SPMS EPE
Serviços Partilhados do Ministério da Saúde

Privacidade da Informação no setor da Saúde

Privacidade da Informação no setor da Saúde

Guia sobre o Regulamento Geral de Privacidade de Dados

A transformação digital é hoje uma realidade na Sociedade em geral e nas Organizações em particular, com as tecnologias emergentes a potenciarem um conjunto de oportunidades de satisfação das necessidades das partes interessadas, de otimização dos recursos disponíveis e de otimização dos riscos relacionados. Neste contexto, a SPMS, EPE. tem vindo a acompanhar a inovação digital e a desenvolver um conjunto de iniciativas estratégias relacionadas com a melhoria da prestação dos serviços aos seus parceiros, a melhoria da eficiência organizacional e o lançamento de novos produtos e serviços digitais onde o fator inovação está fortemente presente.

Conscientes de que este novo contexto digital acarreta um conjunto de novos cenários de risco com impactos cada vez mais relevantes na operacionalidade das Organizações, a SPMS, EPE., em alinhamento com o previsto na Estratégia Nacional para o Ecossistema da Informação de Saúde 2020 (ENESIS2020), tem vindo a colocar os temas da Segurança de Informação, Cibersegurança e Privacidade dos dados no topo das suas preocupações, tendo lançado em 2016 o "Programa de Melhoria do Risco e Segurança da Informação", com o objetivo de promover a coordenação e partilha de boas práticas relacionadas com os sistemas de informação do Ministério da Saúde. Em 2017, as competências da SPMS, EPE no contexto da cibersegurança foram reforçadas com o *Despacho nº1348/2017, em Diário da República nº28/2017, Série II de 2017-02-08*, o qual identifica um conjunto de novas competências na coordenação, monitorização da implementação e operacionalização das boas práticas de melhoria contínua da resposta a ciber-riscos no setor da saúde.

Neste contexto, e tendo em consideração os riscos identificados pelo novo Regulamento Geral de Proteção de dados (RGPD), o qual entrará em vigor a partir de 25 de maio de 2018, a SPMS, EPE entendeu ser estratégico para o Setor da Saúde em Portugal a preparação e divulgação junto de todas as Entidades do Ministério da Saúde de um primeiro Guia que serve para auxiliar a reflexão e subsequente ação na área da "Privacidade da Informação no Setor da Saúde". Nesta primeira edição pretende-se clarificar o objetivo e âmbito do novo regulamento europeu, e sobretudo analisar os

impactos concretos que o mesmo terá no ecossistema da Saúde em Portugal. Seguir-se-á um guia de “Boas práticas e passos concretos”. Estes guias, bem como as ferramentas de avaliação e iniciativas de formação e capacitação associadas, serão instrumentos fundamentais para que todas as Entidades do Ministérios da Saúde comecem, desde já, a preparar os seus programas de resposta ao RGPD, analisando o nível atual de cumprimento, definindo as estratégias de resposta às situações de desalinhamento identificadas e implementando as soluções de acordo com as suas necessidades e possibilidades.

A SPMS, EPE, além do compromisso com a melhoria contínua do seu ambiente interno de controlo e gestão dos riscos relacionados com a cibersegurança e privacidade da informação, com muitos desafios ainda por ultrapassar, irá continuar a apoiar as entidades do Ministério da Saúde e a partilhar boas práticas, conhecimento e ferramentas para que todas as Entidades possam garantir que os sistemas de informação contribuam para a criação de valor e satisfação das necessidades dos Cidadãos.

Contamos com o vosso apoio e compromisso!

O Presidente do Conselho de Administração da SPMS,

Henrique Manuel Gil Martins

Assinado de forma digital por Henrique Manuel Gil Martins
Dados: 2017.03.21 08:12:12 Z

Henrique Martins

Índice

Nota Introdutória

A transformação digital no setor da saúde é uma realidade incontornável e tem conhecido, nos últimos anos, um crescimento exponencial.

De facto, constatamos hoje um crescimento considerável tanto da oferta, pelo lado dos prestadores de serviços, como da procura, por parte dos utentes, de produtos e serviços tecnológicos e digitais no setor da saúde.

A desmaterialização dos processos, a digitalização do acesso à informação e a introdução de novas tecnologias associadas à prestação de cuidados médicos constituem um passo importante no contexto da reforma do Serviço Nacional de Saúde ("SNS").

Associado a esta revolução digital, surgem naturalmente preocupações ao nível da segurança, privacidade e proteção dos dados dos utentes, em particular dos dados de saúde e informação clínica.

A aprovação do Regulamento (UE) 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")[1], e consequente necessidade de adaptação de processos e metodologias aplicáveis à forma como as Organizações passarão a tratar os dados pessoais, torna imprescindível o conhecimento das regras que, a partir de maio de 2018, serão aplicáveis ao tratamento dos dados pessoais.

Este Guia pretende precisamente abordar as vertentes jurídica e legal envolvidas no tratamento de dados pessoais no âmbito da prestação de cuidados de saúde, elucidando o leitor sobre os diversos aspetos a ter em conta aquando do tratamento de dados pessoais e apontar caminhos para a definição de programas de melhoria da organização, processos, tecnologias e competências das Entidades no SNS.

O teor deste Guia é meramente informativo e orientador e não desonera a consulta da legislação aplicável.

[1] Regulamento (UE) 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 e que revoga a Diretiva 95/46/CE. O Regulamento foi publicado no Jornal Oficial da União Europeia no passado dia 4 de maio de 2016.

Âmbito, Objetivos e Metodologia do Guia

A SPMS – Serviços Partilhados do Ministério da Saúde, EPE ("SPMS") tem como missão a prestação de serviços partilhados – nas áreas de compras e logística, serviços financeiros, recursos humanos e sistemas e tecnologias de informação e comunicação – às Entidades com atividade específica na área da saúde, de forma a centralizar, otimizar e racionalizar a aquisição de bens e serviços no SNS.

A SPMS assume, atualmente, um conjunto de responsabilidades na área da governação e gestão das TIC no Ministério da Saúde, procurando ajustar boas práticas, produtos e serviços às necessidades dos utentes, do SNS e do Ministério da Saúde.

No âmbito da sua missão, a SPMS tem sido responsável pelo desenvolvimento e implementação de várias iniciativas no âmbito da Estratégia Nacional para o Ecossistema de Informação de Saúde 2020 – ENESIS 2020, bem como iniciativas em domínios temáticos como é o caso da segurança e privacidade.

Estas iniciativas têm vindo a ser desenvolvidas na generalidade das Entidades integrantes do SNS – i.e. os serviços e Entidades públicas prestadoras de cuidados de saúde, da administração direta e indireta, assim como do setor público empresarial, designadamente: (i) os agrupamentos de centros de saúde; (ii) os estabelecimentos hospitalares, independentemente da sua designação e natureza jurídica (v.g. As Entidades de saúde e centros hospitalares tanto do setor público administrativo como do setor público empresarial); e (iii) as unidades locais de saúde.

As iniciativas do ENESIS 2020 integram-se num processo global de mudança e transformação digital que se tem verificado, nos últimos anos, no setor da saúde em Portugal, dando assim continuidade à uniformização dos sistemas de informação hospitalar no SNS, tendo por objetivo principal a melhoria na prestação de cuidados aos utentes.

Pretende-se assim promover a evolução dos atuais sistemas clínicos da SPMS para um processo clínico eletrónico, permitindo, aos utentes, uma visão 360º da informação centrada no utente, permitindo o acesso constante e integral a tal informação.

Acresce que a transformação digital no setor da saúde em Portugal, no âmbito do ENESIS 2020, impõe a necessidade de adaptação das tecnologias, pessoas e processos que intervêm em todo o ciclo de vida da informação de saúde, com natural impacto ao nível da privacidade e proteção de dados pessoais dos utentes.

Os desafios decorrentes dos fluxos contínuos de dados pessoais, no contexto de iniciativas da SPMS como o Registo de Saúde Eletrónico, a Plataforma de Partilha de Dados de Saúde (PDS) e o Acesso dos Utentes aos seus dados de saúde, assim como a consagração do princípio da portabilidade de informação de saúde no âmbito da utilização de Apps e de outras formas de interligação de sistemas de informação com impacto na saúde, tornam essencial o conhecimento das regras aplicáveis ao tratamento dos dados pessoais.

Nesse sentido, a SPMS elaborou o presente Guia de Privacidade da Informação do Setor da Saúde em Portugal ("Guia"), de forma a dar a conhecer, às Entidades públicas integrantes do SNS[2], as condições a que se encontram sujeitas em relação ao tratamento de dados pessoais em Portugal.

O Guia tem, assim, como objetivo fornecer algumas informações sobre as condições de tratamento de dados pessoais, permitindo que as Entidades públicas integrantes do SNS, por um lado, realizem uma avaliação preliminar do nível de adequação e cumprimento das respetivas regras e, por outro lado, conheçam as regras e impacto que o RGPD e a Diretiva de Segurança das Redes e da Informação[3] ("Diretiva SRI") terá nas Entidades.

Neste Guia[4] encontrará também as principais regras acerca do tratamento de dados pessoais em Portugal que regem, até 25 de maio de 2018 (data em que o RGPD será aplicável) relativas quer aos procedimentos a adotar perante a Comissão Nacional de Proteção de Dados[5] ("CNPD"), quer às regras a observar para garantir os direitos dos titulares dos dados (direitos com consagração constitucional, como resulta do artigo 35.º da Constituição da República Portuguesa). Atualmente, o regime jurídico de proteção das pessoas singulares no que respeita ao tratamento e livre circulação dos dados pessoais encontra-se consagrado, em termos genéricos, na Lei de Proteção de Dados Pessoais[6] ("LPDP"), que transpõe a Diretiva de Proteção de Dados Pessoais[7].

---

[2] Consideram-se para o efeito todos os estabelecimentos e serviços do Serviço Nacional de Saúde, independentemente da respetiva natureza jurídica, sejam Entidades públicas empresariais, sejam Entidades do Sector Público Administrativo, bem como aos órgãos e serviços do Ministério da Saúde e a quaisquer outras Entidades quando executem atividades na área da saúde.

[3] Diretiva (UE) 2016/1148, de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. A Diretiva SRI terá que ser transposta para o ordenamento jurídico nacional até 25 de maio de 2018.

[4] A informação veiculada no presente Guia não é exaustiva e não pretende espelhar, de forma detalhada, os procedimentos a adotar no domínio do tratamento de dados pessoais.

[5] A CNPD é a autoridade nacional que controla e fiscaliza o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, competindo-lhe em especial autorizar ou registar, consoante os casos, os tratamentos de dados pessoais e emitir pareceres sobre disposições legais ou legislação em preparação nesta matéria.

[6] Lei n.º 67/98, de 26 de outubro, alterada pela Lei nº 103/2015, de 24 de agosto.

[7] Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ("Diretiva de Proteção de Dados Pessoais").

Existe também legislação específica para o setor da saúde, com impacto ao nível da proteção de dados, como é o caso da Lei da Informação Genética Pessoal e Informação de Saúde[8], da Lei da Investigação Clínica[9] e do Regulamento arquivístico das Entidades de saúde e demais serviços do Ministério da Saúde[10].

As Entidades integrantes do SNS devem ainda ter em consideração as Deliberações emitidas pela CNPD, sejam as aplicáveis a qualquer Organização (nomeadamente em sede de proteção da privacidade dos colaboradores), sejam as que regulam o tratamento de dados no setor da saúde (como a Deliberação aplicável aos tratamentos de dados pessoais efetuados no âmbito de Investigação Clínica[11]; a Deliberação aplicável ao acesso a dados de saúde[12]; e a Deliberação aplicável ao acesso a dados de saúde de titulares falecidos[13]).

Apenas através do conhecimento das regras aplicáveis à matéria de proteção de dados pessoais as Entidades integrantes do SNS poderão definir procedimentos e adotar medidas que permitam, por um lado, evitar os riscos de incumprimento da lei e, por outro, retirar maiores benefícios dos dados recolhidos.

[8] Lei n.º 12/2005 de 26 de janeiro.

[9] Lei n.º 21/2014 de 16 de abril, alterada pela Lei n.º 73/2015, de 27 de julho.

[10] Aprovado pela Portaria n.º 247/2000, de 8 de maio, alterada pela Portaria nº 157/2014, de 19 de agosto.

[11] Deliberação da CNPD n.º 1704/2015.

[12] Deliberação da CNPD n.º 51/2001.

