



Universidade do Minho

Mestrado Integrado em Engenharia Informática

ENGENHARIA DE SEGURANÇA

Trabalho TP5

Grupo 2

Paulo Gameiro - A72067

Pedro Rodrigues - PG41092

Rafaela Soares - A79034

Braga, Portugal
29 de Março de 2020

Conteúdo

| | | |
|----------|---|----------|
| 1 | Experiência 1.1: Regulamento (UE) 2016/679 (RGPD) | 2 |
| 2 | Pergunta 1.1: <i>Data protection by default in practice</i> (secção 3) | 3 |
| 2.1 | 1º Critério: Quantidade mínima de dados pessoais | 3 |
| 2.2 | 2º Critério: Extensão mínima do processamento dos dados pessoais | 3 |
| 2.3 | 3º Critério: Período mínimo de armazenamento dos dados pessoais | 3 |
| 2.4 | 4º Critério: Acessibilidade mínima dos dados pessoais | 3 |
| 3 | Experiência 1.2 | 4 |
| 4 | Experiência 1.3 | 5 |
| 5 | Pergunta P1.2: <i>Recruitment</i> | 6 |

1 Experiência 1.1: Regulamento (UE) 2016/679 (RGPD)

O Regulamento (UE) 2016/679 (RGPD) tem como intuito advogar o tratamento de dados pessoais como um direito fundamental e garantir a livre circulação destes entre os Estados-Membros.

Como a garantia de segurança de um sistema informático, neste contexto, parece, cada vez mais, exigir uma consciencialização acrescida por parte de quem concede o sistema, uma vez que, atualmente, são disponibilizados diversos produtos de *software*, que gerem informações pessoais, este regulamento pode influenciar positivamente o desenvolvimento de *software*, caso as medidas definidas por este sejam cumpridas.

Para além de ser necessário ter em consideração os princípios relativos ao tratamento de dados pessoais (Artigo 5.º), de forma a transmitir, com clareza, aos utilizadores a finalidade do tratamento dos seus dados, é necessário também estar ciente de que a proteção de dados se inicia na primeira instância do processo de conceção (Artigo 25.º).

Posto isto, só "devem ser tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento"(Schulz,2016,p.48).

A segurança de tratamento (Artigo 32.º) também tem um papel fulcral no desenvolvimento de *software*. Medidas como "pseudonimização e a cifragem dos dados pessoais", "capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento", "capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico" e "processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento" são necessárias para estabelecer um nível de segurança apropriado (Schulz,2016,p.51-52).

Para que tudo isto seja, de certeza forma, monitorizado, tem de se designar um encarregado da proteção de dados (Artigo 37.º). Este deve ser envolvido em "todas as questões relacionadas com a proteção de dados pessoais"(Artigo 38.º), no intuito de colocar em prática as suas incumbências (Artigo 38.º). Estas são informar e aconselhar os envolvidos, controlar a conformidade, cooperar com a autoridade de controlo e considerar riscos.

Em suma, acredita-se que, se no primeiro momento de desenvolvimento de *software*, já se tiver como foco a conformidade com o RGPD, é possível estabelecer procedimentos que façam jus à proteção de dados.

2 Pergunta 1.1: *Data protection by default in practice* (secção 3)

Apresenta-se, de seguida, algumas práticas recomendadas para definir os padrões de proteção de dados.

2.1 1º Critério: Quantidade mínima de dados pessoais

No contexto de minimização de dados, destacam-se diversas práticas, sendo a mais óbvia a "Quanto menos dados, melhor".

Práticas como coleta granular de dados com base na necessidade, uso de tecnologias para melhorar a privacidade, mínimo diferente por finalidade, minimização de risco e consideração de todas as cópias e tipos de dados permitem minimizar a quantidade de dados.

2.2 2º Critério: Extensão mínima do processamento dos dados pessoais

A prática "Quanto menos processamento, melhor" não implica reduzir o número de operações, mas sim minimizar o risco dos direitos e liberdades das pessoas singulares. É necessário que os desenvolvedores pensem em formas de evitar o armazenamento permanente, se houver finalidades em que tal não seja necessário.

