|  |  |
| --- | --- |
| *Sumário* | O presente documento contém **instruções de trabalho** relativas à função de DPO (encarregado de proteção de dados) e às orientações que este presta a outros colaboradores que efetuem tratamento de dados pessoais. |
| Síntese  RGPD | O Regulamento Geral sobre a Proteção de Dados (RGPD) é o novo quadro legal que está em vigor a partir do dia 25 de maio de 2018 na União Europeia. A aplicação de coimas que podem ir até 4% do volume de negócios global anual ou 20 milhões de Euros, torna indispensável que a **(nome da empresa)** e respetivos colaboradores cumpram na íntegra o RGPD. |
| Conteúdos | [Pré-requisitos](#Prerequisitos) • [Acessos/Permissões](#acessos) • [Instruções Gerais](#InstrucoesGerais) • [Instruções Específicas](#Instrucoesespecificas) • [Previsão de Cenários e Atuação](#cenarios) |

• PRÉ-REQUISITOS•

|  |  |
| --- | --- |
| **1.**  Nomeação do DPO  (encarregado de proteção de dados) | Ainda que não seja obrigatório a designação de um DPO para todas as empresas portuguesas, o documento de orientação disponibilizado pela CNPC faz referência à recomendação de, enquanto boa prática, nomear-se um colaborador a título voluntário que apoie e controle as políticas de cumprimento do RGPD.  Esta nomeação deve ser feita com base nas qualidades profissionais, em especial no que respeita aos conhecimentos especializados no domínio do direito e proteção de dados, como também nas suas apetências e disponibilidade para desempenhar as funções de DPO que abaixo indicamos.  Este encarregado poderá ser um elemento do pessoal ou alguém em regime de prestação de serviços.  No ARTSOFT este encarregado terá permissões totais sobre o tratamento de Dados Pessoais. Além do DPO incluímos a função de delegado, que poderá ser um utilizador com permissões superiores à maioria dos utilizadores, mas que age sob a supervisão/orientação do DPO. |
| **2.**  **Publicar contactos à CNPD** | Após nomeação do encarregado da proteção de dados, o responsável pelo tratamento de dados ou o subcontratante deve publicar os contactos do encarregado da proteção de dados junto da CNPD.  Os contactos do DPO devem incluir informações como endereço postal, número de telefone e/ou endereço de correio eletrónico.  Como boa prática, é recomendável que a organização informe também internamente os contactos do DPO, em *intranet*/listas telefónicas e em organogramas. |
| **4.** Responsabilizar e Assinar | Após tomar conhecimento deste documento, o colaborador acima indicado deve assinar a **declaração de compromisso de honra** sobre o uso e tratamento de dados pessoais que a **(nome da empresa)** tem em sua posse. |

• **ACESSOS/PERMISSÕES** •

|  |  |
| --- | --- |
| **5.**  **Acessos &**  **Permissões** | O DPO é responsável pela gestão, controlo e análise do tratamento de dados pessoais dentro da empresa. No ARTSOFT considerou-se a seguinte divisão: DPO responsável – total controlo sob o tratamento de dados; DPO delegado – utilizador com permissões superiores à maior parte dos elementos da equipa, mas que responde às indicações do primeiro DPO.  No GDPA[[1]](#footnote-1). estes utilizadores têm as seguintes funções ativas:   * DPO responsável – Acesso a todas as funções/permissões/ferramentas, quer na secção terceiros quer nos recursos humanos. Consultar *Help* da solução. * DPO delegado - Ver/Alterar/Analisar/Usar/Tratar todos os dados nos quais o DPO considere importante haver necessidade. Consultar *Help* da solução. |