[13] Deliberação da CNPD n.º 72/2006.

Contexto: A Transformação digital das organizações e da sociedade

Em apenas umas curtas décadas, as Tecnologias de Informação e Comunicações (TIC) deslocaram-se do back office, a 1ª Plataforma, para o front office, a 2ª Plataforma e, finalmente, integraram-se em quase todos os aspetos das vidas profissionais e pessoais das pessoas, alimentadas por tecnologias da 3ª Plataforma, incluindo mobilidade, social, cloud e big data e analítica. Esta nova era em que as tecnologias e processos que as Organizações implementam estão de tal forma ligadas aos seus clientes/utentes e mercados, que as fronteiras entre as operações internas da Organização e o seu ecossistema externo (clientes/utentes, mercados, concorrentes, parceiros, reguladores) estão a desaparecer rapidamente.

Neste contexto os líderes, do setor público e privado, são desafiados a levar as suas Organizações ao nível seguinte, o da transformação digital, empregando tecnologias digitais em conjunto com a inovação organizacional, de modelos operacionais para criar novas formas de operar e de expandirem a sua atividade.

Apesar do nome “digital”, há muito mais na transformação digital para além da tecnologia. A IDC define a Transformação Digital como “o processo contínuo através do qual as Organizações se adaptam ou apresentam mudanças inovadoras aos seus clientes/utentes e mercados (ecossistema externo) ao potenciar competências digitais para inovar novos modelos operacionais, produtos e serviços que misturam de forma uniforme o digital, o físico, as experiências da Organização e do cliente, ao mesmo tempo que melhoram a eficácia operacional e o desempenho organizacional”.

A Transformação Digital corresponde muitas vezes a uma disrupção da forma como é entendido o funcionamento das Indústrias e Organizações, influenciando uma inversão do modelo operacional da sua orientação tradicional de disponibilização de produtos ou serviços para uma orientação mais dependente do ecossistema externo (por exemplo: utentes, clientes/utentes, mercados, parceiros, concorrentes, reguladores, etc), exigindo um processo contínuo de adaptação às condições de mudança interna e externa.

No centro do novo ecossistema digitalmente transformado não está a Organização, mas o individuo envolvido numa miríade de Omni-experiências que incluem interações pessoais, profissionais, comerciais e relações sociais - tudo tornado possível por interfaces digitais pessoais e profissionais.

O número e diversidade de dispositivos de interface pessoais é um indicador de vanguarda da chegada da Internet of Things (IoT), um indicador que representa todo um novo desafio para a segurança empresarial, assim como as oportunidades de marketing, prestação de serviços, experiência social e comunicação. Estudos recentes da IDC estimam que cada indivíduo pode chegar a ter 24 identidades digitais. Se apenas 35% da população mundial se inclui no "comum" digital, o Universo de Identidade Digital (UID) mundial encontra-se em cerca de 55 biliões.

As implicações organizacionais e sociais da transformação digital, estendem-se do Órgão de governança até às áreas operacionais e passando cada vez mais pelas clouds privadas dos clientes/utentes, colaboradores e parceiros. Estas incluem, mas não se limitam a:

- ✓ Partilhar experiências pessoais e profissionais;
- ✓ Redefinir como as Organizações geram receita e monetizam produtos e serviços;
- ✓ Desenvolver um plano de marketing focado nas experiências contextualizadas e personalizadas dos clientes/utentes;
- ✓ Gerir os maiores riscos de falhas na segurança;
- ✓ Explorar a inovação dos clientes/utentes para orientar o desenvolvimento de produtos e serviços;
- ✓ Redefinir a natureza dos serviços;
- ✓ Redefinir a natureza do trabalho e como o mesmo é realizado;
- ✓ Obter e gerir uma força laboral dispersa 24 x 7 x 365;
- ✓ Ligar a cadeia de valor virtualmente;
- ✓ Conectar pessoas através de experiências;
- ✓ Criar organizações temporárias;
- ✓ Promover papéis profissionais passageiros;
- ✓ Automatizar interfaces utilizador-máquina e máquina-utilizador;
- ✓ Fazer desaparecer as restrições de tempo e espaço.

A transformação digital é, assim, um elemento fundamental não apenas para as Organizações prosperarem, mas, em muitos casos, as falhas nesta matéria poderão mesmo influenciar a sua sustentabilidade.

Impactos da transformação digital no setor da saúde

A revolução digital nos serviços de saúde veio disponibilizar novas oportunidades para o desenvolvimento da qualidade da prestação de cuidados, investigação de novos tratamentos e uma melhor utilização dos recursos. No entanto, na maioria dos países, o sistema de saúde está fortemente pressionado por vários fatores. O efeito conjugado de uma maior esperança de vida e a prevalência de doenças crónicas tem sido responsável pelo crescimento dos custos dos cuidados de saúde e ameaçam a sustentabilidade do modelo tradicional de prestação de cuidados de saúde em muitos dos países. Assim, novos modelos de atendimento suportados por novas tecnologias e pela digitalização têm vindo a aparecer como solução para este cenário.

A utilização digital da informação tornou-se uma componente essencial de um novo sector de saúde orientado para a qualidade dos serviços prestados e para a eficiência dos recursos. Trata-se de uma transformação, desencadeada e suportada por novas tecnologias e partilha de informação, mas também pelas exigências das novas gerações para que o sistema público de saúde corresponda ao estilo de vida cada vez mais digital.

A maioria da informação que, presentemente, é partilhada digitalmente, anteriormente era partilhada em papel, suscitando assim, novos desafios e ameaças digitais ao nível da segurança e privacidade, nomeadamente em relação à proteção dos dados pessoais numa sociedade cada vez mais digital.

Os sistemas de informação de saúde têm um conjunto de características gerais que impactam diretamente as oportunidades e ameaças relacionadas com a segurança e privacidade dos dados e informação, designadamente:

- Os dados e informação sobre utentes são recolhidos através de uma vasta quantidade de sistemas TIC (centrais ou locais) e equipamentos médicos (eminentemente locais). Existe, por vezes, pouco conhecimento sobre a arquitetura informacional de suporte, nomeadamente no que refere ao armazenamento dos dados dos utentes.

- Os processos de tratamento são operacionalizados através do ecossistema do doente num ambiente de cuidados integrados, no qual todos os prestadores de serviços, incluindo os utentes, têm acesso aos dados dos utentes.
- O tratamento dos utentes está cada vez mais dependente de dados e de informação, como o caso da medicina de precisão ou de processos de cuidados pessoais.
- Os dados e informação são partilhados para outros objetivos que não o tratamento direto dos utentes. Tal poderá acontecer para investigação, gestão de saúde pública ou gestão da procura.
- Os dados e informação são utilizados juntamente com analítica, Big Data e sistemas cognitivos para permitirem novos regimes de tratamento, melhor otimização dos riscos e melhor otimização dos recursos.

Neste contexto as Entidades do setor da saúde têm vindo a proceder à transformação digital das suas atividades em redor de cinco dimensões fundamentais:

Liderança

Os responsáveis das EntidadesEntidades do setor da saúde nem sempre estão conscientes das oportunidades disponibilizados pelos sistemas de informação e tecnologias, pelo que se torna difícil a incorporação de uma visão da transformação digital na estratégia geral das Entidades. Também ao nível clínico, alguns médicos são mais ávidos à mudança do que outros, em particular no que diz respeito ao relacionamento com os utentes. Assim, em algumas Entidades começam a aparecer funções de Chief Clinical Information Officer (CCIO) ou Chief Medical Information Officer (CMIO). As Entidades ainda estão muito focadas na conformidade TIC e é difícil alterar os modelos de funcionamento com tantos regulamentos em vigor.

Omni-Experiência

Os utentes têm expectativas de ter o mesmo tipo de experiência, independentemente do modo como interagem com os prestadores de cuidados de saúde (online ou pessoalmente). Existe uma vasta gama de atividades (além das administrativas) que podem ser automatizadas ou transformadas para permitir um melhor envolvimento com os utentes.

Gestão de Talentos

Os profissionais de saúde necessitam de se concentrar naquilo que é importante: a qualidade dos serviços prestados e uma melhor experiência dos utentes. Presentemente, a conformidade regulamentar e a burocracia absorvem imenso tempo e as TIC não têm aliviado esse trabalho. Assim, a experiência dos utilizadores e a usabilidade dos sistemas de informação clínicos é muitas vezes colocada em causa. Muitos dos sistemas precisam de mobilidade mas tecnologias como a IoT não são utilizadas corretamente para resolver problemas transacionais e de segurança dos utentes. As Entidades de saúde necessitam de ser cada vez menos autorreferenciais, sendo necessário aumentar o foco nos fluxos de processos centrados nos utentes (ex., disponibilizando visibilidade através do sistema para possibilitar a calendarização de pessoas e recursos).

Modelo Operacional

A coordenação entre o interior e exterior das Entidades de saúde é um fator crítico. Existe cada vez mais a necessidade de se alterar o foco para os fluxos de processo centrados nos utentes e ajustar as operações para terem condições de dar respostas mais adequadas. Por exemplo a analítica de dados em tempo real é essencial para a otimização dos processos, sendo que esta ou outras boas práticas necessitam de ser partilhadas para que possam ser escaladas. Os projetos bem-sucedidos não devem ser mantidos ao nível departamental e devem ser explorados modelos de inovação que promovam uma verdadeira integração e colaboração entre as diferentes partes interessadas no ecossistema.

Informação

As Entidades de saúde estão sobrecarregadas de informação. Não se trata apenas de implementar sistemas de informação clínica, sistemas de analítica ou semelhantes, mas, igualmente, de desenhar e implementar estruturas e referencias que permitam extrair e desenvolver o valor e a utilidade da informação relativa aos utentes, serviços, ativos físicos e experiências. As Entidades de saúde devem, cada vez mais, tratar os dados e a informação como qualquer outro ativo. Existem ainda desafios relacionados com problemas técnicos relacionados com a integração e interoperabilidade (ex. sistemas legados), assim como receios de implementação de uma cultura de decisão baseada na evidência dos factos. As Entidades de saúde necessitam de adotar uma cultura de transparência e a gestão que garanta que todas as partes interessadas reconheçam os benefícios relacionados com a valorização do ativo informação.

Aspetos críticos de segurança e privacidade no processo de transformação digital

Num ambiente moderno e integrado de cuidados de saúde personalizados, a qualidade da informação ganha uma importância crítica, destacando-se requisitos fundamentais, tais como:

- Confidencialidade;
- Integridade;
- Disponibilidade;
- Conformidade legal e normativa, nomeadamente a Privacidade.

Confidencialidade significa que a informação está protegida contra o acesso ou exposição a entidades não autorizadas. Basicamente, significa que um utente deve ser capaz de confiar que a informação pessoal confidencial não é acedida por ninguém que não tenha os direitos e uma finalidade concreta para aceder a essa mesma informação. Devido à informação sensível nas aplicações clínicas e da quantidade de dados partilhados através do ecossistema de saúde, a confidencialidade assume-se como um dos pilares cruciais.

Integridade significa que a informação mantém todas as características definidas pelo seu responsável, incluindo o controlo das alterações ao longo do seu ciclo de vida. Os utentes devem ser capazes de confiar que os dados a que os profissionais de saúde têm acesso são precisos e completos e que o tratamento prescrito se baseie nesses mesmos dados.Na prestação de cuidados de saúde a integridade ganha um peso ainda mais relevante na medida em que uma falha na integridade dos dados pode ter como resultado danos diretos para a saúde do utente.

Disponibilidade significa que a informação está acessível ao pessoal autorizado sempre que for relevante. Trata-se de dar acesso à informação quando ela é necessária e, muitas vezes, num determinado contexto.

Quando os tratamentos são baseados em grandes quantidades de dados e as equipas clínicas são móveis, a acessibilidade aos dados é crucial. Não somente num cenário crítico relacionado com Electronic Medical Records (EMR) ou Electronic Health Records (EHR), mas também quando um especialista médico supervisiona outra enfermaria ou quando o pessoal clÍnico visita o utente na sua residência ou, ainda, quando realizam tratamentos aos utentes através de equipamentos de telemedicina.

Somente quando a confidencialidade, a integridade e a disponibilidade são geridas de um modo seguro e otimizado, o sistema de saúde poderá evoluir e dar suporte à procura futura.

