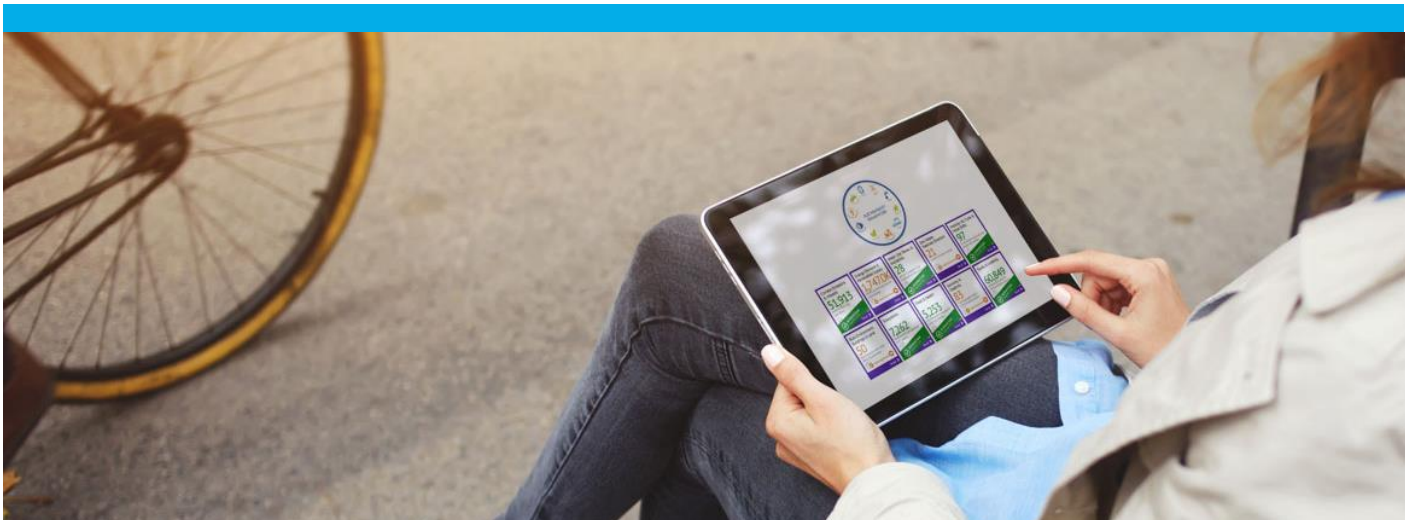

Documento de Apoio ao RGPD

Ciclo de desenvolvimento de software

Em progresso

Versão: 2

20/02/2018

Nelson Lopes

ASSOFT – Associação Portuguesa de Software

Conteúdo

ASSOFT
ASSOCIAÇÃO PORTUGUESA DE SOFTWARE

Conceitos e princípios chave

A. DADOS PESSOAIS (*PERSONAL DATA*)

Toda e qualquer informação relativa a uma pessoa singular identificada ou identificável (o «titular dos dados»); uma pessoa singular será considerada como sendo identificável, direta ou indiretamente, se conseguirmos chegar à sua identificação por referência a um número de identificação, ou pela conjugação de específicos fatores físicos, psicológicos, mentais, económicos, culturais ou sociais.

Exemplo: Número de Identificação Fiscal, Número de Identificação Civil representam dados pessoais que identificam de forma imediata um titular dos dados pessoais. Dados como altura, peso, idade, número de seguro de saúde, composição do agregado familiar, são dados que conjugados podem permitir identificar uma pessoa, sendo dados pessoais que permitem identificar uma pessoa.

Normais legais: artigo 4.º do RGPD.

B. CATEGORIAS ESPECIAIS DE DADOS PESSOAIS (*SPECIAL CATEGORIES OF PERSONAL DATA*)

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

Normais legais: artigo 9.º do RGPD.