| **6.**  **Recursos necessários** | Segundo o artigo 38º do RGPD, é exigido à organização que apoie o DPO. O responsável pelo tratamento, ou o subcontratante, deve fornecer os recursos necessários às suas funções e à manutenção dos seus conhecimentos, dando-lhe acesso total aos dados pessoais e às operações de tratamento.  Em especial, há a destacar:   * Tempo suficiente para o DPO exercer as suas atribuições, sem que haja conflito de prioridades que se sobreporiam ao exercício das funções de DPO. * Apoio em termos financeiros, infraestruturas (locais, instalações, equipamento) e pessoal, sempre que necessário. * Acesso a serviços, como recursos humanos, serviços jurídicos, informáticos, de segurança, etc., sempre que o DPO precisar de informações essenciais. * Formação contínua. Atualização no que respeita aos desenvolvimentos no domínio da proteção de dados. * Analisar a necessidade de criar uma equipa só relacionada com controlo e tratamento de dados pessoais, consoante a dimensão e estrutura da organização ou a dimensão e estrutura dos dados pessoais.   Para apoio à função de DPO, consulte o documento “Sobre o tratamento e proteção de dados pessoais do ARTSOFT”, disponível no seu ARTSOFT. |
|  |  |

• **INSTRUÇÕES GERAIS** •

|  |  |
| --- | --- |
| **7.**  **Independência** | Ao abrigo do artigo 39º, o DPO não deve receber instruções relativamente ao exercício das suas funções. Por exemplo, o DPO não deve ser desconsiderado perante um resultado que deve ser obtido, à forma de investigar uma queixa ou à necessidade de consultar a autoridade de controlo. |
| **8.**  **Limitações** | A autonomia do DPO não implica, contudo, que lhes sejam conferidos poderes decisórios que extravasem as suas funções em conformidade com o artigo 39º. |
| **9.**  **Objetividade e imparcialidade** | O DPO deverá ser capaz de fazer o tratamento de perfis de titulares, o mais objetivamente, no que respeita à previsão de aspetos relacionados com desempenho profissional, situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações, etc. |
| **10.**  **Confidencialidade** | A confidencialidade é igualmente importante: por exemplo, os trabalhadores podem mostrar-se relutantes em apresentar queixas ao DPO caso a confidencialidade das suas comunicações não seja garantida. É importante que o DPO esteja por isso vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções. |
| **11.**  **Conflito de Interesses** | O responsável pelo tratamento ou o subcontratante permanece responsável pelo cumprimento das normas de proteção de dados e deve poder comprovar esse cumprimento. Se estes tomarem decisões incompatíveis com o RGPD e o parecer do DPO, deve ser dada a possibilidade ao último de transmitir o seu parecer ao mais alto nível da direção.  O DPO pode exercer outras funções e atribuições desde que essas não resultem num conflito de interesses com as suas funções de DPO. É por exemplo, recomendável, que o DPO não tenha funções ao nível do departamento de marketing. |
| **12.**  **Funções** | As instruções gerais para a função do DPO passam por:   * Informar e aconselhar o responsável pelo tratamento de dados, ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do RGPD e de outras disposições de proteção de dados da União ou dos Estados-Membros; * Controlar a conformidade com o RGPD, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes; * Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto[[2]](#footnote-2) sobre a proteção de dados e controlar a sua realização nos termos do artigo 35º; * Cooperar com a autoridade de controlo e ser ponto de contacto com a CNPD ou o titular dos dados sobre questões relacionadas com o tratamento, incluindo a consulta prévia em eventuais dúvidas no exercício da função; * Ter sempre em consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento. |
| **11.**  **Obrigações em caso de violação do RGPD** | As violações identificadas e que sejam suscetíveis de resultar num risco para os direitos dos titulares devem ser reportadas à autoridade de controlo (CNPD), num prazo máximo de 72 horas após terem sido descobertas. Todas as violações, com mais ou menos riscos, após serem comunicadas ao DPO ou responsável de proteção de dados da empresa, devem ser inseridas em documento e resolvidas assim que possível para evitar repetições. No caso de violações de maior risco, o DPO deve avisar também o titular dos dados. Nessa comunicação deverá descrever a natureza da violação de dados pessoais e dirigir recomendações à pessoa singular em causa para atenuar potenciais efeitos adversos, em estreita cooperação com a CNPD.  Todas as violações devem ser devidamente documentadas, de forma a compreender os factos relacionados, os efeitos que causaram e as medidas necessárias para a resolução das mesmas. |
