POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

Índice

1. Objetivo e Âmbito

A AIM LIFE, Lda. (AIM Cancer Center) valoriza a privacidade e a proteção de dados pessoais, dispondo de práticas e instrumentos no domínio da segurança e da proteção de dados, bem como assegura o cumprimento do disposto no Regulamento (EU) 2016/679, do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados – Regulamento Geral sobre a Proteção de Dados (RGPD) – e na Lei n.º 58/2019, de 08 de Agosto, que assegura a execução na ordem jurídica portuguesa do RGPD.

A AIM Cancer Center aplica medidas de segurança, técnicas e organizativas, adequadas para garantir que o tratamento dos dados pessoais é lícito, leal, transparente e limitado às finalidades autorizadas e assegurando um nível de segurança dos dados pessoais adequado ao risco, em cumprimento do RGPD.

Neste sentido, este manual de procedimentos e respectivos anexos definem os princípios gerais e as regras a serem aplicadas pela AIM Cancer Center como responsável pelo Tratamento aos Dados Pessoais por si recolhidos.

A política de proteção de dados pessoais da AIM Cancer Center que agora se pretende implementar, está associada a um conjunto de procedimentos e tem como objectivo esclarecer e regular a forma como a AIM Cancer Center, os seus trabalhadores e colaboradores devem dar cumprimento às disposições legais referidas.

Os responsáveis de cada área devem garantir que a respetiva atividade e os processos inerentes a mesma, cumprem a política de proteção de dados pessoais da AIM Cancer Center providenciar pela formação dos respetivos trabalhadores, os quais deverão seguir e cumprir todos os procedimentos estabelecidos neste âmbito com uma obrigação indissociável dos respectivos deveres.

O cumprimento da política de proteção de dados pessoais e obrigatório para todos os trabalhadores da AIM Cancer Center, para a administração, assim como para todos os que com a AIM Cancer Center queiram colaborar.

Esta Política integra-se num conjunto mais vasto de documentos de privacidade e proteção de dados da AIM Cancer Center. Em especial, deve ser lida em articulação com a Política de Privacidade, a Política de Cookies, os Termos e Condições, os acordos de subcontratação de tratamento de dados vigentes, bem como com a Política de Responsabilidade pelo Tratamento, Responsabilidade Conjunta e Subcontratação da AIM Cancer Center.

Em caso de dúvida, devem ser solicitados à AIM Cancer Center os necessários esclarecimentos.

2. Conceitos e Princípios

2.2. Principais Conceitos

a) *Dados Pessoais:* informação relativa a uma pessoa singular identificada ou identificável. É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador. Exemplos de dados pessoais:

- Nome;
- Morada ou endereço de e-mail;
- CV;
- Número de segurança social ou NIF;
- Matrícula de veículo;
- Dados de localização;
- Gravações CCTV (camaras videovigilância);
- Recibos de Vencimento;
- Cartões de visita;

b) *Dados especiais:* dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos a saúde ou dados relativos a vida sexual ou orientação sexual de uma pessoa.

c) *Tratamento de Dados pessoais:* uma operação ou um conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados, tais come a recolha, o registo, a organização, a estruturação, a

conservação, a alteração, a recuperação, a consulta, a utilização, a transmissão, a interconexão, a limitação, o apagamento ou a destruição.

d) *Responsável pelo tratamento:* a entidade (pública ou privada) que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais. No contexto das atividades da AIM Cancer Center, esta assume geralmente a posição de Responsável pelo Tratamento dos dados pessoais que recolhe, mas poderá também atuar como Subcontratante ou Responsável Conjunto em determinadas situações.
e) *Subcontratante:* entidade (pública ou privada) que trate os dados pessoais por conta do responsável pelo tratamento destes;
f) *Terceiro:* entidade (pública ou privada) que não seja o titular dos dados, o responsável pelo tratamento ou o subcontratante, mas que esta autorizada a tratar os dados pessoais;
g) *Área responsável:* corresponde a área da AIM Cancer Center responsável por cada operação que envolva o tratamento de dados pessoais, i.e., a área que define as finalidades e os meios de tal tratamento;
h) *Área terceira:* corresponde a área da AIM Cancer Center que, não sendo a área responsável, necessita de aceder a dados pessoais tratados por outras áreas da AIM Cancer Center;
i) *Data Breach:* violação de dados pessoais com origem numa falha de segurança (física ou lógica) que comprometa a confidencialidade, integridade e disponibilidade de dados pessoais (i.e., que possa levar a destruição, perda, alteração, acesso ou divulgação não autorizada de dados pessoais);
j) *Avaliação de Impacto sobre a Proteção de Dados (AIPD):* Procedimento prévio a ser efetuado pela AIM Cancer Center sempre que um tratamento de dados, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for susceptível de implicar um elevado risco para os direitos e liberdades das pessoas singulares.
k) *Data Protection Officer (DPO) ou Encarregado de Proteção de Dados (EPD):* designação (e funções) divulgada através de Ordem de Serviço e comunicada a autoridade de controlo nacional de proteção de dados.

2.2 Princípios reguladores do tratamento de dados pessoais

Na recolha e tratamento dos dados pessoais que lhes sejam confiados, a AIM Cancer Center e os seus trabalhadores e colaboradores devem pautar a sua conduta pelos seguintes princípios:

- *Princípio da Transparência, Licitude, Lealdade:* o tratamento de dados pessoais deve ser lícito, leal e transparente;
- *Princípio da Minimização:* o tratamento dos dados pessoais deve ser adequado, pertinente e limitado ao que e necessário para cumprimento da(s) finalidade(s);
- *Princípio da Limitação do Tratamento:* os dados pessoais devem ser tratados para finalidades determinadas, explicitas e legitimas, sendo que o tratamento deve limitar-se a(s) finalidade(s) para a(s) qual(is) os dados são recolhidos; por outro lado, os dados devem ser conservados até ao termo da finalidade para o qual foram recolhidos ou, se superior, para cumprimento de prazos legais ou durante a pendencia de processes judiciais;
- *Princípio da Exatidão:* só devem ser tratados dados exatos e atualizados;
- *Princípio da Proteção de dados por defeito:* por defeito, só devem ser tratados os dados pessoais que forem necessários para cada finalidade (quanto à quantidade de dados pessoais recolhidos, a extensão do seu tratamento, ao seu prazo de conservação e a sua acessibilidade).
- *Princípio da Proteção de dados desde a concepção:* dever de, quer no momento de definição dos meios de tratamento, como no momento do tratamento, serem aplicadas as medidas técnicas e organizativas adequadas destinadas a garantir estes princípios e o exercício dos direitos dos titulares, bem como garantir a confidencialidade, integridade e disponibilidade dos dados. Deve igualmente existir registos associados aos diversos tratamentos para efeitos de controlo;

3 Condições de licitude, formas de recolha e tipos de dados e de titulares

3.1 Fundamentos inerentes ao tratamento de dados pela AIM Cancer Center

Todos os dados recolhidos e tratados pela AIM Cancer Center têm por fundamento uma das seguintes condições de licitude:

- *Consentimento:* Quando a recolha e o tratamento são precedidos do consentimento expresso, específico, livre e informado do respetivo titular, através de suporte escrito ou via web. É recolhido o consentimento, por exemplo, quando o titular de dados fornece um conjunto de dados pessoais para efeitos de uma proposta ou orçamento, ou para a subscrição de ações de marketing direto. Sempre que a condição de licitude consista no consentimento, o mesmo deve referir expressamente a finalidade do tratamento, remetendo ainda para a Política de Privacidade AIM Cancer Center;
- *Execução de contrato ou diligências pré-contratuais:* quando o tratamento e necessário para a execução de um contrato no qual a AIM Cancer Center e titulares são parte ou para diligencias pré-contratuais. Esta condição estará preenchida, nomeadamente no caso de contratos de fornecimento e prestação de serviços;
- *Cumprimento de obrigações legais:* quando o tratamento é necessário para o cumprimento de uma obrigação jurídica. Aqui se inclui, por exemplo, a comunicação de dados a organismos públicos por aplicação de obrigação prevista na lei; incluem-se organismos públicos (nacionais e comunitários), fiscais, policiais ou judiciais;
- *Interesse legítimo*: quando o tratamento se mostra necessário para a prossecução de interesses legítimos da AIM Cancer Center ou de terceiros, sem prejudicar os direitos e as liberdades dos seus clientes e/ou utilizadores.

3.2 Finalidades para as quais a AIM Cancer Center trata dados pessoais

Os dados pessoais recolhidos pela AIM Cancer Center apenas são tratados para fins específicos, explícitos e legítimos. Sempre que sejam recolhidos dados pessoais, os mesmos destinam-se exclusivamente as finalidades expressamente identificadas aquando da recolha.

As principais finalidades que justificam a recolha e tratamento de dados pessoais pela AIM Cancer Center são:

- Elaboração, negociação e execução de contratos, com clientes, trabalhadores, prestadores de serviços, fornecedores, utilizadores e outros;
- Gestão de eventos promovidos pela AIM Cancer Center;
- Divulgação de newsletters;

- Segurança Física das Instalações e Pessoas;
- Necessários para instaurar ou sustentar um processo judicial ou a defesa numa ação judicial;
- Necessários para evitar fraudes ou outras atividades ilícitas, como sejam ataques voluntários aos sistemas de tecnologia de informação da AIM Cancer Center.

