Aula TP - 18/Mar/2019

Cada grupo deve colocar a resposta às perguntas dos seguintes exercícios na área do seu grupo no Github até ao final do dia 18/Abr/2019. Por cada dia de atraso será descontado 0,15 valores à nota desse trabalho.

Exercícios

1. RGPD (Regulamento Geral de Proteção de Dados)

Na diretoria Aula7 estão disponibilizados os seguintes documentos, entre outros:

- Regulamento (UE) 2016/679 (RGPD), em português e inglês;
- Draft da ISO 27552 (*Security techniques - Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy management — Requirements and guidelines*);
- *Standard Data Protection Model* publicado pelo DPA (*Data Protection Atuhority*) alemão;
- *Handbook on European data protection law*, publicado pelo *European Data Protection Supervisor*;
- Vários documentos disponibilizados pela ENISA (*European Union Agency for Network and Information Security*) a partir da sua página de Data Protecion

Pergunta P1.1

Nesta pergunta cada grupo vai efetuar uma pequena análise do Regulamento (UE) 2016/679 (RGPD) ou do ISO 27552 (*Security techniques - Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy management — Requirements and guidelines*) ou do *Handbook on European data protection law*, de acordo com as regras seguintes:

- Se o grupo escolher o RGPD, deverá analisar o seguinte artigo do regulamento e escrever um pequeno texto (entre 1/2 e 1 página A4) em que reflita sobre a forma como esse artigo do regulamento pode influir no desenvolvimento do software. Note que o documento tem 173 considerandos iniciais, podendo alguns serem relevantes para esta reflexão.
  - Artigo 5º - Grupos 1, 5, 9, 13
  - Artigo 25º - Grupos 2, 6, 10, 14
  - Artigo 32º - Grupos 3, 7, 11
  - Secção 4 (Encarregado de Proteção de Dados) - Grupos 4, 8, 12
- Se o grupo escolher o draft do ISO 27552, deverá analisar o seguinte ponto e escrever um pequeno texto (entre 1/2 e 1 página A4) em que reflita sobre as implicações que esse ponto tem no desenvolvimento do software e/ou na operação do mesmo.
  - 6.4 (*Human resource security*) e 6.5 (*Asset management*) - Grupos 1, 5, 9, 13
  - 6.9 (*Operations Security*) - Grupos 2, 6, 10, 14
  - 6.13 (*Information security incident management*) - Grupos 3, 7, 11
  - 6.15 (*Compliance*) - Grupos 4, 8, 12
- Se o grupo escolher o *Handbook on European data protection law*, deverá analisar as secções indicadas e e escrever um pequeno texto (entre 1/2 e 1 página A4) em que reflita sobre as implicações que esse assunto tem no desenvolvimento do software:
  - *Lawfulness, fairness and transparency of processing principles* - secção 3.1 - Grupos 1, 13;

- *Principle of purpose limitation* - secção 3.2 - Grupos 2, 14;
- *Data minimisation principle* - secção 3.3 - Grupo 3;
- *Data accuracy principle* - secção 3.4 - Grupo 4;
- *Storage limitation principle* - secção 3.5 - Grupo 5;
- *Data security principle* - secção 3.6 - Grupo 6;
- *Accountability principle* - secção 3.7 - Grupo 7;
- *Right to be informed* - secção 6.1.1 - Grupo 8;
- *Right to rectification* - secção 6.1.2 - Grupo 9;
- *Right to erasure* - secção 6.1.3 - Grupo 10;
- *Right to restriction of processing* - secção 6.1.4 - Grupo 11;
- *Right to data portability* - secção 6.1.5 - Grupo 12;

Note que a análise deverá apenas ser efectuada a um dos documentos, devendo o grupo escolher qual prefere, de acordo com as regras anteriores.

Pergunta P1.2

A ENISA (*European Union Agency for Network and Information Security*) tem feito um trabalho relevante na produção de documentação relevante para a proteção de dados.

No documento [*Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation*](Aula7/ENISA.WP2018 O.2.2.5 - Recomendations on shaping technology according to GDPR provisions - Part 1.pdf) analise as *Pseudonymisation techniques* (secção 3), e faça um resumo das mesmas (entre 1/2 e 1 página A4), se pertence aos Grupos 1, 2, 3, 4 ou 5.

No documento [*Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default*](Aula7/ENISA.WP2018 O.2.2.5 Recommendations on shaping technology according to GDPR provisions - Part 2.pdf) analise o *Data protection by default in practice* (secção 3), e faça um resumo das mesmas (entre 1/2 e 1 página A4), se pertence aos Grupos 6, 7, 8, 9 ou 10.

No documento [*Privacy and Data Protection by Design – from policy to engineering*](Aula7/ENISA.Privacy and Data Protection by Design.pdf) analise as oito estratégias de *privacy design* (secção 3.2), e faça um resumo das mesmas (entre 1/2 e 1 página A4), se pertence aos Grupos 11, 12, 13 ou 14.

Experiência 1.1

Na tabela 1 do documento [*Online privacy tools for the general public - Towards a methodology for the evaluation of PETs for internet & mobile users*](ENISA.Study on the availability of trustworthy online privacy tools for the general public.pdf) são apresentados os portais web mais relevantes na promoção da utilização de ferramentas que garantem a privacidade dos dados (e/ou do utilizador).

Baseado nos portais web identificados, efetue as seguintes experiências:

- Utilize a ferramenta Panopticlick da *Electronic Frontier Foundation* (EFF) para verificar se o seu browser é seguro contra *tracking* - https://panopticlick.eff.org/
- No *PRISM Break* verifique que aplicações deve evitar e aquelas que deve preferir na sua plataforma - https://prism-break.org/en/
- No *Security in-a-box* verifique a tática para proteger ficheiros sensíveis no seu computador - https://securityinabox.org/en/guide/secure-file-storage/

- O privacytools.io disponibiliza informação sobre um conjunto alargado de ferramentas que preservam a privacidade - https://www.privacytools.io/

Pergunta P1.3

O *ARTICLE 29 DATA PROTECTION WORKING PARTY* publicou o *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* em que indica 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.

1. Identifique os nove critérios
2. Imagine que está a iniciar um projeto que envolve a utilização de dados pessoais cujo processamento resulta num risco elevado. Explique sucintamente esse projeto e processamento, assim como os critérios que o processamento satisfaz.
3. Preencha o template DPIA (pode preencher em português).

Pergunta P1.4

O CNIL (*Commission Nationale de l'Informatique et des Libertés*) disponibilizou uma ferramenta open-source para ajudar no *Data Protection Impact Assessment* (DPIA) em https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

1. Instale a ferramenta (disponível para Linux, Windows e MacOS) que se encontra em https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
2. Utilize a ferramenta para o DPIA do mesmo projeto imaginado na pergunta anterior, preenchendo sucintamente (pode preencher em português) todas as componentes pedidas.
3. No final do preenchimento e validação, vá ao dashboard e escolha a apresentação em lista, selecione "Display PIA" e imprima para ficheiro PDF que coloca no github como resposta a esta pergunta.

Projeto de Engenharia de Segurança

Pode utilizar o resto da aula para o projeto de Engenharia de Segurança