| **13.**  **Transferências de dados pessoais** | O DPO deve informar subcontratantes/terceiros que tenham consentimento para tratamento de dados de todas as alterações que o titular dos dados solicite, de forma atempada e dentro dos *timings* definidos. |

• **INSTRUÇÕES ESPECÍFICAS** •

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **14.**  **Inventariação de acessos** | | Em conjunto com o responsável pelo tratamento de dados ou subcontratante, o DPO deve proceder a uma inventariação do tratamento de dados (quais dados, onde estão, para onde são transmitidos, quem tem acessos, qual o propósito principal para o seu processamento, por quanto tempo serão retidos). Ver anexo. | | |
| **15.**  **Formulários e Documentos de Obtenção de Dados[[3]](#footnote-3)** | | O DPO, em conjunto com os departamentos em questão, deve rever todos os campos solicitados ao utilizador aferindo se há razões para os solicitar. Se sim, criar um documento interno (ver inventariação de tratamento de dados[[4]](#footnote-4)) onde deverão estar indicadas quais as razões.  Algumas notas a reter nesta revisão: verificar se foi acrescentada *CheckBox* com Lista de interesses para subscrição. Lista a ser feita com base no *core business* ou no tema concreto do formulário/documento de obtenção de dados, para garantir que há consentimento do titular para enviar comunicação;  Botão *Opt-in*: não deve ser utilizado *Opt-out* nem *CheckBox* pré-selecionadas, para garantir o consentimento do titular;  Deve indicar a empresa ou terceiros que poderão ter acesso ou utilizar os dados pessoais do titular;  Informar os titulares sobre o direito de retirar o consentimento e dar-lhes formas fáceis de o fazer a qualquer altura;  Associar política de privacidade[[5]](#footnote-5) no final do formulário. | | |
| **15.**  **Ações a fazer no ARTSOFT – preparar o módulo** | | - Definir Listas de Subscrições/consentimentos e implementá-las no ARTSOFT;  - Importar listas de códigos postais provenientes dos CTT, para que os dados colocados no software sejam os mais exatos possíveis;  - Importar listas de e-mails e telemóveis “proibido usar” que poderá usar para rastrear futuramente usos indevidos;  - Acrescentar nas fichas adicionais outros dados pessoais que a empresa recolha;  - Definir os possíveis motivos de consultas de outros utilizadores ARTSOFT sobre os dados que estiverem anonimizados, para que fiquem depois registadas todas as consultas feitas, quem consultou e quais os motivos;  - Os dados pessoais de titulares que já tenham sido recolhidos em conformidade com o RGPD devem agora ser atualizados no ARTSOFT;  - Definir os campos para a Lista de Dados Pessoais a enviar para a plataforma dadospessoais.artsoft.pt;  - Formar e explicar aos utilizadores ARTSOFT o novo módulo GDPA. | | |
| **16.**  **Ações rotineiras**  **Que o DPO deva fazer no ARTSOFT** | | - Importar listas “proibido usar” regularmente para que as mesmas possam estar sempre atualizadas;  - Aplicar restrições de dados pessoais em bases de dados antigas, sempre que se fizerem alterações na atual;  - Guardar em lugar seguro, cópia do e-mail que a plataforma dadospessoais.artsoft.pt vai enviar ao titular dos dados em resposta às alterações solicitadas por este. | | |
| **17.**  **Definir procedimentos relativamente às informações que são recolhidas** | | O DPO deve ter a preocupação de elaborar processos de condução da informação que é recolhida até ao seu armazenamento. Quem são os intervenientes, em que locais devem estar guardados os documentos de origem, onde devem ser armazenados os dados e como devem ser tratados.  Este fluxo deve depois ser comunicado a todos os intervenientes. | | |