3.3 Formas de recolha

A AIM Cancer Center apenas recolhe dados pessoais que se mostrem adequados, pertinentes e limitados ao que é necessário relativamente as finalidades para as quais são tratados.

A recolha de dados deve ser feita por escrito, em papel (nomeadamente através de formulários e contratos validados para este efeito), ou digitalmente via e-mail, mensagem, WhatsApp formulário via link e redes sociais da AIM Cancer Center e de acordo com os procedimentos em anexo a esta política.

Regra geral, a AIM Cancer Center recolhe dados pessoais diretamente de cada titular.

3.4 Tipos de titulares de dados

Para execução das atribuições da AIM Cancer Center podem ser recolhidos e tratados dados dos seguintes tipos de pessoas singulares:

- Clientes e respetivos colaboradores;
- Utilizadores;
- Prestadores de serviços e respetivos colaboradores;
- Candidatos e estagiários;
- Participantes em eventos promovidos pela AIM Cancer Center;
- Visitantes das instalações AIM Cancer Center.

3.5 Categorias de dados pessoais tratados pela AIM Cancer Center

Para execução das diferentes finalidades descritas em 3.2, a AIM Cancer Center recolhe os seguintes tipos de dados pessoais:

- dados de identificação (como o nome, naturalidade, cartão do cidadão ou data de nascimento);
- dados de caraterísticas físicas (como altura, peso, idade ou género);

- dados de comportamento (como hábitos alimentares ou de exercício físico);
- dados médicos e de saúde (como patologias, tratamentos ou resultados de exames);
- dados da situação pessoal (como composição do agregado familiar ou as idades dos mesmos);
- dados de contacto (como o telemóvel, morada ou e-mail);
- dados de habilitação e situação profissional (como nível de escolaridade e CV);
- dados bancários, financeiros e transações (como IBAN ou número de identificação fiscal);
- dados de localização (como endereço de IP);
- imagens recolhidas através de sistemas de videovigilância, sem prejuízo da legislação em vigor.

4. Direitos dos titulares de dados

4.1. **Deveres de Informação**

Por imposição legal, devem ser prestados junto dos titulares um conjunto de informações inerentes à forma como os dados são tratados pela AIM Cancer Center.

Tais informações devem ser fornecidas no momento da recolha de dados (sempre que possível) ou, se os dados pessoais tiverem sido obtidos a partir de outra fonte, informar dentro de um prazo razoável, de forma clara e acessível, em conformidade com o princípio da transparência.

Em face do tipo de tratamentos operados pela AIM Cancer Center, as seguintes informações devem ser prestadas junto dos titulares:

a) A identidade e os contactos do responsável pelo tratamento (AIM Cancer Center);
b) Os contactos do encarregado da proteção de dados;
c) A(s) finalidade(s) do tratamento a que os dados pessoais se destinam;
d) O fundamento jurídico para o tratamento;
e) Os interesses legítimos do responsável pelo tratamento ou de um terceiro (quando aplicável);
f) Os destinatários ou categorias de destinatários dos dados pessoais a quem os dados podem ser comunicados;

g) Eventuais transferências para países terceiros (se aplicável);
h) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
i) A existência e forma de exercício dos direitos de acesso, de rectificação, eliminação, oposição, limitação do tratamento e portabilidade;
j) Se o tratamento dos dados se basear no consentimento, a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
k) O direito de apresentar reclamação a uma autoridade de controlo.

4.2. **Forma de prestação dos deveres de informação**

Toda a informação descrita no ponto anterior, consta na política de privacidade da AIM Cancer Center, de acesso público, divulgada no respetivo website. E como tal, dever-se-á, em todos os textos onde haja necessidade de prestar esta informação, fazer-se referência a essa política de privacidade.

Nos diferentes suportes de recolha (formulários, contratos ou outros) o titular de dados deve ser informado da política de privacidade da AIM Cancer Center. Este é o documento, por excelência, para onde devem ser encaminhados todos os titulares de dados, para efeitos de informação, de esclarecimento de questões ou mesmo para exercício de direitos.

Todas as atualizações a política de privacidade da AIM Cancer Center, são disponibilizadas no respetivo website.

4.3. **Exercício de Direitos**

Nos termos da legislação em vigor, existe um conjunto de direitos que os respetivos titulares podem, a qualquer momento, exercer junto da AIM Cancer Center.

- *Direito de acesso:* direito que permite obter informação relativamente ao tratamento dos seus dados e respetivas características (nomeadamente o tipo de dados, a finalidade do tratamento, a quem podem ser comunicados os seus dados, prazos de conservação e licitude do tratamento).
- *Direito de retificação:* direito que permite solicitar a rectificação de dados, exigindo que estes sejam exatos, atuais e completos.
- *Direito a eliminação dos dados ou "Direito a ser esquecido":* direito de solicitar a eliminação dos dados, quando o titular considere que não existem

fundamentos validos para a conservação dos seus dados e desde que esta eliminação seja legalmente permitida (por exemplo, não decorra da execução de um contrato ou do cumprimento de uma obrigação legal ou regulamentar);

- *Direito a Limitação:* direito que permite a suspensão do tratamento ou a limitação do tratamento a certas categorias de dados ou finalidades. Quando o titular exercer este direito de limitação, os seus dados pessoais não serão eliminados, mas só podem voltar a ser tratados com o consentimento expresso do titular, ou para efeitos de defesa de direitos num processo judicial ou par motivo de interesse público;
- *Direito à Portabilidade:* direito através do qual o titular poderá solicitar o envio dos seus dados, em formato digital e de uso corrente, que permita a reutilização de tais dados. Em alternativa, poderá o titular solicitar a transmissão dos seus dados para outra entidade que passe a ser responsável pelo tratamento dos seus dados. Este direito apenas pode ser exercido quando a condição de licitude do tratamento seja o consentimento do titular ou a execução de um contrato, estando também limitado a tratamentos automatizados;
- *Direito de Oposição:* direito que permite ao titular opor-se a determinadas finalidades (por exemplo, oposição a finalidades de marketing.) Esse direito não pode ser exercido quando existam interesses legítimos que prevaleçam sobre os seus interesses (por exemplo, quando o tratamento seja necessário para a execução de um contrato);
- *Direito de Retirar o Consentimento:* o direito que permite ao titular retirar o seu consentimento, mas que apenas pode ser exercido quando o seu consentimento seja a única condição de legitimidade;
- *Direito de reclamação junto da Autoridade Nacional de Controlo* (CNPD).

4.4. **Forma de os titulares de dados exercerem os seus direitos**

O **ANEXO I** descreve o procedimento a utilizar para o exercício de direitos pelos titulares de dados pessoais, assim como o fluxo associado a execução dos seus pedidos (incluindo os prazos de resposta legalmente impostos).

5. Tratamento de dados pessoais

5.1. **Linhas orientadoras**

Sem prejuízo da lei aplicável, é proibida a divulgação de Dados Pessoais, incluindo a partilha informal com outros trabalhadores ou colaboradores.

Quando o acesso a determinada informação carecer de determinado perfil de acesso, o mesmo deve ser solicitado de acordo com os procedimentos em vigor.

Os dados pessoais devem ser regularmente revistos e atualizados. Caso já não sejam necessários dever-se-á proceder a sua eliminação, excepto quando existam outras condições que impeçam tal eliminação.

Devem ser seguidas todas as recomendações/procedimentos existentes na utilização dos sistemas de informação (com especial atenção nas questões relacionadas com o tratamento de dados pessoais).

Todos os processos que contenham dados pessoais, devem estar documentados e ser do conhecimento do DIRETOR DE OPERAÇÕES.

A transferência de dados pessoais para países terceiros (fora da União Europeia) implica o cumprimento de um conjunto de regras especificas. Sempre que ocorra estas situações, recomenda-se a obtenção de um parecer do DIRETOR DE OPERAÇÕES.

Sempre que exista a necessidade de celebrar contratos ou outros textos legais onde haja tratamento de dados pessoais devem utilizar-se minutas/modelos já aprovados ou solicitar os mesmos, com o conhecimento do DIRETOR DE OPERAÇÕES.

Qualquer pedido de esclarecimento ou parecer sobre a proteção de dados deve ser encaminhado para o DIRETOR DE OPERAÇÕES.

5.2. **Meios de suporte**

a) *Papel:* Os documentos que contenham dados pessoais, devem estar guardados em áreas e compartimentos que não permitam o acesso a pessoas não relacionadas com o seu tratamento legítimo. Controlos a implementar:

i. Procedimento de controlo e acesso a pastas/documentos que contenham dados pessoais, especialmente quando se trate de dados pessoais sensíveis, incluindo regras sobre o acesso, a utilização e a posterior devolução/guarda das pastas/documentos;

ii. Verificação de falhas no procedimento anterior (por exemplo, assegurar que não se deixam documentos (originais, cópias ou impressos) em áreas onde pessoas não autorizadas possam ter acesso aos mesmos).Procedimento de inutilização de documentos (originais, cópias ou impressos), recorrendo aos destruidores de papel.

b) *Digital:* A informação em formato digital, deverá estar protegida de acessos não autorizados, eliminação acidental e de ataques informáticos maliciosos. Controlos a implementar:

i. Proteção da informação com recurso a formas de autenticação robustas e perfis de acesso;

ii. Encriptação de todos os dispositivos de armazenamento portáteis ou amovíveis (computadores, discos, etc.);

iii. Criação de rotinas de guarda dos referidos dispositivos em lugares seguros (armários fechados, utilização de cadeados, etc.);

iv. Criar a obrigação de guardar toda a informação produzida nos sistemas centrais e evitar sempre que possível o armazenamento local;

v. Aplicar as transferências de dados pessoais para fora da AIM CANCER CENTER, os procedimentos dos sistemas de informação em vigor, garantindo, designadamente, a encriptação dos dados;

vi. Eliminar toda a informação dos equipamentos retirados do ativo, designadamente por abate, segundo os procedimentos da área de sistemas de informação.