C. TRATAMENTO DE DADOS PESSOAIS (*PROCESSING OF PERSONAL DATA*)

Qualquer operação ou conjunto de operações realizadas, de forma automática ou não automática, sobre dados pessoais.

Exemplo: Toda e qualquer operação que implique a recolha, o registo, a organização, a estruturação, a conservação, a consulta, a utilização, o apagamento ou a destruição, a combinação de dados, etc.

Normas legais: artigos 5.º, 6.º e 9.º a 11.º do RGPD.

D. DEFINIÇÃO DE PERFIS (*PROFILING*)

Tratamento automatizado de dados pessoais com vista a avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações

Normas legais: artigo 22.º do RGPD.

E. SEGURANÇA DO TRATAMENTO (*SECURITY OF PROCESSING*)

O responsável pelo tratamento e o subcontratante devem aplicar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco do tratamento. De acordo com um princípio de proporcionalidade, as técnicas e medidas utilizadas para este fim devem ter em conta as técnicas mais avançadas, aos custos de aplicação, à natureza, âmbito, contexto e finalidades do tratamento, assim como aos riscos do tratamento. São consideradas medidas técnicas e organizativas adequadas, entre outros, a encriptação, a pseudonimização e a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento.

Normas legais: artigo 32.º do RGPD.

F. CONSENTIMENTO DO TITULAR DOS DADOS (*CONSENT OF THE DATA SUBJECT*)

Declaração expressa e inequívoca de vontade do titular dos dados, o qual de forma livre, específica, informada e explícita, aceita, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

Exemplo: Nos formulários on-line de preenchimento pelos utilizadores apenas haverá consentimento efetivo se o mesmo for dado de forma expressa, o consentimento meramente tácito, como é exemplo a expressão " ao continuar a navegar nesta página concorda com a recolha e tratamento dos seus dados" não é considerado consentimento correto do titular dos dados.

Normais legais: artigos 7.º e 8.º do RGPD.

G. DIREITO À RETIFICAÇÃO, À LIMITAÇÃO E AO APAGAMENTO DE DADOS PESSOAIS (*RIGHT TO RECTIFICATION, TO RESTRICTION AND TO ERASURE OF PERSONAL DATA*)

Direito do titular dos dados a obter do responsável pelo tratamento, sem demora injustificada, a retificação e completude dos dados pessoais inexatos ou incompletos que lhe digam respeito, o apagamento dos seus dados pessoais em determinadas circunstâncias, e a limitação de processamento dos dados pessoais inexatos, sujeitos a tratamento ilícito ou desnecessário ou que tenham sido alvo de oposição.

Normas legais: artigos 16.º, 17.º e 18.º do RGPD.

H. DIREITO DE OPOSIÇÃO (*RIGHT TO OBJECT*)

Direito do titular dos dados a opor-se, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito. Se os dados pessoais forem tratados para efeitos de comercialização direta, incluindo definição de perfis, o titular dos dados tem o direito de se opor a qualquer momento. Se os dados pessoais forem tratados para o exercício necessário de funções de interesse público ou por autoridade pública, o direito

de oposição não leva à cessação do tratamento se este for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros e se não 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.

Normas legais: artigo 21.º do RGPD.

I. DIREITO À PORTABILIDADE E TRANSMISSÃO (RIGHT TO DATA PORTABILITY AND TRANSMISSION)

Direito do titular dos dados a receber os dados pessoais que lhe digam respeito e que tenha fornecido ao responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, assim como a que esses dados sejam transmitidos automaticamente a outro responsável pelo tratamento, sempre que tecnicamente possível.

Normas legais: artigo 20.º do RGPD.