| **18.**  **Avaliação de Impacto de Proteção de Dados** | | A probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverão ser determinadas por referência à natureza, âmbito, contexto e finalidades do tratamento de dados.  O DPO deverá fazer uma avaliação objetiva que determine se as operações de tratamento de dados implicam risco ou risco elevado. No caso da avaliação de impacto sobre a proteção de dados (AIPD), ao indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais.  Nos termos do artigo 35º, cabe ao responsável pelo tratamento, e não ao DPO, proceder, quando necessário, a uma avaliação de impacto sobre a proteção de dados. No entanto, o DPO pode desempenhar um papel muito importante e útil, prestando assistência ao responsável pelo tratamento.  A este nível, é recomendado que a empresa consulte o DPO sobre:   * Se deve ou não efetuar uma AIPD; * Qual a metodologia a seguir na realização de uma AIPD; * Se deve realizar a AIPD interna ou externalizá-la; * Quais as salvaguardas (incluindo medidas técnicas e organizativas) a aplicar no sentido de atenuar os eventuais riscos para os direitos e interesses dos titulares de dados; * Se a avaliação de impacto sobre a proteção de dados foi ou não corretamente efetuada e se as suas conclusões (se o tratamento deve ou não ser realizado e quais as salvaguardas a aplicar) estão em conformidade com o RGPD. | | |
| **19.**  **Medidas de segurança** | | A fim de preservar a segurança e evitar o tratamento em violação do RGPD, o responsável pelo tratamento deverá avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a cifragem. O DPO poderá ajudar na deteção de algumas medidas operacionais, tendo em conta os riscos apresentados pelo tratamento dos dados pessoais, tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a danos físicos, materiais ou imateriais.  Como medidas de segurança, e em específico no ARTSOFT, é recomendado ao DPO que:  - Escale níveis de permissões por utilizadores, definindo quem pode ver e fazer alterações nos dados pessoais de terceiros, empregados e independentes;  - Defina o número de tentativas que o ARTSOFT possibilita até que este bloqueie o acesso a determinado utilizador por tentativas de acesso indevido (para desbloquear será necessário que um utilizador com permissões superiores lhe desbloqueie a ficha);  - Defina um tamanho mínimo para palavras-passe, evitando o uso de palavras-passe muito fáceis de quebrar;  - Proceda a uma verificação do ambiente de trabalho de cada utilizador ARTSOFT (poderá testar permissões/acessos), utilizando para o efeito a função de “alter/ego” que o software permite.  A nível geral, é ainda recomendável ao DPO:  - Não partilhar passwords de acesso ao PC ou outros acessos como emails, etc.;  - Em caso de partilhar dados com terceiros, verificar se tem declaração de compromisso de honra para salvaguardar o envio e se tem meio de rastrear quem poderá ter acesso a eles;  - Apagar dados que não sejam necessários. Por exemplo, email dos enviados, se tiverem dados pessoais;  - Manter os dados o mais centralizados possível para que seja ágil e simples o acesso e o tratamento;  - Guardar em local seguro e protegido (com chave/cadeado) todo e qualquer documentos e suporte físico com dados pessoais;  - Sempre que se afasta do PC bloqueá-lo (*ctrl+alt+del* + “Bloquear” no caso de *Windows*);  - Não tirar “*screenshots*” ou fotografias quando há dados sensíveis no ecrã;  - Não utilizar o verso de folhas com dados pessoais como folhas de rascunho;  - Não facultar qualquer informação com dados pessoais pelo telefone, a menos que seja possível certificar a identidade da pessoa que solicita a informação;  - Definir em conjunto com os recursos humanos, uma política de segurança documental na qual cada trabalhador assuma a responsabilidade pelos documentos que lhe são confiados, não os deixando em cima da secretária sem vigilância ou noutro local onde não consiga garantir o sigilo. |
