

Universidade do Minho



Mestrado Integrado em Engenharia Informática
Engenharia de Segurança

Aula 6 - 30/Mar/2020

Grupo 8



João de Macedo
A76268



João Aloísio
A77953



Nelson Gonçalves
A78173

30 de Março de 2020

1 Experiência 1.1

Para a resolução desta experiência o grupo optou por analisar o documento *Handbook on European data protection law*, mais concretamente a secção 6.1.5, que define o direito à portabilidade de dados. Na sua definição, pode-se definir duas entidades existentes de um processo em que, um denomina-se como o controlador, sendo este a entidade que processa os dados pessoais do sujeito, e o outro o sujeito, que é identificado pelos dados pessoais possuídos pelo controlador.

Este direito é aplicado no lado do sujeito, sendo o controlador a ter o dever de providenciar as ferramentas para que o sujeito possa usufruir desse direito. É aplicado com a existência de um consentimento ou de um contrato entre ambos.

O direito à portabilidade dos dados, resume-se na possibilidade do sujeito transmitir os seus dados pessoais de um controlador para outro. Tendo isto em conta, este direito segue-se por 4 critérios:

- O sujeito tem o direito de receber os seus dados pessoais numa forma estruturada, num formato comum e legíveis por uma máquina;
- O sujeito tem o direito de transmitir os seus dados pessoais de um controlador para o outro, sem obstáculos técnicos nesse processo;
- O controlador não é responsável pela conformidade com a lei de protecção de dados do destinatário dos dados pessoais de um sujeito, após pedido de portabilidade realizado pelo mesmo;
- O exercício deste direito não influencia qualquer outro direito declarado no RGPD;

No desenvolvimento do software, com estes critérios, é necessário ter preocupações adicionais, visto que este tem que estar conforme a lei de protecção de dados, incluindo assim o direito à portabilidade de dados.

Concluindo assim que é necessário no desenvolvimento do software, os dados devem estar sempre disponíveis para serem recolhidos e reunidos por um sujeito, num formato comum que permita a este transmitir para um outro controlador, podendo este ter outro tipo de software e mesmo assim conseguir utilizar, pois este se encontra num formato comum.

2 Pergunta 1.1

2.0.1 Melhores práticas para protecção de dados por default

Após ler a secção proposta do documento sobre **Data protection by default in practice** verificamos que as práticas recomendadas para os "default settings" estão divididas em

nos critérios explicados posteriormente. Apesar desses critérios apenas servirem para dar exemplo de como proteção de dados "by default" pode ser aplicado na prática.

- **Critério 1 : Quantidade mínima de informação pessoal**

- Quanto menos dados/informação melhor : Focar-nos na informação "need-to-know", por exemplo, ao pedir a um utilizador para preencher um formulário, apenas dados essenciais devem ser obrigatórios.
- Colectar informação gradualmente consoante a necessidade: Por exemplo, num site de compras online, o utilizador deve primeiro decidir o que e se quer comprar algo e só depois pedir o endereço de envio.
- Uso de tecnologias para melhorar a privacidade : Utilizar técnicas de pseudonimização ou criptografia, por exemplo, cenários e-commerce onde o site tem de validar a idade, em vez de a armazenar pode utilizar um mecanismo de IDcard onde em vez de guardar/requesitar a data de nascimento apenas faz um request ao IDcar (que se associa ao utilizador) e devolve-lhe a idade.
- Diferentes mínimos consoante a finalidade : Dependendo da finalidade a quantidade mínima de informação pode ser diferir, por exemplo, nas apps moveis o uso do microfone não pode ser uma definição default geral, apesar de em alguns casos seja essencial.
- Minimizar o risco : Para determinar a quantidade mínima de informação a ser armazenada, além do tamanho a nível de bits e bytes serem importantes o objetivo também é reduzir o risco preferindo dados/informação menos sensíveis.
- Considerar todas as cópias e tipo de dados : Reduzir copias temporárias ou transferência de dados. Se não forem essenciais não devem ser armazenados por default.

- **Critério 2: Mínimo de processamento de dados pessoais**

- Quanto menos processamento melhor : Reduzir o processamento de dados não significa reduzir o numero de operações sobre este mas sim reduzir o risco associado á liberdade e direitos naturais das pessoas.
- Ferramentas de autorização do utilizador : Oferecer ao utilizador fácil e rápido acesso aos seus dados, por exemplo uma dashboard.

- **Critério 3: Tempo mínimo de armazenamento de dados pessoais**

- Armazenamento - quanto menos tempo melhor : O tempo de armazenamento de dados deve ser o mínimo, as vezes armazenamento permanente não é necessário.

- **Critério 4 : Mínimo acessibilidade dos dados pessoais**

- Restringir o acesso tendo em conta a necessidade
- Limitar os métodos de partilha de informação
- Sem padrão default sem intervenção activa

2.0.2 Defaults e usabilidade

Os padrões default são um parâmetro importante para melhorar a usabilidade em sistemas e aplicações, permitindo o uso simples pois não requer o utilizador de efectuar múltiplas escolhas. Isto contribui para um sistema "user-friendly".

