Universidade do Minho
Criptografia e Segurança da Informação
Departamento de Informática

Engenharia de Segurança

TP4 - Aula 7

Grupo 7
Carlos Pinto Pedrosa A77320
José Francisco Gonçalves Petejo e Igreja Matos A77688
25 de Março de 2019

Conteúdo

1 RGPD (Regulamento Geral de Proteção de Dados) 2
1.1 Pergunta 1.1 2
1.2 Pergunta 1.2 3
1.3 Pergunta 1.3 4

1 RGPD (Regulamento Geral de Proteção de Dados)

1.1 Pergunta 1.1

Tendo em conta que o número do nosso grupo é o 7, o artigo a estudar é o número 32 do Regulamento Geral de Proteção de Dados.

Este artigo foca-se na segurança do tratamento dos dados recolhidos por software. Graças às tecnicas atuais de proteção de dados, qualquer entidade é capaz de aplicar as medidas adequadas para garantir a segurança destes, sendo que o artigo foca-se em garantir a privacidade destes.

Tendo em conta algumas das considerações iniciais, mais especificamente as considerações 74 até 77, que, resumidamente implicam:

- Consideração 74 - O responsável pelos dados está encarregado de executar as medidas necessárias que garantem a segurança destes
- Consideração 75 - Os riscos provenientes do uso dos dados pessoais de individuos, com especial atenção para o roubo de dados relativos a crianças
- Consideração 76 - Analíse da gravidade e probabilidade dos riscos para os direitos do titular dos dados deve ser determinado e devidamente catalógado para se poder concluir o nível de segurança das operações de tratamento de dados
- Consideração 77 - O Comité poderá emitir orientações sobre as operações de tratamento de dados que ajudem no aumento da segurança dos dados pessoais

Feita esta análise, é possível ter um melhor entendimento do artigo 32º, que começa por informar quais as garantias de segurança que o software tem de demonstrar, começando pela pseudonimização e cifragem dos dados pessoais, ou seja, os dados não devem estar ligados diretamente ao seu titular, e se for necessário, então essa ligação deve ser escondida, e os dados deste devem ser cifrados de forma a dificultar a leitura destes. De seguida, é necessário garantir a confidencialidade, integridade, disponibilidade e resiliência dos sistemas que realizam o tratamento de dados, para que não existam momentos de falha em que dados não sejam devidamente protegidos. Tendo isso

em conta, também é necessário que exista a possibilidade de restabelecer a disponibilidade e acesso aos dados pessoais de forma segura no caso de um incidente físico ou técnico dos sistemas. Por fim, de forma a garantir que as técnicas que estão a ser utilizadas são viáveis, devem ser realizados testes para avaliar a eficácia das técnicas usadas.

O próximo ponto do artigo indica as considerações que devem ser feitas depois da analíse do nível de segurança do nível de segurança, nomeadamente os riscos apresentados pelo tratamento de dados, em particular a destruição, perda e alterações destes, a divulgação não autorizada entre outros.

O terceiro ponto refere que deve ser seguido um código de conduta referido nos artigos $40^{\underline{o}}$ e $42^{\underline{o}}$ de forma a demonstrar o cumprimento dos requisitos de segurança dos dados.

Por fim, o último ponto refere que o acesso aos dados por parte dos responsáveis só é possivel se o titular lhe der a devida autorização ou se for exigido pelo direito da União.

Depois desta análise do artigo $32^{\underline{o}}$ é possível concluir, que no processo de desenvolvimento de Software, deve se ter especial atenção ao tratamento dos dados pessoais dos titulares, usando sempre técnicas que garantam a segurança destes e realizar avaliações periódicas dessas mesmas técnicas de forma a manter o sistema sempre atualizado com técnicas seguras.

1.2 Pergunta 1.2

A secção *Data Protection by Default in Practice* apresenta e discute uma seleção de standards relativos às políticas de privacidade e proteção de dados. De notar que estas não são atómicas, isto é, normalmente não se podem tratar separadamente, mas sim, em conjunto.