O estudo da IDC "European Industry Solutions and Insights Survey" realizado no terceiro trimestre de 2016, que contou com a participação de107 hospitais e 69 prestadores de cuidados de saúde da Europa Ocidental, identificou a segurança e a proteção dos dados entre as principais prioridades operacionais de 2016, sem que isso afete diretamente a experiência dos utentes ou a eficiência geral da prestação e serviços de saúde. Os CIO reconhecem a segurança das TIC como estratégica e planeiam implementar iniciativas nos próximos anos, pelo que mecanismos inapropriados de proteção de dados e de privacidade não constituem barreiras para o crescimento e transformação.

Relativamente aos requisitos de conformidade diretamente relacionados com a Informação, existem atualmente 28 leis de proteção de dados diferentes baseados na EU Data Protection Directive de 1995, a qual foi desenhada há 20 anos atrás, antes da introdução generalizada da Internet e do crescimento das preocupações com a privacidade. Apesar dos avanços tecnológicos, a regulamentação existente permaneceu estagnada e cada vez mais inadequada para proteger os dados dos indivíduos ou das Organizações. Neste contexto, um novo regulamento europeu sobre proteção de dados vai entrar em vigor em maio de 2018 e vai transformar o modo como os requisitos de conformidade deverão ser respondidos pelas Organizações europeias.

Para além de atualizar a regulamentação de modo a haver um maior alinhamento com as as alterações tecnológicas, a Comissão Europeia pretendeu, igualmente, criar uma única lei, pan-europeia, para a proteção de dados, que substituísse as atuais legislações nacionais no espaço comunitário. Adicionalmente, pretende-se a criação de um mecanismo de balcão único, permitindo que as Organizações lidem com uma única autoridade de supervisão.

É neste contexto que este Guia pretende abordar as vertentes jurídica e legal envolvidas no tratamento de dados pessoais no âmbito da prestação de cuidados de saúde, elucidando o leitor sobre os diversos aspetos a ter em conta aquando do tratamento de dados pessoais.

Contexto jurídico atual da proteção de dados no setor da saúde em Portugal

A transformação digital no sector da saúde em Portugal terá, naturalmente, de acompanhar as exigências de proteção dos dados pessoais dos intervenientes neste setor, em particular dos utentes e dos profissionais de saúde.

São considerados dados pessoais, para efeitos da LPDP, quaisquer informações que, direta ou indiretamente, identifiquem uma pessoa singular (o "titular dos dados"), tais como o nome, a morada, o endereço de correio eletrónico, mas também dados relativos a historiais clínicos, historial e características de doenças e perfis de utilizadores/utentes.

As Entidades integrantes do SNS que levem a cabo um conjunto de operações de tratamento de dados pessoais, entendidas como todas as operações que incidam sobre dados pessoais (tais como a recolha, o registo, a organização, a consulta, a conservação ou a comunicação, entre muitas outras), ficam sujeitas ao cumprimento de um conjunto de obrigações enquanto Entidades responsáveis pelo tratamento dos dados.

Para além das obrigações gerais que decorrem da LPDP, as Entidades integrantes do SNS deverão ainda assegurar o cumprimento das demais regras previstas na legislação e/ou disposições regulamentares específicas do sector da saúde, as quais regulam a propriedade, o acesso e a legitimidade do tratamento da informação de saúde dos utentes.

a) As regras gerais do tratamento de dados pessoais

Assumindo-se como responsáveis pelo tratamento, incumbe às Entidades integrantes do SNS, em termos genéricos, assegurar que:

1. Os dados pessoais são recolhidos para finalidades determinadas, explícitas e legítimas e não sejam posteriormente tratados de forma incompatível com as finalidades da recolha;
2. Apenas são recolhidos os dados pessoais adequados, pertinentes, e não excessivos relativamente às finalidades da recolha – princípio de minimização;
3. Os dados pessoais recolhidos são exatos e atualizados;
4. Os dados pessoais apenas são conservados durante o período necessário

para a prossecução das finalidades da recolha/tratamento (garantido o cumprimento das Deliberações da CNPD aplicáveis);

5. São disponibilizadas ao titular dos dados todas as informações relacionadas com o tratamento efetuado, concedendo-lhe o direito de acesso e retificação dos seus dados;
6. É obtido o consentimento do titular para o tratamento dos seus dados, exceto nos casos em que tal consentimento é dispensado nos termos da lei, como é o caso do tratamento de dados para a finalidade de proteção de interesses vitais do seu titular;
7. São postas em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais, designadamente contra a sua destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizado (nomeadamente quando o tratamento implicar a sua transmissão por rede) e qualquer outra forma de tratamento ilícito;
8. O tratamento dos dados encontra-se devidamente notificado à CNPD e, quando legalmente exigido, é obtida a respetiva autorização prévia.

b) A obrigação de notificação e o controlo prévio da CNPD

A lei estabelece que, para deter e tratar dados pessoais, qualquer Entidade integrante do SNS terá que notificar previamente a CNPD.

Existem, porém, certos casos em que não basta a notificação da CNPD, sendo necessário obter uma autorização, antes de recolher, conservar e/ou tratar determinado tipo de informação relativa a pessoas singulares, como o caso dos "dados sensíveis". Nesta categoria incluem-se, entre outros, os dados de saúde, dados genéticos, dados de vida privada, origem racial ou étnica.

No caso de tratamento de dados de saúde, incluindo dados genéticos, e não obstante constituírem dados sensíveis, o seu tratamento está sujeito a mera notificação à CNPD, na medida em que tal tratamento será necessário para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou ainda de gestão de serviços de saúde. Além disso, o tratamento desses dados terá que ser efetuado por um profissional de saúde ou por outra pessoa sujeita a sigilo profissional.

Contudo, se houver tratamento de outros dados (v.g. raça, fé religiosa ou outros dados da vida privada – toxicodependência, comportamento de risco, hábitos alcoólicos, problemas sociais de integração, etc.), se os dados de saúde, da vida sexual ou genéticos forem utilizados para finalidades diversas (v.g. para fins de investigação científica) ou forem tratados em circunstâncias distintas das referidas, as Entidades integrantes do SNS devem submeter tal tratamento a controlo prévio, submetendo um pedido de autorização à CNPD.

c) O consentimento

O tratamento de dados pessoais pressupõe, em regra, o consentimento dos titulares dos dados, exceto nas situações previstas na LPDP. Desde logo, quando o tratamento de dados é necessário, para a execução de um contrato entre o responsável pelo tratamento e o titular dos dados (como sucede, por exemplo, no contrato de trabalho), para cumprimento de obrigação legal ou para a prossecução de interesses legítimos.

Quando estão em causa dados sensíveis (por exemplo, dados de saúde ou genéticos), a regra é a da proibição. Isto é, o tratamento de tais dados é genericamente proibido, exceto se o tratamento decorrer de disposição legal, o titular dos dados tiver dado o seu consentimento e a CNPD tiver autorizado ou o tratamento for indispensável ao exercício das atribuições legais ou estatutárias do responsável. Além disso, o tratamento de dados sensíveis é ainda permitido, por exemplo, para proteção de interesses vitais do titular ou de uma outra pessoa e o titular estiver física ou legalmente incapaz de dar o seu consentimento.

Nas situações em que não é necessário o consentimento para o tratamento de dados, tem que se prestar informação acerca dos termos em que os dados serão tratados.

d) Direito de informação e acesso a dados de saúde

Sempre que sejam recolhidos dados pessoais, mesmo que não seja necessário o consentimento, as Entidades integrantes do SNS devem prestar um conjunto de informações aos titulares dos dados (tais como a identificação da Instituição responsável, as finalidades do tratamento dos dados, as comunicações de dados, o caráter obrigatório ou facultativo da disponibilização dos dados e as condições de acesso, retificação e eliminação dos dados).

Estas informações devem ser incluídas em todos os formulários de recolha de dados. A informação poderá, no entanto, ser prestada de forma verbal sempre que os dados sejam recolhidos por inquérito verbal junto dos titulares, sendo desejável que, nos locais onde tais dados são sistematicamente recolhidos, haja avisos afixados com tais informações.

Os titulares dos dados (colaboradores, utentes, entre outros) têm, em regra, o direito a aceder aos dados pessoais que as Entidades dispõem sobre eles; porém quando a informação contem dados de saúde, o acesso é sempre efetuado através de um profissional de saúde.

e) A utilização de dados de saúde para investigação científica

Os dados de saúde recolhidos no âmbito da prestação de cuidados de saúde poderão ser utilizados para fins de investigação científica, contanto que os titulares dos dados tenham sido informados acerca dessa possibilidade e prestado o seu consentimento para o efeito.

Sempre que possível, os estudos de investigação científica deverão ser realizados sem dados nominativos dos utentes.

f) A comunicação de dados e a subcontratação

No âmbito da sua atividade, as Entidades integrantes do SNS transmitem dados dos utentes e dos profissionais de saúde, pelos quais são responsáveis, a várias Entidades:

(i) por um lado, a Entidades a quem estão obrigados a comunicar tais dados para efeitos de cumprimento de obrigações legais (os "terceiros");

(ii) por outro, a Entidades que contratam para a prestação de serviços e que, nesse contexto, tratam os dados pessoais a que têm em acesso em nome e por conta das Entidades integrantes do SNS (os "subcontratantes").

A comunicação de dados é a operação que se traduz na transmissão de dados pessoais a um terceiro, como é o caso da Direção-Geral da Saúde ("DGS") e da Administração Central do Sistema de Saúde, I.P. ("ACSS"), da SPMS e ainda dos tribunais.

Por outro lado, a subcontratação de prestadores de serviços (outsourcing) que acedem e tratam dados pessoais da responsabilidade das Entidades integrantes do SNS é cada vez mais frequente.

Sempre que a Instituição pública pretenda recorrer aos serviços de subcontratantes (como, por exemplo, empresas fornecedoras de software ou manutenção e suporte de sistemas de informação), deverá assegurar-se, em primeiro lugar, que o subcontratante oferece as garantias suficientes em relação ao tratamento a realizar, devendo este último comprometer-se a zelar pelo cumprimento dessas mesmas medidas. Para esse efeito deverá ser celebrado, nos termos da lei, um contrato escrito entre o responsável pelo tratamento e o subcontratante.

g) Implementação de especiais medidas de segurança

Sempre que esteja em causa o tratamento de dados sensíveis, as Entidades do SNS deverão adotar medidas especiais de segurança, atenta à sensibilidade dos dados em causa. Estas medidas visam reforçar o controlo de entradas nas instalações, o acesso aos dados e suportes de dados, o controlo da utilização dos sistemas de tratamento automatizados por pessoas não autorizadas ou o controlo da transmissão dos dados.

No que diz respeito aos dados de saúde, deve ser assegurada a implementação de medidas destinadas a impedir o acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde, incluindo as respetivas cópias de segurança, assim como a separação lógica entre dados de saúde e dados administrativos.

As medidas de segurança deverão assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado aos riscos que o tratamento apresenta e à natureza dos dados a proteger.

Como tal, será necessária a identificação das potenciais vulnerabilidades do sistema, bem como uma previsão do impacto que essas falhas de segurança possam causar, de modo a proceder a uma análise e avaliação de riscos correta e realista que conduzam a uma definição eficaz das medidas de segurança que melhor poderão dar resposta às necessidades da Instituição.

h) Consequências do incumprimento

O desrespeito por algumas das regras constantes da LPDP constitui uma contraordenação, punível com coima que poderá atingir os € 29.927,88 (sendo as sanções aplicadas às contraordenações cumuladas materialmente).

A LPDP prevê ainda a possibilidade de aplicação, pela CNPD, de sanções acessórias, como o bloqueamento ou destruição de dados, a proibição, temporária ou definitiva, do tratamento de dados pessoais (o que na prática é suscetível de impedir o desenvolvimento da atividade), ou ainda a publicidade da sentença condenatória. O responsável pelo tratamento poderá ainda incorrer em responsabilidade civil ou criminal. Por exemplo, a utilização intencional de dados pessoais, de forma incompatível com a finalidade determinante da recolha, constitui crime punível com pena de prisão até um ano ou multa até 120 dias. No caso de dados sensíveis, a pena é agravada para o dobro.

Para além dos custos jurídicos e financeiros, o incumprimento da lei tem ainda outros custos associados que podem ter um impacto negativo muito significativo para as Entidades integrantes do SNS: os custos de imagem e de reputação.

RGPD: Mudança de paradigma e principais obrigações

O RGPD irá alterar profundamente a forma como os organismos públicos, incluindo as Entidades integrantes do SNS, tratam dados pessoais. Trata-se de um instrumento legislativo que implica, por um lado, um reforço claro dos direitos dos titulares dos dados e, por outro lado, uma ampliação das obrigações das Organizações em matéria de privacidade.

