PROGRAMA DE DESENVOLVIMENTO RURAL 2014·2020

APROVO.

A Gestora

ANA RITA DE SOUSA VELOSO BARRADAS DA COSTA PINHEIRO

Assinado de forma digital por ANA RITA DE SOUSA VELOSO BARRADAS DA COSTA PINHEIRO
Dados: 2020.12.04 13:01:14 Z

(Rita Barradas)

Regulamento de Proteção de Dados Pessoais da Autoridade de Gestão do PDR2020

Dezembro de 2020

UNIÃO EUROPEIA
Fundo Europeu Agrícola de Desenvolvimento Rural
A Europa investe nas zonas rurais

PORTUGAL 2020

REPÚBLICA PORTUGUESA
AGRICULTURA

Histórico de Alterações:

Data	Versão	Autor	Descrição da Alteração
10/08/2018	0.0	EPD	Versão inicial do documento
04/12/2020	1.0	EPD	Atualização do documento

Índice

Objetivos

O presente regulamento visa estabelecer o compromisso da **Autoridade de Gestão do Programa de Desenvolvimento Rural do Continente 2014-2020** (**PDR 2020**) para com a proteção de dados das pessoas singulares e para com o tratamento legal, justo e limitado, em conformidade com Regulamento Geral da Proteção de Dados (RGPD) e demais normativos aplicáveis.

1. Âmbito de Aplicação

O Regulamento é aplicável a todo o tratamento de dados pessoais e livre circulação desses dados, em defesa dos direitos e das liberdades fundamentais dos seus titulares, quando a responsabilidade do tratamento seja do PDR 2020.

O presente regulamento aplica-se ao tratamento de dados pessoais contidos em qualquer suporte, seja físico, virtual, tecnológico, sonoro ou gráfico.

2. Destinatários

Este documento é destinado a todos os colaboradores, prestadores de serviços, fornecedores e outras pessoas singulares e coletivas que, a qualquer título, se relacionem com o PDR 2020 e tenham acesso, direito de uso ou controlo sobre ativos de informação de dados pessoais da organização e/ou aos recursos a eles associados.

3. Documentos de Referência

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

Lei da Proteção de Dados Pessoais, aprovada pela Lei n.º 58/2019, de 08 de agosto.

4. Definições

1) **«Dados pessoais»**, a 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) **«Dados pessoais sensíveis»**, os dados pessoais relativos à origem racial ou étnica do indivíduo, às suas opiniões políticas, crenças religiosas ou convicções filosóficas, vida privada, pertença a um sindicato, saúde ou doença física ou mental, vida sexual, prática efetiva ou alegada de qualquer ato ilícito ou qualquer processo relacionado com a prática efetiva ou alegada de qualquer ato ilícito pelo indivíduo.
3) **«Titular dos dados»**, uma pessoa singular identificada ou identificável.
4) **«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.
5) **«Finalidade de Tratamento»,** o propósito de uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados.
6) **«Limitação do tratamento»**, a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro.
7) **«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.
8) **«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.
9) **«Ficheiro»**, qualquer conjunto estruturado de dados pessoais, acessível segundo critérios

específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico.

10) **«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.

11) **«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.

12) **«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.

13) **«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.

14) **«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.

15) **«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.

16) **«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.

17) **«Dados biométricos»**, os dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que

permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.

18) **«Dados relativos à saúde»**, os dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde.

