ter conhecimento de que os seus dados pessoais são ou não objeto de tratamento e, se o forem, tem o direito de aceder aos seus dados pessoais, às informações relativamente às finalidades do tratamento, categorias de dados pessoais em causa, destinatários, prazos de conservação, processo de eliminação, entre outras.

3) Direito de Retificação: O titular dos dados pessoais tem o direito de obter, sem demora injustificada a retificação ou atualização dos seus dados pessoais que estejam incorretos ou desatualizados.

4) Direito ao Apagamento dos Dados/Esquecimento: O titular dos dados pessoais tem o direito de obter o apagamento/eliminação/esquecimento dos seus dados pessoais, sem demora injustificada, dentro dos limites legalmente previstos.

5) Direito à Limitação do Tratamento: O titular dos dados pessoais tem o direito de obter a limitação do tratamento, se se aplicar uma das condições previstas no Regulamento Geral de Proteção de Dados.

6) Direito de Portabilidade dos Dados: O titular dos dados pessoais tem o direito de receber os seus dados pessoais transmitidos, de forma simples, acessível e de leitura automática.

7) Direito de Oposição: O titular dos dados pessoais tem o direito de se opor, a qualquer momento, ao tratamento dos dados pessoais que lhe digam respeito, dentro dos limites legalmente admissíveis.

8) Direito de não ficar sujeito a decisões individuais automatizadas: O titular dos dados pessoais tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado dos seus dados pessoais, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente.

9) Direito de Reclamação: Tem ainda o direito de apresentar reclamação junto da Autoridade de Controlo: Comissão Nacional de Proteção de Dados – CNPD - Av. D. Carlos I, 134 - 1.º 1200-651 Lisboa; Tel: 351 213928400, Fax: +351 213976832 e e-mail geral@cnpd.pt ou www.cnpd.pt.

11. Exercício dos direitos dos titulares dos dados

Na qualidade de Responsável pelo Tratamento de Dados, a APCV obriga-se a cumprir os direitos dos titulares de dados pessoais de informação, acesso, retificação, apagamento/esquecimento, limitação, portabilidade, oposição e a não ficar sujeito a decisões individuais automatizada, através do cumprimento do dever de informar os titulares dos dados, dos seus direitos e de que forma os poderão exercer, sem prejudicar os direitos e liberdades de terceiros.

O Dever de Informação será realizado através das respetivas fichas de inscrição, contratos de trabalho e prestação de serviços e nos regulamentos internos das diferentes respostas sociais.

A APCV é responsável por analisar os pedidos dos titulares dos dados pessoais para o exercício dos seus direitos e responde a tais pedidos, salvo exceções devidamente fundamentadas, no prazo máximo de 30 dias.

Quaisquer pedidos de informações sobre o tratamento dos dados pessoais, bem como quaisquer questões relacionadas com o exercício de direitos, deverá ser realizado através do email privacidade@apcviseu.org.pt

12. Limitações ao exercício dos direitos dos titulares dos dados

O exercício dos direitos dos titulares dos dados será limitado quando certa medida legislativa interna ou comunitária faça prevalecer outros interesses, considerados superiores aos direitos dos titulares, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcional numa sociedade democrática para assegurar, designadamente:

1) A segurança do Estado;

2) A defesa;

3) A segurança pública;

4) A prevenção, investigação, deteção ou repressão de infrações penais, ou a execução

de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública;

5) Outros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social;

6) A defesa da independência judiciária e dos processos judiciais;

7) A prevenção, investigação, deteção e repressão de violações de deontologia de profissões regulamentadas;

8) Uma missão de controlo, de inspeção ou de regulamentação associada, ainda que ocasionalmente, ao exercício da autoridade pública;

9) A defesa do titular dos dados ou dos direitos e liberdades de outrem

10) A execução de ações cíveis. Todos os trabalhadores/colaboradores que tratem dados pessoais estão obrigados ao sigilo profissional e confidencialidade sobre os mesmos sendo-lhes vedado revelar o utilizar esses dados para fins que não sejam os estritamente contratados.