As definições e os princípios constantes da Diretiva de Proteção de Dados Pessoais, são adotadas, no entanto, introduzindo-se novas definições – como a de "violação de dados pessoais" ou a de "limitação do tratamento" – e o princípio da transparência, designadamente ao prever-se uma regra de "data minimisation" (minimização dos dados recolhidos face ao necessário para as finalidades do tratamento) e de responsabilização efetiva do responsável pelo tratamento (princípio da responsabilidade).

Esta maior responsabilização traduz-se no aumento das obrigações do responsável pelo tratamento, o qual, mais do que solicitar uma validação externa para os termos e as condições em que realiza as operações de tratamento de dados pessoais, passa a ter de demonstrar que cumpre as regras aplicáveis a tais operações de tratamento. Observa-se, assim, uma mudança de paradigma no que à forma de encarar as responsabilidades pelo tratamento de dados (uma espécie de inversão de papéis entre o "regulador" e o "regulado").

O novo RGPD vem criar um modelo que obriga as Entidades a tomarem em consideração as preocupações e os riscos de privacidade desde o momento inicial da conceção de um dado projeto, em vez de apenas considerar esses riscos posteriormente – privacy by default e privacy by design. Espera-se que este novo paradigma contribua para que os projetos levados a cabo pelas Entidades que tratam dados pessoais tenham o mínimo de impacto possível na privacidade dos titulares dos dados.

São, assim, várias as alterações decorrentes do RGPD, pretendendo destacar-se neste Guia as principais obrigações aplicáveis às Entidades integrantes do SNS que implicarão, em matéria de proteção de dados pessoais, uma mudança nas organizações. As referidas alterações poderão traduzir-se tanto em novas obrigações face ao regime legal atualmente em vigor como em alterações (reforço) das obrigações já existentes.

De uma forma geral, estas medidas deverão ser desenhadas e implementadas tendo em consideração os requisitos locais das Entidades do SNS mas também os modelos de governança e gestão do sistema de informação da saúde (eSIS) em vigor.

Podem-se agrupar as alterações do RGPD em cinco vetores de mudança principais:

1. Governança dos Dados

O RGPD estabelece que todas as Organizações devem implementar um conjunto alargado de medidas com vista a reduzir o risco de incumprimento das regras de privacidade e proteção de dados pessoais, demonstrando, assim, o seu compromisso relativamente a estas matérias e comprovando, sempre que solicitado, o cumprimento das regras aplicáveis.

Na prática, tal deve traduzir-se, designadamente, nas seguintes medidas:

(a) Implementação dos conceitos de "privacy by design" e "privacy by default"

As Entidades integrantes do SNS devem respeitar, em todas as operações e projetos, os princípios de:

(i) Privacy by design (privacidade desde a conceção) – o que significa que a preocupação do risco de privacidade deve estar presente em todo o processo de conceção ou contratação de um novo produto, serviço ou projeto (por exemplo na implementação de procedimentos adequados desde o início) para garantir que o tratamento está em conformidade com o RGPD e protege os direitos dos titulares dos dados em causa;

(ii) Privacy by default (privacidade por defeito) – o que implica que as Entidades devem assegurar que são colocados em prática, dentro da sua Organização, mecanismos para garantir que, por defeito, apenas a quantidade necessária de dados pessoais é recolhida, utilizada e conservada para cada tarefa, tanto em termos da quantidade de dados recolhidos, como do tempo pelo qual eles são mantidos (minimização, pseudonimização e transparência).

(b) Realização de "privacy impact assessment" e consulta prévia à CNPD

Antes do início de qualquer operação de tratamento de dados, e sempre que a mesma seja considerada de risco, as Entidades integrantes do SNS devem realizar uma avaliação de impacto de tais operações sobre a proteção de dados pessoais ("privacy impact assessment" – "PIA").

Através do PIA, as Entidades integrantes do SNS avaliam e identificam os riscos de determinada operação para a proteção de dados, por forma a, por um lado, antecipar eventuais constrangimentos e, por outro lado, permitir a adoção de medidas que enderecem, minimizem ou eliminem os riscos identificados.

O RGPD prevê que a CNPD elabore e torne pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de realização de PIAs.

Em relação aos tratamentos de dados considerados de risco e que a avaliação efetuada determine que existem riscos específicos em matéria de dados pessoais, as Entidades integrantes do SNS deverão consultar a CNPD, de forma a garantir o cumprimento das disposições do RGPD. Tanto a avaliação de impacto como a consulta prévia da CNPD devem cumprir determinados requisitos e incluir certas informações e ações mínimas previstas no RGPD.

Ainda que se tenha que aguardar pela emissão de orientações específicas nesta matéria, será expectável que, entre outras, sejam consideradas de risco, por exemplo, as operações que envolvam o tratamento de dados de saúde ou dados genéticos e que utilizem novas tecnologias.

(c) Designação de Data Privacy Officer

As Entidades integrantes do SNS, enquanto organismo público, passam a estar obrigadas a designar um encarregado da proteção de dados ("Data Privacy Officer"), que passará a ser o contacto preferencial junto da CNPD, dos titulares dos dados e a centralizar todas as questões de proteção de dados pessoais.

De entre as suas várias responsabilidades[14], destaca-se a monitorização do cumprimento das regras de proteção de dados pessoais, a gestão e registo de toda a documentação relevante, assim como o acompanhamento regular dos projetos que tenham um impacto na privacidade.

O "Data Privacy Officer" poderá ser um recurso interno da Instituição pública ou externo, exercendo as suas funções com base num contrato/acordo de prestação de serviços – em qualquer uma das opções é necessário ter formação e experiência adequadas.

(d) Realização de auditorias de conformidade e adoção de políticas

O RGPD prevê, como analisado, que as Entidades integrantes do SNS adotem as medidas organizativas adequadas para assegurar e poder comprovar que o tratamento de dados é realizado em conformidade com as regras de proteção de dados pessoais. Tais medidas podem incluir a realização de auditorias, a elaboração e implementação de políticas e procedimentos internos, a serem veiculados por toda a Organização.

(e) Registo das atividades de tratamento

As Entidades integrantes do SNS são obrigadas a conservar um registo de todas as atividades de tratamento sob a sua responsabilidade, que inclua, designadamente, a seguinte informação: tipo de dados tratados, finalidades, descrição das categorias de titulares dos dados e destinatários dos mesmos, medidas de segurança e prazo de conservação. Da mesma forma, os subcontratantes (neste caso, os prestadores de serviços) deverão conservar um registo de todas as atividades de tratamento realizadas em nome das Entidadesintegrantes do SNS.

Ou seja, o registo interno deverá replicar a informação que, pelo menos atualmente, deve constar dos pedidos de notificação e autorização submetidos à CNPD.

(f) Maior responsabilização na escolha de entidades externas

O RGPD cria uma maior responsabilização das Entidades integrantes do SNS na escolha e atividade dos subcontratantes, sendo impostas obrigações claras e precisas nesta matéria.

[14] O RGPD estabelece em maior detalhe as funções mínimas do "Data Privacy Officer".

Esta maior responsabilização é conjugada com a sujeição dos subcontratantes aos termos do RGPD. Isto é, pela primeira vez os subcontratantes são regulados diretamente, passando a estar sujeitos a uma série de obrigações – e também sanções – até agora apenas impostas aos responsáveis pelo tratamento.

O RGPD clarifica a posição do subcontratante, adicionando alguns elementos novos, como sendo o facto de, se o subcontratante tratar dados para além das instruções do responsável pelo tratamento, passar a ser considerado como um corresponsável.

Relativamente à relação entre responsável e subcontratante, mantém-se a obrigação de celebração de um contrato ou documento escrito que regule a relação contratual e os termos do tratamento.

O subcontratante passa a assumir mais responsabilidades diretas, recaindo sobre ele um conjunto de obrigações.

(g) Códigos de conduta e certificação

Prevê-se a possibilidade de elaboração, nomeadamente por autoridades de controlo, de códigos de conduta destinados a contribuir para a correta aplicação do RGPD.

Reconhece-se ainda a possibilidade de estabelecer procedimentos de certificação de conformidade de proteção de dados, bem como selos ou marcas de garantia de proteção de dados. A certificação é voluntária e pode ser emitida por um período máximo de 3 anos – renovável nas mesmas condições –, por um organismo de certificação ou pela autoridade de controlo competente.

As Entidades integrantes do SNS poderão ponderar a adoção de um código de conduta aprovado nos termos do RGPD, designadamente como forma de demonstrar o cumprimento do mesmo. Poderão, igualmente, ponderar obter uma certificação em matéria de proteção de dados, bem como um selo ou marca[15], de forma a comprovar – e publicitar junto dos utentes – a conformidade das operações de tratamento de dados que efetua com o RGPD.

A certificação prevista no RGPD não diminui a responsabilidade dos responsáveis pelo tratamento e subcontratantes pelo cumprimento do mesmo, nem prejudica as funções e competências das autoridades de controlo competentes.

[15] Existem já diversas Entidades certificadas no mercado que, após um processo de avaliação rigoroso das atividades de uma organização ou de um determinado projeto, atribuem um selo ou marca de conformidade com a legislação europeia em privacidade e proteção de dados pessoais.

2. Consentimento

O RGPD vem clarificar as condições que devem ser verificadas para que o consentimento do titular dos dados seja considerado válido e, como tal, um fundamento legal para o tratamento de dados.

Em particular, estabelece-se que cabe ao responsável pelo tratamento demonstrar que o titular dos dados deu o seu consentimento (livre, específico, informado e agora, também, explícito) e que, caso o consentimento seja dado por escrito num documento que diga também respeito a outros assuntos, este deverá estar devidamente destacado (de modo inteligível, numa linguagem clara e de fácil acesso) dos outros aspetos regulados no documento.

Não sendo admitidos consentimentos implícitos (por exemplo, por aceder e navegar simplesmente num site/portal ou não responder a um pedido), as Entidades integrantes do SNS devem rever os mecanismos de pedido de consentimento online, para o caso da utilização de cookies[16].

Prevê-se agora expressamente que o titular dos dados tenha o direito de retirar o seu consentimento a qualquer momento (o que não afeta a licitude do tratamento feito até ao momento), devendo ser tão fácil de retirar quanto de dar – direito ao esquecimento.

Em relação ao tratamento de "dados sensíveis", não foram introduzidas alterações específicas quanto à obtenção do consentimento. O RGPD menciona também o tratamento de categorias especiais de dados pessoais (como os dados relativos à saúde), designadamente, se o tratamento for necessário para efeitos de medicina preventiva, para o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social.

Estes dados podem ser tratados para os fins acima referidos, contanto que sejam tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade.

Sem prejuízo do referido, prevê-se que os Estados-Membros possam manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde.

[16] Espera-se também que a Diretiva e-Privacy e, por conseguinte, a Lei n.º 41/2004, de 18 de agosto (alterada pela Lei n.º 46/2012, de 29 de agosto), venha a sofrer alterações de forma a ser compatibilizada com o RGPD.

3. Direitos dos Titulares dos Dados

(a) Reforço do direito de informação e de acesso dos titulares dos dados

São, desde logo, reforçados os direitos dos titulares dos dados. Em especial, são estabelecidos requisitos mais exigentes aplicáveis à informação a prestar ao titular dos dados, entre os quais a obrigação dos responsáveis pelo tratamento dos dados disponibilizarem mais informações, de forma mais transparente e acessível.

Deverão, ainda, ser adotados mecanismos que permitam agilizar o exercício dos direitos dos titulares dos dados (incluindo meios para pedidos eletrónicos e de resposta aos titulares num determinado prazo).

Uma das novidades do RGPD é a consagração do direito de informação dos titulares dos dados em relação aos destinatários dos dados (i.e., o titular dos dados tem o direito de ser informado sobre quem irá tratar de facto os seus dados e/ou a quem serão transmitidos).

Para além do conteúdo atual das informações a prestar, as Entidades integrantes do SNS deverão passar a prestar informação adicional (como o fundamento jurídico para o tratamento, o prazo de conservação dos dados e o direito de apresentação de reclamações às autoridades competentes tais como a CNPD). São ainda previstas obrigações específicas de informação sempre que as Entidades integrantes do SNS tenham recebido os dados pessoais de terceiros e não tenham sido recolhidos diretamente junto do respetivo titular.