2.3 3º Critério: Período mínimo de armazenamento dos dados pessoais

Foca-se na prática "Quanto menor, melhor", isto é, quanto menor for o período de armazenamento dos dados pessoais, melhor, uma vez que o objetivo é que este seja minimizado. De referir que tal não se limita apenas à base de dados, mas também às cópias temporárias ou dados pessoais nas entradas de *log*.

2.4 4º Critério: Acessibilidade mínima dos dados pessoais

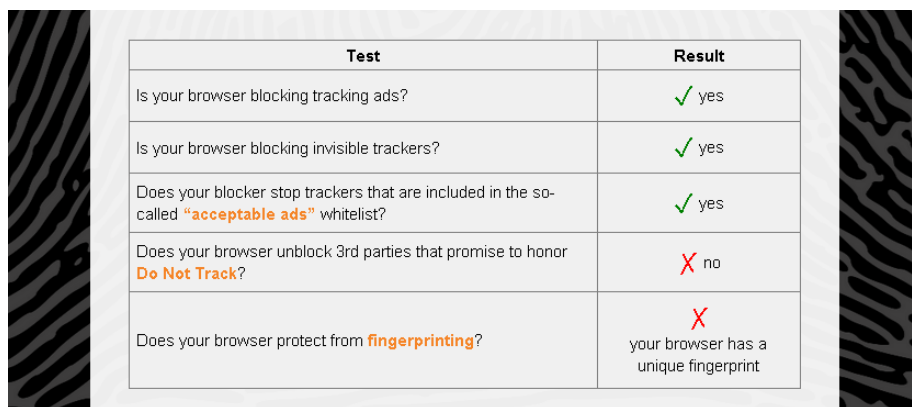
A acessibilidade mínima de dados pessoais pode ser garantida através das seguintes práticas: restringir o acesso com base na necessidade (política de acesso e controle de acesso), limitar as formas de partilha (a acessibilidade aumenta se os dados pessoais forem copiados) e nenhum público por padrão sem intervenção ativa (impedir que dados pessoais sejam tornados públicos por padrão).

Importante mencionar que, por vezes, os "padrões de *design* específicos têm como objetivo direcionar os usuários para escolhas não amigáveis à privacidade", pelo que é necessário estabelecer um equilíbrio, de forma a que os utilizadores possam exercer os seus direitos.

3 Experiência 1.2

Após a análise da tabela 1 do documento "*Online privacy tools for the general public - Towards a methodology for the PETs for internet mobile users*", foram feitas as seguintes experiências:

- Utilizar a ferramenta Panopticklick da Electronic Frontier Foundation (EFF) para verificar se o seu *browser* é seguro contra *tracking*, em que o resultado foi o seguinte:



| Test | Result |
|--|--|
| Is your browser blocking tracking ads? | ✓ yes |
| Is your browser blocking invisible trackers? | ✓ yes |
| Does your blocker stop trackers that are included in the so-called "acceptable ads" whitelist? | ✓ yes |
| Does your browser unblock 3rd parties that promise to honor Do Not Track? | ✗ no |
| Does your browser protect from fingerprinting? | ✗ your browser has a unique fingerprint |

Figura 1: Exemplo de estruturação da base de dados.

- A PRISM disponibiliza um *site* em que indica, consoante o serviço que se utiliza, quais as aplicações que se deve ou não utilizar, caso se queira preservar a privacidade. Por exemplo, para utilizadores do sistema operativo Windows, deve-se evitar utilizar os *browsers* Google Chrome, Opera, Microsoft Edge e deve-se utilizar o Firefox ou Tor Browser;
- No security in-a-box é abordado o dilema de encriptar os dados pessoais ou não, se nos incrimina ou faz nos parecer criminosos com algo a esconder e alternativas de como salvaguardar dados pessoais.
- O *site* privaytools.io disponibiliza uma data de recomendações para todas as pessoas que queiram perceber como certas aplicações estão a comprometer a sua privacidade e respetivas alternativas.