5.3 Acessos físicos

O acesso de pessoas externas a instalações da AIM Cancer Center deve ser protegido e controlado, em particular nos locais onde haja tratamento de dados pessoais (inclui o acesso a sistemas informáticos ou documentos físicos).

5.4 Acessos lógicos a dados pessoais

As informações que contenham dados pessoais devem estar protegidas com acessos específicos e validados, quer ao nível das credenciais para o seu acesso quer dos perfis existentes. A utilização de sistemas de 'logging' e importante para comprovar a eficácia dos mesmos. Os dados pessoais não podem ser acedidos - lidos, copiados, modificados ou removidos - sem um acesso valido e autorizado.

5.5 Formulários de recolha

Sempre que haja recolha de dados de dados pessoais através de um formulário, dever-se-á seguir o procedimento no **ANEXO II**

5.6 Documentação e registo das conformidades

Com a finalidade de dar cumprimento a obrigação legal de demonstrar a todo o tempo, a observância da presente política e dos seus diversos procedimentos, devem as áreas responsáveis seguir os procedimentos especificados no **ANEXO III**.

5.7 Orientações para a conformidade das bases de dados

Todas as Base de Dados que contenham dados pessoais devem obedecer as medidas que constam na presente política de proteção de dados.

5.8 Utilização dos sistemas de informação

Para uma correta utilização dos sistemas de informação, devem seguir-se as diversas recomendações/procedimentos existentes. A encriptação dos dados pessoais (associado ao controlo de acessos) constitui uma das medidas que permite uma maior salvaguarda nesta matéria e como tal deve ser utilizada sempre que possível.

6. Fluxos internos de dados pessoais

Entende-se por fluxos internos de dados a transferência de dados pessoais entre áreas da AIM Cancer Center.

Uma área pode necessitar de determinados dados pessoais para concluir um processo e para tal solicita os mesmos a área responsável por esses dados pessoais.

A transmissão de dados pessoais entre as diferentes áreas da AIM Cancer Center deve estar regulada e documentada. Sempre que tal ocorra, devem ser seguidos os procedimentos de regulação dos fluxos internos de dados pessoais constantes do **ANEXO IV**.

7. Conservação de dados

O tratamento dos dados pessoais deve respeitar o princípio da limitação do tratamento, i.e., os dados devem ser conservados até ao termo da finalidade para os quais forem recolhidos; findo esse prazo e caso não existam outros motivos que justifiquem a conservação dos mesmos por períodos superiores, devem ser executados os procedimentos definidos v.g. eliminação ou anonimização.

Os procedimentos e princípios aplicáveis a conservação de dados constam no **ANEXO V**.

8. Entidades Subcontratantes e Terceiras

Neste ponto, é abordado a forma como o tratamento de dados pessoais deve estar enquadrado na legislação aplicável, nas relações que a AIM Cancer Center estabelece com outras entidades.

Este enquadramento passa por identificar o tipo de entidade (Subcontratante ou Terceiro), a formalização de contratos ou outros acordos jurídicos onde conste clausulado específico e validado sobre o tratamento de dados pessoais, bem como a transmissão desses dados se irá processar (havendo inclusive a necessidade de se identificar se esta transmissão ocorre para países terceiros, fora da União Europeia).

Os procedimentos a serem seguidos pelas áreas responsáveis, na relação com outras entidades no âmbito da proteção de dados pessoais, constam no **ANEXO VI**.

9. Colaboradores da AIM Cancer Center

O tratamento de dados pessoais dos trabalhadores e colaboradores da AIM Cancer Center obedece sempre as disposições legais e regulamentares aplicáveis a proteção de dados pessoais.

Os procedimentos e princípios aplicáveis ao tratamento dos dados pessoais dos trabalhadores e colaboradores da AIM Cancer Center constam no **Anexo VII**.

10. Violação de dados ("Data breach')

Considera-se um 'data breach', uma violação de dados pessoais, originada por uma falha de segurança que tenha como consequência a divulgação não autorizada de dados pessoais ou a destruição/alteração dos mesmos.

Um 'data breach' pode potencialmente ter uma serie de efeitos adversos significativos sobre os titulares dos dados, que podem resultar em danos materiais ou não materiais.
É, portanto, essencial serem adotadas, não só medidas preventivas destinadas a evitar situações de “data breach” de dados pessoais, como também medidas correctivas que garantam uma imediata correcção e minimização dos efeitos de um “data breach”.

Os procedimentos e princípios aplicáveis a prevenção e ocorrência de “data breach” constam no **Anexo VIII**.

11. Avaliações de Impacto sobre a Proteção de Dados (AIPD)

Sempre que existam novas situações que possam ser suscetíveis de implicar riscos elevados para os direitos e as liberdades das pessoas singulares deve-se realizar uma Avaliação de Impacto sobre a Proteção de Dados (AIPD). O objetivo de uma AIPD, é o de avaliar e identificar os riscos de determinada operação para a proteção de dados pessoais, permitindo, por um lado, antecipar eventuais constrangimentos e, por outro lado, garantir a adopção de medidas que minimizem ou eliminem os riscos identificados.

Os procedimentos e princípios aplicáveis a realização de AIPD constam no **Anexo IX**.

ANEXO I: Procedimento exercício dos direitos dos titulares

1. Objetivo e âmbito:

Os titulares de dados pessoais devem poder exercer os seus direitos de acordo com a legislação nacional e comunitária sobre esta matéria. O presente procedimento visa regular a forma como a recolha do pedido e feita até à sua conclusão.

2. A quem se destina:

a) Aos titulares dos dados pessoais;

b) Aos colaboradores que recebam pedidos de titulares de dados;

c) Às áreas responsáveis pela execução dos pedidos referidos.

3. Forma:

Todos os pedidos dos titulares de dados devem ser submetidos por escrito e pelo canal formal disponibilizado para esse efeito, i.e., sempre que um titular pretenda exercer os seus direitos, deve ser aconselhado e direccionado para a página do site da AIM Cancer Center sabre a política de privacidade. Nessa página pode ser consultada toda a informação sobre esta temática que pode ser útil ao titular de dados, bem como o acesso ao contacto do DIRETOR DE OPERAÇÕES, para onde o requerente pode submeter o seu pedido.

4. Execução do pedido:

É centralizado no DIRETOR DE OPERAÇÕES, a receção e a gestão dos pedidos dos titulares, sendo estes depois encaminhados para as áreas responsáveis para sua execução.

A execução do pedido deve contemplar todos os repositórios que contenham dados pessoais desse titular e obedecer aos prazos fixados (*vide* 5. *infra*). A execução do pedido poderá estar legalmente limitada em determinadas situações. Em caso de dúvida solicite apoio do DIRETOR DE OPERAÇÕES.

Uma vez executado o pedido, a área responsável deverá informar o DIRETOR DE OPERAÇÕES de todas as ações efetuadas e prestar todos os esclarecimentos que este considere necessários.

A conclusão do pedido é feita pelo DIRETOR DE OPERAÇÕES com consequente notificação ao titular de dados.

5. Prazos legais:

Os pedidos dos titulares de dados devem ser executados no prazo máximo de 30 dias (contados desde a data de entrada no sistema da AIM Cancer Center, até à data de resposta ao titular).

Findo tal prazo, a AIM Cancer Center está em situação de incumprimento de uma disposição legal, pelo que, em caso de dúvida ou se por qualquer motivo não for possível dar resposta a um pedido nos prazos descritos, deverá contactar-se o DIRETOR DE OPERAÇÕES da AIM Cancer Center, informando-o da razão do incumprimento.

ANEXO II: Procedimento para formulários com recolha de dados pessoais

1. Objetivo e âmbito:

O presente procedimento visa regular a recolha de dados pessoais, através de formulários eletrónicos definidos pela AIM Cancer Center.

2. A quem se destina:

a) As áreas responsáveis pelos formulários, i.e., as que definem o seu conteúdo e/ou solicitam a sua publicação, quer on-line quer por outra via, são as responsáveis por assegurar a implementação destas recomendações. Devem-se articular com as áreas ou entidades competentes que tenham como missão a sua implementação técnica.

b) As áreas ou entidades competentes que tenham como missão a implementação técnica dos formulários.

3. Pré-requisitos:

Utilização das ferramentas nos serviços de informação da AIM Cancer Center.

A utilização de plataformas externas carece de uma análise prévia e de uma regulamentação escrita (acordos formais / contratos / "data processing agreements") no sentido de certificar o seu cumprimento com as leis nacionais e comunitárias sobre a proteção de dados pessoais.

4. Regras para a construção de formulários que tratem dados pessoais

Tipicamente numa página web que suporte um formulário, existe um texto inicial informativo onde se descreve o objetivo que se pretende alcançar e quais as razões para a recolha da informação. Deve ser incluído neste texto, num paragrafo específico, onde se descreva as finalidades específicas, legítimas e de uma forma explícita, para as quais e feito a recolha/tratamento dos dados pessoais.

A recolha de dados pessoais deve seguir o princípio da minimização, i.e., apenas devem ser solicitados os dados estritamente necessários ao tratamento pretendido.