J. PROTEÇÃO DE DADOS DESDE A CONCEÇÃO E POR DEFEITO (*PRIVACY BY DESIGN AND PRIVACY BY DEFAULT*)

Os meios de tratamento de dados pessoais devem ser concebidos para garantir o cumprimento das obrigações em matéria de proteção de dados pessoais e devem por defeito assegurar que apenas são processados os dados pessoais necessários. De acordo com um princípio de proporcionalidade, as técnicas e medidas utilizadas para este fim devem atender ao estado da arte, aos custos de implementação, à natureza, âmbito, contexto e finalidades do tratamento, assim como aos riscos do tratamento. São consideradas medidas técnicas e organizativas adequadas a encriptação, a pseudonimização e da minimização de dados.

Normas legais: artigo 25.º do RGPD.

K. REGISTOS DAS ATIVIDADES DE TRATAMENTO (*RECORDS OF PROCESSING ACTIVITIES*)

O responsável pelo tratamento e o subcontratante organiza e conserva um registo de todas as atividades de tratamento dos dados pessoais sob a sua responsabilidade, que possa ser disponibilizado à autoridade de controlo, do qual devem constar, entre outros, a descrição das categorias de titulares de dados e das categorias de dados pessoais, as finalidades do tratamento de dados, e uma descrição geral das medidas técnicas e organizativas no domínio da segurança do tratamento.

Ficam dispensadas desta obrigação as entidades com menos de 250 trabalhadores, salvo se o tratamento efetuado for suscetível de implicar um risco para os direitos e liberdades das pessoas singulares, não for ocasional ou abranja as categorias especiais de dados ou dados pessoais relativos a condenações penais e infrações.

Normas legais: artigo 30.º do RGPD.

L. AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS (*PRIVACY IMPACT ASSESSMENT*)

O responsável pelo tratamento, antes de iniciar o tratamento de dados pessoais que seja suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos dados, deve proceder a uma avaliação do impacto das operações de tratamento previstas sobre a proteção de dados pessoais.

Normas legais: artigo 35.º do RGPD

M. VIOLAÇÃO DE DADOS PESSOAIS (*PERSONAL DATA BREACH*)

Violação da segurança que provoca, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação não autorizada de dados pessoais transmitidos, conservados ou tratados de outro modo, ou o acesso não autorizado a esses dados. Quando a violação de dados pessoais possa resultar em riscos para os direitos e liberdades dos titulares dos dados, a mesma pode dar origem a obrigação de comunicação à autoridade de controlo e aos titulares dos dados afetados.

Normas legais: artigos 33.º e 34.º do RGPD.

N. RESPONSÁVEL PELO TRATAMENTO DOS DADOS (*DATA CONTROLLER*)

Entidade singular ou coletiva, pública ou privada, que isolada ou conjuntamente determina a forma como os dados são tratados e a finalidade desse mesmo tratamento.

Exemplo 1: A entidade que disponibiliza formulários online e onde recolhe dados dos utilizadores do site, utilizando estes dados para prestar serviços aos seus utilizadores.

Exemplo 2: A entidade que solicita dados dos seus clientes para efeitos de faturação de serviços ou comercialização de bens.

Normas legais: artigo 24.º, 26.º e 27.º do RGPD.

O. SUBCONTRATANTE (*DATA PROCESSOR*)

Pessoa que trata os dados pessoais por conta do responsável pelo tratamento;

Exemplo: Entidade externa que trabalha com CRM usando dados do responsável pelo tratamento.

Normas legais: artigos 27.º e 28.º do RGPD.

P. ENCARREGADO DA PROTEÇÃO DE DADOS (*DATA PROTECTION OFFICER*)

Entidade designada pelo responsável pelo tratamento e pelo subcontratante que é envolvido de forma adequada e em tempo útil, a todas as questões relacionadas com a proteção de dados pessoais, o qual informa e aconselha o responsável pelo tratamento em matérias de proteção de dados pessoais; controla a conformidade legal dos procedimentos internos do responsável pelo tratamento; presta aconselhamento; coopera com as autoridades de controlo; assumindo também as funções de ponto de contacto entre o responsável pelo tratamento e as autoridade de controlo sobre questões relacionadas com o tratamento.