4 Experiência 1.3

Os nove critérios mencionados são :

- Avaliação ou pontuação, um exemplo disso podem ser uma instituição financeira que rastreia seus clientes numa base de dados de referência de crédito
- Tomada de decisões automatizadas com impactos significativos legal ou semelhantes
- Monitorização sistemática, processo usado para observar, monitorizar ou controlar titulares de dados, incluindo dados recolhidos através de redes ou "um monitorização sistemática de uma área acessível ao público"
- Dados sensíveis ou de natureza altamente pessoal, isto inclui categorias especiais de dados pessoais. Um exemplo seria um hospital guardar os dados médicos de um paciente
- Processamento de Dados em grande escala, o GDPR não define o que constitui grande escala
- *Matching* ou combinando conjunto de dados
- Dados relativos a pessoas vulneráveis
- Uso inovativo ou aplicar novas tecnologias ou soluções organizacional, por exemplo combinar o uso de impressões digitais e reconhecimento de rosto para melhorar o controle de acesso físico
- Quando o processamento em si "impede os titulares de dados de exercer um direito ou usar um serviço ou contrato"

De seguida, o projeto escolhido consiste num programa de gestão de utilização de tempo, onde todos os dados de utilização do sistema operativo como programas de email, editores de texto, IDE's, git, chamadas, sms e localizações GPS são guardadas para inferir quando é que o utilizador esteve a trabalhar e em atividades de lazer.

Deste modo, irá-se satisfazer os critérios:

- Processamento de dados em grande escala;
- Dados relativos a pessoas vulneráveis, visto que um menor pode usar o computador que está a ser analisado/monitorizado;
- Dados sensíveis ou de natureza altamente pessoal.

De referir que o *template* DPIA está preenchido e carregado no repositório.

5 Pergunta P1.2: *Recruitment*

Esta secção tem como objetivo apresentar os padrões para a proteção de dados na prática. O recrutamento de pessoal é um processo executado pelo Recursos Humanos e consiste em inúmeras atividades organizacionais destinadas à seleção de pessoas que possuem habilidades específicas ou são capazes de executar determinadas tarefas.

Após a publicação do aviso de vaga, os candidatos são convidados a enviar os seus *curriculum vitae* electronicamente. O *curriculum vitae* por norma tem a formação e qualificações académicas descritas, experiência de trabalho, treinamento profissional ou académico adicional, detalhes pessoais, como nome e sobrenome, endereço, números de telefone, data de nascimento.

O comité de selecção analisa e avalia as inscrições e apresenta uma lista de candidatos a serem convidados para uma entrevista. Durante a entrevista, os membros do comité de selecção anotam o desempenho do candidato e, no final, redigem um relatório detalhado que é submetido à alta gerência. O processamento é facilitado por um sistema de TI que suporta o envio de solicitações, a lista de candidatos e os relatórios de entrevistas e é operado por um funcionário de Recursos Humanos.

Segundo a análise de impacto, as consequências da perda de confidencialidade, perda de integridade e perda de disponibilidade é considerado de impacto médio.

Além das suposições feitas neste exemplo, pode haver casos em que o impacto geral possa ser maior do que o calculado acima. Por exemplo, esse poderia ser o caso de um processo de avaliação incluindo testes psicológicos ou características comportamentais específicas dos candidatos. Outro caso poderia ser se os dados pessoais relacionados a deficiências, origem étnica, entre outros não menos relevantes, também forem processados.

Após a avaliação, a probabilidade geral de ocorrência de ameaças é calculada como BAIXA, tendo como destaque as partes envolvidas no processamento de dados pessoais em que a probabilidade é média, porque pode incluir um grande número de empregados envolvidos no processamento e é assumido que parte dos empregados não têm formação em segurança da informação.

Em particular, de forma geral, o risco deste *use case* é considerado médio, mas muito dependente das condições de processamento.