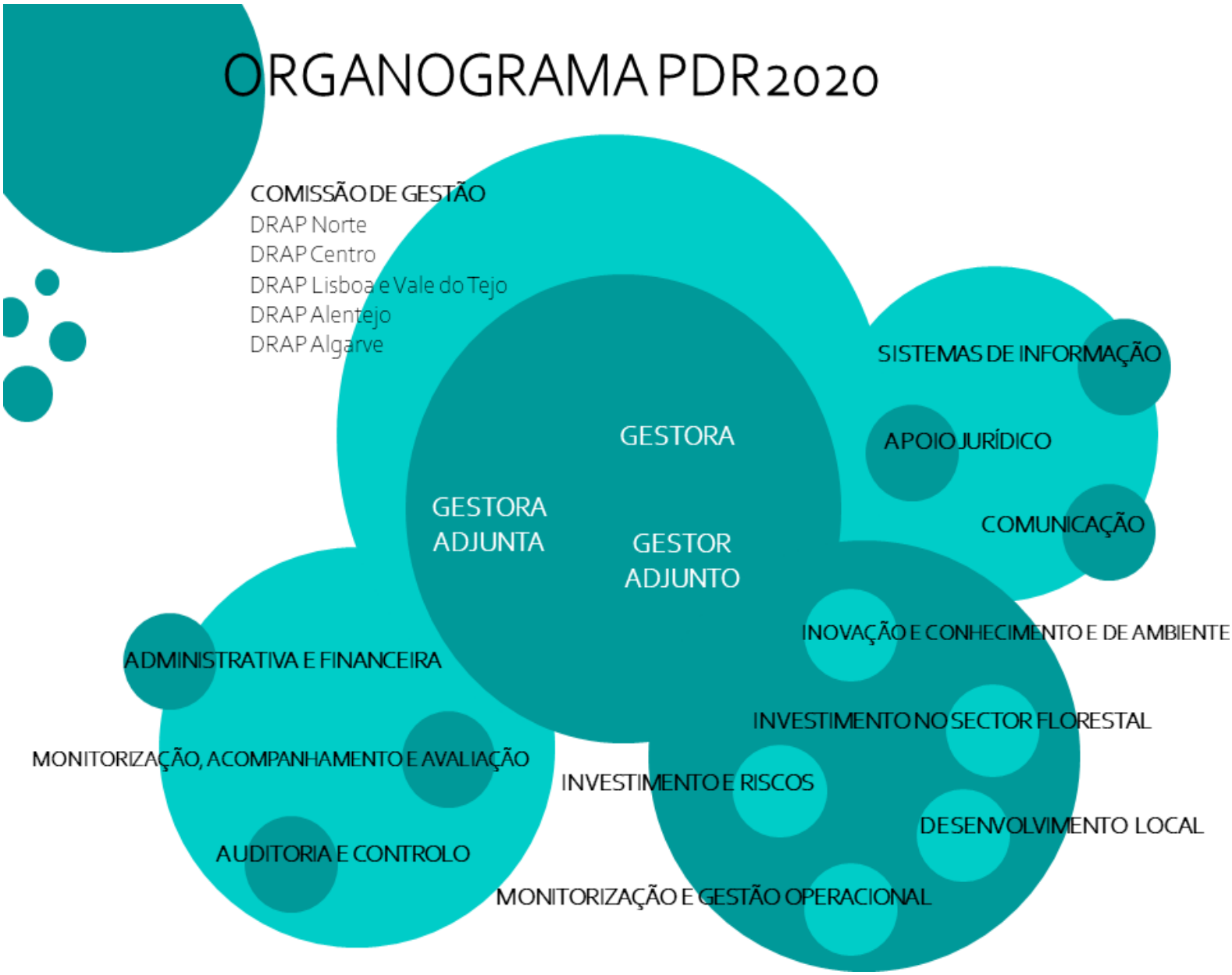
19) **«Representante»**, uma pessoa singular ou coletiva estabelecida na União que, designada por escrito pelo responsável pelo tratamento ou subcontratante, nos termos do artigo 27.º do RGPD, representa o responsável pelo tratamento ou o subcontratante no que se refere às suas obrigações respetivas nos termos do presente regulamento.

20) **«Autoridade de controlo»**, a autoridade pública independente criada por cada Estado-Membro responsável pela fiscalização da aplicação do RGPD, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União.

21) **«Organização internacional»**, uma organização e os organismos de direito internacional público por ela tutelados, ou outro organismo criado por um acordo celebrado entre dois ou mais países ou com base num acordo dessa natureza.

5. Orgânica e Responsabilidades

5.1 Organograma



5.2 Responsabilidades do PDR2020

No âmbito da proteção de dados, cabe ao PDR2020:

a) Aprovar o Regulamento de Proteção de Dados;
b) Demonstrar liderança e comprometimento com a proteção de dados pessoais;
c) Providenciar e disponibilizar os recursos necessários para o cumprimento dos requisitos de proteção de dados;
d) Nomear um Encarregado de Proteção de Dados (EPD);
e) Garantir a comunicação com a Autoridade de Controlo nos casos previstos neste Regulamento e na Lei, segundo os critérios e procedimentos estabelecidos;
f) Rever o desempenho de segurança na proteção de dados pessoais.

5.3 Enquadramento do Encarregado de Proteção de Dados

a) Responsável pela supervisão, revisão e ajustamento dos procedimentos e mecanismos de proteção de dados pessoais;
b) Deve ser nomeado com base nas qualificações profissionais e conhecimentos especializados no domínio do direito e das práticas de proteção de dados;
c) Os seus contactos devem ser publicados no portal do PDR2020 e comunicados à Autoridade de Controlo;
d) O PDR2020 deve apoiar o exercício das suas funções e fornecer os recursos necessários, nomeadamente na manutenção dos seus conhecimentos e garantindo o acesso aos dados e operações de tratamento;
e) Não pode ser destituído nem penalizado, pelo PDR2020 ou subcontratantes, pelo facto de exercer as suas funções, e reporta diretamente à gestão do PDR2020;
f) Pode ser contactado pelos titulares dos dados pessoais sobre todas as questões relacionadas com as atividades de tratamento e com os direitos que lhes são conferidos;
g) Está vinculado à obrigação de sigilo ou confidencialidade no exercício das suas funções;
h) Pode acumular outras funções caso se assegure a inexistência de conflito de interesses.