| **20.**  **Rever políticas de proteção de dados com empresas subcontratantes** | | Confirmar e garantir que todos os responsáveis pelo tratamento de dados em regime de subcontratação estão em conformidade com as medidas do RGPD. Esta revisão pode ser feita em conjunto com o apoio de outros departamentos internos. |
| **21.**  **Apoio na conservação do registo de atividades** | | Nos termos do artigo 30º, é o responsável pelo tratamento dos dados ou o subcontratante, e não o DPO, que é responsável por conservar o registo de todas as atividades de tratamento de dados ainda que este possa ser incumbido dessa função. Ainda assim, é o DPO que deve criar os inventários e manter um registo das operações de tratamento com base nas informações que recebe dos vários departamentos.  Com esses registos, o DPO criará um instrumento de controlo para conferir a conformidade com o RGPD e, eventualmente, disponibilizar esse documento à CNPD, como prova.  No ARTSOFT, estão definidos dois campos: Consultas [Motivos de consultas para dados pessoais] e Modificações [Alterações feitas por utilizadores ARTSOFT em registos de pessoas singulares]. Estes campos permitem um controlo de ações feitas sobre os dados pessoais inseridos no ARTSOFT. |
| **22.**  **Documento que pode ser solicitado por terceiros sobre a finalidade dos dados** | | É ainda das competências do DPO, em conjunto com outros departamentos, criar um documento base[[6]](#footnote-6) que detenha informação sobre a finalidade e o tipo de tratamento a que os dados serão sujeitos.  Este documento servirá de base a pedidos de terceiros que pretendam ter conhecimento sobre a forma como os seus dados estão a ser tratados. O envio desta comunicação ao terceiro deve ficar registado no ARTSOFT e poderá fazê-lo manualmente. |
| **23.**  **Verificar comprovativos** | | É importante que o DPO controle e confirme os comprovativos dos consentimentos dos titulares que são recolhidos pelos vários departamentos. Sempre que este identificar incongruências deve solicitar ao departamento novo pedido de consentimento, antes dos dados serem novamente tratados.  Nas fichas de Terceiros, botão Digitalizar, poderá associar estes documentos a cada uma das fichas.  No que respeita à plataforma dadospessoais.artsoft.pt, o DPO irá receber o comprovativo por e-mail das alterações que foram solicitadas através da plataforma, servindo este como comprovativo. |
| **24.**  **Prazos a cumprir em pedidos do titular dos dados** | | O DPO, em conjunto com o responsável do tratamento dos dados, terá de adotar medidas que lhe permita facultar informações aos titulares dos dados, mediante pedido apresentado por estes, sem demora injustificada e no prazo de um mês a contar da data da receção do pedido. Para este efeito, deverão ser previstas regras para facilitar o exercício pelo titular dos dados dos direitos que lhes assistem, incluindo procedimentos para solicitar e obter, a título gratuito, o acesso a dados pessoais, a sua retificação ou o seu apagamento, bem como o exercício do direito de oposição.  No ARTSOFT o campo Data Limite de Tratamento deverá estar preenchido para um maior controlo. O DPO ou delegado, deverá controlar a correta atualização.  Importa ainda dizer que após o prazo de conservação ter expirado, a ficha do utilizador torna-se privada (direito à oposição).  Para facilmente disponibilizar o acesso aos dados pessoais, é recomendável o uso da plataforma dadospessoais.artsoft.pt. O DPO deverá instruir todos os utilizadores ARTSOFT sobre o uso desta plataforma, para que estes possam validar dados daqui provenientes. |
| **25.**  **Política de Privacidade e Termos e Condições** | | Em conjunto com o responsável pelo tratamento dos dados ou subcontratante, o DPO deve ajudar na criação de documentos que manifestem a posição da empresa relativamente à proteção de dados. Ver exemplos. |