Normais legais: artigos 37.º a 39.º do RGPD.

Q. CÓDIGO DE CONDUTA (*CODE OF CONDUCT*)

Um código de conduta de proteção de dados é um conjunto de regras especificando a aplicação do RGPD e contribuindo para a sua correta aplicação em contextos específicos de tratamento de dados ou em determinados setores de atividade ou para pequenas e médias empresas. Deve conter mecanismos que permitam a monitorização compulsiva da sua aplicação e pode conter normas sobre resolução extrajudicial de litígios. O código de conduta pode ser preparado por associações ou outros organismos representativos de categorias de responsáveis pelo tratamento ou subcontratantes, carecendo de aprovação pela autoridade de controlo. Ficam sujeitos ao cumprimento do código de conduta todos aqueles que a ele aderirem

Normas legais: artigos 40.º e 41.º do RGPD.

R. CERTIFICAÇÃO (*CERTIFICATION*)

A certificação, selos ou marcas em proteção de dados são mecanismos de demonstração de cumprimento das normas do RGPD, sendo a sua atribuição efetuada a quem voluntariamente a solicitar por um organismo de certificação que tenha sido reconhecido como tal pela autoridade de controlo em função da sua independência e competência.

Normas legais: artigos 42.º e 43.º do RGPD.

S. AUTORIDADE DE CONTROLO (*SUPERVISORY AUTHORITY*)

Autoridade pública independente responsável pela fiscalização da aplicação do RGPD, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União Europeia. As autoridades de controlo contribuem ainda para a aplicação coerente do regulamento em toda a União.

Exemplo: Em Portugal, o papel de autoridade de controlo caberá à Comissão Nacional de Proteção de Dados (CNPD).

Normas legais: artigos 51.º a 59.º do RGPD.

Direitos dos titulares dos dados pessoais no âmbito da proteção de dados pessoais

A. DIREITO À COMUNICAÇÃO TRANSPARENTE

Por forma a assegurar que os dados pessoais são tratados de forma lícita, legal e transparente os responsáveis pelo tratamento devem prestar aos titulares dos dados pessoais um conjunto de informação mínima legal e necessária, nomeadamente, mas sem exceção quanto à recolha e tratamento dos seus dados. O Regulamento obriga os responsáveis pelo tratamento a fornecer essas informações de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças.

Normais legais: artigo 5.º, 12.º, 14.º do RGPD

B. DIREITO À INFORMAÇÃO BÁSICA

Os titulares dos dados pessoais têm direito a receber, do responsável pelo tratamento dos seus dados pessoais, um conjunto de informação básica prévia à recolha e tratamento dos seus dados. Informação quanto à identidade e os contactos do responsável (pessoa coletiva ou individual) pelo tratamento, quais as finalidades da recolha e tratamento dos dados pessoais concretamente recolhidos.

Normais legais: artigo 13.º e 14.º do RGPD

C. DIREITO DE ACESSO DO TITULAR DOS DADOS

O novo RGDPR concede o direito aos titulares dos dados pessoais de exercerem os seus direitos sobre os responsáveis pelo tratamento dos seus dados pessoais, desta forma o RGDPR obriga os responsáveis pelo tratamento

de dados pessoais a fornecer aos titulares desses dados um conjunto vasto de informação e de acesso aos dados pessoais recolhidos.

Assim os titulares dos dados pessoais têm direito a obter a seguinte informação:

a) Confirmação se os seus dados pessoais estão ou não estão a ser objeto de tratamento e se for caso disso aceder aos seus dados pessoais;
b) Obter informação quanto à finalidade do tratamento dos seus dados pessoais;
c) Obter informação quanto as categorias dos dados pessoais em questão;
d) Obter informação relativa aos destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados
e) Informação relativa ao prazo de conservação dos dados (ou o critério usado para a determinação desse prazo de conservação);
f) Informação relativa à existência dos direitos de retificação, apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento.
g) Informação relativa ao direito de apresentar reclamação a uma autoridade de controlo;
h) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;
i) Informações sobre a existência de, e uma explicação da lógica envolvida, sobre qualquer processamento automatizado que tenha um efeito significativo nas pessoas em questão.
j) J) Os titulares dos dados pessoais podem solicitar uma cópia dos dados pessoais que se encontram a ser objeto de tratamento.