13. Cuidados a ter no dia-a-dia

A detenção de informação confidencial, como é o caso dos dados pessoais, reveste-se de elevado grau de criticidade, pelo que todos os trabalhadores/colaboradores deverão pautar a sua atuação garantindo cuidados "extraordinários" no tratamento desses dados.

Os documentos devem ser guardados, de preferência no computador, em pastas digitais, arquivadas em servidor, com parametrizações e soluções técnicas adequadas à prevenção de ataques e perdas de dados voluntárias e/ou involuntárias. A solução de arquivo em pasta física deve, tendencialmente, ser abandonada, tendo em conta o risco de fuga e/ou perda de dados. Sempre que possível a documentação deve ser analisada no seu formato digital, evitando-se a impressão desnecessária de documentos com dados pessoais, que ao serem impressos tornam-se, inevitavelmente, mais acessíveis por elementos não autorizados.

No caso de ser necessária a impressão de documentos com dados pessoais, deve ter-se atenção para não deixar os documentos nas impressoras. Um documento abandonado numa impressora pode ser facilmente copiado, e terceiros não autorizados podem ter acesso a informação confidencial.

É essencial que não se deixe documentação em locais cujo acesso e consulta sejam

possíveis por qualquer pessoa. Cada um é responsável pela documentação que está em sua posse, e como tal não pode deixar que essa informação se torne pública.

Não deve ser conservada documentação que já não seja necessária ou cujo prazo de armazenamento já tenha sido cumprido.

Quando se quiser destruir documentação com informações pessoais, essa documentação deve ser inutilizada em destruidora de papel, de forma a não ser possível ser visionar ou reconstituída. Em caso de documentação com dados pessoais, deve ainda ser elaborado um auto de eliminação, sendo o arquivo do auto da responsabilidade da Instituição.

Uma vez que muitos documentos são armazenados no computador, o acesso aos mesmos deve ser restrito e vinculado ao utilizador autorizado. Cada trabalhador tem acesso ao seu terminal de trabalho (computador) através de palavra passe única, pessoal e intransmissível. Entenda-se que essa palavra passe não pode ser divulgada a mais nenhum trabalhador/colaborador e o acesso ao computador deve ser sempre feito exclusivamente pelo seu utilizador.

Existem alguns cuidados a ter com os computadores, nomeadamente, não deixar as palavras-passe visíveis, não deixar documentos abertos no computador, quando não se está a trabalhar e optar sempre pelo bloqueio de ecrã e/ou sessão de trabalho, quando se está ausente do posto, mesmo que por curto espaço de tempo.

Os documentos e/ou softwares devem ser fechados sempre que o utilizador sai de perto do seu Terminal de trabalho/computador.

Relativamente à cópia de informação para dispositivos de armazenamento, como Pen's e/ou discos externos, é feito um controlo restrito dessa utilização, só sendo possível para dispositivos da propriedade da APCV. O trabalhador/colaborador que pretender copiar informação para ser utilizada e tratada fora do local de trabalho, terá não só que preencher uma declaração, na qual descreve a documentação que está a ser copiada, mas também as razões que justificam essa mesma cópia. O trabalhador/colaborador será inteiramente responsável pela informação que está a copiar e pelos riscos associados. A declaração inerente à cópia é arquivada no RGPD da APCV.

Este tipo de cópia de informação só é autorizado em situações extraordinárias, justificadas pelo volume de trabalho, sendo ainda necessário o consentimento explícito da chefia direta e parecer favorável do DPO/EPD da APCV.

14. Disponibilização de dados pessoais a terceiros - Subcontratantes

Como responsável pelo tratamento de dados pessoais, a APCV poderá ter de recorrer a entidades terceiras para a prestação de determinados serviços que poderá implicar o acesso e tratamento de dados pessoais, em nome e por conta da APCV.

Ao transmitir dados pessoais a terceiros, temos de prestar garantias de que os nossos subcontratantes oferecem as medidas de tratamento e segurança exigidas para que o tratamento realizado cumpra as exigências do RGPD, inclusive a segurança e proteção dos direitos dos titulares dos dados, nos termos do acordo de subcontratação celebrado com as referidas entidades subcontratantes.