5.3.1 Responsabilidades do Encarregado de Proteção de Dados

Tendo em conta a natureza, o âmbito, o contexto, as finalidades do tratamento e os riscos associados, cabe ao EPD:

a) Informar e aconselhar o PDR2020, os subcontratantes e os trabalhadores que tratem os dados sobre as suas obrigações na proteção dos dados pessoais;
b) Comunicar os princípios, políticas, requisitos e procedimentos de proteção de dados pessoais a todos os envolvidos nas atividades de processamento de dados pessoais;
c) Controlar a conformidade com o RGPD, com os requisitos de proteção de dados e com os regulamentos e diplomas legais aplicáveis;
d) Coordenar, colaborar ou executar avaliações de impacto sobre a proteção de dados, conforme adequado;
e) Servir de ponto de contacto e cooperar com a Autoridade de Controlo.

O EPD deverá promover, pelo menos uma vez por ano, uma avaliação de conformidade com o RGPD, que possibilite aferir a evolução do nível de conformidade e maturidade da organização quanto aos processos de gestão e operações de proteção de dados pessoais.
Trimestralmente, o EPD deverá também dar informação à gestão do PDR2020 do grau de execução do *roadmap* de implementação das recomendações resultantes das avaliações de conformidade e das medidas de mitigação de risco em curso adotadas pela organização.

5.4 Responsabilidades do Gestor de Segurança da Informação

No âmbito da proteção de dados, cabe ao Gestor de Segurança da Informação (GSI):

a) Definir, estabelecer, monitorizar, avaliar e otimizar objetivos e requisitos de segurança em articulação com o EPD, tendo em vista a proteção da confidencialidade, integridade e disponibilidade da informação;
b) Garantir o correto alinhamento e comunicação dos processos do sistema de gestão de segurança da informação com os processos de gestão, tratamento e proteção de dados pessoais;

c) Garantir o envolvimento do EPD na introdução de conteúdos pedagógicos de proteção de dados pessoais no programa de formação do PDR2020 e na execução de ações de sensibilização e formação;
d) Articular com o EPD a concretização de processos de auditoria interna e externa, assegurando o adequado escrutínio do grau de cumprimento dos requisitos de segurança da informação e de proteção de dados, o reporte e o *follow-up* necessário;
e) Avaliar o desempenho da segurança dos dados pessoais em conjunto com o EPD.

5.5 Responsabilidades das Áreas Orgânicas Transversais e Operacionais

No âmbito das matérias relacionadas com a proteção de dados, cabe às Áreas Orgânicas Transversais e Operacionais:

a) Subscrever e cumprir os princípios de proteção de dados pessoais, as disposições presentes neste Regulamento e os procedimentos aplicáveis a cada um dos serviços;
b) Cumprir com as disposições deste Regulamento, aplicar os procedimentos estabelecidos, operacionalizar e monitorizar os mecanismos de segurança e de proteção dos dados pessoais;
c) Comunicar eventos adversos, falhas, pontos fracos e incidentes respeitantes à proteção de dados pessoais através dos canais para o efeito.

6. Princípios de Privacidade e de Proteção de Dados Pessoais

a) Princípio da licitude, lealdade e transparência: Os dados pessoais tratados pelo PDR2020 devem ser objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados;
b) Princípio da limitação das finalidades: Os dados pessoais são recolhidos segundo finalidades determinadas, explícitas e legítimas e não podem ser tratados de forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais.
c) Princípio da minimização dos dados: Os dados pessoais são recolhidos em quantidade mínima, adequados e limitados ao que é necessário pelas finalidades para as quais são tratados;

d) Princípio da exatidão: Os dados pessoais são mantidos exatos e atualizados, sempre que necessário, e são apagados ou retificados, sempre que se verifique algum grau de inexatidão;

e) Princípio da limitação da conservação: Os dados pessoais apenas são conservados pelo período necessário para as finalidades para as quais são tratados. O prazo de conservação dos dados pessoais pode ser alargado, desde que sejam tratados para fins de arquivo de interesse público ou para fins estatísticos ou de investigação histórica, e sejam aplicadas medidas e controlos de segurança que salvaguardem os direitos e liberdades do titular dos dados;

f) Princípio da integridade e confidencialidade: Os dados pessoais devem ser sujeitos a medidas e controlos de segurança no seu tratamento, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição, danificação, corrupção, acesso, alteração, disponibilização, roubo ou cópia, sejam as ocorrências involuntárias ou intencionais;

g) Princípio da responsabilidade demonstrada: O PDR2020 é responsável pelo cumprimento dos princípios relativos ao tratamento de dados pessoais e tem de poder comprová-lo.

