



Bombeiros das
Caldas da Rainha



CÓDIGO DE CONDUTA

Índice

1. Enquadramento.....	3
2. Princípios a seguir.....	4
3. Conceitos aplicáveis	5
4. Licidade do tratamento de dados	10
5. Direitos dos titulares dos dados	11
6. Consentimento	16
7. Acesso a dados pessoais por parte das autoridades competentes	17
8. Marketing	18
9. Responsabilidade da AHBVCR enquanto responsável de tratamento de dados	19
10. Relação com subcontratantes	21
11. Segurança do tratamento.....	22
12. Violação de dados.....	23
13. Registos	24
14. Videovigilância	25
15. Titulares de dados pessoais	26
16. Procedimentos de proteção de dados pessoais.....	27
17. Processos para o futuro	28

1. Enquadramento

A 25 de Maio de 2016 entrou em vigor o Regulamento Geral de Proteção de Dados. Sendo que a partir de 25 de Maio de 2018 se deu início à fiscalização das normas aí contidas. Neste documento utilizaremos as siglas REPD e RGPD para nos referirmos ao Regulamento.

O Regulamento diz respeito ao tratamento de dados pessoais e à proteção de pessoas singulares, aplicando-se em todos os Estados Membros.

Apesar de já existirem normas neste âmbito – pela Lei de Proteção de Dados – o Regulamento Europeu visa agora uniformizar essas regras, trazendo novas obrigações e reforçando assim as matérias de proteção de dados pessoais em todos os Estados Membros.

Assim, e tendo em conta que a AHBVCR, na prossecução da sua atividade, tem acesso e trata dados pessoais, elaborou o presente Código de Conduta para especificar as boas práticas a seguir nesta matéria, assegurando o cumprimento de todas as normas previstas no REPD de modo transversal.

Como tal, o presente visa, assegurar e demonstrar o compromisso e respeito pela Lei, mas sobretudo ser um instrumento de apoio a todos os colaboradores, dado que no mesmo se transmitem informações que visam a proteção dos dados pessoais de cada um.

A presente Política de Privacidade aplica-se em exclusivo à recolha e tratamento de dados pessoais efetuados pela AHBVCR e tem de ser seguida por todos os colaboradores.

2. Princípios a seguir

O tratamento dos dados pessoais deve obedecer aos seguintes princípios:

- Tratamento lícito, leal e transparente;
- Recolha de dados efetuada de acordo com a sua finalidade específica, explícita e legítima;
- Utilização dos dados apenas para a finalidade inicialmente definida;
- Recolha de dados de modo adequado, relevante e limitado ao necessário no âmbito da prestação do serviço em causa;
- Precisão e atualização dos dados;
- Manutenção de dados apenas pelo tempo necessário;
- Tratamento dos dados de modo a assegurar um nível de segurança adequado ao disposto no RGPD.

3. Conceitos aplicáveis

Para o pleno cumprimento do RGPD, todos devem conhecer os termos aplicáveis nesta matéria.

São eles:

- **Autoridade de controlo:**
Comissão Nacional de Proteção de Dados.
- **Consentimento:**
O consentimento do titular dos dados, é 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.
- **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.
- **Dados genéticos:**
Dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que dêem 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.
- **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
- **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.

- **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.

- **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.

- **Empresa:**

Uma pessoa singular ou coletiva que, independentemente da sua forma jurídica, exerce uma atividade económica, incluindo as sociedades ou associações que exercem regularmente uma atividade económica.

- **Estabelecimento principal:**

a) No que se refere a um responsável pelo tratamento com estabelecimentos em vários Estados-Membros, o local onde se encontra a sua administração central na União, a menos que as decisões sobre as finalidades e os meios de tratamento dos dados pessoais sejam tomadas noutra estabelecimento do responsável pelo tratamento na União e este último estabelecimento tenha competência para mandar executar tais decisões, sendo neste caso o estabelecimento que tiver tomado as referidas decisões considerado estabelecimento principal;

b) No que se refere a um subcontratante com estabelecimentos em vários Estados-Membros, o local onde se encontra a sua administração central na União ou, caso o subcontratante não tenha administração central na União, o estabelecimento do subcontratante na União onde são exercidas as principais atividades de tratamento no contexto das atividades de um estabelecimento do subcontratante, na medida em que se encontre sujeito a obrigações específicas nos termos do regulamento.

