Centro de Reabilitação e Integração de Deficientes – CRID

Código de Conduta de Proteção de Dados Pessoais

Artigo 1º
(Objetivos)

O Centro de Reabilitação e Integração de Deficientes – CRID, de ora em diante também denominado por CRID, tem como missão desenvolver respostas sociais e de saúde, com foco prioritário na pessoa com deficiência, com intervenção nas várias etapas da vida, garantindo a excelência nos serviços prestados ao cidadão.

O Código de Conduta de Proteção de Dados Pessoais 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.

Artigo 2º
(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

Artigo 3º
(Princípios de proteção e tratamento de dados)

I) Princípio da responsabilidade pelo tratamento dos dados em conformidade com o RGPD:

O Responsável pelo Tratamento ou Subcontratante tem de aplicar as medidas técnicas e organizativas adequadas para assegurar e poder comprovar que o tratamento de dados é realizado em conformidade com o Regulamento.

O pedido de autorização e a notificação feitos anteriormente à CNPD são agora substituídos pela autorresponsabilização do Responsável pelo Tratamento e Subcontratantes.

Cabe assim aos responsáveis pelo tratamento e subcontratantes assumirem a responsabilidade de respeito pelo RGPD e deterem as provas documentais de tal tratamento.

II) Princípio da segurança do tratamento:

Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, âmbito, contexto e finalidades do tratamento, bem como os riscos para os direitos e liberdades das pessoas singulares, devemos aplicar as medidas técnicas e organizativas mais adequadas para assegurar um nível de segurança adequado ao risco; a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; a disponibilidade e o acesso aos dados pessoais de forma eficaz no caso de um incidente físico ou técnico e avaliarmos regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

III) Princípio da licitude, lealdade e transparência:

Licitude: O tratamento dos dados só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

1) O titular dos dados tiver dado o seu consentimento expresso, mediante um ato positivo do qual resulte a clara e informada autorização para o tratamento dos seus dados pessoais para uma ou mais finalidades;

2) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

3) O tratamento seja necessário para cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

4) O tratamento seja necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

5) O tratamento seja necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;

6) o tratamento seja necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Lealdade: O tratamento dos dados tem de respeitar a finalidade para a qual os dados foram recolhidos e não podem ser tratados para fins diferentes sem o consentimento do titular dos dados

Transparência: O titular dos dados deve ser informado por forma a conhecer o tratamento a que foram sujeitos os seus dados pessoais.

IV) Princípio da limitação das finalidades e da conservação:

Os dados pessoais deverão ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados para finalidades distintas a menos que exista um claro interesse superior que o preveja, nomeadamente, fins de arquivo de interesse público.

O período de conservação dos dados deve ser o prazo estritamente necessário, devendo neste aspeto conhecer-se e respeitar-se os prazos de conservação e arquivo previstos na lei.

V) Princípio da minimização dos dados:

O responsável pelo tratamento e o subcontratante devem orientar o momento da recolha de dados pelo princípio da minimização, devendo recolher apenas os dados pessoais que considere adequados, pertinentes e limitados ao tratamento que pretende fazer.

VI) Princípio da exatidão:

Os dados pessoais devem estar permanentemente exatos e atualizados sempre que necessário, devendo ser adotados mecanismos para garantir a exatidão e atualização permanentes.

VII) Princípio da integridade e confidencialidade:

Os dados são tratados de uma forma que garante a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental.

O tratamento informático dos dados pessoais, respeita as regras entendidas como adequadas no sentido de assegurar a confidencialidade, integridade e segurança dos dados: segurança no acesso às aplicações ou sistemas pela utilização de *password* ou outro método de autenticação ou identificação; possibilidade de rastreamento dos acessos, da informação produzida e processada.

Artigo 4º
(Direitos dos Titulares dos Dados)

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.

Artigo 5º
(Exercício dos direitos dos titulares dos dados)

O CRID na qualidade de Responsável pelo Tratamento de Dados, 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.

O CRID 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, salvo prazo em contrário.

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 E-mail: rgpd@crid.pt

Artigo 6º
(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.