Poderá ainda, ocorrer a transmissão de dados pessoais a entidades terceiras, quando tais comunicações de dados sejam necessárias ou adequadas à luz da lei aplicável, no cumprimento de obrigações legais/ordens judiciais, ou para responder a solicitações de autoridades públicas ou governamentais.

Os dados poderão ser fornecidos aos nossos prestadores de serviços de contabilidade, higiene e segurança no trabalho, medicina no trabalho, entidades bancárias, AT, Segurança Social, ACT, entre outros contratual ou legalmente obrigatórias, para assegurar as finalidades em causa e que têm, obrigatoriamente os mesmos deveres de conservação e utilização dos dados pessoais cedidos.

A APCV compromete-se a tomar todas as medidas razoáveis para garantir a proteção efetiva dos dados pessoais que trata, não comercializa a sua base de dados com terceiros e também não transfere quaisquer dados pessoais para países terceiros.

Para tanto, solicita a todos os subcontratantes que prestem as garantias técnicas e organizativas de Compliance com o RGPD, através de requerimento, declaração ou aditamento aos contratos de prestação de serviços ou qualquer outra forma que evidencie que a escolha ou continuidade do subcontratante se baseou na comprovação de compliance.

Quando existe necessidade de contratação de serviços a entidades terceiras (empresas subcontratantes), que possam ter acesso a dados pessoais de utentes/clientes e trabalhadores/colaboradores, estas empresas ficam obrigadas a adotar todas as medidas de segurança e protocolos utilizados na APCV, nomeadamente no que respeita à proteção de dados pessoais e ao estrito cumprimento do Regulamento. Este vínculo é plasmado em Contrato de Prestação de Serviço ou através de Declaração de Compliance com o RGPD.

A Declaração de Compliance e/ou a cláusula contratual deve obrigatoriamente respeitar e obrigar o compromisso de que a empresa subcontratante se compromete a tomar as

medidas necessárias para proteção da confidencialidade e segurança dos dados pessoais, assim como prevenir o acesso e utilização indevidos, perdas ou mesmo destruição não autorizada de dados pessoais.

A APCV assume o compromisso de apenas contratar empresas que apresentam garantias suficientes para assegurar a defesa dos direitos dos utentes/clientes e trabalhadores/colaboradores.

Quando esteja em causa o cumprimento de obrigações legais e dentro das funções de interesse público, exercício da Autoridade Pública e/ou Judicial, de que está investido o Responsável pelo tratamento, existe a obrigação de fornecimento de determinados dados pessoais, dentro do estritamente necessário para a finalidade em causa.

15. Disponibilização de dados a nível internacional

Em relação à transferência de dados pessoais para entidades externas ou países da e fora União Europeia, a APCV, enquanto responsável de tratamento, só poderá efetivá-la com expresso consentimento do titular dos dados ou por cumprimento de alguma exigência legal.

As transferências internacionais só poderão ser realizadas, se, sob reserva das demais disposições do RGPD, as condições constantes das disposições relativas a transferências de dados pessoais para países terceiros e organizações internacionais forem cumpridas pelo responsável pelo tratamento ou subcontratante.

16. Prazos de conservação dos dados

Segundo o artigo 5º, n.º 1, alínea e) do RGPD: "O*s dados pessoais são:*

(…) conservados de uma forma que permita a identificação do titular dos dados apenas durante o período necessário para as finalidades para os quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para os fins de investigação científica ou histórico ou para fins estatísticos, (…)"

A APCV conserva os dados recolhidos durante o prazo estabelecido na lei e quando estejam em causa obrigações legais:

1 - Contratos de Trabalho/Trabalhadores:

a) 5 anos: Prazo de conservação dos documentos laborais, nomeadamente, os registos de trabalho suplementar; registos dos tempos de trabalho; contratos de trabalho e aditamentos; documentos de cessação do contrato de trabalho; mapas de férias e de horários de trabalho; registos de sanções disciplinares; registo individualizado do trabalhador, acidentes de trabalho, consulta anual aos trabalhadores sobre matérias de segurança, higiene e saúde no local de trabalho, planos de formação profissional e respetivos comprovativos, pelo período de 5 anos após cessação do contrato de trabalho, atendendo aos prazos de prescrição das contraordenações laborais e da Segurança Social.