Na mesma linha, e em relação ao direito de acesso aos dados, as Entidades integrantes do SNS deverão dar resposta a um pedido de acesso do titular dos dados ou fornecer-lhe as informações sobre as medidas tomadas relativamente aos seus dados pessoais sem demora injustificada e no prazo de um mês a contar da data de receção do pedido.

(b) Garantia dos direitos de apagamento dos dados, limitação do tratamento e portabilidade

O RGPD introduz também novos direitos:

(i) O "direito a ser esquecido" (the right to be forgotten) – que implicará que, perante um pedido de eliminação de dados e desde que se verifiquem as condições previstas no RGPD, as Entidades integrantes do SNS devam adotar mecanismos que assegurem que todos os dados foram efetivamente eliminados (incluindo cópias ou reproduções dos mesmos)[17];

(ii) O direito à limitação do tratamento – que prevê que o titular dos dados possa opor-se ao apagamento dos seus dados pessoais e solicitar, em contrapartida, a limitação do tratamento dos seus dados[18]. Nesta ótica, as Entidades integrantes do SNS deverão comunicar a cada destinatário a quem os dados pessoais tenham sido transmitidos e qualquer limitação do tratamento que tenham efetuado;

(iii) O direito à portabilidade dos dados – passando o titular dos dados a ter direito:
• A receber os dados pessoais que lhe digam respeito e que tenha fornecido às Entidades integrantes do SNS, num formato estruturado, de uso corrente e de leitura automática;
• Se o tratamento for realizado por meios automatizados, a transmitir esses dados a outro responsável pelo tratamento. A transmissão deve ocorrer diretamente de um sistema de processamento eletrónico de um responsável para outro, sempre que tal seja tecnicamente possível.

4. Segurança

(a) Reforço das medidas de segurança dos dados

O RGPD dá um enfoque especial ao tema da segurança no tratamento dos dados, prevendo uma responsabilidade conjunta do responsável pelo tratamento e do subcontratante na adoção das medidas de segurança necessárias para proteger os dados pessoais contra acessos indevidos.

Prevêem-se que sejam adotadas medidas técnicas e organizativas que permitam assegurar um nível de segurança adequado ao risco existente consoante o que for adequado em cada caso:

(i) A pseudonimização[19] e a encriptação dos dados pessoais;

(ii) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;

[17] Este direito é afastado na medida em que o tratamento se revele necessário por motivos de interesse público no domínio da saúde pública, nos termos previstos no RGPD.

[18] Esta operação é definida pelo RGPD como a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro.

[19] Tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

(iii) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;

(iv) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

(b) Notificação de violações de dados pessoais e de incidentes de segurança

Consagra-se a obrigação de notificação de violações de dados pessoais (data breaches) à CNPD, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares (o que terá de ser analisado caso a caso).

As Entidades integrantes do SNS devem proceder à notificação da violação de dados pessoais, sem demora injustificada e, sempre que possível, até 72 horas após terem tido conhecimento da mesma. Todas as violações ocorridas e informação relativa às mesmas devem ser documentadas pelas Entidades integrantes do SNS, de forma a permitir verificar perante a CNPD o cumprimento das regras previstas no RGPD.

Adicionalmente, caso a violação de dados pessoais possa afetar negativamente a privacidade do titular dos dados (i.e., for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares), as Entidades integrantes do SNS deverão também notificar os titulares dos dados.

É ainda de referir a "Diretiva SRI", que impõe um nível de segurança mínimo para as tecnologias, redes e serviços digitais, prevendo ainda a obrigatoriedade, nomeadamente para Entidades como as do sector da saúde, de comunicar a ocorrência de incidentes com impacto significativo na segurança das redes e dos sistemas de informação.

5. Reforço dos poderes das autoridades e aumento do valor das coimas

Em geral, o RGPD trará um reforço dos recursos e dos poderes de fiscalização das autoridades nacionais de proteção de dados – em Portugal, da CNPD.

A par do reforço dos poderes das autoridades reguladoras, o RGPD estabelece sanções consideravelmente mais gravosas do que o atual quadro legal, podendo ascender os 20 milhões de Euros (por exemplo, por incumprimento das regras de consentimento).

Os Estados-Membros podem ainda prever normas que permitam determinar se e em que medida as coimas podem ser aplicadas às autoridades e organismos públicos estabelecidos no seu território.

Para além da aplicação de coimas, os Estados-Membros poderão igualmente estabelecer outras sanções aplicáveis em caso de violação do RGPD[20].

Assim, considerando as regras de tratamento de dados pessoais atualmente em vigor e analisadas no Capítulo IV., bem como as novas regras introduzidas pelo RGPD, as Entidades integrantes do SNS deverão, já a partir de maio de 2018, cumprir com uma panóplia de obrigações aplicáveis aos tratamentos de dados que levam a cabo o âmbito da sua atividade.

[20] Atualmente encontram-se previstas na LPDP a possibilidade de aplicação das seguintes sanções acessórias, as quais é possível que "transitem" para o novo quadro legal: (i) a proibição temporária ou definitiva do tratamento, o bloqueio, o apagamento ou a destruição total ou parcial dos dados, (ii) a publicidade da sentença condenatória, ou (iii) a advertência ou censura públicas do responsável pelo tratamento.

Resumo das Obrigações a cumprir pelas Entidades:

Tratar os dados recolhidos para finalidades determinadas, explícitas e legítimas
Implementar os princípios de “privacy by design” e o “privacy by default”
Prestar informação aos titulares dos dados
Obter o consentimento dos titulares para finalidades de tratamento específicas
Garantir os direitos de acesso, retificação, apagamento e oposição
Assegurar os direitos de apagamento, limitação do tratamento e portabilidade dos dados
Implementar as adequadas medidas de segurança
Conservar os dados apenas pelo período necessário
Efetuar registos das atividades de tratamento de dados
Realizar “privacy impact assessments”
Designar o Data Privacy Officer
Notificar violações de dados e de incidentes de segurança
Celebrar contratos escritos com os prestadores de serviços
Pedir, nos casos aplicáveis, consulta prévia à CNPD para os tratamentos de dados
Realizar auditorias de conformidade e adotar políticas
Adoção de cuidados na escolha de prestadores de serviços

Como resulta dos Capítulos anteriores, o RGPD e a Diretiva SRI, assim como os desafios decorrentes da transformação digital, terão um impacto na forma como as Entidades integrantes do SNS tratam os dados pessoais. Este impacto revela-se nos tratamentos atuais e futuros, a diferentes níveis:

Algumas boas práticas. Como estar preparado?

Governance das matérias de dados pessoais	Maior responsabilização das Entidades na verificação do cumprimento do RGPD e da existência de documentação que evidencie tal cumprimento
Sistemas de Informação	Reforço das medidas de segurança e da interoperabilidade dos sistemas
Relacionamento com terceiros e prestadores de serviços	Maior responsabilização na escolha de terceiros e necessidade de celebração de contratos com conteúdos específicos (v.g. limitação do tratamento à execução do contrato e respeito pelas instruções do responsável, indicação das medidas de segurança, entre outros aspetos) como…?
Gestão de recursos humanos	Formação e sensibilização de todos aqueles que intervêm no ciclo de vida do tratamento de dados
Gestão da relação com utentes	Reforço do direito dos titulares dos dados e a capacidade da organização em garantir o seu cumprimento
Relação com a CNPD	Documentação de evidências do cumprimento do RGPD e interação em caso de ocorrência de violações de dados pessoais

Com isto, e com vista a responder aos desafios decorrentes, existe um conjunto de boas práticas que deverão ser implementadas pelas Entidades públicas integrantes do SNS até 25 de maio de 2018.

De seguida, serão detalhadas algumas boas práticas e ações especificamente dirigidas aos diferentes perfis de intervenientes (gestores hospitalares, profissionais de saúde e profissionais de tecnologias de informação) e de Entidades (SPMS, hospitais, centros hospitalares, centros de saúde e PPPs).

GESTORES HOSPITALARES

Tendo em consideração o prazo de implementação do RGPD, os gestores hospitalares devem, até 25 de maio de 2018, garantir que o tratamento de dados pessoais é efetuado em consonância com as novas regras.

Assim, existem algumas boas práticas que poderão ser adotadas:

Equipa Afeta à implementação do RGPD

Os primeiros passos deverão ser o alinhamento da estratégia da Entidade com a estratégia global do sistema de informação da saúde bem como com o ENESIS 2020. Deverá ainda assegurar-se a constituição de uma equipa de projeto temporária responsável pelo acompanhamento e garantia da implementação dos requisitos da RGPD. A equipa deverá ser multidisciplinar, de forma a cobrir todas as variantes – desde logo, com elementos do departamento jurídico, do departamento de recursos humanos, da direção de compras, da área médica, e do IT. Será essencial que o DPO integre, naturalmente, esta equipa e coordene os trabalhos de implementação do RGPD na Entidade.
Esta equipa deverá efetuar um levantamento do tratamento de dados existentes, identificando aspetos como, até à data, os dados estão a ser tratados, para que, posteriormente, se possam identificar as áreas que carecem de alteração de forma a assegurar o cumprimento do RGPD.

No final do projeto de implementação do RGPD as responsabilidades pela monitorização das práticas e controlos relacionadas deverão ser integrados nas estruturas transversais do eSIS e estruturas organizacionais da Instituição.

Governança

Tendo em consideração as obrigações que impendem sobre as Entidades integrantes do SNS, é essencial que, dentro de cada Entidade e em alinhamento com os modelos de governança e gestão do sistema de informação da saúde e do eSIS, se defina a estrutura de governança da proteção de dados pessoais e se identifique um DPO. O DPO será responsável pelo acompanhamento dos temas de proteção de dados dentro de cada Entidade.

Uma maior responsabilização implica necessariamente um maior acompanhamento destas matérias.

Consciencialização e Sensibilização

É fundamental que todos as partes interessadas do SNS estejam conscientes e sensíveis para a necessidade de cumprir o RGPD, pelo que deverá existir um compromisso de todas as Entidades para o tema, devendo ser passada essa mensagem para todo o sistema de informação da saúde.

Assim, a formação interna e sensibilização de todos os trabalhadores e colaboradores para os temas de proteção de dados pessoais é essencial para garantir um conhecimento das regras e princípios que deverão ser seguidos na recolha e tratamento de dados pessoais e, consequentemente, assegurar o cumprimento dos requisitos decorrentes do RGPD.

Processos e Procedimentos

A mudança de paradigma introduzida pelo RGPD implica uma maior responsabilização das Entidades integrantes do SNS, pelo que será fundamental adaptar e/ou criar processos e procedimentos internos que evidenciem o cumprimento das novas disposições legais. A partilha de boas práticas entre as Entidades do sistema de informação da saúde será uma mais valia para a garantia de um ambiente de controlo adequado em todo o SNS.

Desde logo, os processos e procedimentos internos devem especificar a necessidade de realização de avaliações de risco (PIA) pelo DPO, assim como a inclusão dos temas de proteção de dados em toda a cadeia de atividade da Entidade. O cumprimento destes requisitos deverá ser assegurado pelo DPO.

Os processos deverão ainda incluir regras sobre a criação de ficheiros e bases próprias pelos colaboradores e prestadores de serviços, estipulando, nomeadamente, que não deverão ser criados ficheiros que repliquem a informaçlão constante das bases de dados e aplicações em utilização na Entidade integrante do SNS.

Relações com Terceiros

Deverá ser assegurado que qualquer contratação de terceiros que, no âmbito da prestação de serviços, tenham acesso a dados pessoais da responsabilidade da Entidade, deverá ser precedida de uma análise das garantias de cumprimento da legislação de proteção de dados pessoais e da implementação de medidas de segurança por parte de tais terceiros.

Os contratos a celebrar com estas entidades deverão, assim, incluir cláusulas específicas de proteção de dados que, desde logo, limitem o tratamento dos dados à execução do contrato e às instruções da Entidade.

Estratégia de Comunicação

Tendo em consideração a maior visibilidade que um incidente de segurança e uma violação de dados pessoais terá, é essencial definir, de antemão, uma estratégia de comunicação com as autoridades e os utentes. A comunicação deverá ser adaptada aos interlocutores e, naturalmente, às situações em causa – i.e. dependerá do tipo de incidente/violação, do número de registos afetados e da natureza dos dados em causa.

Toda a comunicação externa, nomeadamente de incidentes de segurança e privacidade, deverá ser realizada de acordo com os procedimentos em vigor no sistema de informação da saúde.