Normais legais: artigo 15.º do RGPD

Nota: O cumprimento deste direito poderá ser cumprido através da prestação de informação por parte da empresa aos seus trabalhadores a partir de um portal interno da empresa (intranet), ou qualquer meio equivalente.

D. DIREITO DE RETIFICAÇÃO

Os Responsáveis pelo tratamento de dados pessoais devem assegurar aos titulares dos dados pessoais o direito destes retificarem os seus dados pessoais que estejam inexatos ou incompletos.

Normais legais: artigo 5.º n.º 1 alínea d) e artigo 16.º do RGPD

E. DIREITO AO APAGAMENTO DOS DADOS (DIREITO A SER ESQUECIDO)

Os titulares de dados pessoais têm o direito de exigir ao responsável pelo tratamento dos seus dados pessoais que o mesmo apague os seus dados, sem demora justificada, sempre que:

Os dados pessoais deixaram de ser necessários para a finalidade que originalmente fundamentou a sua recolha.

O titular dos dados pessoais retira o seu consentimento e não há qualquer outro fundamento legal para o tratamento dos seus dados pessoais.

O titular dos dados pessoais opõe-se ao tratamento, e não existem interesses legítimos prevalecentes que justifiquem o tratamento (ver infra Direito de Oposição).

Os dados pessoais foram tratados ilicitamente.

Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito.

Normais legais: artigo 17.º do RGPD

F. DIREITO À LIMITAÇÃO DO TRATAMENTO

Em certos casos o titular dos dados pessoais não terá direito a requerer o apagamento dos seus dados perante o responsável pelo tratamento, antes terá apenas o direito a limitar o seu tratamento, nos seguintes casos:

Se a exatidão dos dados foi contestada pelo titular dos dados pessoais e apenas durante o período de tempo necessário a confirmar a sua exatidão;

Se o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;

O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

No caso de exercício do direito de oposição por parte do titular dos dados pessoais, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

Normais legais: artigo 18.º do RGPD

G. OBRIGAÇÃO DE NOTIFICAÇÃO DA RECTIFICAÇÃO OU APAGAMENTO OU LIMITAÇÃO DO TRATAMENTO

Só será possível efetivar os direitos dos titulares dos dados pessoais se todas as entidades envolvidas no tratamento dos dados pessoais tiverem conhecimento que o seu titular exerceu esses mesmos direitos.

O RGDP estabelece assim uma obrigação para os responsáveis pelo tratamento de dados pessoais de notificar quaisquer terceiros com os quais tenham compartilhado os dados pessoais relevantes, mais informando dos direitos que o titular exerceu ou pretende exercer quanto à retificação, apagamento ou limitação do tratamento.

Os titulares dos dados pessoais podem solicitar informação ao responsável quanto às entidades terceiras com quem partilhou a sua informação.

Normais legais: artigo 19.º do RGPD

H. DIREITO DE PORTABILIDADE DOS DADOS

Os titulares dos dados pessoais têm o direito de receber uma cópia dos seus dados pessoais num formato estruturado, de uso corrente e de leitura automática e o direito de transferir os seus dados pessoais de um responsável para outro ou de ter os seus dados pessoais transmitidos diretamente entre responsáveis.

Normais legais: artigo 20.º do RGPD

Notas: O ficheiro PDF não será considerado com um ficheiro estruturado e adequado a cumprir com a formalidade constante desta norma. O fornecimento de informação encriptada será considerado uma boa prática.