- **Ficheiro:**

Qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico.

- **Grupo empresarial:**

Um grupo composto pela empresa que exerce o controlo e pelas empresas controladas.

- **Limitação do tratamento:**

A inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro.

- **Objeção pertinente e fundamentada:**

Uma objeção a um projeto de decisão que visa determinar se há violação do presente regulamento ou se a ação prevista relativamente ao responsável pelo tratamento ou ao subcontratante está em conformidade com o presente regulamento, demonstrando claramente a gravidade dos riscos que advêm do projeto de decisão para os direitos e liberdades fundamentais dos titulares dos dados e, eventualmente, para a livre circulação de dados pessoais no território da União.

- **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.

- **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.

- **Regras vinculativas aplicáveis às empresas:**

As regras internas de proteção de dados pessoais aplicadas por um responsável pelo tratamento ou um subcontratante estabelecido no território de um Estado-Membro para as transferências ou conjuntos de transferências de dados pessoais para um responsável ou subcontratante num ou mais países terceiros, dentro de um grupo empresarial ou de um grupo de empresas envolvidas numa atividade económica conjunta.

- **Representante:**

Uma pessoa singular ou coletiva estabelecida na União que, designada por escrito pelo responsável pelo tratamento ou subcontratante, nos termos do artigo 27º, representa o responsável pelo tratamento ou o subcontratante no que se refere às suas obrigações respetivas nos termos do presente regulamento.

- **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.

- **Serviços da sociedade da informação:**

Um serviço definido no artigo 1º, nº 1, alínea b), da Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, ou seja, qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços. Para efeitos da presente definição, entende-se por:

i) «à distância»: um serviço prestado sem que as partes estejam simultaneamente presentes,

ii) «por via eletrónica»: um serviço enviado desde a origem e recebido no destino através de instrumentos eletrónicos de processamento (incluindo a compressão digital) e de armazenamento de dados, que é inteiramente transmitido, encaminhado e recebido por cabo, rádio, meios óticos ou outros meios eletromagnéticos,

iii) «mediante pedido individual de um destinatário de serviços»: um serviço fornecido por transmissão de dados mediante pedido individual;

- **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.

- **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.

- **Tratamento Transfronteiriço:**

a) O tratamento de dados pessoais que ocorre no contexto das atividades de estabelecimentos em mais do que um Estado-Membro de um responsável pelo tratamento ou um subcontratante na União, caso o responsável pelo tratamento ou o subcontratante esteja estabelecido em mais do que um Estado-Membro; ou

b) O tratamento de dados pessoais que ocorre no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, mas que afeta substancialmente, ou é suscetível de afetar substancialmente, titulares de dados em mais do que um Estados-Membro.

- **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.

- **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.

4. Licitude do tratamento de dados

Para que o tratamento de dados possa ser lícito tem de preencher uma (ou mais) das seguintes condições (bases de licitude):

- Consentimento do titular
- Obrigação legal
- Necessidade de efetuar um contrato
- Diligências pré-contratuais que o titular dos dados solicite
- Fundamento previsto por lei (por exemplo, defesa dos legítimos interesses da empresa, defesa dos interesses vitais do titular).

Os dados pessoais devem ser utilizados apenas para a finalidade específica, devem ser mantidos de forma segura e não devem ser divulgados a terceiros, excepto quando autorizado ou nas situações previstas na lei.

5. Direitos dos titulares dos dados

A AHBVCR, enquanto responsável pelo tratamento deverá assegurar os direitos dos titulares quanto à proteção de dados.

Assim, deve assegurar-se que toma medidas para garantir que a pessoa que pretende exercer os direitos sobre dados é de facto o titular dos mesmos. Se existirem dúvidas razoáveis sobre a identidade da pessoa que apresenta o pedido, a AHBVCR pode pedir informação adicional para confirmar a identidade/legitimidade.

A AHBVCR fornece ao titular dos dados informações sobre a/s medida/s tomada/s relativamente ao/s seu/s pedido/s sem demora injustificada e no prazo de um mês. Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. Se assim, for, a AHBVCR informa o titular dos dados da prorrogação e motivo a ela associado.

