MEMO

Regulamento Geral de Protecção de Dados

A Solicitação e no seguimento da entrada em vigor do Novo Regulamento Geral de Protecção de Dados, **preparou-se o presente Memorando a ser submetido a aprovação da Administração** em ordem a ser aprovada, implementada e aperfeiçoada a Política de Protecção de Dados vigente.

Assim, segue-se:

1. **Introdução (1) e Alterações Essenciais (2)**
2. **Aprovação de Política de Protecção de Dados Pessoais (Anexo A), Cláusulas a inserir em Contratos de trabalho e outros (Anexo B e C) e Contrato a celebrar com prestadores de Serviços que tratem dados Pessoais (D).**
3. **Aprovação do Envio da Política de Protecção de Dados Pessoais para aceitação de todos os clientes em Base de Dados que não tenham já registada aceitação expressa.**
4. **Nomeação de um responsável pelos Dados Pessoais.**
5. **Realização de uma Auditoria interna (3)**
6. **Sugestão de Medidas a implementar após resultados da Auditoria (4)**
7. **Glossário (5)**

1. Introdução

O RGPD irá alterar profundamente a forma como se 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 as principais obrigações 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.

2. **Alterações Essenciais:**

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

2.1 Governança de 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 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 devem realizar uma avaliação de impacto de tais operações sobre a proteção de dados pessoais ("privacy impact assessment" – "PIA").

Através do PIA, as Entidades 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 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 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, 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 que as Entidades 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 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

(f) Maior responsabilização na escolha de entidades externas

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

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.

2.2. 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 sujeitasdevem rever os mecanismos de pedido de consentimento online, para o caso da utilização de cookies**.**

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.

2.3 Direitos dos Titulares dos Dados

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 sujeitas 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 sujeitas 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 sujeitas 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 sujeitasdevam adotar mecanismos que assegurem que todos os dados foram efetivamente eliminados (incluindo cópias ou reproduções dos mesmos)

(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. Nesta ótica, as Entidades sujeitasdeverão 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 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.

2.4 Segurança

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 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;
(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 sujeitas 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, 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 sujeitasdeverão 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.

2.5 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.

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

2.6 Em Suma, são as seguintes as obrigações essenciais

- 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
- **Deverá ser assegurado que os <u>sistemas e aplicações</u> 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.

3. **Auditoria:**

1. **Há um processo padrão para mapear e classificar os dados pessoais de forma consistente em todo a Instituição?**
2. **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?**
3. **É comunicado de forma clara e transparente aos titulares dos dados que é feita a recolha dos seus dados pessoais?**
4. **Há na Instituição um controlo que relaciona os dados recolhidos à finalidade de processamento, e que permite a correta utilização e eliminação de dados?**
5. **Existe um processo definido para a revisão de dados, em cada registo, quando esses dados são processados?**
6. **Há na Instituição um processo, mesmo que manual, para rever a utilidade dos dados e sua remoção?**
7. **Em caso de armazenamento de dados 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?**
8. **A Instituição já nomeou, mesmo que a tempo parcial, um Responsável de Proteção de Dados?**
9. **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?**
10. **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?**
11. **A Instituição já iniciou a revisão dos contratos com os fornecedores externos que processam dados pessoais?**
12. **Há na Instituição processos de consentimento que integram especificação, tais como: autorização de uso; duração de consentimento; e consentimento dado de livre vontade?**

13. **Existe na Instituição um processo de verificação de idade e obtenção de consentimento parental?**
14. **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?**
15. **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?**
16. **A Instituição tem um processo automatizado para identificação dos dados a retificar ou as objeções ao processamento solicitadas pelos detentores dos dados?**
17. **A Instituição tem no sistema de informação, mesmo que não seja uma solução específica, funcionalidades que permitam a implementação do direito à eliminação?**
18. **Há na Instituição um processo implementado, mesmo que manual, para efetuar a portabilidade de dados pessoais?**
19. **Os sistemas de informação da Instituição permitem a pseudonimização dos dados pessoais através da sua anonimização e/ou tokenização?**
20. **A Instituição tem sistemas que registam o consentimento, mas não de forma centralizada?**
21. **O sistema de informação da Instituição permite garantir um processo padronizado para codificação dos dados pessoais?**

4. **A implementar:**

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
<u>Sistemas de Informação</u>	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)
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

4.1. **Quadro Resumo Medidas a implementar:**

Governance	**Processos**	**Segurança**	**Direitos**
Nomeação de um DPO	Revisão e adaptação de formulários de consentimento, textos informativos, contratos, regulamentos e manuais internos à luz do RGPD	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	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
Nomeação de equipa interna de implementação do RGPD	Registos das atividades de tratamento de dados	
Definição de regras de comunicação de questões de segurança, privacidade e proteção de dados pessoais	Definição de procedimentos aplicáveis à elaboração de PIAs	
Divulgação interna das novas regras e formação	Inclusão de cláusulas de proteção de dados nos contratos a celebrar, em consonância com o RGPD	
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	Definição de processos aplicáveis à comunicação de dados a terceiros (incluindo SPMS), de relação com as autoridades (CNPD) e de informação aos utentes	
Mapear as bases de dados e aplicações utilizadas e identificar as bases de dados em relação às quais assumem responsabilidades pelo tratamento		
		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

5. GLOSSÁRIO

As definições abaixo foram adaptadas do texto do RGPD.

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	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.
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.
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.