b) Permanente: Os dados relativos a declarações contributivas para efeitos de aposentação ou reforma são conservados sem limite de prazo, a fim de auxiliar o titular na reconstituição das carreiras contributivas.

c) 1 ano: Prazo de conservação dos dados constantes nos Curriculum Vitae por forma a cumprir os princípios da exatidão e minimização.

d) 5 anos: A Lei 105/97 de 13 de setembro, artigo 6º, prevê a conservação pelo período de 5 anos os registos de todos os recrutamentos realizados para garantir a igualdade de tratamento de ambos os sexos, no trabalho e no emprego.

e) 10 anos: Quanto à documentação de caráter fiscal, ou seja, relativa à retribuição, processamento de salários e quaisquer pagamentos deverá ser conservada pelo período mínimo de 10 anos.

f) 12 anos: A documentação produzida de 2014 a 2016 deve ser conservada pelo período de 12 anos. A Lei n.º 2/2014, de 16 de janeiro aplica-se apenas para a documentação produzida a partir de 2014 e durou 2 anos, sendo atualmente de 10 anos, resultado do OE de 2016, que reduziu de 12 para 10 anos o prazo de conservação do processo de documentação fiscal e conservação dos livros, registos contabilísticos e respetivos documentos de suporte.

g) 40 anos: Quando envolve riscos sérios para a saúde e património genético do trabalhador, relativamente à conservação dos resultados da vigilância da saúde do trabalhador, respetivo posto de trabalho ou função que devem constar da ficha médica de cada trabalhador;

h) 30 anos: Quando o trabalhador é exposto a riscos devidos ao ruído.

2 – Clientes/utentes:

a) 5 anos: Após o fim da relação contratual com o cliente. Este prazo não prejudica a conservação da informação se existir previsão legal específica, nomeadamente a exigível

quanto à Segurança Social.

b) 10 anos: Uma vez que realizam pagamentos e faturação, os dados devem ser conservados pelo período mínimo de 10 anos.

c) 12 anos: A Lei 2/2014 de 16 de janeiro, alterou o prazo de conservação entre 01/01/2014 a 01/01/2017 em que os livros, registos contabilísticos e respetivos documentos de suporte devem ser conservados em boa ordem durante o prazo de 12 anos.

3 -Prestadores de Serviços/ Subcontratantes:

a) 5 anos: Após o fim da relação contratual - Este prazo não prejudica a conservação da informação se existir previsão legal específica.

b) 10 anos: Dados contabilísticos e fiscais - uma vez que realizam pagamentos e faturação, os dados devem ser conservados pelo período mínimo de 10 anos.

c) 12 anos: A Lei 2/2014 de 16 de janeiro, alterou o prazo de conservação entre 01/01/2014 a 01/01/2017 em que os livros, registos contabilísticos e respetivos documentos de suporte devem ser conservados em boa ordem durante o prazo de 12 anos. A documentação fiscal/contabilística é armazenada durante o prazo de 10 anos, de forma a cumprir as exigências legais em matéria tributária.

A documentação relativa a dados clínicos e de saúde, para efeitos de Segurança, Higiene e Saúde no Trabalho, não é armazenada/arquivada pela APCV, cabendo esta obrigação à empresa contratada para o efeito.

É interdito o armazenamento de informação/documentação desnecessária.

17. Eliminação de dados pessoais

Quando os dados pessoais deixam de ser necessários para um determinado propósito, ou quando os fins que motivaram o seu armazenamento tiverem sido cumpridos ou terminado o prazo de conservação definido, a informação deve ser eliminada.

A conservação dos dados pessoais pressupõe o cumprimento do:

i) Princípio da exatidão: Os dados só poderão ser conservados se estiverem atualizados.

ii) Princípio da minimização: Os dados só devem ser conservados pelo período estritamente necessário à finalidade para a qual foram recolhidos.

Por este motivo, a eliminação de documentos é realizada regularmente, sempre que nos arquivos exista um número razoável de processos e documentos em condições de serem eliminados, de acordo com a seguinte metodologia: Selecionar a documentação a eliminar; descrever a documentação a eliminar; elaborar o auto de eliminação; assinar e arquivar o

auto.