I. DIREITO DE OPOSIÇÃO

O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.º, nº 1, alínea e) ou f), ou no artigo 6.º, n.º 4, incluindo a definição de perfis com base nessas disposições.

Falamos concretamente da possibilidade do titular dos dados poder opor-se a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito e que sejam i) necessários ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento, ou ii) necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento, ou por último iii) tratamento de dados para fins de segurança de estado, defesa, segurança pública, prevenção, justiça, etc.

O responsável pelo tratamento terá que cessar o tratamento dos dados pessoais, sempre que o titular exerça o seu direito de oposição, a não ser que apresente razões imperiosas e legítimas para esse tratamento as quais prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Em suma: O direito de oposição dos titulares dos dados pessoais não é um direito absoluto, pelo que tem de ser obrigatoriamente conjugado com razões e

motivações imperiosas e legítimas que podem justificar, em determinados casos, o tratamento de dados pessoais mesmo contra a vontade expressa do seu titular.

Normais legais: artigo 21.º do RGPD

J. DIREITO DE OPOSIÇÃO – COMERCIALIZAÇÃO DIRECTA

Nas situações em que os dados pessoais forem tratados para efeitos de comercialização direta (marketing direto / mail marketing), o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito Esta oposição abrange a definição de perfis, na medida em que esteja relacionada com a comercialização direta.

Nestes casos, quanto do titular se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais tem de ser obrigatoriamente deixados de ser tratados.

Normas legais: Artigo 21.º, n.º 2 e 3.

K. OBRIGAÇÃO DE INFORMAR OS TITULARES DOS DADOS QUANTO AO DIREITO DE OPOSIÇÃO

O responsável pelo tratamento dos dados pessoais tem a obrigação de informar o titular da possibilidade de oposição ao tratamento logo no primeiro momento em que se dirija ao titular.

Normas legais: Artigo 13.º, n.º 2 alínea b); 14 n.º 2 alínea c); 15.º, n.º 1 alínea e).

RGPD ao longo do ciclo de vida do software

A introdução do Regulamento Geral da Proteção de Dados (RGPD) enceta para a maioria das organizações da União Europeia novas obrigações de conformidade.

O RGPD tem muito que ver com o âmbito e a forma como os dados pessoais são processados. Isto é, como são adotados os procedimentos e as políticas necessárias caso a caso para a recolha, salvaguarda e tratamento dos dados dos cidadãos, tendo presente à partida que são exigidas às organizações evidências destes aspetos.

O desafio é tanto maior quanto maior forem as dinâmicas sociais das organizações, os seus processos e a complexidade das suas relações. É nos produtos de software que está assente a gestão e o controlo da generalidade destes processos, sendo por essa razão correto afirmar-se que o impacto do RGPD no que ao software diz respeito é enorme, em especial no seu ciclo de desenvolvimento.

Arriscamos a dizer, inclusive, que nenhuma outra matéria com carácter legal teve tanto impacto no ciclo de vida do software e nos correspondentes processos de adaptação das organizações como esta. Isso acontece porque se trata de um projeto de dimensão Europeia, em primeiro lugar, mas também pela sua abrangência em termos globais, considerando que a UE, os seus cidadãos e as suas organizações têm relações com praticamente todo o mundo.

O ciclo de vida de desenvolvimento software é normalmente referenciado num modelo em seis fases: **1) análise e definição de requisitos** (o que fazer); **2) projeto** (como fazer); **3) implementação** (fazer); **4) testes** (testar); **5) colocação em produção** e **6) manutenção**. Estas seis 6 fases são essenciais para a concretização de bons projetos de software e nos dias que correm já não existe nenhuma software house que, independentemente da metodologia ou metodologias adotadas (Agile, DevOPS, entre outras), não tenha em consideração estas fases na execução dos seus projetos.