Caso não seja dado seguimento ao/s pedido/s, a AHBVCR informa o titular dos dados no prazo de um mês, indicando os motivos que levaram a não tomar a/s medida/s, bem como a possibilidade do titular dos dados reclamar dessa situação junto da autoridade de controlo e intentar ação judicial.

As informações e comunicações a este nível têm um carácter gratuito – contudo, caso os pedidos sejam manifestamente infundados ou excessivos (nomeadamente pelo seu carácter repetitivo), a AHBVCR reserva-se o direito de cobrar uma taxa ajustada aos custos que possa ter com o pedido, ou a recusar o seguimento do pedido.

O titular de dados que pretenda exercer qualquer um dos direitos previstos no Regulamento, deverá enviar o seu pedido por escrito para privacidade@bombeirosrainha.pt.

Nesse pedido o titular dos dados deverá indicar que direito pretende exercer, descrevendo-o, bem como identificar-se e fornecer os seus contactos. Depois de tratada a situação (com a respetiva resposta ao titular dos dados) a situação deverá ser arquivada com registo das medidas adotadas.

- **Informações a prestar na recolha de dados pessoais:**
 - a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante e do encarregado da proteção de dados;
 - b) As finalidades do tratamento e o respetivo fundamento jurídico;

- c) Especificar se o tratamento dos dados se baseia em interesse legítimos da AHBVCR, ou de terceiros;
- d) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
- e) Se for caso disso, o facto da AHBVCR tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas;
- f) Prazo para conservação dos dados pessoais, ou não sendo possível, os critérios para definir o prazo;
- g) Os direitos que tem e como os pode exercer;
- h) O direito de apresentar reclamação a uma autoridade de controlo;
- i) Se a comunicação de dados pessoais constitui ou não 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;
- j) A existência de decisões automatizadas bem como a importância e as consequências previstas de tal tratamento para o titular dos dados, caso existam.

- **Direito ao acesso**

O titular dos dados tem o direito por parte da AHBVCR a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:

- a) As finalidades do tratamento;
- b) As categorias dos dados pessoais em questão;
- c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;
- d) O prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;
- e) Direito de retificação, apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;
- f) O direito de apresentar reclamação a uma autoridade de controlo;
- g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;

h) A existência de decisões automatizadas, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados – se aplicável.

- **Direito à rectificação**

O titular dos dados tem direito à rectificação de dados pessoais inexatos ou incompletos que lhe digam respeito. Para esse efeito o titular dos dados deve solicitar por escrito que alterações devem ser feitas e (se aplicável) apresentar documentação/ informação credível para o efeito. A AHBVCR deve comunicar a retificação dos dados a entidades terceiras para os quais foram transmitidos a menos que não se afigure possível ou que implique um esforço desproporcionado.

- **Direito à portabilidade**

A AHBVCR tem de fornecer, se solicitado pelo titular, os dados pessoais que lhe digam respeito e que foram objeto de tratamento, num formato estruturado, de uso corrente e de leitura automática.

Além disso, não se pode opor à transmissão desses dados a outro responsável pelo tratamento.

- **Direito à oposição**

O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular.

A esse título, a AHBVCR, quando o titular pretenda exercer o direito de oposição, cessa o tratamento de dados, a menos que existam razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

- **Direito à limitação do tratamento**

O titular dos dados tem o direito de obter a limitação do tratamento, se se aplicar uma das seguintes situações:

- a) Contestar a exatidão dos dados pessoais, durante um período que permita à AHBVCR verificar a sua exatidão;
- b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;

c) A AHBVCR não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;

d) Se tiver oposto ao tratamento por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, seja no âmbito de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento, seja no caso de o tratamento prosseguir os interesses legítimos prosseguidos pela AHBVCR ou por terceiros, ou ainda quando o tratamento seja efectuado para fins diferentes daqueles para os quais os dados foram recolhidos ou sem autorização do titular.

Nesses casos, a AHBVCR, suspende o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, até se verificar que os motivos legítimos da AHBVCR prevalecem sobre os do titular dos dados.