| **26.**  **Direito à portabilidade** | | No ARTSOFT poderá ser gerado um ficheiro estruturado em formato .XML para suportar o direito à portabilidade dos dados. Deve o DPO certificar-se de que a exportação deste ficheiro é conduzida sem infrações ao RGPD, (ex: ter o cuidado de guardar o ficheiro em local pouco seguro). É ainda importante que o DPO confirme se foi mesmo o titular dos dados a solicitar este envio. |
|  | |  |

• **CENÁRIOS / PREVISÃO DE ATUAÇÃO** •

|  |  |
| --- | --- |
| **CENÁRIOS** | **COMO ATUAR** |
| Vou transferir este contacto para parceiros de negócio. Devo avisar o titular? | Se tiver consentimento do titular para transferir esse contacto para parceiros poderá fazê-lo sem avisar o mesmo, ainda que deva registar a ação da transferência.  Se não tiver consentimento, deve solicitar ao titular a permissão com um comprovativo, antes da transferência dos seus dados pessoais. Esta ação deverá estar definida na politica de tratamento de dados. |
| O DPO é externo à empresa. Como pode a empresa responsável pelo tratamento garantir o controlo? | O DPO pode nomear colaboradores internos que ajam como delegados do DPO. Estes colaboradores terão mais permissões dentro do ARTSOFT, podendo assim facilitar e controlar o tratamento dos dados na ausência do Delegado que poderá por sua vez, validar as atuações do delegado. |
| O titular dos dados pessoais pediu alterações. Qual o tempo de resposta da empresa? | Tem um mês a contar da data da receção do pedido (que deverá guardar e anexar à ficha de terceiro) para proceder à alteração, a título gratuito. Esta mesma alteração deverá ser comunicada por escrito ao titular dos dados, confirmando ao próprio que a ação solicitada foi cumprida.  Poderá cumprir esta obrigação usando a plataforma dadospessoais.artsoft.pt.  Nota: Deve verificar se a alteração solicitada, nomeadamente o direito ao esquecimento, é possível. |
| Não sei como definir o prazo de tratamento de dados. | O prazo do tratamento dos dados de cada titular depende do tipo de terceiro e do tipo de relação com o mesmo. Deverá, por isso, definir o prazo consoante as políticas internas da empresa. Ex.: Dados de terceiro obtidos através de um formulário de recrutamento. Certifique-se se: Pretende ficar com os dados desse titular em base de dados para futuras oportunidades? Por quanto tempo? E tem o consentimento para conservar os dados para esse fim? |
| Foi definido que todos os titulares de dados estarão por defeito, anonimizados. Como posso proceder? | No ARTSOFT pode definir que qualquer terceiro, enquanto particular, seja anonimizado. Assim, sempre que alguém aceder aos dados, terá de solicitar um motivo para o aceder, o que o poderá ajudar no controlo do acesso aos dados pessoais. |
| A empresa onde sou DPO disponibiliza por motivos profissionais dados pessoais a terceiros. Como devo proceder? | Sempre que a sua empresa partilhar dados com subcontratantes, e se alguma das empresas preencher os critérios de designação obrigatória de DPO, é obrigatório que seja nomeado um DPO e que este passe a cooperar com ambas as entidades.  A sua empresa, considerando que é a responsável dos dados, deve celebrar um contrato onde esteja estabelecida a política que deve obedecer no que respeita ao RGPD. Consulte a nossa minuta de cláusula para acrescentar no contrato.  Quando existir um subcontratante, deve informá-lo de todas as alterações solicitadas pelo titular dos dados. Defina um procedimento para garantir se o subcontratante procedeu à alteração (ex. cópia de um e-mail a confirmar o procedimento).  Na prática o DPO poderá, periodicamente, enviar uma listagem de fichas alteradas aos subcontratantes.  Na eventualidade de existirem titulares a solicitar o direito ao esquecimento nessas listas, deve o DPO certificar-se de que só deve remover essas fichas do ARTSOFT se o subcontratante já tiver dado garantias de que o apagou.  Por boa prática, é também recomendável que o responsável pelo tratamento de dados guarde uma lista de oposições para comprovar os pedidos. |