Artigo 7º
(Operações de tratamento de dados pessoais)

O tratamento de dados pessoais é realizado na medida do estritamente necessário, através de sistemas ou ferramentas informáticas, tais como e-mail, processamento de texto; bases de dados; folhas de cálculo, *Software* de ERP ou CRM; processamento salarial, página de *Facebook* ou *website, entre outros.*

A nossa ***Política de Privacidade*** relativa aos dados pessoais está publicada e, pode ser consultada, a qualquer momento, no nosso site institucional em https://crid.pt

Artigo 8º
(Recolha dos dados pessoais)

A recolha de dados só pode ser realizada para finalidades determinadas e estar limitada à informação estritamente necessária para a prestação dos serviços ou atividade em causa, cumprindo os deveres da licitude e de informação.

O tratamento de dados pessoais assenta na licitude e, para isso, o CRID só o realiza quando se verifica uma das seguintes condições: O consentimento; a execução de um contrato no qual o titular dos dados é parte ou de diligências pré-contratuais a pedido do titular dos dados; o cumprimento de obrigação legal; a defesa de interesses vitais do titular dos dados; o exercício de funções de interesse público ou exercício da autoridade pública ou ainda os interesses legítimos do responsável pelo tratamento ou de terceiros.

Sempre que seja necessário o consentimento do titular dos dados pessoais, este tem de resultar de uma manifestação de vontade expressa, informada e voluntária - ato positivo inequívoco.

O pedido de consentimento é realizado através dos contactos atuais dos titulares dos dados para que prestem o seu consentimento de forma livre e esclarecida ou, através de declarações e contratos celebrados.

Artigo 9º
(Finalidades da Recolha de Dados pessoais)

Relações contratuais: os dados pessoais são tratados para celebração e manutenção de contratos, nomeadamente, de trabalho, prestação de serviços, entre outros, na medida do estritamente necessários ao desenvolvimento da atividade do CRID.

Prestações de Serviços: para o desenvolvimento da nossa atividade, se necessário, podemos ainda partilhar os dados pessoais recolhidos com os nossos prestadores de serviços que atuam em nosso nome, tal como a Contabilidade, Seguradora, Medicina no Trabalho, Higiene e Segurança no Trabalho, entre outras ou com entidades terceiras para cumprimento

de obrigações legais, tais como Tribunal, a Autoridade Tributária, Segurança Social, ACT, entre outros.

Marketing: Os dados pessoais, são igualmente tratados para efeitos de promoção e divulgação dos serviços prestados pelo CRID caso o titular dos dados tenha autorizado.

Artigo 10º
(Dever de informação)

O titular dos dados dispõe do direito à informação e à transparência das informações, comunicações e regras para o exercício dos direitos pelo que, enquanto responsável pelo tratamento, garantimos que aquando da recolha dos dados do titular, são facultadas as informações legalmente exigidas

Este dever apenas deixa de existir quando o titular dos dados já tenha conhecimento de todas estas informações ou, no caso de dados recolhidos na ausência do titular dos dados, quando o titular já tenha conhecimento das informações; se comprove a impossibilidade de disponibilizar a informação; a obtenção ou divulgação dos dados esteja expressamente prevista na lei ou os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional.

Artigo 11º
(Política de acesso aos dados pessoais)

O CRID, recolhe e trata os dados pessoais estritamente necessários para a sua boa gestão e prestação das suas atividades e serviços:

1) Os dados pessoais recolhidos incluem, nomeadamente, o nome, os elementos de identificação, contactos, IBAN, saúde, agregado familiar, rendimentos, e quaisquer outros quando estritamente necessários para a realização dos serviços da Instituição.

2) A proteção dos direitos dos menores é particularmente importante, pelo que a recolha de dados pessoais de menores de 13 anos está dependente do consentimento dos respetivos pais/responsáveis parentais.

3) Todos aqueles que têm acesso a dados pessoais recolhidos pelo CRID e que não têm a qualidade de subcontratantes, trabalhadores ou outros com qualquer vínculo contratual formalizado por escrito, têm de assinar a respetiva declaração com a obrigação do dever de sigilo e confidencialidade.

4) Existem regras internas, veiculadas em políticas, procedimentos e códigos de conduta, por um lado, para assegurar a consciencialização de todos os colaboradores para os temas da privacidade e proteção de dados, e, por outro lado, responsabilizar em caso de incumprimento.