Assim, existem vários critérios, entre os quais, Minimização dos Dados Pessoais Recolhidos e Usados, Minimização do Processamento dos Dados Recolhidos, Minimização do Período de Armazenamento dos Dados e, por último, Minimizar a Acessibilidade dos Dados que, como mencionado anteriormente devem ser usados conjuntamente entre si.

Efetivamente, no primeiro critério apresentado, é evidente que o objetivo final é reduzir a quantidade de informação que é recolhida e processada. Este objetivo pode ser facilmente realizado seguinte algumas normais básicas. A primeira delas é seguir a norma "Need To Know", isto é, recolher apenas a informação que é mesmo necessária. A segunda norma é a de recolher informação apenas quando esta é necessária. Como exemplo podemos ter uma

loja online onde só é pedida a morada e informação de pagamento quando o utilizador realmente vai comprar algum produto. Uma terceira norma é o uso de tecnologias que permitem anonimizar ou cifrar a informação recolhida. A quarta é avaliar o mínimo de informação necessária a ser recolhida para cada caso em particular e está directamente ligada com a quinta que é minimizar o risco de exposição dos dados. Esta quinta norma pretende avaliar que dados são mais sensíveis e, assim sendo, ser melhor protegidos. Como última norma, é sugerido que se guarde apenas uma cópia dos dados, apagando os dados de ficheiros temporários e de logs que, como sabemos, podem ser usados para recolher informações maliciosamente.

A Minimização do Processamento dos Dados, como o nome pode não indicar, tem como objetivo não minimizar o tratamento a que os dados recolhidos são sujeitos, mas sim o risco de cada operação a que os dados são sujeitos.

O terceiro critério tem como objectivo minimizar o tempo de vida dos dados pessoais, isto é, minimizar o tempo que estes são armazenados pelas instituições que os recolhem. Novamente neste critério não se refere apenas à base de dados, mas também a todos os outros ficheiros que possam ter ficado "esquecidos" como ficheiros temporários e de log.

Por último, temos a Minimização da Acessibilidade. Este critério também segue a norma "Need To Know Basis" e está diretamente relacionado com as políticas de controlo de acessos aos dados. Assim, uma primeira norma para este critério será a restrição de acessos com base na necessidade, que é possível separando os dados por tipo, propósito, entre outros. Uma outra norma será limitar a partilha dos dados e evitar a cópia destes. Por último, apresenta-se talvez a mais importante, que diz que a partilha apenas deve ser possível depois do consentimento do titular dos dados.

Como conclusão pode-se dizer que os standards acima explicitados são uma mais valia pois permite melhorar a usabilidade dos sistemas de hoje em dia, tornando-os mais "user friendly". No entanto, vale notar que, não podemos deixar que estes defaults perturbem as funcionalidades do sistema.

1.3 Pergunta 1.3

Os nove critérios que devem ser considerados para avaliar se o processamento de dados pessoais é de alto risco são:

1. Avaliação, ao tratar de dados que involvam a avaliação de performance

de trabalhadores ou profiling de clientes

2. Tomadas de decisões legais automatizadas, no caso de um sistema que realize decisões em indivíduos dependendo de determinados dados

3. Monitorização sistemática, em sistemas que monitorizem redes que trocam informação

4. Dados sensíveis ou extremamente pessoais, como por exemplo opinião política, ou histórico criminal

5. Dados processados a elevada escala, considera-se vários aspetos, como a localização desses dados, a duração, etc.

6. Dados relativos a indivíduos importantes, no caso de entidades em posições políticas poderosas por exemplo

7. Uso inovador ou aplicações de novas tecnologias, no caso de reconhecimento facial ou outras biométricas

8. Se impedir os indivíduos de exercer um serviço, se modificarem o estado, removendo direitos no sistema.

O projeto em causa seria um website com a maior biblioteca física de vinil do mundo, que permite a compra e venda destes mesmos. Neste serviço, o utilizador precisa de fornecer os seus dados pessoas relativos à morada e cartão de crédito.

Neste caso, os critérios que satisfaz são o 1, 4 e 5.