Para salvaguarda de potenciais situações de risco no processo de eliminação de documentação confidencial, esta é feita de modo que seja impossível a reconstituição dos documentos logo que prescrevam os respetivos prazos de conservação.

A eliminação dos documentos é acompanhada pelo preenchimento de um Auto de Eliminação, do qual consta: a identificação do serviço que procede à eliminação; a data da eliminação e o local; o processo de eliminação utilizado; a relação dos documentos eliminados e as assinaturas dos responsáveis pela APCV

O respetivo Auto de Eliminação fica arquivado para fazer prova do mesmo.

18. Proteção de dados e medidas de segurança

Os trabalhadores/colaboradores devem utilizar o material e os recursos informáticos que lhes são disponibilizados exclusivamente para fins profissionais e de forma diligente, zelando pela respetiva manutenção, sendo proibida a troca de periféricos e/ou componentes, ou a abertura dos equipamentos informáticos. A troca de componentes e/ou abertura dos equipamentos informáticos é unicamente autorizada ao Departamento de Gestão Interna de Rede para efeitos de manutenção.

Quando não é tecnicamente viável, poderá existir recurso a assistência técnica por parte de empresa da especialidade, devendo a APCV enquanto Responsável pelo Tratamento assegurar-se que a mesma cumpre com os requisitos estabelecidos no RGPD.

A APCV possui um sistema central de diretório (Gestão Interna de Rede) para gestão das contas e estações de trabalho dos utilizadores, sendo atribuído a cada trabalhador com equipamento informático atribuído, uma conta de utilizador e uma palavra-passe, para acesso aos recursos informáticos disponibilizados, de acordo com o respetivo perfil de acesso.

Para os utilizadores com equipamento informático atribuído que não se encontre, por razões técnicas justificadas, registado no diretório central, é atribuída também uma conta de utilizador e adotadas medidas técnicas ajustadas à segurança dos dados registados nesse equipamento.

Em ambas as situações, é da responsabilidade de cada utilizador a manutenção segura das suas palavras-passe, sendo uma prática de segurança efetuar a encriptação da informação registada nos discos rígidos de todos os equipamentos informáticos atribuídos.

Foram criadas medidas de segurança digital em toda a organização, nomeadamente através da criação de arquivos e bases de dados com acesso restrito aos utilizadores

autorizados, para que os dados pessoais dos titulares não sofram qualquer violação, divulgação ou uso indevido.

A APCV adota ainda medidas de segurança relativamente aos dados pessoais em suporte informático, como:

- Software antivírus que disponibiliza proteção contra malware;
- Software antivírus com proteção para navegação web e e-mail;
- Rede empresarial em arquitetura Microsoft, protegida por firewall;
- Cópias de segurança automatizadas para cloud com certificação Microsoft;
- Rede WiFi disponível para visitantes com tecnologia independente da rede onde fluem os dados pessoais confiados à APCV;
- O acesso remoto à rede empresarial, para efeitos de assistência técnica remota, só é possível através de VPN (rede privada virtual);
- O acesso aos dados sensíveis é controlado e limitado apenas às pessoas que necessitam de aceder aos mesmos;
- Os procedimentos para verificar, detetar, analisar e reportar os incidentes de segurança são desenvolvidos e comunicados dentro da organização, principalmente através do contato frequente com o DPO/EPD;
- As comunicações por e-mail são alicerçadas em tecnologia Office 365 Empresarial;

Em paralelo com todas estas medidas adotadas, a APCV faz um controlo próximo e periódico de todos os procedimentos de forma a perceber se os mesmos são eficazes, correspondem às necessidades e exigências do RGPD e se são cumpridos pelos trabalhadores/colaboradores.

É expressamente proibida a utilização de correio eletrónico para o envio de:

- Material que seja considerado ilegal, nomeadamente conteúdos que violem direitos de autor, material obsceno ou ofensivo, utilização de fins particulares e pessoais;
- Material contendo dados pessoais e sensíveis confiados à APCV enquanto Responsável de Tratamento, que não seja devidamente consentido pelo titular ou pelos fins legais a que se destina.

19. Violação de dados pessoais

Uma violação de dados consiste numa falha de segurança que pode levar à destruição, perda, alteração, divulgação não autorizada, ou acesso indevido a dados pessoais.