- **Direito ao apagamento (“direito a ser esquecido”)**

O titular dos dados pessoais pode solicitar que os mesmos sejam totalmente eliminados, sem demora injustificada e a AHBVCR obriga-se a cumprir com esse pedido, nas seguintes situações:

- a) Os dados deixaram de ser necessários para a finalidade que motivou a recolha ou tratamento;
- b) O titular retirou o consentimento no qual se baseia o tratamento e não existe outro fundamento jurídico que justifique o tratamento dos dados;
- c) O titular exerce o seu direito de oposição por motivos relacionados à sua situação particular e não existem interesses legítimos prevalecentes que justifiquem o tratamento;
- d) O titular exerce o seu direito de oposição quando os dados pessoais são tratados para efeito de comercialização direta;
- e) Existe obrigação jurídica para o apagamento;
- f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.o, n.o 1

Caso a AHBVCR tenha tornado públicos os dados pessoais e se veja obrigada, nos termos anteriores a os eliminar, tomará as medidas que forem razoáveis, incluindo de carácter

técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.

6. Consentimento

A AHBVCR recolhe o devido consentimento de todos os titulares para o tratamento dos dados previamente, ou simultaneamente, à sua recolha.

Se o consentimento for legalmente necessário para o tratamento de dados pessoais, o titular dos dados tem o direito de retirar o seu consentimento em qualquer altura, embora esse direito não comprometa a licitude do tratamento efetuado com base no consentimento previamente dado nem o tratamento posterior dos mesmos dados, baseado noutra base legal, como é o caso do cumprimento do contrato ou da obrigação legal a que a AHBVCR esteja sujeita.

Para revogar o seu consentimento, pode contactar-nos através de:

Correio Postal: Rua 31 de Janeiro, 2500-118 Caldas da Rainha

Telefone: 262 840 550

Email: privacidade@bombeirosrainha.pt

7. Acesso a dados pessoais por parte das autoridades competentes

A Comissão Nacional de Proteção de Dados tem a responsabilidade de fiscalizar o cumprimento do RGPD, portanto, pode solicitar informações sobre essa matéria e ter acesso às instalações da AHBVCR.

O titular que pretenda consultar a Autoridade Nacional de Controlo, poderá utilizar os seguintes contactos:

Comissão Nacional de Proteção de Dados (CNPd)

Rua de São Bento, n.º 148, 3º, 1200-821 Lisboa,

Tel: 351 213928400, Fax: +351 213976832,

e-mail: geral@cnpd.pt

www.cnpd.pt

8. Marketing

Sempre que a AHBVCR proceda ao envio de mensagens de marketing cuja recepção seja independente da intervenção do destinatário, procede ao prévio consentimento do mesmo – caso se trate de pessoa em nome individual. No caso de mensagens para pessoas coletivas, não será solicitado o consentimento, contudo, as mensagens contêm sempre a possibilidade de deixar de receber esse tipo de conteúdo.

É sempre salvaguardada a possibilidade de recusa destas mensagens de forma rápida e fácil (por ex. a opção *unsubscribe* nos emails).

A partir do momento que o destinatário recuse o envio, deixam de ser enviadas as mensagens de marketing.

9. Responsabilidade da AHBVCR enquanto responsável de tratamento de dados

A AHBVCR compromete-se a aplicar as medidas técnicas e organizativas adequadas para assegurar e comprovar que o tratamento dos dados é feito em conformidade com a legislação em vigor.

9.1. Encarregado de Proteção de dados (DPO/EPD)

a. Direitos e deveres

O EPD é uma figura independente que deve prosseguir e controlar a protecção de dados durante o seu tratamento.

O EPD está autorizado a desempenhar outras tarefas, caso estas não deem origem a conflitos de interesses.