7. Tratamento Lícito, Leal e Transparente

a) Para que o tratamento de dados pessoais possa ser executado, é necessário que se verifique, pelo menos, uma das seguintes situações:

   i. Obtenção do consentimento formal do titular dos dados para o tratamento dos seus dados pessoais para uma ou mais finalidades especificadas;
   ii. Se aplicável, para os dados pessoais de menores, salvo situações previstas e devidamente enquadradas na lei, o consentimento deve ser dado ou autorizado pelo titular das responsabilidades parentais;
   iii. Execução de um contrato no qual o titular dos dados é parte ou para diligências pré-contratuais a pedido do titular dos dados;
   iv. Cumprimento de uma obrigação legal a que o PDR2020 esteja sujeito;
   v. Defesa dos interesses vitais do titular dos dados ou de outra pessoa singular;
   vi. Exercício de funções de interesse público ou exercício da autoridade pública;
   vii. Prossecução de interesses legítimos pelo PDR2020 ou por terceiros.

b) A finalidade do tratamento deve ser específica, explícita e legítima, determinada por fundamentos jurídicos que prevejam as condições de licitude do tratamento, os tipos de dados objeto de tratamento, os titulares dos dados em questão, as entidades às quais os dados

poderão ser comunicados e para que efeitos, os limites a que as finalidades devem obedecer, os prazos de conservação, as operações e procedimentos de tratamento, incluindo as medidas destinadas ao controlo e segurança do tratamento;

c) O tratamento para fins que não sejam aqueles para os quais os dados pessoais foram inicialmente recolhidos, realizado sem o consentimento do titular dos dados, está sujeito a uma avaliação de compatibilidade do tratamento que considere:
   i. Qualquer ligação entre a finalidade para a qual os dados foram inicialmente recolhidos e a finalidade do tratamento posterior;
   ii. O contexto em que os dados pessoais foram recolhidos, designadamente o relacionamento entre o PDR2020 e o titular dos dados;
   iii. A natureza e a categoria dos dados pessoais;
   iv. As eventuais consequências do tratamento posterior para os titulares dos dados;
   v. A existência de salvaguardas adequadas.

d) Salvo situações previstas e devidamente enquadradas na lei ou quando o titular dos dados tiver dado o seu consentimento explícito, é proibido o tratamento de categorias especiais de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, os dados genéticos, os dados biométricos, os dados relativos à saúde, vida sexual ou orientação sexual e os dados pessoais relacionados com condenações penais e infrações.

8. Prestação de Informação e Comunicações com os Titulares dos Dados

a) A informação sobre o processamento dos dados pessoais é prestada de forma clara e concisa e gratuita ao titular dos dados, comprovada a sua identidade;

b) Os pedidos de informação relativos às medidas de tratamento tomadas devem ser satisfeitos no prazo máximo de um mês a contar da data de receção do pedido. Este prazo pode ser prorrogado até dois meses, devendo o titular dos dados ser informado de alguma prorrogação e dos motivos da demora;

c) Na impossibilidade de dar seguimento a um pedido apresentado pelo titular dos dados, este deve ser informado, no prazo máximo de um mês a contar da data de receção do pedido, das razões que levaram o PDR2020 a não tomar medidas e deve ser comunicada a possibilidade de apresentar uma reclamação à Autoridade de Controlo e intentar ação judicial;

d) Caso os pedidos de informação dos titulares dos dados se revelem infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, poderá ser cobrada uma taxa razoável – ou – o pedido poderá ser recusado e os motivos comunicados ao requerente.

8.1 Recolha de Dados Pessoais

a) Aquando da recolha dos dados pessoais, deve ser facultada ao titular dos dados a seguinte informação:

i. A identidade e os dados de contacto do PDR2020 e do seu representante, e os contactos do EPD;
ii. As finalidades e o fundamento jurídico do tratamento a que os dados pessoais se destinam;
iii. A origem dos dados pessoais, se estes forem recolhidos de outra fonte que não o titular dos dados;
iv. As categorias dos dados pessoais em questão;
v. Os destinatários dos dados pessoais, se aplicável;
vi. A intenção de transferir os dados para um país terceiro ou organização internacional, se houver, discriminando-se as garantias e os meios para se obter cópias das mesmas;
vii. O prazo de conservação dos dados pessoais ou os critérios para definir esse prazo;
viii. Todos os direitos dos titulares dos dados;
ix. A existência de uma Autoridade de Controlo, à qual podem ser apresentadas reclamações;
x. O enquadramento da comunicação dos dados pessoais, isto é, se constitui uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;
xi. A existência de tratamento automatizado de dados pessoais e as consequências previstas desse tratamento para o titular dos dados;
xii. Caso exista a intenção de proceder ao tratamento posterior dos dados pessoais para um fim diferente do da recolha inicial, o PDR2020 deve fornecer ao titular dos dados informações sobre esse fim, antes desse tratamento.

b) A informação referida em a) é fornecida no momento de recolha dos dados ou no momento da primeira comunicação com o titular dos dados, antes da execução de atividades de tratamento e antes da divulgação dos dados a outro destinatário;
c) Os dados pessoais devem permanecer confidenciais, em virtude da obrigação de sigilo profissional e da obrigação legal de confidencialidade.