Apesar de as definições/padrões default serem um parâmetro importante na usabilidade de um sistema é deveras importante que estes não escondam certos aspectos ou funcionalidades do utilizador.

Deve-se ter em conta para que as definições default de protecção de dados não tornem a aplicação difícil e não intuitiva de utilizar e para que esta situação seja modificado devemos alterar as definições. Esta realidade é muito comum em que a "opção de privacidade" é muito mais complexa que a alternativa. No entanto os padrões não devem ser projectados de forma tão impactante para a usabilidade do sistema.





3 Experiência 1.2

- Ao utilizar a ferramenta Panopticlick da Electronic Frontier Foundation (EFF) para verificar se o browser é seguro contra tracking obtemos o seguinte resultado:

How well are you protected against non-consensual Web tracking? After analyzing your browser and add-ons, the answer is ...

Yes! You have **strong protection against Web tracking**, though your software isn't checking for Do Not Track policies.

Help us defend the Web against tracking:

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

[Show full results for fingerprinting](#)

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

Figura 1

- Após uma pesquisa No PRISM Break verificamos que aplicações devem ser evitadas e aquelas que deve preferir consoante o Sistema operativo. Como por exemplo :
 - Andoird: Evitar utilizar a "google play"e passar a utilizar o "F-Droid"
 - Linux: Evitar utilizar o "Google public dns"e passar a utilizar o "Namecoin"ou o "dnscrypt-proxy"
 - Windowns: Evitar utilizar o "Gmail"e passar a utilizar o "ThunderBird"
- Para proteger ficheiros sensíveis no seu computador podemos utilizar estratégias tais como:
 - Encriptar informação : Medidas de protecção como o sistema de log in do sistema operativo não é suficiente, visto que há maneiras de "bypass"esse sistema, então devemos encriptar informação que consideramos sensível, desta forma apenas aqueles que tem acesso à chave de encriptação pode ter acesso à informação.
 - Guardar informação sensível é um risco, apesar de encriptar diminua esse risco, deve-se sempre reduzir ao máximo informação sensível que guardamos. Sempre

que não precisamos dessa informação devemos apaga-la correctamente do dispositivo.

- Esconder informação sensível: Um risco/problema de guardas este tipo de dados no nosso computador pessoal ou de trabalho, apesar de que devemos encriptar, esses dados não devem estar imediatamente visíveis, ou seja, não deve ser fácil "abusar" dos dados mesmo que sejam visualizados na sua forma de armazenamento.

—

- Tudo isto referido até agora deve ser implementado da forma correta, mais concretamente na encriptação, devemos então usar ferramentas confiáveis.

4 Experiência 1.3

4.1 Os 9 critérios

1. **Avaliação ou classificação**, incluindo desenhar um perfil ou prever, aspetos relativos ao desempenho laboral, estado económico, saúde, gostos pessoais ou interesses, confiabilidade ou comportamento, localização ou deslocamentos.
2. Processamento que envolve a **tomada de decisões com efeitos legais ou semelhantes significativamente**. Isto envolve que, durante o processamento, sejam tomadas decisões no lugar do utilizador, com os efeitos já referidos. Um exemplo disto seria o processamento de dados, que leva à exclusão ou discriminação de certos indivíduos.
3. **Monitorização sistemática**, ou seja, processamento que envolve observação, monitorização ou controlo de dados sobre indivíduos. Isto inclui dados coletados de redes ou monitorização sistemática em locais públicos. Isto é importante considerar, uma vez que podem ser adquiridos dados pessoais, em circunstâncias onde os indivíduos não estejam cientes de tal. Pior ainda, por vezes pode ser impossível que os indivíduos se apercebam que estão a ser coletados dados sobre eles, em locais públicos.
4. **Dados sensíveis ou de num carácter pessoal elevado**, isto inclui algumas categorias em específico definidas no *Artigo 9* (por exemplo, informação sobre ideias políticas dos indivíduos), como também dados pessoais relativos a convicções criminosas ou ofensas definidas no *Artigo 10*.
5. **Dados coletados numa grande escala**. O GDPR não define o que constituiu uma grande escala. No entanto, o *WP29* recomenda ter em conta os seguintes fatores, para determinar se um processamento é feito em grande escala. São os seguintes:
 - O número de indivíduos, cujos dados estão a ser recolhidos, quer seja um número em específico, ou uma proporção de população relevante;

- O volume de dados e/ou o alcance dos diferentes tipos de dados, que estão a ser processados;
 - A duração, ou permanência, atividade de processamento de dados.
 - A extensão geográfica da atividade de processamento.
6. Coincidir ou **combinar datasets**, por exemplo, de duas ou mais operações de processamento, realizadas com propósitos diferentes e/ou por donos dos mesmos diferentes.
 7. **Dados relativos a indivíduos vulneráveis**. Este tipo de processamento é um fator a ter em conta, uma vez que existe um desequilíbrio evidente entre a pessoa recolhe os dados, e o indivíduo cujos dados foram coletados. O que significa que, a decisão dos indivíduos, sobre o acordo ou oposição ao processamento, pode ser afetada mediante a sua posição. Este tipo de sujeitos inclui crianças, operadores, elementos da população que se encontrem debilitados e em qualquer outro caso, onde seja verificada uma relação desequilibrada entre os intervenientes.
 8. **Aplicação tecnológica ou soluções organizacionais**, que combinam o uso de impressão digital e reconhecimento facial, para melhorar o acesso físico.
 9. **Quando o processamento em si** restringe o indivíduo de exercer um direito ou usufruir de um serviço ou contrato. O que inclui operações de processamento que envolvem permitir, modificar ou refutar o acesso ou acordo com um contrato, por parte do indivíduo.

