HISTOCIT
Laboratório de Anatomia Patológica
Director: Dr. Fortunato Vieira

Nota Informativa - RGPD

O novo Regulamento Geral de Proteção de Dados (RGPD) terá que ser implementado por todas as empresas e organizações até 25 de maio de 2018.

A proteção dos dados pessoais exige a adoção de medidas técnicas e organizativas adequadas para assegurar um nível de segurança adaptado ao risco. O RGPD regula a proteção de dados pessoais, ou seja, dados respeitantes às pessoas singulares.

O presente documento é parte integrante de um plano de ação interno que visa:

i. Assegurar as alterações necessárias para cumprimento dos requisitos previstos no RGDP;
ii. Informar os clientes, utilizadores dos serviços web e parceiros do Histocit Laboratório da Anatomia Patológica.

Deste modo para melhor conhecimento de todos, apresentamos um resumo das principais alterações, direitos e exigências do novo Regulamento Geral de Proteção de Dados.

O presente documento não substitui o dever de leitura da legislação em vigor.

Como nota introdutória apresentamos os principais pilares do novo Regulamento Geral de Proteção de Dados (RGPD).

Visão geral do RGPD

Direitos das pessoas singulares

Expande significativamente os direitos das pessoas singulares e a informação que tem de ser facultada relativamente às atividades de tratamento

Consentimento

Tem de ser confirmado por uma declaração ou outro ato positivo inequívoco. Não se pode presumir o consentimento nem usar opções pré-seleccionadas em sites.

Encarregado da Proteção de Dados

Exige conhecimentos especializados em direito da proteção de dados.

Privacidade do princípio ao fim

Considerações de privacidade em todos os aspetos, utilizados os dados estritamente necessários à finalidade a que se destinam.

Notificação obrigatória de violação de dados

Notificar as autoridades de controlo até 72 horas após tomarem conhecimento do facto. Violações graves têm de ser notificadas às pessoas singulares.

Portabilidade de dados

As pessoas singulares têm agora o direito de circulação, cópia ou transferência dos dados pessoais, até mesmo, para uma empresa concorrente.

Coimas

Podem ir até 4% do volume de negócios global anual. A coima poderá ser aplicada mesmo que não haja perda de dados

Principais alterações / exigências do RGPD

1- AUTORIZAÇÃO

Com o estrito cumprimento do previsto no novo RGPD não e necessário notificar e/ou pedir autorização à Comissão Nacional de Proteção de Dados (CNPD) para o tratamento de dados pessoais.

Inversão do modelo de regulação vigente, um modelo de auto-regulação – em que as organizações são responsáveis pela interpretação, operacionalização e manutenção da conformidade com o RGPD e sujeitas à ação inspetiva da CNPD.

2- PESSOA SINGULAR

Qualquer informação relativa a uma pessoa singular identificada ou identificável (titular dos dados) é considerada um dado pessoal.

Uma pessoa singular pode ser identificada, direta ou indiretamente, por referência a dados como o seu nome, email, idade, estado civil, endereço de IP, etc.

Para determinar se uma pessoa é identificável, terão de ser considerados todos os meios suscetíveis de serem razoavelmente utilizados, pelo responsável pelo tratamento ou outra pessoa, para a identificar direta ou indiretamente.

Os princípios da proteção de dados não são aplicáveis a informações anónimas nem a dados pessoais tornados de tal forma anónimos que o titular não seja ou já não possa ser identificado.

A recolha de informação relativa a candidatos a emprego, trabalhadores, clientes e fornecedores é uma operação de tratamento de dados pessoais.

Além do registo, da conservação, da consulta, da adaptação ou alteração, da difusão, do apagamento, entre outras, a recolha é uma operação sobre dados pessoais, motivo pelo qual qualquer organização que proceda apenas à recolha de dados pessoais relativos a pessoas singulares, estará obrigada a observar as novas disposições.

3- SISTEMAS BIOMÉTRICOS

A utilização de sistemas biométricos (que registam uma representação digital da impressão digital, geometria da mão ou da face, padrão da íris ou reconhecimento da retina, etc.) constitui um meio de tratamento de dados sensíveis.

O RGPD impõe uma proibição geral no que diz respeito ao tratamento de dados pessoais de natureza sensível não necessários para prestação dos serviços solicitados.

4- PROIBIÇÃO DE DADOS PESSOAIS SOBRE ORIGENS, CONVICÇÕES E CRENÇAS

Os tratamentos de dados pessoais que revelem origem racial ou étnica, opções políticas, crenças religiosas ou filosóficas, associativismo sindical, assim como os tratamentos de dados genéticos, biométricos, relacionados com a saúde e sexualidade são, por regra, proibidos.

O tratamento destes dados podem ser efetuados, nomeadamente, mediante:

(i) Consentimento explícito para o tratamento desses dados para uma ou mais finalidades específicas;
(ii) Quando necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social;
(iii) Para proteger os interesses vitais do titular dos dados ou de outra pessoa singular física ou legalmente incapacitado de dar o seu consentimento;
(iv) Se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;
(v) Se for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da suas função jurisdicional;
(vi) Por motivos de interesse público importante.