Em termos de funções, cabe ao EPD:

- O EPD é convidado a participar regularmente nas reuniões dos quadros de gestão médios e superiores;
- A sua presença é recomendada sempre que sejam adotadas decisões com implicações na proteção de dados. Todas as informações pertinentes são transmitidas oportunamente ao EPD, para que este possa prestar um aconselhamento adequado;
- O parecer do EPD é sempre devidamente ponderado;
- O EPD é imediatamente consultado após a ocorrência de uma violação de dados ou outro incidente;
- Incumbe ao EPD, entre outras funções, de controlar a conformidade com

No âmbito destas atribuições de controlo da conformidade, os EPD podem, nomeadamente:

- Recolher informações para identificar as atividades de tratamento;
- Analisar e verificar a conformidade das atividades de tratamento;
- Prestar informações e aconselhamento e formular recomendações ao responsável pelo tratamento ou ao subcontratante.

“O controlo da conformidade não significa que a responsabilidade pessoal do EPD seja imputada em caso de incumprimento. O RGPD esclarece que compete ao responsável pelo tratamento, e não ao EPD, aplicar «as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento» (art. 24.º, n.º 1). O cumprimento das regras de proteção de dados é uma competência empresarial do responsável pelo tratamento de dados, e não do EPD.”¹

b. Nomeação e “mandato”

A AHBVCR decide nomear como EPD o secretário adjunto da Direcção, uma vez que, sendo alguém ligado à mesma não detém funções que impliquem conflito de interesses.

Esta atribuição está intimamente ligada ao cargo inerente, seguindo a regra de nomeação e mandato do mesmo.

A composição da Direcção está publicada no site da Associação, <https://www.bombeirosrainha.pt/associacao>

O contacto do EPD é o seguinte:

Telef.: 925964421

Email.: epd@bombeirosrainha.pt

¹ https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf

10. Relação com subcontratantes

Quaisquer pessoas singulares ou coletivas que tratem os dados pessoais por conta da AHBVCR, ou que tenham a eles acesso terão de apresentar garantias do cumprimento de todas as exigências legais assegurando a proteção dos dados.

Para esse efeito, caso o subcontratante não o faça previamente e por iniciativa própria, a AHBVCR solicita a emissão de uma declaração de compromisso para o efeito.

11. Segurança do tratamento

Quer a AHBVCR, quer os seus subcontratantes, aplicam medidas técnicas e organizativas adequadas para assegurar o nível de segurança adequado ao risco.

Para esse efeito, é efetuada a avaliação dos riscos/ vulnerabilidades do sistema de tratamento de dados, prevendo o seu impacto para os titulares, e definindo as medidas de controlo adequadas. Esta situação é particularmente direcionada para os riscos de destruição, perda e alteração acidentais ou ilícitas, bem como para a divulgação ou acesso não autorizado de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Após avaliação do impacto, a AHBVCR poderá recorrer aos seguintes mecanismos – consoante a situação:

- a) Pseudonimização e cifragem dos dados pessoais;
- b) Capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
- c) Capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
- d) Processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

A AHBVCR e seus subcontratantes asseguram que qualquer pessoa singular sob sua autoridade, ao ter acesso a dados pessoais, só procede ao seu tratamento mediante instruções do responsável, a menos que tal represente uma exigência legal.

12. Violação de dados

A violação de dados pessoais representa uma quebra de segurança que provoca, de forma accidental ou ilícita, a destruição, perda, alteração, divulgação ou acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

A AHBVCR, é obrigada a notificar a autoridade de controlo quando detetar violação de dados pessoais, sem demora injustificada e sempre que possível dentro de 72 horas após tomar conhecimento da mesma. Essa situação não se aplica quando a violação de dados não seja suscetível de resultar risco para os direitos e liberdades das pessoas singulares.

Quando não for possível enviar a notificação dentro de 72 horas, a mesma irá acompanhada do fundamento do atraso.

A notificação terá de conter a seguinte informação:

- natureza da violação dos dados pessoais, incluindo, se possível, as categorias e número aproximado de titulares de dados afetados, bem como as categorias e número aproximado de registos de dados pessoais em causa;
- nome e contactos do encarregado de proteção de dados ou de outro ponto de contacto através do qual possam ser obtidas mais informações;
- consequências prováveis da violação de dados pessoais;
- quais as medidas adotadas ou propostas para reparar a violação de dados, e, se aplicável, medidas para atenuar eventuais efeitos negativos.

Se não for possível dar desde logo todas estas indicações, a AHBVCR irá enviá-las faseadamente.