9. Direitos dos Titulares de Dados Pessoais

9.1 Acesso aos Dados

a) Os titulares de dados pessoais têm o direito de aceder aos seus dados, de ser informados sobre as ações de tratamento sobre eles realizadas e ainda ter acesso à seguinte informação:
    i. Finalidades do tratamento dos dados;
    ii. Categorias dos dados pessoais em questão;
    iii. Destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão disponibilizados;
    iv. Prazos de conservação ou os critérios utilizados para a sua definição, caso não seja possível a definição do prazo;
    v. Os direitos dos titulares, que devem ser assegurados pelo PDR2020;
    vi. A origem dos dados, caso não tenham sido fornecidos pelo titular;
    vii. A existência de decisões baseadas no tratamento automatizado.
b) No caso de os dados serem transferidos para um país terceiro ou organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas para a transferência dos dados;
c) O titular dos dados tem o direito de solicitar cópia dos dados pessoais em fase de tratamento. Para o fornecimento de outras cópias, de informação em fase de armazenamento e arquivo, poderá ser aplicável uma taxa razoável, tendo em consideração os custos administrativos inerentes.

9.2 Retificação, Apagamento e Limitação do Tratamento

a) Os dados pessoais devem ser retificados, sempre que solicitado pelo titular dos dados, por motivos de incorreção ou incompletude;
b) O consentimento pode ser retirado pelo titular dos dados, a qualquer momento;
c) Os dados pessoais devem ser apagados, cumprindo-se o "direito ao esquecimento", quando solicitado pelo titular dos dados e quando se verifique um dos seguintes motivos:
    i. Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha;
    ii. É retirado o consentimento pelo titular dos dados;
    iii. O titular dos dados opõe-se ao tratamento dos dados pessoais sem que existam interesses legítimos prevalecentes;
    iv. Seja verificado algum tipo de tratamento ilícito;
    v. Exista uma obrigação jurídica para o apagamento;
d) O apagamento de dados não é aplicável sempre que se revele necessário:
    i. Ao exercício da liberdade de expressão e informação;
    ii. Ao cumprimento de uma obrigação legal que exija o tratamento dos dados;
    iii. Por motivos de interesse público no domínio da saúde pública;
    iv. Para fins de arquivo de interesse público, para fins de investigação científica ou histórica, ou para fins estatísticos, conforme previsto na Lei;
    v. Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.
e) A limitação do tratamento de dados pessoais pode ser solicitada pelo respetivo titular dos dados e deve ser aplicada sempre que:
    i. O titular dos dados contestar a exatidão dos dados pessoais, durante um período que permita ao PDR2020 verificar a sua exatidão;
    ii. Se verificar algum tipo de ilicitude no tratamento dos dados;
    iii. Os dados pessoais deixem de ser necessários para a finalidade que motivou a sua recolha;
    iv. Se o titular dos dados se tiver oposto ao tratamento dos dados pessoais, sem que existam interesses legítimos prevalecentes.
f) Estando limitado o tratamento de dados pessoais, os dados só podem ser objeto de novo padrão de tratamento com o consentimento do titular ou com fundamento legal;

g) O titular dos dados deve ser informado antes de ser anulada a limitação do referido tratamento;
h) O PDR2020 deve notificar, sem demora injustificada, cada destinatário a quem os dados pessoais tenham sido transmitidos de qualquer retificação, apagamento ou limitação de tratamento requeridas pelos titulares dos dados.

9.3 Portabilidade dos Dados

a) Sem prejuízo de direitos e liberdades de terceiros, deve ser assegurado ao titular dos dados a possibilidade de receber os seus dados pessoais num formato estruturado, de uso corrente e de leitura automática;
b) Deve ser assegurada a possibilidade de transmissão dos dados, sempre que tecnicamente possível, para outro responsável pelo tratamento de dados se:
    i. O tratamento for baseado no consentimento explícito do titular dos dados ou num contrato estabelecido entre o novo responsável e o titular dos dados;
    ii. O tratamento for realizado por meios automatizados.