5- OBRIGAÇÕES JURÍDICAS

O consentimento não é o único fundamento jurídico para legitimar o tratamento de dados pessoais.

Qualquer tratamento de dados, para que seja lícito, tem de ter por base um fundamento jurídico. O RGPD prevê para o efeito e além do consentimento, a necessidade do tratamento:

(i) Para efeitos de execução contratual;
(ii) Cumprimento de uma obrigação jurídica;
(iii) Defesa de interesses vitais do titular dos dados ou de terceiro;
(iv) Exercício de funções de interesse público ou em caso de um interesse legítimo prosseguido pelo responsável pelo tratamento, desde que, neste caso, não prevaleçam interesses, direitos ou liberdades fundamentais do titular.

6- VALIDADE

O RGPD alarga o conceito de consentimento e introduz condições mais exigentes para a sua obtenção, criando a necessidade de apurar se o consentimento obtido pelo responsável pelo tratamento respeita todos os novos requisitos – em caso negativo, será imprescindível obter novo consentimento dos titulares dos dados em conformidade com as disposições do RGPD, sob pena de o tratamento se tornar ilícito por falta de fundamento jurídico.

O consentimento deverá resultar de uma ação:

(i) Positiva e explícita;
(ii) Ser facilmente identificável;
(iii) Documentado;
(iv) Concedido em situações de equilíbrio entre as partes e de forma desagregada de demais termos e condições, bem como renovado com a periodicidade possível.

7- OBTENÇÃO DE CONSENTIMENTO

O consentimento deverá ser prestado:

(i) Mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular consente no tratamento dos dados que lhe digam respeito;
(ii) Através de declaração escrita ou oral;
(iii) Validação de uma opção num website ou outra conduta que indique expressamente que o titular aceita o tratamento proposto dos seus dados pessoais.

Não constituem formas válidas de consentimento:

(i) O consentimento genérico;
(ii) A obtenção do consentimento através de termos e condições genéricas;
(iii) A utilização de caixas pré-marcadas;
(iv) O silêncio, ou a omissão.

8- TRANSPARÊNCIA

Enquanto responsável pelo tratamento terá de, no momento de recolha de dados pessoais junto do respetivo titular, facultar-lhe uma série de informações sobre o tratamento dos seus dados.

Em cumprimento do dever de transparência, deverá facultar informação relativa:

(i) À sua identidade e contactos;
(ii) As finalidades do tratamento;
(iii) O fundamento jurídico para o tratamento;

(iv) Informações adicionais necessárias para garantia de um tratamento equitativo e transparente, tais como o prazo de conservação dos dados, os direitos do titular dos dados, etc.

Na qualidade de responsável pelo tratamento, mesmo quando os dados pessoais não sejam recolhidos junto do respetivo titular, terá de lhe prestar um leque de informações relativas à sua identidade e ao tratamento dos dados.

O responsável pelo tratamento deverá prestar, em diferentes prazos, dependendo das circunstâncias, informação respeitante:

(i) À sua identidade e contactos;
(ii) Às finalidades de tratamento dos dados;
(iii) Às categorias dos dados em questão;
(iv) Aos direitos dos titulares;
(v) Origem dos dados pessoais e, eventualmente, a circunstância de provirem de uma fonte acessível ao público.

As organizações terão de tomar medidas adequadas para fornecer informações e dirigir comunicações aos titulares dos dados de forma concisa, transparente, inteligível e de fácil acesso.

O princípio da transparência exige que qualquer informação prestada seja concisa,

(i) De fácil acesso e compreensão;
(ii) Comunicada numa linguagem clara e simples;
(iii) O titular dos dados deve se informado da operação de tratamento de dados e das suas finalidades.

9- TEMPO DE RESPOSTA

Prazo de 1 (um) mês a contar da data da receção do pedido

(i) Regras para facilitar o exercício pelo titular dos dados dos direitos que lhes assistem;
(ii) Procedimentos para solicitar e obter, a título gratuito, o acesso a dados pessoais, a sua retificação ou o seu apagamento, bem como o exercício do direito de oposição.

10- DIREITO DE ACESSO

Assegurar ao titular dos dados:

(i) O direito de obter a confirmação de que os seus dados são objeto de tratamento;
(ii) O direito de acesso aos mesmos e à informação relativa ao seu tratamento;
(iii) Acesso aos respetivos dados pessoais recolhidos a fim de conhecer e verificar a sua licitude;
(iv) Direito de conhecer e ser informado acerca das finalidades para as quais os dados são tratados,
(v) Período durante os quais são tratados, da identidade dos destinatários e da lógica subjacente ao tratamento.

11- RETIFICAÇÃO DOS DADOS

Retificação dos dados pessoais inexatos e completar os dados pessoais incompletos, sempre que seja solicitado pelo titular dos dados, tendo em conta as finalidades do tratamento.