Exemplo de um formulário apresentado de forma abstrata:

<Texto Informativo>

<Formulário:

Campo 1 [ ) *

Campo 2 ( ]
Campo 3 ( ) >

Tratando-se de um formulário que faça recolha de dados pessoais, é necessário acrescentar na parte final o seguinte campo obrigatório referente ao pedido de consentimento (RGPD):

> [ ] Autorizo o tratamento dos dados pessoais recolhidos neste formulário para as finalidades *supra* descritas. Declaro ter tornado conhecimento da política de privacidade da AIM Cancer Center.

NOTAS:

- Deve existir um *hyperlink* na frase política de privacidade para a página correspondente no site da AIM Cancer Center;
- As [tick-box] para estas questões especificas do RGPD, não podem estar previamente preenchidas. O titular de dados tem que ter uma acção positiva, informada e inequívoca;
- Só deverá haver alteração ao texto dos campos RGPD que aqui se reproduzem, quando existir um parecer positivo do DIRETOR DE OPERAÇÕES para esse efeito.

5. Consentimentos opcionais:

Devem individualizar-se os diversos pedidos opcionais de consentimento que se pretendam e permitir a recusa dos que o titular entender.

Exemplo:
[ ] Aceito receber newsletters ou outra informação relacionada com a atividade da AIM Cancer Center.

6. Transferência de dados para países terceiros (fora da União Europeia):

Sempre que exista ou haja a possibilidade de existir transferência de dados pessoais para países terceiros (fora da União Europeia), deve ser incluído, na descrição das finalidades, o seguinte texto (ou similar, dependendo de consulta ao DIRETOR DE OPERAÇÕES):
"Poderá haver lugar a transmissão dos seus dados pessoais para todas as entidades envolvidas na gestão do referido programa, ainda que estejam localizadas em países terceiros, transmissão essa que, neste último caso, poderá implicar riscos no que respeita

aos seus direitos devido a falta de garantias dos referidos países face aos normativos comunitários e nacionais referentes à proteção de dados pessoais."

7. Implementação técnica dos formulários

a) *Double Opt-In*: Dever-se-á implementar o conceito "Double Opt-In" sempre que a base de licitude seja a obtenção direta por via eletrónica do consentimento expresso e informado do titular de dados. Por exemplo, nos casos de divulgação periódica de informação por e-mail.

O conceito "Double Opt-In", grosso modo, passa por assegurar que o endereço de e-mail introduzido no formulário pelo titular de dados e revalidado, i.e., através de um envio de um e-mail automático para a caixa de correio do titular de dados a solicitar uma acção positiva e inequívoca, que nos permite assegurar que o e-mail inicialmente introduzido no formulário é válido e gerido por esse titular de dados.

b) *Registo da prova*: Para todos os formulários devera estar associado um conjunto de registos que assegure à AIM Cancer Center a capacidade de provar a prestação do consentimento pelo titular de dados. Nesses registos, devera constar a seguinte informação:

- Descrição da Finalidade para o tratamento dos dados pessoais;
- Todos os campos do formulário; no caso dos campos RGPD de pedido de consentimento, guardar o texto associado a cada tick-box;
- Data e hora do registo;
- Quando se empregar o conceito "Double Opt-in", o sistema informático deverá registar, preferencialmente em Base de Dados, as diversas interacções com o titular de dados, bem como guardar cópia dos e-mails enviados e registo da aceitação/consentimento do titular (como esta acção de aceitação final pelo titular de dados geralmente e feita através de um click num url ou num botão, o sistema poderá produzir um e-mail interno de controlo com a data e hora do consentimento e ser guardado conjuntamente com os e-mails enviados);
- Área da AIM Cancer Center responsável pelo formulário;
- Data final da conservação de dados (a partir da qual se procederá à eliminação);
- Outros dados que sirvam de prova do consentimento.;

- Todos estes elementos de prova devem estar devidamente salvaguardados e com um controlo de acesso.

8. Documentação

Cada tratamento de dados pessoais deve estar minimamente documentado. Ver procedimento específico sobre esta matéria para mais informação no **ANEXO III**.

9. Prazo de conservação dos Dados

Os dados pessoais deverão ser eliminados após o período estipulado.

Cabe a área responsável pelo tratamento de assegurar o cumprimento dos prazos de conservação/eliminação de acordo com o estabelecido.

Para mais informação sobre esta matéria, consultar o **ANEXO V**.

ANEXO III: Procedimento para documentação e registo tratamento dados pessoais

1. Objetivo e âmbito:

O presente procedimento visa regular a documentação e o registo dos elementos de prova associados a cada tratamento de dados pessoais.

As Entidades são obrigadas a conservar um registo de todos os tratamentos de dados pessoais sob a sua responsabilidade, que inclua a seguinte informação:

- Tipo de dados tratados;
- Finalidades;
- Descrição das categorias de titulares dos dados e dos destinatários dos mesmos;
- Medidas de segurança;
- Prazo de conservação;
- Fundamento jurídico (consentimentos, contratos, outros).

2. A quem se destina:

Áreas responsáveis pelo tratamento de dados pessoais

3. Forma - Digital

Cada área deverá solicitar o apoio da área responsável pelas tecnologias de informação, para que seja criada, dentro do directório "RGPD" da área de rede ("File system") da AIM Cancer Center, uma subpasta com a designação da respetiva área. O pedido deve indicar quais os colaboradores com acesso a mesma e ser dado conhecimento ao DIRETOR DE OPERAÇÕES.

3.1 **Conteúdo da pasta digital**

Cada área responsável pelo tratamento deverá seguir uma organização par tipo de tratamento de dados.

É importante documentar de forma sucinta e objetiva cada tratamento, de acordo com o referido no ponto 1.

Exemplos de alguns conteúdos:

- Documentação dos diversos tratamentos de dados pessoais existentes em cada área.
- Elementos de prova do consentimento, quando este não foi obtido por meios automáticos (validados previamente pelo DIRETOR DE OPERAÇÕES).

- Contratos de subcontratantes.
- Procedimentos associados ao tratamento de dados pessoais.

3.2 **Consentimento**

Sempre que exista tratamento de dados onde a base de licitude é o consentimento, é de extrema importância para a AIM Cancer Center ter os elementos que permitam fazer prova do mesmo.

Caso o registo do consentimento seja feito digitalmente, via aplicações informáticas já adaptadas para cumprir esta exigência, a prova é automaticamente guardada nos sistemas da AIM Cancer Center (em caso de dúvida, esclareça com a área responsável pelas tecnologias de informação ou DIRETOR DE OPERAÇÕES).

Para as restantes situações, devem ser colocadas na pasta referida no ponto 3 supra, todos os elementos que constituem a prova, incluindo os consentimentos obtidos em papel quando os haja, devendo os originais ficar guardados em local protegido e seguro e uma cópia digitalizada na referida pasta.

3.3 **Contratos subcontratantes**

Sempre que exista um novo contrato com entidades do tipo Subcontratante (ver **ANEXO VI**), estes devem ficar guardados em local protegido e seguro, e uma cópia digitalizada na referida pasta.

ANEXO IV- Procedimento Fluxos Internos de dados pessoais

1. Objetivo e âmbito:

O presente procedimento visa regular o fluxo interno de dados pessoais entre as diversas áreas da AIM Cancer Center, i.e., transferência de dados pessoais entre áreas.

Determinados processos podem necessitar de dados pessoais para a sua conclusão (por exemplo, a contratação de seguro de saúde para os colaboradores da AIM Cancer Center, onde a área responsável pelo processo de contratação necessita que a área responsável pelos recursos humanos forneça determinados dados pessoais dos colaboradores da AIM Cancer Center).

2. A quem se destina:

Todas as áreas da AIM Cancer Center que possam necessitar de acesso a dados pessoais existentes em repositórios que não tenham acesso.

3. Área responsável:

Cada repositório/base de dados tem pelo menos uma área responsável, a quem incumbe determinar as finalidades e os meios de tal tratamento.

4. Forma de operacionalizar:

A área que necessita de acesso aos dados pessoais formula um pedido a área responsável pelos mesmos. Esse pedido deve conter as seguintes informações obrigatórias:

- Identificação da área;
- Identificação dos colaboradores dessa área que necessitem do acesso aos dados;
- Tipo de repositório/ base de dados que se pretende ter acesso;
- Tipo de dados pessoais cujo acesso e solicitado (exemplo: nome, morada, NIF, data nascimento, entre outros);
- Finalidade do acesso (explicar o porque da necessidade de acesso a tais dados);
- Período de conservação dos dados (explicar o período temporal durante o qual irão ser tratados os dados, com o compromisso de findo tal período se proceder a sua destruição).

A área responsável pelos dados pessoais precede a analise do pedido e valida o sentido do mesmo com base nos seguintes critérios:

- *Adequação*: deve ser analisada a adequação da finalidade para a qual os dados são solicitados pela área terceira;

- *Necessidade*: deve ser analisado se, em face da finalidade que dita tal acesso, existe a efetiva necessidade de acesso total ou parcial aos dados pessoais solicitados.
- *Proporcionalidade*: além da necessidade, impõe-se ainda a área responsável que verifique se o acesso a tais dados e proporcional face a eventuais riscos na esfera dos direitos, liberdade e garantias dos titulares.

A resposta da área responsável deve conter:

- Deferimento ou indeferimento do acesso;
- Fundamento da decisão;

Em caso de deferimento, deve-se ainda referir:

- Período de utilização dos dados cedidos;
- Eventuais limitações ou restrições.