9.4 Oposição e Decisões Automatizadas

a) O PDR2020 garante ao titular dos dados o direito de oposição ao tratamento. Nesse caso é cessado o tratamento dos dados pessoais, a não ser que existam interesses legítimos e fundamentos legais que prevaleçam sobre a oposição;
b) O titular dos dados pode opor-se ao tratamento de dados pessoais que lhe digam respeito para fins de investigação científica ou histórica ou para fins estatísticos, por motivos relacionados com a sua situação particular, salvo se o tratamento for necessário para a prossecução de atribuições de interesse público;
c) O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar, exceto se a decisão:
    i. For necessária para a celebração ou execução de um contrato entre o titular dos dados e o PDR2020;
    ii. For baseada no consentimento do titular dos dados.

10. Obrigações no Tratamento de Dados

a) Devem ser aplicadas medidas técnicas e processuais adequadas para documentar e comprovar que as atividades de tratamento são realizadas em conformidade com este Regulamento, com o código de conduta e com os procedimentos de tratamento de dados pessoais;
b) As medidas técnicas e processuais de proteção de dados, como a pseudonimização, devem ser definidas e aplicadas desde a conceção do tratamento, garantindo o cumprimento dos princípios de proteção de dados, tais como a minimização;
c) Só devem ser tratados os dados pessoais que forem necessários para cada finalidade específica de tratamento, em termos de:
    i. Quantidade de dados recolhidos;
    ii. Extensão do seu tratamento;
    iii. Prazo de conservação;
    iv. Disponibilidade e acesso.
d) Sempre que o tratamento de dados pessoais ocorra de forma partilhada entre duas ou mais entidades, a responsabilidade do tratamento é conjunta, devendo ser celebrado entre as partes um acordo que estabeleça um compromisso no cumprimento deste Regulamento e da legislação aplicável;
e) O acordo referido na alínea anterior deve conter as funções e relações dos responsáveis conjuntos pelo tratamento e dever ser dado conhecimento do essencial do acordo ao titular dos dados.

10.1 Subcontratação (Subcontratantes)

a) A subcontratação para tratamento de dados só pode ser efetuada relativamente a entidades que apresentem garantias suficientes da execução das medidas técnicas e processuais que satisfaçam os requisitos deste Regulamento e da legislação aplicável e que assegure a defesa dos direitos dos titulares de dados;
b) A subcontratação por um "Subcontratante" e as alterações pretendidas quanto ao número ou à substituição do prestador de serviços de tratamento de dados desse "Subcontratante" só podem ser realizadas mediante autorização escrita e específica do PDR2020;

c) A subcontratação é regulada por contrato ou outro ato normativo vinculativo que estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias de titulares, e as obrigações e direitos do PDR2020. Do contrato, ou outro ato normativo, devem constar ainda as seguintes obrigações do "Subcontratante":
   i. Tratamento dos dados pessoais mediante instruções documentadas;
   ii. Dever de confidencialidade e sujeição às obrigações legais de sigilo;
   iii. Adotar e coordenar com o PDR2020 todas as medidas de proteção de dados previstas neste Regulamento;
   iv. Responder ou prestar assistência na resposta aos pedidos dos titulares dos dados;
   v. Apagamento ou devolução de todos os dados pessoais depois de concluída a prestação de serviços de tratamento de dados;
   vi. Direito a auditar e inspecionar o cumprimento das obrigações de proteção de dados.

10.2 Registo das Atividades de Tratamento

Deve ser conservado um registo de todas as atividades de tratamento, contendo, pelo menos, as seguintes informações:

i. Nome e contactos do responsável pelo tratamento e do seu representante e os contactos do EPD;
ii. Finalidades do tratamento;
iii. Descrição das categorias de titulares e de dados pessoais;
iv. Categorias de destinatários a quem os dados pessoais são fornecidos;
v. Países terceiros ou organizações internacionais para onde são transferidos os dados pessoais;
vi. Descrição geral das medidas técnicas e organizativas de segurança;
vii. Prazos de conservação para as diferentes categorias de dados.

É da responsabilidade dos Secretários Técnicos e dos Coordenadores de cada uma das Áreas Orgânicas Transversais e Operacionais garantir e manter atualizado o registo das atividades de tratamento.
Após a criação dos respetivos registos iniciais de cada uma das atividades de tratamento, os mesmos deverão ser revistos, pelo menos, uma vez por ano.
Sempre e quando existam novas atividades de tratamento, o respetivo registo inicial deverá ser efetuado antes de quaisquer operações de tratamento e após a validação do EPD.

11. Segurança do Tratamento

a) O PDR2020 e os subcontratantes devem aplicar medidas técnicas e organizativas de segurança adequadas ao nível de risco, incluindo:
   i. Pseudonimização e cifragem;
   ii. Capacidade de assegurar a confidencialidade, a integridade, a disponibilidade e a resiliência dos sistemas;
   iii. Um processo de monitorização, avaliação e melhoria das medidas e mecanismos de segurança.
b) O nível de segurança a aplicar é determinado pelo apuramento do nível de risco do tratamento;
c) Deve ser assegurado que qualquer pessoa que tenha acesso aos dados pessoais só procede ao seu tratamento após a adesão ao código de conduta e mediante os procedimentos de tratamento.