Neste documento indicamos alguns aspetos que consideramos serem, pontos de partida, essenciais para o cumprimento dos requisitos do RGPD ao longo do ciclo de vida do software. Em muitos casos serão necessárias alterações de fundo às aplicações, que irão desde a arquitetura ao transporte de dados e naturalmente às interfaces de utilização. Somos, por isso, em crer que o sucesso dos projetos estará

pendente da análise dos requisitos do RGPD logo nas primeiras fases do desenvolvimento.

Boas práticas para o desenvolvimento de software

1. **Desenho e arquitetura do sistema (privacy by design)**
    a. Identifique desde logo as necessidades de recolha e tratamento de dados pessoais na primeira fase do ciclo de desenvolvimento.
    b. Tenha em atenção a proporcionalidade da recolha de dados pessoais.
    c. Realize um PIA (Privacy Impact Assessment).

> O RGPD estabelece a necessidade de implementação de medidas técnicas adequadas para a proteção dos dados pessoais, sendo igualmente claro que "por default" estes apenas podem ser tratados para os fins a que se destinam.
> Importa assim ter perfeitamente identificados, logo nas primeiras fases de desenvolvimento, os ambientes em que são tratados dados pessoais.
> Ao contemplar necessidades no domínio da recolha, tratamento e os fins para que são usados os dados pessoais tornará o desenho e arquitetura do software muito mais eficaz na resposta às disposições previstas no Regulamento.

2. **Segurança, confidencialidade e integridade**
    a. Desenvolva e implemente uma política de segurança de informação na sua organização.
    b. Implemente sempre mecanismos de autenticação nas suas aplicações.
    c. Estabeleça níveis de acesso à informação em função do perfil e dos privilégios dos utilizadores, tendo em atenção o acesso a dados pessoais.
    d. Dote as suas aplicações de registos de auditoria de sistema (logs).
    e. O uso de técnicas de pseudonimização e encriptação são necessários sempre que existam dados sensíveis, devendo ser adequados ao tipo de dados a proteger (de acordo com a política de segurança de informação e a avaliação de risco documentada do PIA).

> O uso de meios técnicos para a segurança dos dados está igualmente previsto no RGPD. Sempre que possível e nos casos em o grau de sensibilidade da informação assim o obrigue, recomenda-se a implementação de técnicas de encriptação ou pseudonimização dos dados por forma a assegurar a sua confidencialidade.

3. Âmbito e autorização explícita para recolha e tratamento de dados

Esta é uma responsabilidade exclusiva do responsável pelo tratamento dos dados, no entanto:

a. Por omissão deve ser garantida a privacidade de todos os dados pessoais (privacy by default).
b. Todas as alterações às definições por omissão devem ser registadas (logs), previamente autorizadas pelo titular dos dados e evidenciáveis.
c. Garanta que nos seus contratos existem as cláusulas necessárias por forma a determinar quem é o responsável e/ou o(s) subcontratante[1](es), relembrando que a responsabilidade relativa ao âmbito e à autorização da recolha cabe sempre ao responsável.
d. Caso pretenda disponibilizar opções para o registo do consentimento explícito para a recolha, consulta ou ainda atualização de dados pessoais pelo titular, é necessário garantir que existe evidência de quem, quando e como deu autorização e respetivo âmbito, não podendo os dados serem tratados fora desse âmbito.
e. Evite dar o acesso direto aos dados pessoais, implementando serviços de disponibilização de dados a pedido, tais como API's ou webservices.

Privacy by default
A recolha e os restantes atos de tratamento de dados pessoais carecem de autorização explicita por parte do titular e apenas podem ser objeto de tratamento para um determinado âmbito.
O titular dos dados tem ainda o direito de aceder à informação que o responsável pelo tratamento dispõe sobre si e para que fins.