12- APAGAR OS DADOS PESSOAIS

Enquanto responsável pelo tratamento está obrigado a apagar os dados pessoais quando:

(i) Os dados pessoais deixem de ser necessários para a finalidade que motivou a sua recolha/tratamento;
(ii) O titular retire o consentimento em que se baseia o tratamento e não subsista outro fundamento para o mesmo;
(iii) O titular se oponha ao tratamento e não existam motivos prevalecentes que o justifiquem;
(iv) Os dados sejam tratados ilicitamente;
(v) Os dados pessoais tenham sido recolhidos no contexto da oferta de serviços da sociedade de informação.

13- LIMITAR O TRATAMENTO

Limitar o tratamento de dados pessoais mediante solicitação do respetivo titular:

(i) Se o titular contestar a exatidão dos dados;
(ii) O tratamento for ilícito e o titular se opuser ao apagamento e solicitar, em contrapartida, a limitação da sua utilização;
(iii) O responsável pelo tratamento já não precisar dos dados para tratamento mas sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;
(iv) Se o titular se tiver oposto ao tratamento até se verificar que os motivos do responsável prevalecem sobre os do titular.

14 - TRANSMISSÃO DE DADOS

Facultar ao respetivo titular os dados que lhe digam respeito e que este lhe tenha fornecido.

Sempre que seja tecnicamente possível, transmitir esses dados diretamente a outro responsável pelo tratamento.

O direito à portabilidade num formato estruturado, de uso corrente e leitura automática.

15 - DIREITO DE OPOSIÇÃO

Perante o exercício do direito de oposição por parte de um titular de dados pessoais, cessar imediatamente o tratamento desses dados.

O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito

16 - TRATAMENTO DE DADOS AUTOMATIZADO

A tomada de decisões exclusivamente com base no tratamento automatizado é, regra geral, proibida.

O responsável do tratamento tem o dever geral de não sujeitar o titular dos dados pessoais a decisões tomadas exclusivamente com base no tratamento automatizado, incluindo a definição de perfis.

Qualquer tomada de decisões com base no tratamento automatizado, apenas poderá ter lugar se expressamente autorizada e acompanhada de garantias adequadas, que deverão incluir informação

específica ao titular dos dados e o direito de obter intervenção humana, o direito de o titular expressar o seu ponto de vista e obter uma explicação sobre a decisão tomada e de a contestar.

Quando seja possível a tomada de decisões com base no tratamento automatizado, o responsável pelo tratamento deve assegurar um tratamento em relação ao titular dos dados.

Para assegurar um tratamento equitativo e transparente, o responsável pelo tratamento deverá utilizar procedimentos adequados à definição de perfis, aplicar medidas técnicas e organizativas aptas a garantir que os fatores que introduzem imprecisões são corrigidos e que o risco de erros é diminuído, bem como a proteger os dados pessoais e prevenir efeitos discriminatórios contra os titulares dos dados.

17 – RESPONSABILIDADE

As organizações têm de estar aptas a apresentar evidências de que os tratamentos de dados pessoais que levam a cabo são realizados em conformidade com o RGPD.

Aplicar e concretizar as medidas adequadas e eficazes de assegurar e comprovar a observância das normas e dos princípios da proteção dos dados pessoais.

Os registos das atividades de tratamento deverão ser abordadas enquanto um pré-requisito para o compliance e são, enquanto tal, uma medida efetiva de responsabilidade.

A obrigação de conservação de registos é um meio de comprovar a observância das normas e exigências do RGPD, e é aconselhável a sua adoção ainda que número de trabalhadores seja inferior, como boa prática de compliance.

18 - PRINCÍPIOS DE PRIVACY BY DESIGN E PRIVACY BY DEFAULT

As organizações deverão aplicar, em sede de tratamento de dados pessoais, os princípios da proteção de dados desde a conceção e por defeito.

Levar o risco de privacidade em conta em todo o processo de conceção de um novo.

Assegurar que são colocados em prática, mecanismos para garantir que, por defeito, apenas será recolhida, utilizada e conservada para cada tarefa, a quantidade necessária de dados pessoais.

Apenas conservados pelo período considerado necessário para cada finalidade de tratamento.

19 - VIOLAÇÃO DE DADOS PESSOAIS

Adotar procedimentos internos de gestão de incidentes (violações de dados pessoais) que incluam a prevenção, deteção e resposta aos mesmos bem como circuitos de informação entre responsável pelo tratamento e subcontratante.

Registar e documentar todas as violações de dados pessoais, de forma a permitir à autoridade de controlo verificar o cumprimento das exigências regulamentares.

Nomear um Encarregado de Proteção de Dados (EPD), ao qual cabe a responsabilidade de pilotar o programa de *compliance* a implementar.

O presente documento tem por base a lei e o resumo de diversas publicações disponíveis para consulta pública.

Para qualquer esclarecimento adicional *geral@histocit.pt*