Políticas e Condutas de Códigos Internos

A definição de regras internas, veiculadas em políticas e códigos de conduta, revela-se um instrumento adequado para, por um lado, assegurar a consciencialização de todos os colaboradores para os temas da privacidade e proteção de dados, e, por outro lado, responsabilizar em caso de incumprimento.

PROFISSIONAIS DE SAÚDE

Os profissionais de saúde são um importante elemento no ciclo de vida do tratamento de dados dos utentes, na medida em que, em regra, serão estes que recolhem e tratam dados de saúde.

Os profissionais de saúde deverão, assim, adotar um conjunto de procedimentos e cautelas na forma como manuseiam os dados, de forma a garantir a confidencialidade dos dados e, consequentemente, evitar falhas de segurança e acessos não autorizados aos mesmos.

Destacam-se as seguintes:

Recolha de Consentimento e Prestação de Informação

Os profissionais de saúde deverão observar, no momento da recolha de dados pessoais, o princípio da minimização – i.e. deverá assegurar-se que apenas são recolhidos os dados pessoais que são estritamente necessários para o ato em questão.

Acresce que, na medida em que são estes profissionais que contactarão diretamente com os utentes, deverá ser sempre garantida a prestação de informação acerca dos termos em que os dados pessoais irão ser utilizados.

A informação a prestar deve incluir os seguintes elementos:

- ✓ Entidade e contactos do responsável pelo tratamento (e seu representante);
- ✓ Contactos do encarregado da proteção de dados (DPO);
- ✓ Finalidades e fundamento do tratamento;
- ✓ Se o tratamento for necessário para prosseguir interesses legítimos, estes devem estar referidos;
- ✓ Eventuais destinatários dos dados;
- ✓ Transferência internacionais de dados e informações a esse respeito (se aplicável);
- ✓ Prazo de conservação dos dados;
- ✓ Possibilidade de o titular retirar o consentimento;
- ✓ Direito a apresentar reclamação perante a Autoridade de Proteção de Dados (CNPD);

- ✓ Se o titular está ou não obrigado a fornecer os dados, e consequências do não fornecimento;
- ✓ Existência de decisões automatizadas (i.e. indicação se o titular dos dados fica sujeito a qualquer decisão tomada exclusivamente com base no tratamento automatizado dos seus dados).

Deverá ainda ser obtido o consentimento para o tratamento dos dados, exceto nas situações previstas no RGPD (nomeadamente, para proteção de interesses vitais do titular). No caso de menores, o consentimento deverá ser prestado pelos titulares das responsabilidades parentais do menor.

Idealmente, deve ser obtido um consentimento escrito e armazenada evidência de tal documento. Caso não seja possível, o profissional deverá registar no registo clínico do utente que recolheu o seu consentimento e prestou informação, incluindo a data em que o fez.

Acesso aos Sistemas de Informação/Plataformas

Os profissionais de saúde devem garantir o acesso reservado aos sistemas de informação e plataformas nos quais são registados dados de saúde dos utentes.

Os profissionais de saúde devem ainda abster-se de duplicar as bases de dados da responsabilidade da Entidade integrante do SNS, criando, por exemplo, ficheiros próprios com a informação da base de dados/aplicação a que acede.

Registo e Acesso à Informação Clínica

O registo da informação clínica dos utentes deve ser efetuado, diretamente, pelo profissional da área de saúde. Apenas devem ser recolhidos e, consequentemente, registados os dados estritamente necessários para assegurar a prestação de cuidados médicos.

O registo deve ser efetuado nas aplicações e sistemas aprovados no contexto do eSIS, não devendo, assim, ser registados quaisquer dados em dispositivos ou equipamentos da propriedade do profissional e/ou não aprovados.

O profissional de saúde deverá apenas aceder à informação clínica do utente, constante do Resumo Clinico Único ou outro, na medida em que tal seja necessário para a prossecução das suas funções.

Partilha da Informação Clínica

A informação clínica não deve ser partilhada com terceiros, exceto para assegurar a continuidade da prestação de cuidados de saúde. Nessa situação, o profissional deve garantir que a partilha é efetuada, de forma segura e confidencial, a outro profissional sujeito à obrigação de confidencialidade e sigilo e que se tem todos os cuidados com esta partilha de informação.

Transporte da Informação Clínica

Os profissionais de saúde devem abster-se de, de alguma forma, transportar informação clínica constante do Resumo Clínico Único ou outro, para fora do serviço e do hospital ou centro de saúde, exceto nos casos autorizados pelos responsáveis da Instituição e para efeitos de garantia da continuidade da prestação de cuidados médios.

Sempre que tal suceda, deverão ser adotadas medidas de segurança especiais, de forma a assegurar que a informação não é acedida por terceiros de forma indevida (em particular, a informação deverá ser anonimizada e/ou encriptada).

Utilização de Dispositivos Pessoais

O profissional da área da saúde não deve utilizar ou, de alguma forma, ligar dispositivos pessoais aos sistemas e plataformas da Instituição do SNS, exceto nos casos em que exista aprovação prévia dos responsáveis da Instituição.

Caso tal suceda, e atenta à natureza da informação, o profissional deve ter em consideração que o acesso à rede através de dispositivos móveis pessoais acarreta riscos de segurança e confidencialidade, pelo que deve adotar as medidas de segurança necessárias para proteger os dados a que aceda, através do seu dispositivo, contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizado, bem como contra qualquer outra forma de tratamento ilícito dos mesmos.

Deve ainda, em qualquer situação, manter a informação confidencial em regime de sigilo e estrita confidencialidade, não permitindo o acesso a terceiros.

Utilização dos Dados para Finalidades Próprias

O profissional da área da saúde não pode tratar os dados recolhidos no âmbito da prestação de cuidados de saúde para finalidades próprias. Caso pretenda utilizar os dados para fins académicos ou de investigação, deverá obter a aprovação dos responsáveis da Instituição do SNS, devendo recolher o consentimento do utente para o efeito, prestando-lhe a informação necessária acerca dos termos em que os dados irão ser utilizados.

Nesta situação, o profissional será considerado responsável pelo tratamento dos dados.

Comunicação de Violações de Dados Pessoais

Caso ocorra qualquer falha ou incidente que envolva dados pessoais, os profissionais de saúde deverão comunicar de imediato ao responsável de Proteção de Dados (DPO), de acordo com os procedimentos estabelecidos para o efeito.

Na medida em que tenham informação acerca do incidente, deverão disponibilizá-la aquando da comunicação. Em particular, deverão comunicar a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa.

PROFISSIONAIS TIC

O RGPD poderá ter um impacto acentuado ao nível dos sistemas de informação das Organizações.

De facto, e uma vez que as atividades de tratamento de dados pessoais conduzidas pelas Entidades integrantes do SNS assentam fundamentalmente na utilização de meios automatizados para o processamento de dados, é essencial que estes estejam preparados para assegurar o cumprimento das novas regras de privacidade e proteção de dados.
Por este motivo, recomenda-se que se avalie se os sistemas de informação utilizados (i) cumprem todos os requisitos decorrentes das obrigações que recairão sobre as Entidades integrantes do SNS e, caso tal não suceda, (ii) identificar as medidas necessárias para garantir tal cumprimento.

Note-se que, atendendo ao impacto transversal dos sistemas de informação, a avaliação deve ser conduzida de forma global e integrada entre todas as áreas/serviços, estabelecimentos e, em geral, todas as Entidades do SNS que integram o eSIS.

Assim, devem ser levadas a cabo as seguintes medidas:

Mapeamento dos Sistemas e Aplicações em Utilização

Deverá ser efetuado um levantamento de todos os sistemas e aplicações nas quais sejam registados dados pessoais, com identificação das respetivas funcionalidades, níveis de acesso e medidas de segurança implementadas.

Verificação das Ferramentas de Rastreabilidade

Deverá ser verificado se existem ferramentas que permitam a rastreabilidade de acesso, inserção, alteração e eliminação de dados (logs) e, em caso afirmativo, se tal ferramenta se encontra implementada para todos os sistemas e/ou aplicações.

Avaliações de Risco e Vulnerabilidade

Por forma a avaliar se os sistemas e/ou aplicações são robustos e, consequentemente, são adequados a assegurar o cumprimento das novas obrigações decorrentes do RGPD e Diretiva SRI, devem ser realizadas avaliações de risco (PIA), efetuados testes de penetração e simulação de ataques.

Adaptação dos Sistemas ao RGDP

Deverá ser assegurado que os sistemas e aplicações permitem, desde logo, as seguintes funcionalidades:

- Portabilidade dos dados;
- Interoperabilidade;
- Anonimização, pseudonimização e encriptação;
- Segurança dos dados;
- O acesso, retificação e apagamento dos dados;
- Sistemas de alerta em caso de incidente de segurança;
- Registo de operações de tratamento;
- Auditorias;
- Rastreabilidade dos dados comunicados a terceiros;
- Controlo de acessos.

Controlo de Qualidade e Melhoria Contínua

No âmbito dos processos internos de garantia de qualidade e melhoria contínua, deve ser dado especial enfoque à segurança da informação.

Partilha de Informação de Segurança

Por forma a criar maior awareness, deverão ser partilhadas informações e dicas de segurança da informação por todos os intervenientes no ciclo de vida do tratamento de dados pessoais, ou de uma forma mais alargada por todas as Entidades integrantes do eSIS.

Mecanismos de Alerta

Os sistemas e aplicações deverão ser implementados, de forma a serem gerados alertas em caso de vulnerabilidade e/ou ocorrência de violações de segurança. Estes mecanismos permitirão, aos responsáveis pelos sistemas de informação, identificar o incidente e por em prática as medidas necessárias de forma a minimizar os riscos para a privacidade.

ENTIDADES DO SERVIÇO NACIONAL DE SAÚDE

As Entidades do Serviço Nacional de Saúde, tais como a SPMS, a ACSS e a DGS, desenvolvem projetos que têm, necessariamente, um impacto em matéria de segurança, privacidade e proteção de dados pessoais.

De facto, nas diferentes áreas de atuação das Entidades do Serviço Nacional de Saúde, são recolhidos e tratados dados pessoais não só da respponsabilidade das Entidades do Serviço Naiconal de Saúde (i.e., dados pessoais que a entidade trata em nome próprio, determinando as finalidades e termos do tratamento), mas também dados a que acede no âmbito da prestação de serviços a terceiros (é, desde logo, o caso do tratamento de dados no âmbito dos serviços e da implementação de plataformas disponibilizadas às Entidades integrantes do SNS).

Desde o desenvolvimento de plataformas de partilha de informação acessível a utentes e profissionais de saúde, ao desenho de apps, passando por produtos de faturação hospitalar às seguradoras, processamento de salários de todas as Entidades públicas integrantes do SNS, a atividade das Entidades do Serviço Nacional de Saúde deverá passar a ter em consideração as disposições do RGPD e, consequentemente, adaptar os seus processos e procedimentos internos de forma a assegurar o seu cumprimento.

Produtos (Exemplificativo)

Destacam-se, em particular, algumas ações a desencadear pelas Entidades do Serviço Nacional de Saúde em diferentes vertentes:

GOVERNANCE	PROCESSOS	SEGURANÇA	DIREITOS
Nomeação de um DPO Nomeação de Equipa Interna de Implementação do RGPD Definição de regras de comunicação de questões de segurança, privacidade e proteção de dados pessoais Divulgação Interna das novas regras e formação	Registos das atividades de tratamento de dados da sua responsabilidade ou de terceiros, quando a SPMS atue como entidade subcontratante Inclusão da privacidade no momento zero do desenvolvimento de produtos e serviços e adaptação às novas regras do RGPD Definição de procedimentos aplicáveis à elaboração de PIAs Inclusão de cláusulas de proteção de dados nos contratos a celebrar, em consonância com o RGPD Definição de processos aplicáveis à relação com as autoridades (CNPD) e com terceiros	Implementação de medidas internas e definição de regras aplicáveis à recolha e tratamento dos dados pessoais e à notificação de violações de dados pessoais e incidentes de segurança, identificando as responsabilidades, prazos e reportes Responsabilização de todos os intervenientes nos processos de recolha e tratamento de dados, através de ações de consciencialização Inclusão de requisitos de segurança, privacidade e proteção de dados nos concursos a lançar para prestação de serviços/ fornecimentos às Entidades Realização de controlos e auditorias a terceiros que tenham acesso a dados pessoais da responsabilidade das Entidades, de forma a aferir do cumprimento do RGPD Definição de regras internas de controlo de acessos	Desenho de produtos e serviços de forma recolher a menor quantidade possível de dados pessoais Implementação de medidas internas de forma a assegurar os direitos dos titulares dos dados, incluindo a prestação de informação, recolha de consentimento, direitos de acesso, retificação, eliminação e portabilidade dos dados

ENTIDADES DE SAÚDE
HOSPITAIS E CENTROS DE SAÚDE

As Entidades de saúde (Hospitais e centros de saúde), independentemente da sua designação e natureza jurídica, tratam, no seu dia-a-dia, um conjunto considerável de dados pessoais, incluindo dados de saúde e informação clínica de utentes.