[1] Data Processor

4. **Portabilidade e acessibilidade de dados**
    a. Permita a exportação de todos os dados pessoais num formato aberto (open standard), sem comprometer a segurança e a privacidade da transmissão.
    b. Sempre que possível, adotar normas abertas para a transferência de dados entre subcontratantes (data processors), sem comprometer a segurança e a privacidade da transmissão.
    c. Previamente à portabilidade deve ser solicitado ao titular dos dados o seu consentimento e ser-lhe dado conhecimento dos dados a transmitir.

> Como vimos anteriormente, os titulares dos dados pessoais têm o direito de receber uma cópia dos seus dados pessoais num formato estruturado, de uso corrente e de leitura automática e o direito de transferir os seus dados pessoais de um responsável para outro ou de ter os seus dados pessoais transmitidos diretamente entre responsáveis.
> Considerado que a informação pode variar se setor para setor, no caso da transferência de dados entre responsáveis é expectável que venham a ser adotados esquemas de comunicação segura e modelos de informação estruturada de acordo com as necessidades de cada um.
> Recomendamos a preferência pelo uso de formatos abertos, como é o caso do XML.

5. **Apagamento e minimização da informação disponível**
    a. Reavalie o modelo de dados e, no limite, crie funcionalidades que permitam apagar dados pessoais sem comprometer a integridade da informação de negócio ou qualquer outro tipo de detalhe.
    b. Tenha formas de evidenciar que o apagamento ou a destruição dos dados e que o mesmo a aconteceu a pedido do titular ou pela extinção do âmbito.
    c. Os dados que por razões legais sejam excluídos do direito ao apagamento devem ser segregados por forma a evitar acesso não autorizado.

> O direito ao esquecimento (apagamento) consiste num dos direitos fundamentais do RGPD. Quer isto dizer que o titular pode revogar parte ou a totalidade da autorização concedida ao responsável pelo tratamento dos seus dados e ainda requerer que os mesmos sejam apagados, sem demora injustificada.
> Para além disso, o regulamento também estabelece que os dados devem ser guardados apenas durante o tempo estritamente necessário.
> Observando estes aspetos, resulta desde logo que os sistemas devem estar dotados da possibilidade de eliminação de dados pessoais mediante pedido expresso ou ainda da sua supressão (armazenamento) dos ambientes produtivos, sem comprometer a arquitetura, o modelo de dados e consecutivamente o bom funcionamento do software.
> Importa, porém, ter presente que em algumas circunstâncias poderão existir impeditivos ao apagamento dos dados pessoais. É por exemplo o que se sucede nos casos em que por força de Lei os dados pessoais tenham que permanecer acessíveis.
> Nos casos em que isso acontece, recomendamos que sejam restabelecidas as funcionalidades de proteção “by default”, armazenando, sempre que possível, esses dados apenas para os fins legais em causa, inutilizando-os e excluindo-os do acesso para outros fins que não aquele(s).

6. **Atenção ao “profiling”**
    a. Não efetue tratamento nem combine dados pessoais para os quais não tem autorização do titular.
    b. Tenha em atenção metadados, identificadores pessoais (PiD) e a recolha de dados pessoais provenientes de serviços de “Singe Sign On”.
    c. Caso esteja a utilizar dados pessoais tornados públicos, deve evidenciar que à data da recolha estes eram públicos, sem prejuízo de

mais tarde o titular dos dados poder reivindicar os seus direitos de acesso, correção e apagamento.

Por exemplo, na Internet as pessoas usam um conjunto de identificadores pessoais (PiD) para aceder aos serviços disponibilizados pelos fornecedores de soluções. Fazem-no, por exemplo, para se autenticarem em websites, em dispositivos, em apps, etc.
Estes identificadores quando são processados em conjunto com outros registos pessoais conhecidos dão origem ao que se define por “profiling”.
É ilícito todo e qualquer ato de tratamento de dados pessoais que não esteja explicitamente autorizado pelo respetivo titular.
Tenha por isso especial atenção ao “profiling”. Assegure que todos os dados pessoais são processados de acordo com as regras de proteção previamente estabelecidas e que o titular tem conhecimento das mesmas.