Nas situações onde haja deferimento, o acesso aos dados solicitados pode ser efetuado usando uma das seguintes formas:

1) Atribuir acessos aplicacionais, aos colaboradores indicados no pedido, auditáveis e limitados aos dados pessoais estritamente necessários e pelo tempo necessário.

2) Envio de ficheiro com essa informação à área que solicitou esses dados, através de pasta lógica partilhada no sistema de informação da AIM Cancer Center, a qual deverão ter acesso apenas os colaboradores referidos no pedido pela área terceira.

3) Envio do ficheiro por e-mail; nesta situação **é fundamental que o ficheiro seja encriptado**, devendo a password ser comunicada por outra via, telefone por exemplo.

Deve ser evitado o envio de ficheiros que contenham dados pessoais não encriptados via e- mail (com vista a serem evitadas possíveis violações de dados i.e., “data breaches").

Recomenda -se a utilização de um Sistema de Tickets, pelas Direcções Responsáveis de dados pessoais, para suporte e documentação a estes pedidos. Caso contrário, deverá obrigatoriamente guardar toda a documentação dos pedidos de acordo com o ANEXO III.

5. Situações em que deve ser envolvido o DIRETOR DE OPERAÇÕES

Em função do tipo de dados, da finalidade para a qual os mesmos necessitam de ser acedidos ou do período durante o qual a área terceira os pretende conservar, poderá haver necessidade de solicitar um parecer junto do DIRETOR DE OPERAÇÕES. Incumbe a área responsável efetuar tal juízo e em caso de dúvida, solicitar o referido parecer.

O DIRETOR DE OPERAÇÕES deve ainda ser consultado em caso de dúvida sabre a documentação obrigatória que é necessário guardar para cada pedido.

ANEXO V- Procedimento referente à Conservação de dados pessoais

1. Objetivo e âmbito:

Todos os documentos que contenham dados pessoais devem respeitar o princípio da limitação do tratamento no que respeita ao respetivo período de conservação.

Os dados devem ser conservados até ao termo da finalidade para os quais forem recolhidos, até ao termo dos prazos legalmente impostos para conservação de tais dados ou até ao termo de processos judiciais que justifiquem a conservação dos mesmos.

Cada área deverá identificar, para cada tratamento de dados pessoais, quais os prazos máximos de conservação e criar os procedimentos a executar quando tais prazos se atingem. Em caso de dúvida, deve ser consultada a área jurídica da AIM Cancer Center.

2. A quem se destina

Todas as áreas da AIM Cancer Center.

3. Períodos de Conservação/Arquivo (recomendação)

A definição dos períodos de conservação é feita nos termos da lei ou por meio de procedimentos internos.

Os seguintes pontos servem como orientação e como tal devem sempre ser validados com as entidades responsáveis (v.g. autoridades de gestão de programas comunitários, área jurídica interna, ...):

- Documentação comercial financeira/fiscal: Deve ser conservada pelo período de 10 anos após o termo da relação comercial. A este respeito, quando se tratem dados pessoais de contactos de empresa que não forem necessários para justificar registos de contabilidade, não existirá legitimidade para os conservar após a cessação do contrato, devendo assim ser eliminados após o termo da relação contratual.
- Documentação Laboral: Em face dos prazos de caducidade e dos diferentes normativos legais existentes, deverão ser atendidos os seguintes prazos de conservação no que respeita a documentação de colaboradores da AIM Cancer Center:
    - Dados biométricos: devem ser conservados apenas durante o período necessário para a prossecução das finalidades do tratamento a que se destinam (controlo de assiduidade) devendo ser destruídos após o termo

da relação laboral ou caso o trabalhador seja transferido para outro local de trabalho (n.º 3 do art.º 18 do Código do Trabalho);

- Documentação contratual e inerente a segurança social (ex. contrato de trabalho, documentos relacionados com a cessação de contratos de trabalho, mapas de férias, mapas de horários de trabalho, registos individualizados de trabalhadores, registo de sanções disciplinares, plano de formação profissional e comprovativos das acções de formação profissional , consulta anual aos trabalhadores sabre matérias de segurança, higiene e saúde no local de trabalho, comunicações de admissão e de cessação de contratos de trabalho) deve ser conservada, no mínimo, ate 5 anos após a cessação do contrato de trabalho;
- Documentação necessária a efeitos fiscais (ex. recibos, retenções na fonte, relatórios AT) deve ser observada durante o prazo de 10 anos após a cessação do contrato de trabalho;
- Documentação relativa a segurança e saúde no trabalho: a AIM Cancer Center deve manter a disposição das entidades fiscalizadoras competentes, pelo prazo de 5 anos após o termo da relação laboral, os registos relativos a realização das atividade inerentes a segurança e saúde no trabalho (ex. resultados de avaliações de riscos profissionais, lista das situações de baixa por doença e do número de dias de ausência ao trabalho, a ser remetida pelo serviço de pessoal e, no caso de doenças profissionais, a relação das doenças participadas, lista das medidas, propostas ou recomendações formuladas pelo serviço de segurança e de saúde no trabalho).
- Processos de recrutamento (*curriculum vitae*, avaliações de candidatura, entrevistas): 5 anos após o termo do processo de recrutamento;
- Restantes dados pessoais de colaboradores AIM Cancer Center, não incluídos nas anteriores categorias (como será o caso de dados de familiares, carta de condução ou outros): devem ser anonimizados ou eliminados no prazo máximo de 10 anos após o termo da relação contratual.

- Videovigilância: As imagens recolhidas através de sistema de videovigilância legalmente instalado devem ser conservadas pelo prazo máximo de 30 dias, findo

o qual serão destruídas, só podendo ser utilizadas nos termos da legislação penal e processual penal.

- Dados inerentes a ações de formação, missões ou catálogos: Não existindo legislação específica que determine os prazos de conservação deste tipo de dados, e fazendo um juízo de necessidade/proporcionalidade inerente aos mesmos, tais dados pessoais de convidados e participantes devem ser conservados pelo prazo necessário ao cumprimento das finalidades para que foram solicitados os dados (exceto se existir alguma outra finalidade que obrigue a um prazo de conservação mais longo, nomeadamente documentação necessária para efeitos fiscais);
- Dados inerentes a finalidades genéricas da AIM Cancer Center (newsletters, site, ficheiros contactos empresas): Os dados podem ser conservados enquanto perdurar a finalidade para a qual são recolhidos, no pressuposto de poder ser sempre garantido o direito de apagamento au de ser retirado o respetivo consentimento.

ANEXO VI- Procedimento Entidades Subcontratantes e Terceiras

1. Objetivo e âmbito:

As entidades que se relacionem com a AIM Cancer Center, enquanto responsável pelo tratamento dos dados pessoais, podem ser de dois tipos:

- Subcontratantes: entidade pública ou privada que proceda ao tratamento de dados pessoais por conta da AIM Cancer Center (responsável pelo tratamento) e para as finalidades definidas por esta última;
- Terceiras: entidade pública ou privada que precede ao tratamento dos dados pessoais para concretização de finalidades decorrentes do exercício da sua própria atividade, não determinando a AIM Cancer Center qual o modo ou as finalidades daquele tratamento.

A diferença fulcral entre estes dois tipos de entidades reside no facto de o subcontratante tratar os dados pessoais em nome e por conta da AIM Cancer Center e de acordo com as instruções desta última.

Cabe à AIM Cancer Center recorrer apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas para que o tratamento satisfaça os requisitos de segurança, integridade e confidencialidade dos dados impostos pelo Regulamento Geral de Proteção de Dados (RGDP), e assegure a defesa dos direitos do titular dos dados.

Esta especificidade obriga a que a relação com os subcontratantes deva ser regulada por contrato escrito que preveja a forma corno o tratamento dos dados e realizado e quais as medidas que o subcontratante adopta no sentido de garantir a segurança e confidencialidade dos dados tratados.

Os subcontratantes não poderão contratar outro subcontratante (subcontratante ulterior) sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral nesse sentido. Poderá, contudo, ser conferida uma autorização genérica para a contratação de subcontratantes ulteriores, recaindo, no entanto, sobre o subcontratante o dever de informar a AIM Cancer Center, por escrito, da identificação de tais prestadores ulteriores (dando-lhe assim a oportunidade de se opor a urna eventual contratação).

No que respeita a entidades terceiras, não obstante poderem ter acesso a dados pessoais da AIM Cancer Center, procedem ao tratamento de tais dados para concretização de finalidades decorrentes do exercício da sua própria atividade, não determinando a AIM Cancer Center qual o modo ou as finalidades daquele tratamento.

2. Identificação das Entidades Relacionadas por tipo

Por referência a distinção estabelecida no ponto anterior, segue urna lista (não exaustiva) dos tipos de entidades a quem a AIM Cancer Center comunica dados pessoais, e a respetiva finalidade da comunicação:

- Entidades subcontratantes:
  - Consultores externos (para finalidades de auditoria ou consultadoria;)
  - Empresa de Medicina no Trabalho (para prestação de serviços de medicina no trabalho);
  - Corretor de Seguros (para gestão de seguros de acidentes pessoais de colaboradores);
  - Agenda de Viagens (para gestão e marcação de viagens e alojamentos);
  - Entidades de recrutamento;
  - Advogados (patrocínio de ações judiciais);
- Entidades terceiras:
  - Segurança Social (para inscrição nos centros distritais da SS);
  - Fundo de Compensação de Garantia do Trabalho (para inscrição no FGCT e FCT);
  - Comissão de Trabalhadores (para efeitos de atribuições legais);
  - Tribunais e Agentes de Execução (gestão de notificações de penhora de remunerações;)
  - Entidades formadoras (para efeitos de formação e emissão de certificados formativos);
  - Companhias aéreas e hotéis (para aquisição directa de bilhetes de avião e alojamento);
  - Autoridades PSP e/ou GNR (para efeitos de gestão de processes contraordenacionais);

Caso tenha alguma dúvida sobre o tipo de uma entidade, contacte o DIRETOR DE OPERAÇÕES da AIM Cancer Center.