Nessa medida, atuam como Entidades responsáveis, para efeitos da LPDP e do futuro RGPD, recaindo sobre as Entidades de saúde as obrigações identificadas neste Guia.

De forma a permitir às Entidades de saúde responderem, com sucesso, aos desafios do RGPD e da Diretiva SRI, identificam-se algumas boas práticas a adotar (às quais acrescem as ações e boas práticas identificadas anteriormente para os gestores hospitalares, profissionais de saúde e técnicos TIC).

GOVERNANCE	PROCESSOS	SEGURANÇA	DIREITOS
Nomeação de um DPO Nomeação de equipa interna de implementação do RGPD Definição de regras de comunicação de questões de segurança, privacidade e proteção de dados pessoais Divulgação interna das novas regras e formação Mapear as bases de dados e aplicações utilizadas e identificar as bases de dados em relação às quais assumem responsabilidades pelo tratamento	Revisão e adaptação de formulários de consentimento, textos informativos, contratos, regulamentos e manuais internos à luz do RGPD Registos das atividades de tratamento de dados Definição de procedimentos aplicáveis à elaboração de PIAs Inclusão de cláusulas de proteção de dados nos contratos a celebrar, em consonância com o RGPD Definição de processos aplicáveis à comunicação de dados a terceiros (incluindo SPMS), de relação com as autoridades (CNPD) e de informação aos utentes	Implementação de medidas internas e definição de regras aplicáveis à recolha e tratamento dos dados pessoais e à notificação de violações de dados pessoais e incidentes de segurança, identificando as responsabilidades, prazos e reportes Responsabilização de todos os intervenientes nos processos de recolha e tratamento de dados, através de ações de consciencialização Inclusão de requisitos de segurança, privacidade e proteção de dados nos concursos a lançar para prestação de serviços/ fornecimentos às Entidades Definição de regras internas de controlo de acessos	Implementação de medidas internas de forma a assegurar os direitos dos titulares dos dados, incluindo a prestação de informação, recolha de consentimento, direitos de acesso, retificação, eliminação e portabilidade dos dados

Existem outras obrigações e boas práticas que deverão ser implementadas num contexto geográfico mais global e não local. De facto, e ainda que, em regra, cada Entidades de saúde tenha personalidade jurídica autónoma, recaindo, sobre cada um deles, todas as obrigações do RGPD e da Diretiva SRI, existem algumas obrigações de cariz organizativo e governança, que poderá fazer sentido uma metodologia diferente, nomeadamente no contexto do eSIS.

É o caso do Responsável de Proteção de Dados (DPO) que, na ausência de diretrizes específicas da CNPD (até à data), poderá ser ponderada a nomeação de um responsável global para as Entidades do SNS.

ENTIDADES DE SAÚDE
CENTROS HOSPITALARES

A integração horizontal da prestação de cuidados de saúde levou à criação de Centros Hospitalares, que resultam da fusão de hospitais que integram o SNS. Como Centros Hospitalares, aglomeram dados pessoais das diferentes Entidades de saúde, assumindo-se, o Centro Hospitalar, como Instituição responsável pelo tratamento de tais dados.

Na medida em que o volume de dados a tratar será, em regra, superior ao tratado por um hospital individualmente considerado, existirão algumas medidas que deverão ser ponderadas pelos Centros Hospitalares, de forma a responder aos desafios do RGPD e da Diretiva SRI.

Assim, e para além das ações e boas práticas identificadas anteriormente para os gestores hospitalares, profissionais de saúde e técnicos TIC, destacam-se, de seguida, medidas suscetíveis de implementação pelos centros hospitalares.

GOVERNANCE	PROCESSOS	SEGURANÇA	DIREITOS
Nomeação de um DPO Nomeação de equipa interna de implementação do RGPD Definição de regras de comunicação de questões de segurança, privacidade e proteção de dados pessoais Divulgação interna das novas regras e formação Mapear as bases de dados e aplicações utilizadas e identificar as bases de dados em relação às quais assumem responsabilidades pelo tratamento	Revisão e adaptação de formulários de consentimento, textos informativos, contratos, regulamentos e manuais internos à luz do RGPD Registos das atividades de tratamento de dados Definição de procedimentos aplicáveis à elaboração de PIAs Inclusão de cláusulas de proteção de dados nos contratos a celebrar, em consonância com o RGPD Definição de processos aplicáveis à comunicação de dados a terceiros (incluindo SPMS), de relação com as autoridades (CNPD) e de informação aos utentes	Implementação de medidas internas e definição de regras aplicáveis à recolha e tratamento dos dados pessoais e à notificação de violações de dados pessoais e incidentes de segurança, identificando as responsabilidades, prazos e reportes Responsabilização de todos os intervenientes nos processos de recolha e tratamento de dados, através de ações de consciencialização Inclusão de requisitos de segurança, privacidade e proteção de dados nos concursos a lançar para prestação de serviços/ fornecimentos às Entidades Definição de regras internas de controlo de acessos	Implementação de medidas internas de forma a assegurar os direitos dos titulares dos dados, incluindo a prestação de informação, recolha de consentimento, direitos de acesso, retificação, eliminação e portabilidade dos dados

ENTIDADES DE SAÚDE PARCERIAS PÚBLICO PRIVADAS

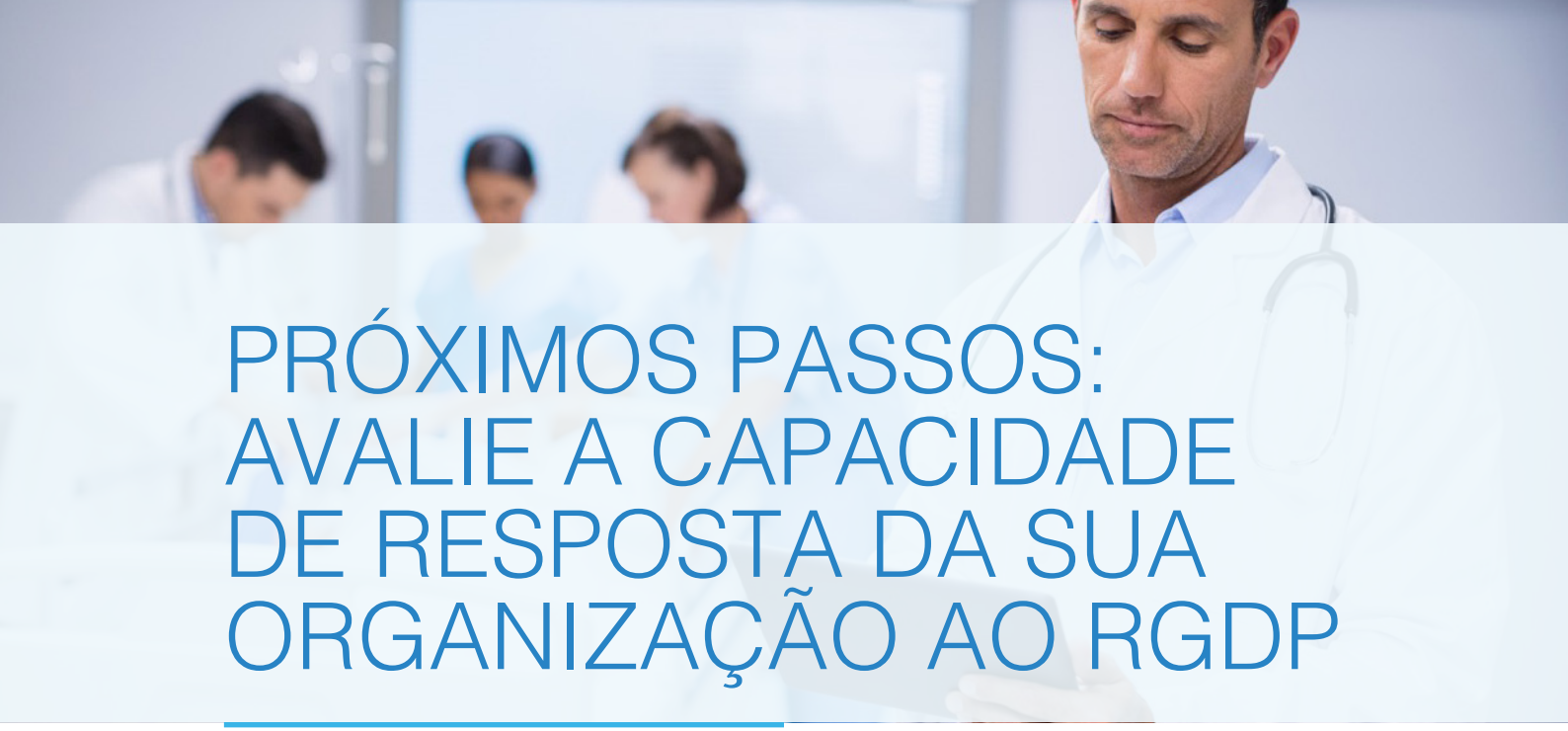
As Entidades de saúde geridas em regime de parcerias público privadas (PPPs), integrantes do SNS, deverão implementar também medidas internas, de forma a assegurar um cumprimento integral do RGPD.

Sem prejuízo das ações e boas práticas identificadas anteriormente para os gestores hospitalares, profissionais de saúde e técnicos TIC, destacam-se, de seguida, algumas medidas a implementar pelas PPPs.

GOVERNANCE	PROCESSOS	SEGURANÇA	DIREITOS
Nomeação de um DPO Nomeação de equipa interna de implementação do RGPD Definição de regras de comunicação de questões de segurança, privacidade e proteção de dados pessoais Divulgação interna das novas regras e formação Definição de regras de comunicação de questões relativas à segurança, privacidade e proteção de dados pessoais com o gestor do contrato e com a ACSS Mapear as bases de dados e aplicações utilizadas e identificar as bases de dados em relação às quais assumem responsabilidades pelo tratamento	Revisão e adaptação de formulários de consentimento, textos informativos, contratos, regulamentos e manuais internos à luz do RGPD Registos das atividades de tratamento de dados Definição de procedimentos aplicáveis à elaboração de PIAs Inclusão de cláusulas de proteção de dados nos contratos a celebrar, em consonância com o RGPD Definição de processos aplicáveis à comunicação de dados a terceiros (incluindo SPMS), de relação com as autoridades (CNPD) e de informação aos utentes	Implementação de medidas internas e definição de regras aplicáveis à recolha e tratamento dos dados pessoais e à notificação de violações de dados pessoais e incidentes de segurança, identificando as responsabilidades, prazos e reportes Responsabilização de todos os intervenientes nos processos de recolha e tratamento de dados, através de ações de consciencialização Inclusão de requisitos de segurança, privacidade e proteção de dados nos concursos a lançar para prestação de serviços/ fornecimentos às Entidades Definição de regras internas de controlo de acessos	Implementação de medidas internas de forma a assegurar os direitos dos titulares dos dados, incluindo a prestação de informação, recolha de consentimento, direitos de acesso, retificação, eliminação e portabilidade dos dados