Qualquer violação de dados pessoais será devidamente documentada, bem como as respetivas medidas de correção aplicadas.

Procedimento interno: em 24 horas será desencadeado inquérito interno para aferir eventuais responsabilidades e danos causados que terminará o mais tardar 7 dias mais tarde.

Notificação ao titular: em 7 dias será comunicada ao titular dos dados as conclusões

Registo dos procedimentos: o procedimento será registado em impresso próprio nos termos já existentes para as restantes ocorrências.

13. Registos

A AHBVCR deve garantir o conhecimento, a todo o tempo, dos ativos de informação relativamente a dados pessoais, de modo a permitir identificar inequivocamente o estado da informação em todo o seu ciclo de vida.

Assim, mantém um registo atualizado de todas as atividades de tratamento sob sua responsabilidade, com as seguintes informações:

- Nome e contactos da AHBVCR, seus representantes legais e encarregado de proteção de dados;
- Finalidades do tratamento de dados pessoais;
- Descrição das categorias de titulares de dados e categorias de dados pessoais;
- Categorias dos destinatários a quem os dados foram ou serão divulgados;
- Transferências de dados pessoais para países terceiros – caso existam;
- Prazos para apagamento dos dados, sempre que possível;
- Descrição geral de medidas técnicas e organizativas no domínio da segurança, sempre que possível.

Para as situações em que a AHBVCR é subcontratante, mantém registo atualizado das atividades de tratamento realizadas em nome do responsável pelo tratamento de dados pessoais, o qual tem as seguintes informações:

- Nome e contactos de cada responsável de tratamento de dados pessoais, seus representantes legais e encarregado de proteção de dados;
- Categorias de tratamento de dados pessoais efetuados em nome de cada responsável;
- Categorias dos destinatários a quem os dados foram ou serão divulgados;
- Transferências de dados pessoais para países terceiros – caso existam;
- Nome e contactos de subcontratante contratado, se aplicável;
- Descrição geral de medidas técnicas e organizativas no domínio da segurança, sempre que possível.

14. Videovigilância e Geolocalização

Existe sistema de videovigilância nas instalações, bem como sistemas de geolocalização nos veículos de assistência e socorro com vista à protecção de pessoas e bens, sistema assegurado pela Skyview nos termos contratualizados.

15. Titulares de dados pessoais

À data da elaboração deste documento, os titulares dos dados pessoais sujeitos a tratamento, no âmbito da relação que detenham com a AHBVCR, são os seguintes:

- a) **Órgãos Sociais**
- b) **Candidatos a emprego**
- c) **Trabalhadores**
- d) **Voluntários**
- e) **Sócios**
- f) **Utentes**
- g) **Público em Geral**
- h) **Fornecedores**

16. Procedimentos de proteção de dados pessoais

Os dados pessoais tratados devem restringir-se, sempre que possível, ao essencial para o cumprimento da finalidade a que se destinam. Por exemplo: para emissão de fatura é necessário apenas o nome e o número de identificação fiscal.

O arquivo de dados é feito em local de acesso restrito, devendo apenas ser acedido por colaboradores cuja função/ responsabilidades assim o justifique.

a. Informática

Cada colaborador (cujas funções dependam do uso de computador) tem um código de acesso individual no sistema informático.

O perfil de acesso a dados/ informação no sistema é definido de acordo com as funções do colaborador (dando-lhe acesso apenas aos dados necessários no âmbito da função).

b. Medidas Técnicas e Organizativas

(descrever medidas informáticas aplicáveis após análise do Relatório e proposta de actuação)