Todos os colaboradores devem estar cientes do que é uma violação de dados ou o que pode provocar ou simplesmente permitir uma violação de dados. Para além da

responsabilidade que têm sobre os seus próprios comportamentos, é igualmente importante estar atento a algum comportamento que possa ser considerado negligente por parte de outros trabalhadores/colaboradores.

Mais do que uma consciência individual, é necessário que exista uma consciência global.

Se forem encontrados ou visualizados documentos com dados pessoais em local público, ou por pessoa não autorizada, deve tentar identificar-se a pessoa que originou tal comportamento, bem como efetivar de imediato medida corretiva, com a entrega dos mesmos ao serviço respetivo por forma a ficarem seguros e a serem direcionados ao local onde deverão ficar arquivados.

É um dever de todos os trabalhadores/colaboradores que tenham conhecimento de qualquer situação que possa implicar uma violação de dados pessoais, comunicá-la, com caráter de urgência, ao DPO/EPD da APCV, através do endereço eletrónico privacidade@apcviseu.org.pt ou através de qualquer outro meio mais expedito.

Quando ocorre uma violação de dados pessoais, depois da análise profunda sobre a notificação, o DPO/EPD deve comunicar a situação à Entidade de Controlo (CNPD), através de meio eletrónico disponibilizado pela mesma para o efeito, num prazo máximo de 72 horas.

A decisão de notificação da violação à CNPD cabe ao DPO/EPD, dentro das suas competências inscritas no RGPD, que fará uma análise casuística para perceber o tipo de violação, os riscos e consequências associadas e as medidas a serem tomadas.

Esta notificação implica a disponibilização de informações específicas sobre a violação de dados, as quais são exigidas pela CNPD. Para que o DPO/EPD apresente um relatório completo, é necessário que todos os Departamentos e Respostas da APCV, assim como todos os trabalhadores/colaboradores envolvidos se mostrem inteiramente disponíveis para auxiliar nesse mesmo relatório, dentro dos prazos estabelecidos no RGPD e nas orientações que consequentemente vão sendo transmitidas pelo DPO/EPD. De forma a dar cumprimento a todas as exigências do RGPD, encontra-se disponível nos Equipamentos da APCV e no site web, a Política de Privacidade, assim como foi criado o presente Código de Conduta, que servirá de manual a todos os trabalhadores/colaboradores.

20. Informação e Formação

Toda a informação relacionada com o RGPD e as medidas a adotar para o seu cumprimento, são disponibilizados a todos os trabalhadores/colaboradores da APCV, através dos respetivos superiores hierárquicos e responsáveis. É também disponibilizado em cada

Equipamento um exemplar do RGPD, bem como da Lei n.º 58/2019 de 8 de agosto.

A informação é igualmente disponibilizada através de ações de formação e informação, desenvolvidas pela APCV para todos os trabalhadores/colaboradores.

21. Interpretação e aplicação do Código de Conduta

Todas e quaisquer dúvidas relativamente à interpretação ou aplicação do presente Código de Conduta deverão ser dirigidas à APCV que, como Responsável pelo Tratamento de Dados, responderá ou reencaminhará para o departamento competente.

A APCV promoverá a divulgação do Código de Conduta, a sensibilização e formação de todos os seus colaboradores, bem como o acompanhamento da aplicação e a respetiva avaliação, em colaboração com a equipa de trabalho constituída.

No caso de dúvida sobre a aplicação das regras do RGPD, da Lei n.º 58/2019 de 8 de agosto e das regras elencadas no presente Código de Conduta, todos os trabalhadores/colaboradores deverão dirigir-se ao DPO/EPD, de forma que esclareçam o mais rapidamente possível qualquer dúvida, evitando assim incidentes com os dados pessoais que tratam.

Em tudo o que não esteja previsto no presente Código de Conduta, será aplicável o Regulamento Geral Sobre a Proteção de Dados, bem como a legislação nacional em vigor.

Aprovado em reunião de direção a 04/12/2023

O Presidente da Direcção: ARMANDO JORGE DOS ANJOS TORRINHA

Assinado de forma digital por ARMANDO JORGE DOS ANJOS TORRINHA