3. Contratualização

Os contratos com entidades que possam, através de qualquer forma ou suporte, aceder a dados pessoais - subcontratantes ou terceiras -, devem utilizar minutas aprovadas e definidas para esse efeito (ver minutas disponibilizadas pela área Jurídica).

As minutas para entidades subcontratantes, carecem de um maior detalhe, devendo incorporar texto que contemple os seguintes itens:

- objeto do tratamento (especificação dos serviços prestados),
- natureza e finalidade do tratamento (especificação das finalidades);
- categorias de titulares dos dados;
- tipo de dados pessoais (dados de identificação, dados de contacto, situação financeira, habilitações, entre outros);
- medidas técnicas e organizacionais a serem utilizadas pelo subcontratante no tratamento dos dados, designadamente as medidas de controlo de acesso, de disposição, de transmissão e de eliminação.

Incumbirá a cada área responsável, diligenciar pela utilização das minutas adequadas.

Sempre que sejam celebrados contratos com subcontratantes, definidos nos termos supra, estes devem ser digitalizados de acordo com o **ANEXO III** e deles deve ser dado conhecimento ao DIRETOR DE OPERAÇÕES.

4. Transmissão de dados pessoais para Entidades Terceiras

4.1 Pedido

Incumbe a cada área responsável analisar eventuais pedidos de informação que envolvam a transmissão de dados pessoais existentes em repositórios/bases de dados da AIM Cancer Center.

Essa análise deve seguir os seguintes pontos:

- Após receção do pedido de acesso, deverá a área responsável analisar se lhe foram fornecidas as seguintes informações obrigatórias:
  - Identificação da Entidade Terceira;
  - Tipo de dados pessoais cujo acesso e pretendido (descrição da categoria dos dados - ex: nome, e-mail, NIF, entre outros);

- Finalidade (justificação) e fundamento de legitimidade do acesso: cumprimento de obrigação legal (devendo ser indicada a respetiva base legal); interesse público; ou interesse legítimo da Entidade Terceira;
- Na eventualidade de não serem fornecidas tais informações obrigatórias, deverá a área responsável solicitar tais informações junto da Entidade Terceira. Caso as mesmas não sejam fornecidas, não deverá ser permitido o acesso aos dados;
- Após o envio das informações obrigatórias supra descritas, deverá a área responsável analisar o pedido, com base nos seguintes critérios:
- Licitude: deve ser analisada a existência de uma das condições de licitude para acesso/comunicação (i) cumprimento de obrigação legal (devendo ser indicada a respetiva base legal); (ii) interesse público; (iii) interesse legítimo da entidade terceira;
- Necessidade: deve ser analisado se, em face da finalidade que dita o acesso, existe a efetiva necessidade de acesso, total ou parcial, aos dados pessoais solicitados.

- Em caso de deferimento da pretensão, a seguinte mensagem devera ser referida com a transmissão da informação: *"A informação ora remetida tem por finalidade <Especificar Qual>. Na medida em que a referida informação contenha dados pessoais, os mesmos apenas deverão ser utilizados para a finalidade supra referida e não para finalidades distintas (em proveito próprio ou de Entidade Terceira), devendo ser tratados em conformidade com a legislação nacional e comunitária que regula o tratamento de dados pessoais".*
- O registo de todos os pedidos de acesso/Informação e respetivas respostas deverá seguir as orientações do **ANEXO III**.

4.2 Para fora da União Europeia

A comunicação de dados para entidades localizadas em países terceiros (fora da União Europeia/EEE - Espaço Económico Europeu) carece de um procedimento mais rigoroso, incumbindo a AIM CANCER CENTER apenas transferir dados para países terceiros ou organizações internacionais que apresentem garantias adequadas nos termos do RGPD.

Incumbe a cada área responsável analisar a existência destas situações (transferência de dados para países terceiros) e em caso de dúvida, consultar o DIRETOR DE OPERAÇÕES da AIM Cancer Center.

Regra geral, só devem ser efetuadas transferências de dados para países terceiros, se:

- Existir relativamente a esse país uma decisão de adequação por parte da Comissão Europeia;
- Existirem regras vinculativas aplicáveis às empresas de um mesmo Grupo;
- Existir, entre as entidades, um contrato com cláusulas-tipo de proteção de dados adotadas/aprovadas pela Comissão Europeia.

Não sendo possível cumprir uma das referidas condições (como sucedera na maioria das situações), apenas poderão ser transferidos dados para outras entidades, caso:

- O titular dos dados tiver dado o seu consentimento expresso a tal transferência, após ter sido informado dos possíveis riscos de tais transferências devido a falta de uma decisão de adequação e das garantias adequadas;
- A transferência for necessária para a execução de um contrato entre o titular dos dados e a AIM Cancer Center, nos termos desse contrato;
- A transferência for necessária para a celebração ou execução de um contrato, celebrado no interesse do titular dos dados, nos termos desse contrato;

4.3 Forma de transmissão

A forma de comunicação de dados pessoais destinados a outras entidades assume especial relevância uma vez que o envio de informação/dados através de meios que não garantam segurança, ou o envio de informação/dados a destinatários errados, pode pôr em causa a segurança e a confidencialidade dos dados pessoais e gerar um incidente de violação de dados pessoais (ver **ANEXO VIII**).

Cabe, portanto, a cada colaborador ter a máxima atenção no momento em que comunica dados pessoais a entidades externas, privilegiando sempre a forma de comunicação que garanta a maior segurança dos dados possível.

No sentido de mitigar riscos de segurança na comunicação de dados com outras entidades, devem seguir-se as seguintes recomendações:

- Sempre que possível, a transmissão deve ser realizada através dos Portais das outras entidades (como é o caso do Portal da Autoridade Tributaria ou da Segurança Social);
- Não sendo possível comunicar dados via Portais, os ficheiros com os dados devem ser enviados de forma encriptada com palavra-chave, de acordo com as recomendações da área de sistemas de informação.

ANEXO VII- Tratamento de Dados Pessoais Colaboradores da AIM Cancer Center

1. Objetivo e âmbito

O presente anexo destina-se a dar a conhecer a forma como os dados pessoais dos Colaboradores AIM Cancer Center são tratados.

Para efeitos do presente documento, o termo "colaboradores" refere-se a trabalhadores (independentemente do tipo de contrato de trabalho: a termo, comissão de serviço, cedência) e estagiários.

A entidade responsável pelo tratamento dos seus dados pessoais e a AIM Cancer Center e como tal, seguira sempre as disposições legais e regulamentares aplicáveis a área da proteção de dados pessoais.

2. Fundamentos inerentes ao tratamento de dados pela AIM Cancer Center

A AIM Cancer Center ira tratar os dados pessoais dos colaboradores na medida do necessário para a execução do respetivo contrato e para dar cumprimento as obrigações legais que sobre si impendem no que respeita a esse contrato (como por exemplo a comunicação dos seus dados a entidades fiscais ou a entidades prestadoras de serviços de segurança e saúde no trabalho), bem como em função dos interesses legítimos da AIM Cancer Center na gestão da sua relação contratual (por exemplo, para controlo de assiduidade e de segurança.)

3. Finalidades para as quais a AIM Cancer Center trata dados pessoais

Os dados pessoais recolhidos pela AIM Cancer Center apenas são processados para fins específicos, explícitos e legítimos, destinando-se exclusivamente as finalidades identificadas aquando da recolha.

A AIM Cancer Center recolhe e utiliza os dados pessoais em questão, principalmente, para gerir a execução do seu contrato de trabalho (aqui incluindo finalidades como a gestão de carreira, gestão de formação, gestão e contratação de seguros e outros benefícios, processamento de salários, gestão de acessos as instalações e equipamentos AIM Cancer Center, organização de viagens de trabalho, cumprimento de obrigações relacionadas com a saúde e segurança no trabalho).

A AIM Cancer Center pode ainda tratar os dados pessoais em questão para cumprir obrigações legais (por exemplo, comunicações junto de entidades fiscais e de segurança social) e ordens judiciais, bem como para exercer ou defender os direitos legítimos da

AIM Cancer Center em Tribunal ou ainda no âmbito de apoios a projetos onde se inclua a contratação de pessoal.

4. Formas de recolha

A AIM Cancer Center apenas recolhe dados que se mostrem adequados, pertinentes e limitados ao que é necessário relativamente as finalidades para os quais são tratados.

A recolha de dados pode ser feita oralmente ou por escrito (nomeadamente através do *curriculum vitae*, ficha individual do trabalhador, documentos de identificação e do contrato de trabalho.)

Regra geral, a AIM Cancer Center recolhe diretamente dados pessoais junto de cada colaborador, podendo igualmente ser recolhidos dados pessoais através de terceiros, nomeadamente das fichas de aptidão médica emitidas pelas entidades prestadoras de serviços de saúde e segurança no trabalho, nos termos da lei.