4.2 Projeto clínica privada

O projeto proposto consiste no desenvolvimento de uma aplicação para o agendamento de consultas numa clínica privada. Nesta aplicação é possível agendar consultas, ver o histórico e resumo de consultas, consultar as receitas médicas e ver o historial dos utentes. Para os utentes se registarem na aplicação têm de indicar o seu nome completo, idade, data de nascimento, número de utente e password. Aos médicos são fornecidas credenciais para posteriormente associarem o seu nome, password e especialidade. A clínica pode apagar a conta de um médico, no entanto a conta de um utente não poderá ser apagada. Portanto, este projeto proposto respeita os critérios 3 e 7 acima mencionados, pelo que seria necessário efetuar uma DPIA.

4.3 Template DPIA

O template encontra-se preenchido nesta diretoria com o nome *dpiaTemplate_GRUPO8*.

5 Experiência 1.4

O *pdf* encontra-se nesta diretoria com o nome *PIA - Privacy Impact Assessment*

6 Pergunta P1.2

O caso de uso designado para o nosso grupo foi o *Recruitment*. Sabendo isto, os passos da metodologia seguidos até à avaliação de risco são:

6.1 Definição da operação de processamento e o seu contexto

Os dados pessoais processados em *Recruitment* estão associados a um currículo com as suas aptidões académicas, primeiro e último nome, experiência profissional, morada, número de telemóvel, entre outros. Estes dados vão ser utilizados com o intuito de fazer uma seleção dos candidatos existentes para recrutar.

6.2 Avaliação do impacto

6.2.1 Perda de confidencialidade

A perda de confidencialidade pode levar à divulgação de dados pessoais que podem levar ao constrangimento ou até difamação dos candidatos, tais como qualidades pessoais. Por esse motivo, as plataformas de recrutamento providenciam uma estrutura de avaliação dos candidatos que baseiam-se especificamente em critérios profissionais e não inclui avaliações de tipos de personalidade ou características do candidato. Visto que a perda destes dados podem levar em alguns casos influenciar a probabilidade de ser empregue. O nível de impacto neste caso pode ser considerado em **MEDIUM**.

6.2.2 Perda de integridade

A perda de integridade pode ser considerada de nível **MEDIUM** porque caso haja alteração não autorizada de dados pessoais, podem influenciar se um candidato é ou não recrutado, sendo este não apto para o cargo.

6.2.3 Perda de disponibilidade

O nível de impacto na perda de disponibilidade é considerado **LOW** dado que é só expectável o menor dos inconvenientes, como o atraso de processamento, o que não invalida.

6.3 Probabilidade de ocorrência de ameaças

De seguida é apresentada a avaliação para cada dimensão do ambiente das operações de processamento:

- **Recursos técnicos e de rede:** a probabilidade de ocorrência de ameaças é **BAIXA**, pois o processamento não é realizado através da Internet. Supõe-se que as melhores técnicas sejam implementadas de maneira a proteger os dados.
- **Procedimentos relacionados com o processamento de dados pessoais:** a probabilidade de ocorrência de ameaças é **BAIXA**, supondo que as funções e responsabilidades dos implementadores envolvidos sejam claramente definidas de acordo com uma política de uso aceitável.
- **Pessoas envolvidas no processamento de dados pessoais:** a probabilidade de ocorrência de ameaças é **MÉDIA**, pois inclui um grande número de implementadores envolvidos no processamento.
- **Setor de negócios e escala de processamento:** a probabilidade de ocorrência de ameaças é **BAIXA**, pois o setor de negócios das *PME* geralmente não é considerado suscetível a ataques *Ciberataque* e nenhuma violação de dados pessoais é conhecida por ter ocorrido no passado.

6.4 Avaliação de risco

Sendo assim o risco para este caso em particular pode ser considerado **MEDIUM**, onde o nível de impacto é **MEDIUM** e a probabilidade da ameaça ocorrer é **LOW**. As medidas que podem ser tomadas para diminuir o risco são especificação de controlos de acesso que envolva o processamento de dados pessoais (Anexo A.1, C.1), planeamento de respostas efectivas a incidentes que podem acontecer a dados pessoais (Anexo A.1, G.1), o uso de um inventário com políticas e procedimentos específicos relacionados com a protecção de dados pessoais (Anexo A.2, A.5).