5) Encriptação de palavras-chave – A encriptação das passwords dos utilizadores e administradores de sistema como garantia adicional de segurança, evitando acessos indevidos ou não autorizados.

6) Definição de perfis de acesso – É possível definir que utilizadores têm acesso a determinadas funcionalidades e que operações podem executar. O utilizador, mediante o seu perfil, só poderá aceder a determinadas funcionalidades e, por conseguinte, aos dados pessoais que estiverem associados, garantindo assim que os dados pessoais apenas são acedidos por quem necessita da informação para execução das suas funções.

7) Realização de auditorias internas por forma a comprovar a continuidade da aplicação dos procedimentos aprovados para o tratamento de dados pessoais.

8) De forma a minimizar comportamentos de risco e responsabilizar objetivamente os intervenientes, a recolha dos dados pessoais é realizada pelo número mais reduzido possível de pessoas que, encaminham a informação na medida do estritamente necessário para a restante equipa, de forma a reunir todas as condições para o exercício do trabalho de cada um.

9) Existem regras de controlo quanto aos contactos telefónicos internos e externos, por forma a não violarem quaisquer dados pessoais.

10) O tratamento da correspondência recebida e expedida, é realizado de forma que a mesma seja tratada e encaminhada para os seus destinatários sem violar a privacidade dos vários intervenientes.

11) As chaves de acesso aos vários departamentos/divisões/armários com dados pessoais, são guardadas em local seguro e confidencial, de acesso restrito a quem tem de aceder necessariamente.

12) VIDEOVIGILÂNCIA: Com a finalidade de proteção de pessoas e bens respeitando os seguintes limites ao tratamento: Não é permitida a recolha de som; A recolha de imagens deve confinar-se à propriedade do responsável, não podendo abranger imagens da via pública ou de propriedades limítrofes;No caso de existirem terminais de pagamento ATM, as câmaras não podem estar direcionadas de modo a captar a digitação dos códigos; Não podem as câmaras incidir regularmente sobre os trabalhadores durante a atividade laboral nem as imagens podem ser utilizadas para o controlo da atividade dos trabalhadores, seja para aferir a produtividade seja para efeitos de responsabilização disciplinar (cf. artigos 20º e 21º do Código do Trabalho);Conservação dos dados - 30 dias

Qualquer pessoa abrangida pela gravação das imagens (titular dos dados) tem o direito de a elas aceder, salvo se as imagens estiverem a ser utilizadas no âmbito de investigação criminal, situação em que o pedido do titular deve ser endereçado à CNPD.

De modo a garantir o direito de informação, são afixados avisos informativos em locais bem visíveis.

Artigo 12º
(Direito à Imagem)

O Direito à Imagem faz parte integrante dos direitos, liberdades e garantias expressamente consagrado na Constituição da República Portuguesa e é um direito consagrado e protegido no Regulamento Geral sobre a Proteção de Dados.

A reserva da imagem e o direito de escolher se a mesma deverá/poderá ser utilizada é pessoal e intransmissível.

Nessa medida, o CRID só utiliza a imagem dos seus trabalhadores, prestadores de serviços, utentes e/ou outros, após recolha do seu consentimento, prestado de forma livre, específica, informada, explicita e inequívoca e com informação da finalidade pretendida.

O período de conservação das imagens é o estritamente necessário para a finalidade determinada e têm o direito de, a qualquer momento, solicitar o acesso às imagens que lhe digam respeito, ao apagamento, o direito de se opor ao tratamento ou retirar o presente consentimento.

Artigo 13º
Segurança e proteção

O CRID tem de assegurar a confidencialidade, proteção e segurança dos dados pessoais dos seus trabalhadores, clientes e quaisquer outros a que tenha acesso no desenvolvimento da sua atividade.

Para tanto, implementou medidas técnicas e organizativas adequadas para proteger os dados pessoais contra qualquer forma de tratamento indevido ou ilegítimo e contra qualquer perda acidental ou destruição.