| Devo ter um DPO só porque uso anúncios em plataformas de marketing *online*? | Se a sua empresa, imagine uma PME, subcontrata, por exemplo, a Google para serviços de marketing direcionado e se a sua atividade não engendrar tratamento de dados em grande escala, não é obrigada a designar individualmente um DPO. No entanto, a Google deverá designar um ao abrigo do artigo 37º. Para saber mais sobre a política de RGPD da Google aceda aqui: https://privacy.google.com/businesses/ |
| Tendo eu, DPO, autonomia nas funções, tenho também poder de decisão? | A sua autonomia enquanto DPO não implica, contudo, que lhe sejam conferidos poderes decisórios que extravasem as suas funções em conformidade com o artigo 39º. |
| Como posso provar que cumpro as funções de um DPO? | No âmbito da sua missão enquanto DPO, é recomendável que faça a comunicação direta de um relatório anual das atividades que desenvolve e que este seja apresentado ao mais alto nível da direção. |
| Quais os cargos que poderão ser mais suscetíveis de gerar conflitos na proteção de dados? | Os mais referenciados são: diretor executivo, diretor de operações, diretor financeiro, diretor do departamento médico, diretor de *marketing*, diretor dos recursos humanos ou diretor informático, mas também outras funções em níveis inferiores da estrutura organizacional, se esses cargos ou funções levarem à determinação das finalidades e dos meios de tratamento. |
| Que boas práticas devem permanecer entre mim, DPO, e a entidade responsável pelo tratamento de dados? | Para que as suas funções enquanto DPO sejam cumpridas, é importante que entre si e o responsável pelo tratamento de dados seja salvaguardado o conflito de interesses, por exemplo, criando entre ambos um conjunto de normas internas que estabeleça as suas prioridades enquanto DPO e que em nada possa afetar, por exemplo, o seu vínculo laboral enquanto colaborador da entidade responsável pelo tratamento de dados. |
| Que método ou ações poderei desenvolver para controlar os dados pessoais? | No âmbito das atribuições de controlo da conformidade, o DPO deve definir métodos de controlo e monitorização, tais como:   * Recolher informação 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 ou ao subcontratante ou aos colaboradores de ambos, sempre que se justificar. |
| Como deverei cooperar com a CNPD? | Nos termos do artigo 39º, deve cooperar e servir de ponto de contacto com a CNPD sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36º, e consultar, sendo caso disso, esta autoridade sobre qualquer outro assunto, ainda que esteja vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções. |

|  |
| --- |
| Notas finais:  As instruções de trabalho aqui sugeridas devem ser alteradas e validadas conforme a política de RGPD da sua empresa. Este documento serve apenas de exemplo e foi constituído a título generalista para poder ser o mais abrangente possível.  Este documento não dispensa a consulta ao RGPD. A ARTSOFT está ainda disponível para troca de informações.  Para o efeito pode deixar sugestões ou notas que considere pertinentes através do e-mail [marketing@artsoft.pt](mailto:marketing@artsoft.pt). |

1. GDPA – Gestor de Dados Pessoais do ARTSOFT [↑](#footnote-ref-1)
2. Consulte o documento [**AIPD**](file:///C:\Users\TaniaL\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\WA67ETFC\AIPD.docx) para mais informações. [↑](#footnote-ref-2)
3. Ver modelos de vários formulários que poderá adaptar para a sua empresa. [↑](#footnote-ref-3)
4. Consulte o documento **Inventariação de Tratamento de Dados** para mais informações. [↑](#footnote-ref-4)
5. Ver modelos de política de privacidade e de termos de responsabilidade. [↑](#footnote-ref-5)
6. Ver **modelo de documento base** com finalidades e tipo de tratamento. [↑](#footnote-ref-6)