Aula 7 TP – 18/março/2019

Grupo 3

1. RGPD (Regulamento Geral de Proteção de Dados)

● *Pergunta 1.1*

Um dos principais objetivos do RGPD é garantir uma maior segurança aos cidadãos, relativamente aos seus dados pessoais. Devido à globalização e às
evoluções tecnológicas mais recentes é necessária uma vigilância mais apertada em relação à origem dos dados pessoais, ao seu armazenamento, tratamento e acesso.
O artigo 32º (Segurança do tratamento) refere as medidas técnicas e organizacionais que são necessárias para estabelecer um nível de segurança apropriado ao risco.

Estas medidas são:

1. Pseudonimização e cifragem dos dados
2. Medidas que asseguram permanentemente tanto a confidencialidade, como a integridade, a disponibilidade e a resiliência dos sistemas e serviços de tratamento.
3. Restabelecimento da disponibilidade e acesso a dados pessoais atempadamente, no caso de incidentes físicos ou técnicos
4. Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Com base nestas quatro medidas, é importante assegurar que o software que processa dados pessoais numa empresa, por exemplo, está apto para as cumprir. É assim necessário, que este software disponibilize certas funcionalidades que garantam o controlo dos processos de tratamento dos dados.

Uma empresa deve ter em grande atenção o software, pois para além de garantir a conformidade com o RGPD, também é benéfico para o negócio, uma vez que automatiza diversos processos que são obrigatórios com este regulamento, e que de outra maneira seriam feitos de forma manual, o que teria um custo superior.

Por exemplo, relativamente à medida 3. o software pode ser bastante importante, pois facilita o rastreamento dos dados para os enviar ao titular.

O software ajuda também a limitar o acesso aos dados, prevenindo assim o abuso de acesso.

- ***Pergunta 1.2***

As várias técnicas de pseudonimização tem como objetivo derivar pseudónimos de identificadores iniciais associados a indivíduos. O principal foco destas técnicas são os casos em que há um identificador único associado a um utilizador. Porém, algumas técnicas podem ser aplicadas também a casos mais complexos, como quando existe combinação de identificadores. Uma boa técnica deve contemplar as seguintes situações:

1. os pseudónimos não devem permitir uma re-identificação "fácil" por qualquer terceiro dentro de um contexto de processamento de dados específico.
2. não deve ser trivial para qualquer terceiro reproduzir os pseudônimos.

A primeira técnica apresentada pela ENISA é ***Hashing without key.*** Uma função de hash criptográfica h é uma função com certas propriedades e que transforma qualquer mensagem m de comprimento arbitrário numa outra de tamanho fixo h (m). Uma função de hash é invertível e resistente a colisões. Porém, quando falámos em pseudonimização, o hash simples de identificadores de dados para fornecer pseudónimos tem grandes desvantagens. A situação ***2*** não é válida, pois sempre que algum terceiro aplique a mesma função de hash ao mesmo identificador então irá obter o mesmo pseudónimo. Em relação à situação ***1*** também não é necessariamente validada, uma vez que é trivial para algum terceiro verificar se um pseudónimo corresponde a um certo identificador. Assim conclui-se que as funções de hash não são recomendadas para a pseudonimização de dados pessoais, embora possam contribuir para aumentar a segurança em certos contextos.

Outra técnica é ***Hashing with key or salt*****.** Nestas funções de hash a saída não depende apenas da entrada, mas também de uma chave secreta. Ao contrário das funções de hash convencionais, vários pseudónimos diferentes podem ser produzidos através da mesma entrada, de acordo com a escolha da chave específica e assim, a situação **2** está assegurada. Além disso, a situação 1 também é válida, desde que qualquer terceiro não tenha conhecimento da chave secreta e não esteja em condições de verificar se um pseudónimo corresponde a um identificador conhecido específico.

Encryption as a pseudonymisation technique é também outra técnica eficiente. A criptografia simétrica dos identificadores é considerada um método eficiente para obter pseudónimos. O identificador original de um sujeito de dados pode ser criptografado através de um algoritmo de criptografia simétrica, fornecendo assim um texto cifrado que deve ser usado como um pseudónimo e a mesma chave secreta é necessária para a decifração. Assim são satisfeitas as situações **1** e **2** Desde que nenhum terceiro tenha acesso à chave privada. A principal diferença em relação às funções de hash é que o proprietário da chave secreta pode sempre obter os identificadores.

Tokenisation é outra técnica e refere-se ao processo em que os identificadores dos titulares de dados são substituídos por valores gerados aleatoriamente (tokens), sem que estes tenham qualquer relação matemática com os identificadores originais. Assim, o conhecimento de um token não tem utilidade para um terceiro. Esta técnica também satisfaz as situações **1** e **2**.

Cryptography-based techniques**,** ou seja, a combinação apropriada de vários esquemas criptográficos, também pode fornecer abordagens robustas de pseudonimização.

Existem ainda outras técnicas que podem ser utilizadas.

- ***Pergunta 1.3***

1) Os nove critérios que devem ser considerados para avaliar se o processamento de dados pessoais irá resultar num risco elevado, devendo ser efetuado um DPIA sempre que o processamento satisfizer dois desses critérios, são os seguintes:

1. Avaliação ou classificação;

2. Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar;

3. Controlo sistemático;

4. Dados sensíveis ou dados de natureza altamente pessoal;

5. Dados tratados em grande escala;

6. Estabelecer correspondências ou combinar conjuntos de dados;

7. Dados relativos a titulares de dados vulneráveis;

8. Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais;

9. Quando o próprio tratamento *impede os titulares dos dados* «*de exercer um direito ou de utilizar um serviço ou um contrato*» (artigo 22.º e considerando 91). Estão incluídas operações de tratamento destinadas a autorizar, alterar ou recusar o acesso dos titulares dos dados a um serviço ou que estes celebrem um contrato.

2) Imaginemos que estávamos a iniciar um projeto que tinha como principal intuito desenvolver um site que envolvia a utilização de dados pessoais cujo processamento resulta num risco elevado. O objetivo deste site seria informar os utilizadores que estivessem

registados no mesmo sobre os estados da meteorologia. Para tal existem alguns dados que seriam necessários para o fornecimento da informação meteorológica, nomeadamente:

- Nome do utilizador;
- Morada do utilizador (região geográfica);
- Endereço de email;
- Dados bancários (a informação enviada iria ter custos)

3) Em anexo encontra-se preenchido o *template DPIA* (*DPIA_Pergunta1.3.pdf*)

- ***Pergunta 1.4***

1,2 e 3) Depois de instalada a ferramenta open-source *Data Protection Impact Assessment (DPIA)* procedemos ao preenchimento sucinto de todas as componentes pedidas em relação ao nosso projeto acima descrito. Em anexo está o ficheiro *DPIA_grupo3.pdf* correspondente ao formulário.