17. Processos para o futuro

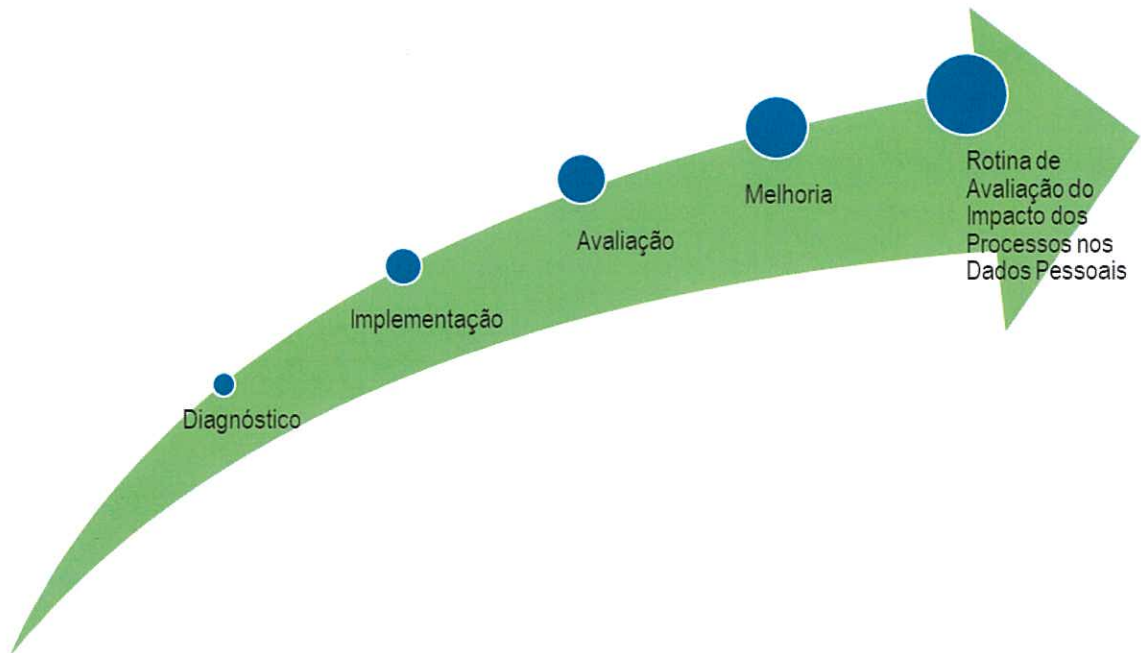
Medida	Tarefa	Responsável	Observações
Analisar anualmente a necessidade de EPO	Efetuar análise do impacto para a proteção de dados quanto ao tipo de dados tratados e aos titulares	Serviços Administrativos	Anual
Rever a Política de Privacidade	Rever regras existentes, nomeadamente período de retenção	Direcção	Imediata
Criar Regulamento Interno de RGPD	Rever regras existentes, nomeadamente período de retenção, regras de destruição e arquivo	Direcção	Imediata
Rever impressos de RH	Rever declaração de confidencialidade, ficha de funcionário, procedimentos de cópia de documentos de identificação, entre outros.	Serviços Administrativos	Imediata
Rever procedimentos (recolha de contactos, ficha de clientes, arquivo)	Rever procedimentos internos	Serviços Administrativos	Semestral
Rever procedimentos informáticos	Rever acessos e segurança de equipamentos e softwares, criação e atribuição de passwords e chaves, relações com fornecedores e outros.	Serviços Administrativos e Informática	Imediata
Rever procedimentos de segurança física	Rever acesso e segurança do arquivo final	Direcção	Imediata
Arquivo final	–	Todos as áreas	Anual

A AHBVCR deve avaliar rigorosamente o tipo de tratamentos de dados que tenha projetado realizar num futuro próximo, de modo a analisar a sua natureza e contexto e os potenciais riscos que possam comportar para os titulares dos dados, de modo a aplicar com eficácia os princípios da proteção de dados desde a conceção e por defeito. Incluindo:

- Especificar periodicidade na qual revêm o sistema.
- Explicar como avaliam o impacto de cada tipo de tratamento.
- Decidir sobre as medidas mais ajustadas, seja tendentes à pseudonimização, à minimização dos dados, ao cumprimento dos prazos de conservação da informação ou à acessibilidade dos dados, deve ter em devida conta as características do tratamento e os efeitos que este pode ter nos direitos dos cidadãos; se for suscetível de resultar num elevado risco, deve realizar uma avaliação de impacto sobre a proteção de dados, de modo a adotar as medidas adequadas para mitigar os riscos.

b. Avaliação de impacto

Os processos de avaliação de impacto realizados na AHBVCR serão registados em impresso interno próprio.



Caldas da Rainha, 1 de Julho de 2025

Direcção



Assinatura manuscrita em tinta preta.