11.1 Notificação de Violação de Dados Pessoais à Autoridade de Controlo

a) Em caso de violação de dados pessoais suscetível de resultar em risco para os direitos e liberdades dos titulares dos dados, a Autoridade de Controlo deve ser notificada num prazo de até 72 horas;
b) O subcontratante deve notificar o PDR2020, sem demora injustificada, após o conhecimento de uma violação de dados pessoais;
c) A notificação deve:
   i. Descrever a natureza da violação dos dados pessoais, as categorias afetadas, o número de titulares de dados afetados e o número de registos de dados pessoais em causa;
   ii. Indicar o nome e os contactos do EPD;
   iii. Descrever as consequências prováveis do evento;
   iv. Descrever as medidas adotadas para tratamento e resolução da violação de dados pessoais.
d) O tratamento de quaisquer violações de dados pessoais deve ser devidamente documentado e os registos conservados para posterior rastreamento e histórico.

Quando os Secretários Técnicos ou Coordenadores das Áreas Orgânicas Transversais e Operacionais tenham conhecimento de uma violação de dados pessoais, deverão comunicá-la ao EPD e ao gestor do PDR2020.

O PDR2020, representado pelo seu gestor, deverá notificar a respetiva violação de dados pessoais à Autoridade de Controlo, sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar em conformidade com o principio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares.

Se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso.

11.2 Comunicação da Violação de Dados Pessoais ao Titular dos Dados

a) Sempre que a violação de dados pessoais envolva risco para os direitos e liberdades de pessoas singulares, o titular dos dados deve ser informado sem demora injustificada;
b) A comunicação deve:
    i. Indicar o nome e os contactos do EPD;
    ii. Descrever as consequências prováveis do evento;
    iii. Descrever as medidas adotadas para tratamento e resolução da violação de dados pessoais.
c) A comunicação não é exigida:
    i. Se os dados pessoais estiverem cifrados e, por isso, ilegíveis para terceiros;
    ii. Se os riscos para os direitos e liberdades forem imediatamente mitigados e não suscetíveis de se concretizar;
    iii. Se implicar um esforço desproporcionado, devendo, neste caso, ser efetuada uma comunicação pública.

O PDR2020, representado pelo seu gestor, deverá informar, sem demora injustificada, o titular dos dados da violação de dados pessoais quando for provável que desta resulte um elevado risco para os direitos e liberdades da pessoa singular, a fim de lhe permitir tomar as precauções necessárias.

A comunicação deverá descrever, em linguagem simples e clara, a natureza da violação de dados pessoais e dirigir recomendações à pessoa singular em causa para atenuar potenciais efeitos adversos. Essa comunicação aos titulares dos dados deverá ser efetuada logo que seja razoavelmente possível, em estreita cooperação com a Autoridade de Controlo e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de polícia.

12. Avaliação de Impacto e Consulta Prévia

a) Antes de iniciar um novo tratamento dos dados pessoais, deve ser conduzida uma avaliação de impacto sobre os direitos e liberdades dos titulares dos dados, caso seja passível de acarretar um elevado risco para os direitos e liberdades das pessoas singulares;
b) Sempre que o tratamento for automatizado, envolver uma avaliação sistémica e completa dos dados pessoais, incluir definição de perfis, envolver categorias especiais de dados ou incidir sobre o controlo sistemático de zonas acessíveis ao público em grande escala, a realização de avaliação de impacto de proteção de dados é obrigatória;
c) A avaliação deve incluir, pelo menos:
    i. A descrição das operações de tratamento previstas e a finalidade do tratamento;
    ii. A avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;
    iii. A avaliação dos riscos para os direitos e liberdades dos titulares dos dados;
    iv. As medidas para fazer face aos riscos e assegurar a proteção dos dados pessoais.
d) Quando necessário, pode ser efetuada uma consulta junto dos titulares dos dados para a identificação e caracterização mais precisa dos riscos e impactos;
e) Sempre que necessário ou quando ocorram alterações aos riscos ou às operações de tratamento, deve ser realizado um controlo para avaliar a conformidade do tratamento com a avaliação de impacto;
f) Caso a avaliação de impacto resulte num elevado nível de risco e se verifique a impossibilidade de aplicação de medidas ou mecanismos de atenuação do risco, deve ser realizada uma consulta à Autoridade de Controlo antes de proceder a quaisquer operações de tratamento. Nesta consulta devem ser comunicados os seguintes elementos:
    i. A repartição de responsabilidades entre o PDR2020, responsáveis conjuntos e subcontratantes envolvidos no tratamento;

ii. As finalidades e meios de tratamento;
iii. As medidas e garantias previstas para a defesa dos direitos e liberdades dos titulares dos dados;
iv. Os contactos do EPD;
v. A avaliação de impacto.