5. Categorias de dados pessoais tratados pela AIM Cancer Center

Para execução das finalidades *supra* descritas, a AIM Cancer Center trata os seguintes tipos de dados pessoais:

- Dados de identificação como por exemplo o nome, a fotografia, o género e a data de nascimento;
- Documentos de identificação, como por exemplo o cartão de cidadão, passaporte, os detalhes relativos a pedidos de vistas, a carta de condução, NIF e NISS;
- Detalhes de contacto, como por exemplo morada, telem6vel, e-mail e os detalhes de contacto de pessoas a contactar em case de emergência e/ou dos parentes mais pr6ximos;
- Detalhes inerentes às funções desempenhadas, como por exemplo o seu cargo, categoria profissional, local ou locais onde exerce funções, horário, antiguidade, avaliações, registos disciplinares, ausências e férias;
- Informações relativas a qualificações académicas e profissionais;
- Dados financeiros, como por exemplo nível salarial, retenções e dados bancários;
- Informações relativas a pensões e outros benefícios, como por exemplo, informações relativas a contribuições para o regime de pensões, subsídios, seguros e equipamentos disponibilizados ou financiados pela AIM Cancer Center;
- Informações relacionadas com a utilização de sistemas, instalações e equipamentos disponibilizados pela AIM Cancer Center, como por exemplo o ID do seu

computador e/ou de dispositivos móveis ou outros, informações sobre o acesso as instalações da AIM Cancer Center e filmagens de CCTV;

- Informações relativas a saúde e a segurança, como por exemplo registos de acidentes de trabalho, atestados médicos e relatórios médicos de avaliação da aptidão para o exercício de funções.

6. Com quem partilha a AIM Cancer Center os dados pessoais dos colaboradores

A AIM CANCER CENTER apenas permite o acesso aos dados pessoais dos colaboradores, a quem necessite dos mesmos para executar tarefas e deveres associados com obrigações contratuais ou legais, bem como a terceiros que tenham uma finalidade legítima para aceder aos mesmos.

Sempre que se permite um acesso aos dados pessoais, são adoptadas medidas adequadas para garantir o acesso apenas aos dados estritamente necessários, bem como a integridade e a confidencialidade dos mesmos.

A nível do fluxo interno, alem da área de recursos humanos, responsável pela gestão dos dados de colaboradores AIM Cancer Center, os dados pessoais em questão apenas são partilhados com outras áreas da AIM Cancer Center na medida do necessário (por exemplo, para efeitos de processamento de salários, para gerir viagens de negócios ou de deslocações para feiras ou outros eventos).

A nível de fluxo com entidades externas, são disponibilizados certos dados pessoais a fornecedores/subcontratantes que prestam serviços a AIM Cancer Center, segundo critérios de necessidade e em conformidade com a legislação aplicável. A título de exemplo, são partilhados dados pessoais com terceiros ou subcontratantes para efeitos de gestão de viagens de colaboradores, contratualização de seguros, soluções de arquivo (físico e digital) e serviços de saúde e segurança no trabalho.

Também podem ser divulgados dados pessoais a terceiros com base noutras razões legítimas, tais como, a título de exemplo:

- Para dar cumprimento a obrigações legais, incluindo quando seja necessário para cumprir um normativo legal ou ordem judicial (v.g. transmissão de dados a entidades

fiscais e segurança social, bem como a tribunais e agentes de execução ou a Comissão de Trabalhadores da AIM Cancer Center).

- Quando for necessário para efeitos de interesses legítimos da AIM Cancer Center ou de terceiros (aqui incluindo, nomeadamente organismos públicos e ministeriais).
- Quando a transmissão decorrer das obrigações inerentes ao desempenho das funções ao abrigo do contrato de trabalho.

Para informações adicionais sobre estes terceiros ou subcontratantes, deve contactar-se a área responsável pela disponibilização dos dados ou, em caso de dúvida, a área dos recursos humanos.

7. Prazo para Conservação de Dados

A AIM Cancer Center conservará os dados pessoais dos colaboradores até um ano após o termo da relação contratual, exceto os dados que, por imposição legal, devam ser conservados por períodos temporais superiores.

A AIM Cancer Center procura garantir que os dados pessoais dos colaboradores são mantidos e, se for

caso disso, apagados ou destruídos de forma segura, em conformidade com as políticas, orientações e regras sobre a conservação de dados pessoais, existentes.

8. Direitos dos titulares de dados pessoais

Consultar a Política de proteção de dados pessoais, Exercício de Direitos.

ANEXO VIII- Procedimento em caso de Violação de Dados (“Data Breach”)

1. Objetivo e âmbito

Um "data breach” - para efeitos de aplicação do Regulamento Geral de Proteção de Dados (RGPD) - é uma violação de dados pessoais, intencional ou acidental, que pode levar a destruição, perda, alteração e divulgação não autorizada dos mesmos. Abrange igualmente situações onde seja comprometida a confidencialidade, integridade e disponibilidade desses dados.

Os seguintes exemplos constituem situações, efectivas ou potenciais, de "data breaches":

- Divulgação de dados de forma não autorizada, por "hackers" ou por falhas de proteção/segurança;
- Transmissão de ficheiro com diversos dados pessoais de um conjunto de colaboradores da AIM Cancer Center (para efeitos do presente documento abrange trabalhadores e estagiários), de forma não encriptada, para um destinatário incorreto;
- Roubo ou perda de equipamento que contenha repositórios de dados pessoais e não esteja encriptado;
- Material que seja considerado obsoleto/lixo e que saia das instalações da AIM CANCER CENTER, sem ter havido a preocupação de tornar ilegível os dados pessoais contidos em suportes digitais ou em papel, pode levar a uma situação de "data breach".

2. A quem se destina

Todos os colaboradores da AIM Cancer Center.

3. Procedimento a seguir

Como deve o colaborador proceder em caso de "Data Breach" ou suspeita de "Data Breach"?

Sempre que o colaborador tomar conhecimento au suspeitar de um incidente desta natureza (ver ponto 1), devera seguir os seguintes passos:

1. Guarde sempre que possível, toda a documentação de suporte ou outra evidência da violação detetada, bem como qualquer troca de comunicações sobre o tema (registos informáticos, troca de emails, print screens, entre outros);
2. Reporte o incidente ao DIRETOR DE OPERAÇÕES, no prazo máximo de 24 horas, através do formulário que se encontra no final deste documento. Procure descrever o melhor possível a violação detectada e que dados pessoais possam estar envolvidos. indique se já houve quaisquer medidas corretivas adotadas e, em caso afirmativo, refira quais;
3. Envie o formulário e as informações que entender serem relevantes, ao DIRETOR DE OPERAÇÕES para o endereço de e-mail dpo@aim.clinic, e estabeleça um contacto telefónico após esse envio de forma a assegurar a celeridade necessária, dado que estas situações implicam a existência de prazos legais muito curtos.
4. O DIRETOR DE OPERAÇÕES analisa de imediato o incidente e certifica-se de que a comunicação da violação de dados consubstancia ou pode vir a consubstanciar uma violação de dados pessoais nos termos do RGPD. Em caso afirmativo, o DIRETOR DE OPERAÇÕES toma as medidas legalmente definidas.

<u>No caso de o incidente consubstanciar uma violação de dados pessoais:</u>

1. No prazo máximo de 48h após a detecção da violação de dados, a Administração ou o seu legal representante, determina que as áreas da AIM Cancer Center envolvidas, em conjunto com o DIRETOR DE OPERAÇÕES, devem identificar as falhas e os riscos em termos dos direitos e liberdades dos titulares dos dados.
2. A AIM Cancer Center (Responsável pelo tratamento) deve de imediato implementar as medidas que permitam colmatar as falhas existentes e minimizar os potenciais danos nos direitos e liberdades dos titulares dos dados.
3. Caso se conclua que o incidente de violação de dados afecta os direitos e liberdades dos titulares dos dados, o DIRETOR DE OPERAÇÕES deverá, no prazo máximo de 72 horas após o incidente de violação de dados, reportar o incidente junto da CNPD, através de formulário online disponível em www.cnpd.pt.

Se a conclusão for de que o incidente de violação de dados não afeta os direitos e liberdades dos titulares dos dados, a AIM Cancer Center fica dispensada de notificar a CNPD acerca de tal incidente, competindo-lhe apenas registar internamente o incidente (bem como as medidas de correcção adoptadas e consequentes ganhos esperados).

4. Na situação em que que o incidente de violação de dados representar um elevado risco para os direitos e liberdade das pessoas singulares, a AIM Cancer Center comunica o incidente aos titulares dos dados afetados sem demora justificada, devendo fornecer-lhes, pelo menos, as seguintes informações:

- O nome e os contactos do encarregado da proteção de dados e/ou de outro ponto de contacto onde possam ser obtidas mais informações;
- As consequências prováveis da violação de dados pessoais;
- As medidas adotadas ou propostas pela AIM Cancer Center para reparar a violação de dados pessoais, inclusive, se for case disso, medidas para atenuar os seus eventuais efeitos negativos.