RESUMO DE RECOMENDAÇÕES

	VETORES			
ENTIDADES	**GOVERNANCE**	**PROCESSOS**	**SEGURANÇA**	**DIREITOS**
ENTIDADES DO SERVIÇO NACIONAL DE SAÚDE	Nomeação de estrutura de governance (DPO) e definição de regras de divulgação e comunicação interna das novas regras do RGPD	Registos das atividades de tratamento de dados da sua responsabilidade ou de terceiros, bem como definição e implementação de processos e procedimentos internos de forma a cumprir as novas regras do RGPD (desde logo, inclusão da privacidade no momento zero do desenvolvimento de produtos e serviços e adaptação às novas regras do RGPD)	Implementação de medidas internas e definição de requisitos de segurança e controlo de acessos e auditoria a terceiros, bem como de regras aplicáveis à recolha e tratamento dos dados pessoais e à notificação de violações de dados pessoais e incidentes de segurança	Desenho de produtos e serviços de forma recolher a menor quantidade possível de dados pessoais, bem como implementação de medidas internas de forma a assegurar os direitos dos titulares dos dados
HOSPITAIS E CENTROS DE SAÚDE	Nomeação de estrutura de governance (DPO) e definição de regras de divulgação e comunicação interna das novas regras do RGPD	Revisão e adaptação de documentos com impacto na proteção de dados à luz do RGPD, bem como definição e implementação de processos e procedimentos internos de forma a cumprir as novas regras do RGPD	Implementação de medidas internas e definição de requisitos de segurança e controlo de acessos, bem como de regras aplicáveis à recolha e tratamento dos dados pessoais e à notificação de violações de dados pessoais e incidentes de segurança	Implementação de medidas internas de forma a assegurar os direitos dos titulares dos dados
CENTROS HOSPITALARES	Nomeação de estrutura de governance (DPO) e definição de regras de divulgação e comunicação interna das novas regras do RGPD	Revisão e adaptação de documentos com impacto na proteção de dados à luz do RGPD, bem como definição e implementação de processos e procedimentos internos de forma a cumprir as novas regras do RGPD	Implementação de medidas internas e definição de requisitos de segurança e controlo de acessos, bem como de regras aplicáveis à recolha e tratamento dos dados pessoais e à notificação de violações de dados pessoais e incidentes de segurança	Implementação de medidas internas de forma a assegurar os direitos dos titulares dos dados
PPPs	Nomeação de estrutura de governance (DPO) e definição de regras de divulgação e comunicação interna das novas regras do RGPD e de comunicação de dados	Revisão e adaptação de documentos com impacto na proteção de dados à luz do RGPD, bem como definição e implementação de processos e procedimentos internos de forma a cumprir as novas regras do RGPD	Implementação de medidas internas e definição de requisitos de segurança e controlo de acessos, bem como de regras aplicáveis à recolha e tratamento dos dados pessoais e à notificação de violações de dados pessoais e incidentes de segurança	Implementação de medidas internas de forma a assegurar os direitos dos titulares dos dados



PRÓXIMOS PASSOS: AVALIE A CAPACIDADE DE RESPOSTA DA SUA ORGANIZAÇÃO AO RGDP

Para além do presente Guia, desenvolvido com o objetivo de a dar a conhecer, às Entidades públicas integrantes do SNS[21], as condições a que se encontram sujeitas em relação ao tratamento de dados pessoais em Portugal no contexto do RGPD e da Diretiva SRI, a SPMS irá disponibilizar uma ferramenta online para autoavaliação preliminar do nível de adequação e cumprimento das respetivas regras ("RGDP – Ferramenta para Autoavaliação Preliminar do Cumprimento das Regras").

Os resultados obtidos pelas Entidades devem ser utilizados apenas como uma avaliação preliminar. A ferramenta tem como principal objetivo identificar as áreas, mais ou menos críticas, a serem endereçadas pela Instituição no sentido de estarem preparadas para cumprir as regras do RGDP a partir de maio de 2018.

A "RGDP – Ferramenta para Autoavaliação Preliminar do Cumprimento das Regras" está divida em cinco grandes grupos de questões:

Estratégia **Dados** **Processos** **Pessoas** **Tecnologia**

[21] Consideram-se para o efeito todos os estabelecimentos e serviços do Serviço Nacional de Saúde, independentemente da respetiva natureza jurídica, sejam Entidades públicas empresariais, sejam Entidades do Sector Público Administrativo, bem como aos órgãos e serviços do Ministério da Saúde e a quaisquer outras Entidades quando executem atividades na área da saúde.

As questões foram mapeadas com os cinco vetores de mudança principais do RGPD descritas neste Guia, permitindo desta forma implementar um processo de melhoria contínua que vai além da conformidade legal e normativa:

- ✓ Governança dos Dados;
- ✓ Consentimento;
- ✓ Direitos dos titulares;
- ✓ Segurança;
- ✓ Poder Sancionatório.

Além da ferramenta de autoavaliação preliminar, as Entidades poderão ainda utilizar o questionário abaixo, o qual espelha, de uma forma não exaustiva, os requisitos mínimos para o nível de adequação e cumprimento das respetivas regras do RGDP.

GRUPO	QUESTÃO	SIM	NÃO	COMENTÁRIOS
Estratégia (REQ.EST)	REQ.EST.01 - A comunicação sobre os requisitos de responsabilidade para a conformidade com o RGPD foi divulgada a todo a Instituição?			
	REQ.EST.02 - As melhores práticas de proteção de dados foram documentadas e divulgada a toda a Instituição?			
	REQ.EST.03 - A Instituição já documentou todos os riscos associados ao processamento de dados pessoais que formam a base para as auditorias?			
	REQ.EST.04 - A Gestão da Instituição está a par dos níveis detalhados de multas e infrações do RGPD?			
	REQ.EST.05 - A Gestão da Instituição conhece e entende as hipóteses de ações judiciais coletivas e potencial suspensão de atividades de processamento de dados por incumprimento continuado?			

GRUPO	QUESTÃO	SIM	NÃO	COMENTÁRIOS
Dados (REQ.DAD)	REQ.DAD.01 - Há um processo padrão para mapear e classificar os dados pessoais de forma consistente em todo a Instituição?			
	REQ.DAD.02 - Foi realizada uma análise para documentar a utilização e o fluxo de dados pessoais na Instituição. Esta documentação serve de base para a monitorização das atividades de processamento?			
	REQ.DAD.03 - É comunicado de forma clara e transparente aos titulares dos dados que é feita a recolha dos seus dados pessoais?			
	REQ.DAD.04 - Há na Instituição um controlo que relaciona os dados recolhidos à finalidade de processamento, e que permite a correta utilização e eliminação de dados?			
	REQ.DAD.05 - Existe um processo definido para a revisão de dados, em cada registo, quando esses dados são processados?			
	REQ.DAD.06 - Há na Instituição um processo, mesmo que manual, para rever a utilidade			
	REQ.DAD.07 - Há na Instituição um plano de continuidade hospitalar (incluindo pessoas, processos e tecnologias), implementado e testado?			
	REQ.DAD.08 - Há na Instituição um processo que identifica os dados que podem ser removidos e que posteriormente envolve equipas individuais para remoção?			
	REQ.DAD.09 - Em caso de armazenamento de dados na cloud, há a definição clara dos termos do contrato que permitem escolher a localização dos dados e a realização de auditorias?			
Pessoas (REQ.PES)	REQ.PES.01 - A Instituição comunica a gestão de dados pessoais à autoridade supervisora nacional (CNPD), mesmo que não esteja estabelecida formalmente uma organização de governança ou de procedimentos para este efeito?			
	REQ.PES.02 - A Instituição já nomeou, mesmo que a tempo parcial, um Responsável de Proteção de Dados?			

GRUPO	QUESTÃO	SIM	NÃO	COMENTÁRIOS
 Processos (REQ.PRO)	REQ.PRO.01 - A Instituição tem implementada um processo de resposta em caso de incidente de violação de dados pessoais, mesmo que não esteja testado?			
	REQ.PRO.02 - A Instituição tem implementado um processo de comunicação aos titulares dos dados e parceiros externos em caso de incidente de violação de dados pessoais, mesmo que não esteja testado?			
	REQ.PRO.03 - A Instituição opera de acordo com os princípios e práticas gerais de boas práticas de segurança da informação (ex. ISO 27001), mesmo que não tenha uma certificação?			
	REQ.PRO.04 - A Instituição já iniciou a revisão dos contratos com os fornecedores externos que processam dados pessoais?			
	REQ.PRO.05 - Há na Instituição processos de consentimento que integram especificação, tais como: autorização de uso; duração de consentimento; e consentimento dado de livre vontade?			
	REQ.PRO.06 - Existe na Instituição um processo de verificação de idade e obtenção de consentimento parental?			
	REQ.PRO.07 – Existem requisitos de segurança definidos e documentados que se aplicam a departamentos/processos específicos, como os RH, TI e marketing, mesmo que não seja testado regularmente?			
 Tecnologias (REQ.TEC)	REQ.TEC.01 - A Instituição tem capacidade de controlo dos sistemas para detetar todas as violações de dados pessoais num prazo de 72 horas e para implementar imediatamente medidas para reportar a violação?			
	REQ.TEC.02 - A Instituição tem um processo automatizado para identificação dos dados a retificar ou as objeções ao processamento solicitadas pelos detentores dos dados?			
	REQ.TEC.03 - A Instituição tem no sistema de informação, mesmo que não seja uma solução específica, funcionalidades que permitam a implementação do direito à eliminação?			

GRUPO	QUESTÃO	SIM	NÃO	COMENTÁRIOS
	REQ.TEC.04 - Há na Instituição um processo implementado, mesmo que manual, para efetuar a portabilidade de dados pessoais?			
	REQ.TEC.05 - Os sistemas de informação da Instituição permitem a pseudonimização dos dados pessoais através da sua anonimização e/ou tokenização?			
	REQ.TEC.06 - O sistema de informação da Instituição permite garantir um processo padronizado para codificação dos dados pessoais?			
	REQ.TEC.07 - A Instituição tem um sistema de single sign-on que permite a otimização do controlo de acesso em todo a Instituição e a monitorização contínua da conformidade?			
	REQ.TEC.08 - A Instituição tem sistemas que registam o consentimento, mas não de forma centralizada?			

GLOSSÁRIO

As definições abaixo foram adaptadas do texto do RGPD.

GRUPO	QUESTÃO
Dados Pessoais	Qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável (”titular dos dados”); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um identificador como o nome, número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, mental, económica, cultural ou social.
Tratamento de Dados Pessoais (tratamento)	Qualquer operação ou conjunto de operações efetuados sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão, bem como a limitação, apagamento ou destruição.
Responsável eplo tratamento	A pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais.
Subcontratante[22]	A pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.
Terceiro	Pessoa singular ou coletiva, autoridade pública, o serviço ou qualquer outro organismo que, não sendo o titular de dados, o responsável pelo tratamento, o subcontratante ou outra pessoa sob autoridade direta do responsável pelo tratamento ou do subcontratante, esteja autorizado a tratar os dados.
Destinatário	A pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo a quem sejam comunicados dados pessoais, independentemente de se tratar ou não de um terceiro.

[22] Na tradução para português da expressão “data processor”, denominou-se esta Entidade como “subcontratante”, em vez de “subcontratado” – em todo o caso, ambas as expressões têm o mesmo significado.

GRUPO	QUESTÃO
Consentimento do Titular dos Dados	Qualquer manifestação de vontade, livre, específica, informada e explicita, nos termos da qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os seus dados pessoais sejam objeto de tratamento.
Dados Pessoais relativos à Saúde	O RGPD define-os expressamente como dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, no passado, presente e no futuro, incluindo a inscrição e prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde.
Dados Genéticos	O RGPD define-os expressamente como dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que forneçam informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa, nomeadamente de analise de cromossomas, ADN , ARN ou de outro elemento que permita obter informações equivalentes.
Privacy by design (privacidade desde a conceção)	Significa levar o risco de privacidade em conta em todo o processo de conceção de um novo produto ou serviço, em vez de considerar as questões de privacidade apenas posteriormente. Tal significa avaliar cuidadosamente e implementar medidas e procedimentos técnicos e organizacionais adequados desde o início para garantir que o tratamento está em conformidade com o RGPD e protege os direitos dos titulares dos dados em causa.
Privacy by default (privacidade por defeito)	Significa assegurar que são colocados em prática, dentro de uma Organização, mecanismos para garantir que, por defeito, apenas será recolhida, utilizada e conservada para cada tarefa, a quantidade necessária de dados pessoais. Esta obrigação aplica-se à extensão do seu tratamento, ao prazo de conservação e à sua acessibilidade. Estas medidas asseguram que os dados pessoais não sejam disponibilizados sem intervenção humana a um numero indeterminado de pessoas singulares.
Limitação do Tratamento	Inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro.
Pseudonimização	Tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

GRUPO	QUESTÃO
Data minimisation (minimização dos dados)	Significa que os dados pessoais recolhidos devem ser limitados ao que é necessário relativamente às finalidades para as quais são tratados.
Violação de dados pessoais	Violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.
Violação de segurança (incidentes de segurança)	Evento com um efeito adverso real na segurança das redes e dos sistemas de informação, tal como um acesso não autorizado ao sistema de informação.


SPMS EPE
Serviços Partilhados do Ministério da Saúde