A fim de promover o cumprimento do RGPD nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares o PDR2020 deverá promover, sob proposta dos Secretários Técnicos e os Coordenadores de cada uma das Áreas Orgânicas Transversais e Operacionais, a realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco.

Antes da realização de uma avaliação de impacto sobre a proteção de dados, deverá ser solicitado o parecer do EPD.

Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o RGPD.

Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o PDR2020 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.

É da responsabilidade dos Secretários Técnicos e dos Coordenadores de cada uma das Áreas Orgânicas Transversais e Operacionais propor ao gestor do PDR2020, uma vez por ano, uma avaliação de impacto da proteção de dados das atividades de tratamento em operação.

13. Transferências de Dados Pessoais para Países Terceiros

a) O PDR2020 ou os subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.

b) As garantias adequadas referidas na alínea a) podem ser previstas, sem requerer nenhuma autorização específica da Autoridade de Controlo, por meio de:
   i. Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos;
   ii. Regras vinculativas aplicáveis às empresas;
   iii. Cláusulas-tipo de proteção de dados adotadas pela Comissão ou adotadas pela Autoridade de Controlo e aprovadas pela Comissão;
   iv. Um código de conduta, acompanhado de compromissos vinculativos e com força executiva assumidos pelo PDR2020 ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados; ou
   v. Um procedimento de certificação, aprovado nos termos do artigo 42.º do RGPD, acompanhado de compromissos vinculativos e com força executiva assumidos pelo PDR2020 ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados.

c) Sob reserva de autorização da Autoridade de Controlo, podem também ser previstas garantias adequadas, nomeadamente por meio de cláusulas contratuais entre o PDR2020 ou subcontratantes e os responsáveis pelo tratamento, subcontratantes ou destinatários dos dados pessoais no país terceiro ou organização internacional ou através de disposições a inserir nos acordos administrativos entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados.

d) O PDR2020 ou os subcontratantes podem realizar uma transferência de dados pessoais para um país terceiro ou uma organização internacional, sem necessidade de autorização específica da Autoridade de Controlo, se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado.

e) As decisões judiciais e as decisões de autoridades administrativas de um país terceiro que exijam que o PDR2020 ou o subcontratante transfiram ou divulguem dados pessoais só são reconhecidas ou executadas se tiverem como base um acordo internacional, como um acordo de assistência judiciária mútua, em vigor entre o país terceiro em causa e a União ou um dos Estados-Membros.

f) Na falta de uma decisão de adequação da Comissão ou de garantias adequadas, as transferências ou conjunto de transferências de dados pessoais para países terceiros ou organizações internacionais só podem ser efetuadas pelo PDR2020 caso se verifique uma das seguintes condições:

i. O titular dos dados tiver explicitamente dado o seu consentimento à transferência prevista, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas;

ii. A transferência for necessária para a execução de um contrato entre o titular dos dados e o PDR2020 ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados;

iii. A transferência for necessária para a celebração ou execução de um contrato, celebrado no interesse do titular dos dados, entre o PDR2020 e outra pessoa singular ou coletiva;

iv. A transferência for necessária por importantes razões de interesse público;

v. A transferência for necessária à declaração, ao exercício ou à defesa de um direito num processo judicial;

vi. A transferência for necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento;

vii. A transferência for realizada a partir de um registo que, nos termos do direito da União ou do direito nacional, se destine a informar o público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar nela ter um interesse legítimo, mas apenas na medida em que as condições de consulta estabelecidas no direito da União ou no direito nacional se encontrem preenchidas nesse caso concreto.

14. Revisão e Melhoria Contínua

O presente Regulamento e as medidas de tratamento de dados pessoais devem ser revistas e atualizadas consoante aos requisitos legais e normativos do PDR2020.

15. Matriz de Responsabilidades (RACI)

Atividade	Gestão	EPD	GSI	Áreas
Aprovação do Regulamento	A	C I	I	I
Comunicação do Regulamento	A R	A R	I	I
Revisão do Regulamento	I	A	C	C
Revisão e Melhoria Contínua	I	A	C	C

Legenda:

Responsabilidade (R):	Responsável por executar a atividade, o executante.
Autoridade (A):	Responsável pela atividade, o dono.
Consultado (C):	Quem deve ser consultado e participar na decisão/atividade no momento em que for executada.
Informado (I):	Quem deve receber a informação de que a atividade foi executada.

16. Documentos Associados

Roadmap de implementação das recomendações resultantes das avaliações de conformidade.