Dispõe de sistemas e equipas destinadas a garantir a segurança dos dados pessoais tratados, criando e atualizando procedimentos que previnam acessos não autorizados, perdas acidentais e/ou destruição dos dados pessoais, comprometendo-se a respeitar a legislação relativa à proteção de dados pessoais e a tratar estes dados apenas para os fins para que foram recolhidos, assim como a garantir que estes dados são tratados com adequados níveis de segurança e confidencialidade.

Quer os funcionários, quer a tecnologia estão atualizados com os novos métodos de ataque;Usamos ferramentas de deteção de violação de dados porque para além de manter sistemas, servidores e aplicativos, implementamos ferramentas de deteção de falhas;

Monitorizamos a organização por forma a detetar e investigar os incidentes de segurança de forma mais eficaz, o que inclui a elaboração de políticas de segurança e procedimentos internos, controlo ao nível de rede, logins e eventos de infraestrutura subjacente, aplicações e sistemas de segurança.

Formação regular de consciencialização de toda a equipa para garantir a permanente sensibilização dos nossos colaboradores, os quais assumem o compromisso de não revelar a terceiros ou utilizar para fins contrários à lei, qualquer informação pessoal, cujo conhecimento lhes advenha do exercício das suas funções.

Têm níveis de permissões que restringem o acesso aos dados pessoais de acordo com as funções e necessidades de cada colaborador.

Quando há a necessidade de transmitir dados pessoais a terceiros, o CRID tem definidas regras claras de contratualização do tratamento de dados pessoais com os seus subcontratantes, e exige que estes adotem as medidas técnicas e organizacionais apropriadas para proteger os seus dados pessoais.

Todos os documentos existentes em suporte físico estão devidamente identificados e guardados ou arquivados em local que garante a sua integridade e segurança, não acessível por parte de terceiros ou de trabalhadores que não devam ter acesso a essa informação.

Os dados pessoais de caráter sensível estão conservados em local de acesso totalmente restrito e condicionado e só os trabalhadores estritamente necessários é que terão acesso aos mesmos, oferecendo garantias de segurança e à prova de vulnerabilidades, perda, destruição e outros.

O acesso aos documentos tratados em suporte informático está condicionado aos trabalhadores estritamente necessários para o cabal desempenho das suas funções, não colocando em causa a sua máxima confidencialidade, com nome de utilizador e palavras-passe, pessoais e intransmissíveis; a existência de *firewall* e antivírus atualizados.

Artigo 14º
(Deveres dos Trabalhadores)

Os nossos trabalhadores, estão obrigados a guardar rigoroso sigilo sobre quaisquer informações ou conhecimentos de natureza pessoal, técnica, institucional, pedagógica ou outra, adquiridos, direta ou indiretamente durante a relação laboral ou por causa desta, relativos à entidade empregadora ou a quaisquer outras pessoas, singulares ou coletivas, que com aquela se relacionem, nomeadamente, outros trabalhadores, prestadores de serviços, utentes, familiares, salvo se previamente autorizados por escrito.

São expressamente proibidas quaisquer reproduções, cópias, modificações, comunicações públicas, distribuição ou qualquer outro tipo de cedência, gratuita ou onerosa, de quaisquer documentos, incluindo programas informáticos, publicações, informações contidas em bases de dados, ou qualquer outro material intelectual pertencente ou relativo ao CRID ou a qualquer terceiro que com esta se relacione, salvo se previamente autorizados por escrito.

O incumprimento das obrigações dos trabalhadores, constituirá infração disciplinar grave e impeditiva da subsistência da relação de trabalho, sem prejuízo de incorrer na obrigação de indemnizar os lesados pelos prejuízos patrimoniais e/ou não patrimoniais.

Artigo 15º
(Subcontratantes)

Como responsável pelo tratamento de dados pessoais, por vezes, temos necessidade 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 do CRID.

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.

O CRID 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.*

Artigo 16º
(Prazos de Conservação)

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) Imediato: Os Dados biométricos são eliminados imediatamente após saída do trabalhador/cliente.

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

e) 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.

f) 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.

g) 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.

h) 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;

i) 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.

Artigo 17º
(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.

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 pelo CRID.

Artigo 18º
(Interpretação e aplicação do Código de Conduta)

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

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

Artigo 19º
(Lacunas)

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.

Artigo 20º
(Entrada em vigor)

O presente Código de Conduta entra em vigor no dia 14 de Outubro de 2026