

ANEXO - Articulado da Norma

Índice

<i>Artigo 2º</i>	2
Âmbito de aplicação material	2
<i>Artigo 3º</i>	2
Âmbito de aplicação territorial	2
<i>Artigo 6º</i>	2
Licitude do tratamento	2
<i>Artigo 7º</i>	3
Condições aplicáveis ao consentimento	3
<i>Artigo 12º</i>	3
Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados	3
<i>Artigo 15º</i>	4
Direito de acesso do titular dos dados	4
<i>Artigo 16º</i>	4
Direito de retificação	4
<i>Artigo 17º</i>	4
Direito ao apagamento dos dados («direito a ser esquecido»)	4
<i>Artigo 18º</i>	4
Direito à limitação do tratamento	4
<i>Artigo 24º</i>	5
Responsabilidade do responsável pelo tratamento	5
<i>Artigo 25º</i>	5
Proteção de dados desde a conceção e por defeito	5
<i>Artigo 28º</i>	5
Subcontratante	5
<i>Artigo 30º</i>	6
Registos das atividades de tratamento	6
<i>Artigo 32º</i>	6
Segurança do tratamento	6
<i>Artigo 33º</i>	7
Notificação de uma violação de dados pessoais à autoridade de controlo	7

Artigo 2º

Âmbito de aplicação material

1. O presente regulamento **aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados**, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.
2. O presente regulamento não se aplica ao tratamento de dados pessoais:
 - a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União;
 - b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, Capítulo 2, do TUE;
 - c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas;
 - d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Artigo 3º

Âmbito de aplicação territorial

1. O presente regulamento aplica-se ao **tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.**

Artigo 6º

Licitude do tratamento

1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
 - a) O titular dos dados **tiver dado o seu consentimento** para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
 - b) O tratamento for **necessário para a execução de um contrato** no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
 - c) O tratamento for necessário para o **cumprimento de uma obrigação jurídica** a que o responsável pelo tratamento esteja sujeito;

- d) O tratamento for **necessário para a defesa de interesses vitais** do titular dos dados ou de outra pessoa singular;
- e) O tratamento for necessário ao **exercício de funções de interesse público ou ao exercício da autoridade pública** de que está investido o responsável pelo tratamento;
- f) O tratamento for necessário **para efeito dos interesses legítimos** prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial **se o titular for uma criança**.

O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica.

Artigo 7º

Condições aplicáveis ao consentimento

1. Quando o tratamento for realizado com base no consentimento, **o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento** para o tratamento dos seus dados pessoais.
2. Se o consentimento do titular dos dados for dado no contexto de uma **declaração escrita** que diga também respeito a outros assuntos, **o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente** desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento.
3. O titular dos dados **tem o direito de retirar o seu consentimento** a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento **deve ser tão fácil de retirar quanto de dar**.

Artigo 12º

Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados

3. O responsável pelo tratamento fornece ao titular as **informações sobre as medidas tomadas**, mediante pedido apresentado nos termos dos artigos 15º a 20º, sem demora injustificada e **no prazo de um mês** a contar da data de receção do pedido. Esse prazo **pode ser prorrogado até dois meses**, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos.
4. **Se o responsável pelo tratamento não der seguimento ao pedido apresentado** pelo titular dos dados, **informa-o** sem demora e, o mais tardar, **no prazo de um mês** a contar da data de receção do pedido, **das razões** que o levaram a não tomar medidas e **da possibilidade de apresentar reclamação** a uma autoridade de controlo e intentar ação judicial.

Artigo 15º

Direito de acesso do titular dos dados

1. O titular dos dados tem o **direito de obter** do responsável pelo tratamento a **confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento** e, se for esse o caso, o **direito de aceder aos seus dados** (...)

Artigo 16º

Direito de retificação

O titular tem o **direito de obter**, sem demora injustificada, do responsável pelo tratamento a **retificação dos dados pessoais** inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.

Artigo 17º

Direito ao apagamento dos dados («direito a ser esquecido»)

1. O titular tem o **direito de obter** do responsável pelo tratamento o **apagamento** dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:

- a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;

Artigo 18º

Direito à limitação do tratamento

1. O titular dos dados tem o **direito de obter** do responsável pelo tratamento a **limitação do tratamento**, (...)

CAPÍTULO IV

Responsável pelo tratamento e subcontratante

Secção 1

Obrigações gerais

Artigo 24º

Responsabilidade do responsável pelo tratamento

1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento **aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento.**

Artigo 25º

Proteção de dados desde a conceção e por defeito

2. O responsável pelo tratamento **aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários** para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade.

Em especial, essas medidas asseguram que, por defeito, **os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.**

Artigo 28º

Subcontratante

1. Quando o tratamento dos dados for efetuado por sua conta, o responsável pelo tratamento **recorre apenas a subcontratantes que apresentem garantias suficientes** de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados.

3. O tratamento em **subcontratação é regulado por contrato** ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros,

9. O contrato ou outro ato normativo a que se referem os nºs 3 e 4 **devem ser feitos por escrito, incluindo em formato eletrónico.**

Artigo 30º

Registos das atividades de tratamento

1. Cada responsável pelo tratamento e, sendo caso disso, o seu representante conserva um registo de todas as atividades de tratamento sob a sua responsabilidade. (...)
2. (...) conserva um registo de todas as categorias de atividades de tratamento realizadas (...)
5. As obrigações a que se referem os n.ºs 1 e 2 **não se aplicam às empresas ou organizações com menos de 250 trabalhadores**, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional (...)

Secção 2

Segurança dos dados pessoais

Artigo 32º

Segurança do tratamento

1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante **aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco**, incluindo, consoante o que for adequado:
 - a) A **pseudonimização** e a cifragem dos dados pessoais;
 - b) A capacidade de **assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento**;
 - c) A capacidade de **restabelecer a disponibilidade e o acesso aos dados pessoais** de forma atempada **no caso de um incidente físico ou técnico**;
 - d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para **garantir a segurança do tratamento**.
2. Ao **avaliar o nível de segurança adequado**, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular **devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados**, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.
3. O cumprimento de um **código de conduta** aprovado conforme referido no artigo 40º ou de um procedimento de certificação aprovado conforme referido no artigo 42º pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas no n.º 1 do presente artigo.

4. O responsável pelo tratamento e o subcontratante **tomam medidas para assegurar que qualquer pessoa singular que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, só procede ao seu tratamento mediante instruções do responsável pelo tratamento, exceto se tal lhe for exigido pelo direito da União ou de um Estado-Membro.**

Artigo 33º

Notificação de uma violação de dados pessoais à autoridade de controlo

1. **Em caso de violação de dados pessoais**, o responsável pelo tratamento **notifica** desse facto a **autoridade de controlo competente** nos termos do artigo 55º, sem demora injustificada e, sempre que possível, **até 72 horas** após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.
2. O **subcontratante notifica** o responsável pelo tratamento sem demora injustificada **após ter conhecimento de uma violação** de dados pessoais.
3. **A notificação** referida no nº 1 **deve**, pelo menos:
 - a) **Descrever 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;
 - b) Comunicar o **nome e os contactos do encarregado da proteção de dados** ou de outro ponto de contacto onde possam ser obtidas mais informações;
 - c) Descrever **as consequências prováveis** da violação de dados pessoais;
 - d) Descrever **as medidas adotadas ou propostas** pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, **medidas para atenuar** os seus eventuais efeitos negativos;
4. Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas por fases, sem demora injustificada.