Formulário de reporte de um "Data Breach"

1. Identificação do Colaborador

Nome	
Área	
Contacto	
Função	

2. Informação do Incidente:

Hora/Data início da violação	
Hora/Data fim da violação	
Hora/Data conhecimento da violação	
Forma como teve conhecimento da violação	

Tipo da violação:	☐	Integridade (alteração indevida)
	☐	Confidencialidade (acesso ou divulgação indevida)
	☐	Disponibilidade (eliminação indevida)

Natureza da violação:	☐	Equipamento perdido ou roubado
	☐	Documentos perdidos ou roubados
	☐	Correio perdido ou acedido indevidamente
	☐	Hacking
	☐	Malware
	☐	Phishing
	☐	Outra

Causa da violação:	☐	Acto interno não malicioso
	☐	Acto interno malicioso
	☐	Acto externo não malicioso
	☐	Acto externo malicioso
	☐	Outra

Descrição do Incidente:

_____

_____

_____

_____

3. Consequências da violação:

Integridade

A alteração/corrupção dos dados pode ter consequências para os titulares? ☐ Sim ☐ Não

Indique quais: _____

A alteração/corrupção dos dados é passível de ser revertida para o estado original? ☐ Sim ☐ Não

Os dados foram cifrados? ☐ Sim ☐ Não

Confidencialidade

A alteração/corrupção dos dados pode ter consequências para os titulares? ☐ Sim ☐ Não

Indique quais: _____

Disponibilidade

A perda de disponibilidade dos dados pode ter resultado em consequências para o titular dos dados (durante a violação ou no futuro)? ☐ Sim ☐ Não

Indique quais: _____

Notas adicionais:

_____

_____

_____

_____

4. Dados Pessoais:

Tipos de dados pessoais:

☐ Dados de identificação (Nome, CC, NIF)
☐ Dados de contacto (telefone, e-mail, morada)
☐ Dados financeiros
☐ Dados sensíveis (ex: dados de saúde)

Outros dados:

_____

Possível determinar o número de sujeitos envolvidos? ☐ Sim ☐ Não

Número de sujeitos envolvidos: _____

5. Titulares de Dados:

Titulares de dados pessoais

☐ Trabalhadores
☐ Clientes
☐ Outros

Notas adicionais:

_____

_____

_____

_____

6. Informação aos titulares:

Os titulares foram informados da violação? ☐ Sim ☐ Não

Hora/Data da comunicação da violação:	
Forma de comunicação da violação:	
Número de titulares contactados:	
Mensagem remetida aos titulares:	

7. Medidas Preventivas/Correctivas:

Que medidas foram aplicadas

ANEXO IX- Procedimento de Avaliação de Impacto sobre a Proteção de Dados (AIPD)

1. Objetivo e âmbito:

Uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) e um processo que visa estabelecer e demonstrar conformidade com os princípios de proteção de dados. Estas avaliações surgem em alternativa as autorizações prévias emitidas pela CNPD, impostas pela Lei 67/98, de 26 de outubro (LPDP) para certos tipos de tratamento de dados pessoais. Encontram-se previstas nos artigos 35°e seguintes do RGPD.

Sempre que um certo tipo de tratamento utilize novas tecnologias e, tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, a AIM Cancer Center inicia previamente uma AIPD para as operações em causa.

Uma AIPD deve ser realizada antes de se iniciar o tratamento de dados pessoais, sendo para tal imprescindível elaborar uma descrição detalhada do tratamento previsto, de modo que se tome possível fazer uma avaliação da necessidade e proporcionalidade do tratamento em questão.

Ao efetuar uma avaliação de impacto sobre a proteção de dados, a entidade responsável pelo tratamento solicita o parecer do encarregado da proteção de dados (DPO).

2. A quem se destina

Todas as áreas da AIM Cancer Center.

3. Quando deve ser efetuada uma AIPD?

Só existe obrigação de realizar uma AIPD quando o tratamento for "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (artigo 35.º, n.º 1 do RGPD).

A AIPD é obrigatória. pelo menos, nos casos seguintes:

- Quando se proceda a uma avaliação sistemática e completa de dados pessoais, baseada em tratamentos automatizados, incluindo a definição de perfis;
- Quando se tratem, em grande escala, categorias especiais de dados (dados relativos a saúde, dados que revelem opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, dados biométricos, etc.), ou de dados pessoais relacionados com condenações penais e infracções;
- Quando se efetue, em grande escala, um controlo sistemático de zonas publicas.

Podem, contudo, existir outras operações que possam carecer de uma AIPD. Mostra-se assim essencial a detecção e análise das seguintes situações, com vista a poder concluir-se se determinada operação pode constituir ou não um elevado risco para os direitos e liberdades das pessoas singulares:

- Tratamento de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados.
- Geração de decisões automatizadas (i.e., sem intervenção humana) que produzam efeitos jurídicos ou afetem significativamente o titular dos dados.

- Controlo sistemático dos dados, envolvendo a observação, monitorização ou controlo dos titulares dos dados, incluindo dados recolhidos através de redes, ou um "*controlo sistemático de zonas acessíveis ao publico*".
- Tratamento de dados especiais ou dados de natureza altamente pessoal, tais como dados referentes a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos, dados relativos a saúde ou dados relativos a vida sexual ou orientação sexual, bem como dados pessoais relacionados com condenações penais e infracções.
- Operações de tratamento em grande escala, considerando-se os seguintes factores como determinantes da existência de tratamento em grande escala:

a. o número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente;
b. o volume de dados e/ou a diversidade de dados diferentes a tratar;
c. a duração da atividade de tratamento de dados ou a sua pertinência;
d. a dimensão geográfica da atividade de tratamento.

- Tratamento de dados relativos a titulares de dados vulneráveis, considerando-se como tal os titulares que não sejam capazes de consentir ou opor-se, fácil e livremente, ao tratamento dos seus dados ou de exercer os seus direitos.
- Utilização de soluc6es inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais que possam envolver novas formas de recolha e utilização dos dados pessoais recolhidos.
- Situações em que o próprio tratamento impeça os titulares dos dados "de exercer um direito ou de utilizar um serviço ou um contrato".
- Correspondências ou combinações de conjuntos de dados que excedam as expectativas razoáveis do titular dos dados.

Analisados todos os referidos critérios, quanto maior for o número de critérios preenchido pela operação de tratamento que se pretende realizar, maior será a probabilidade de este significar um elevado risco para os direitos e as liberdades dos titulares dos dados e, por conseguinte, de necessitar de uma AIPD, independentemente das medidas de segurança que o responsável pelo tratamento adopte.

Em caso de dúvida a este respeito, deverá ser consultado o DIRETOR DE OPERAÇÕES da AIM Cancer Center.

Pontes a detalhar numa AIPD:

A AIPD devera começar pela análise detalhada dos seguintes itens:

a) Uma descrição sistemática da operação e do tipo de tratamento de dados, devendo destacar-se:

- A finalidade do tratamento;
- Os fundamentos de legitimidade para tal tratamento (por exemplo, a execução de um contrato, o cumprimento de uma obrigação legal ou os interesses legítimos do responsável pelo tratamento);
- A duração de tal operação;
- Os suportes (físicos ou digitais) nos quais os dados poderão circular;
- A(s) área(s) responsável (eis) pela operação.

b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos (explicação do porquê da necessidade do tratamento de dados, efetuando-se um juízo de necessidade e proporcionalidade);

c) Uma avaliação dos riscos para os direitos e liberdades dos titulares - análise de como são assegurados os princípios da confidencialidade, integridade e disponibilidade dos dados pessoais a serem tratados e riscos de poderem não ser assegurados tais princípios; e
d) As medidas previstas para mitigar os riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com os princípios da confidencialidade, integridade e disponibilidade dos dados, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

ANEXO X- Procedimento de Proteção de Dados Pessoais a Adoptar Pelos Trabalhadores

1. As passwords automáticas devem ser alteradas pelo trabalhador para que sejam só do seu conhecimento. Devem ser tão complexas quanto possível e alteradas com frequência, mesmo nos sistemas que não obriguem a fazê-lo;

2. As passwords são pessoais e intransmissíveis, não devem ser partilhadas ou escritas em locais acessíveis a todos;

3. Não devem ser utilizadas as mesmas passwords para os sistemas da organização e sistemas pessoais;

4. O trabalhador deve bloquear o computador sempre que se ausentar da sala;

5. As aplicações e plataformas com dados pessoais não devem ser deixadas abertas no ecrã, caso não estejam a ser utilizadas;

6. Os dispositivos de armazenamento de dados (PEN, disco externo) não devem ser deixados no computador ou em local acessível, caso não estejam a ser utilizados;

7. Os documentos com dados pessoais não devem ser deixados junto da impressora e não devem ser rasgados, deve optar-se por triturar esses documentos numa destruidora de papel;

8. O trabalhador não deve deixar documentos com dados pessoais acessíveis na sua secretária. Estes devem ser guardados dentro de pastas/dossiers ou em armários fechados, evitando-se a sua acessibilidade por terceiros;

9. Caso o trabalhador perca o seu computador ou documentos de trabalho que contenham dados pessoais, ou suspeite que um terceiro lhes tenha acedido, deve de imediato comunicá-lo ao Encarregado de Proteção de Dados.

ANEXO XI- Procedimento de Proteção de Dados Pessoais a Adoptar Pela Área de Recursos Humanos

1. O acesso ao processo individual de cada trabalhador só é facultado ao próprio;

2. Os processos individuais dos trabalhadores são guardados em armários fechados com chave, cujo acesso é restrito;

3. A correspondência recebida pela AIM Cancer Center é tratada por funcionário específico, sendo posteriormente distribuída e/ou arquivada em papel em armário próprio e em suporte digital numa pasta de acesso restrito;

4. A AIM Cancer Center privilegia o envio de correspondência que contenha dados pessoais por correio registado com aviso de receção.