# TP Class Assignment - 18/Mar/2019

Each group must answer the questions of the following exercises in the Github area of their group until the end of 18/Apr/2019. For each day of delay, 0.15 points will be deducted from the grade of this assignment.

# Exercises

## 1. GDPR (General Data Protection Regulation)

Among others, the following documents are available in the Aula7 directory:

- Regulation (UE) 2016/679 (GDPR), in portuguese and english;
- Draft of the ISO 27552 (*Security techniques - Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy management — Requirements and guidelines*);
- *Standard Data Protection Model* published by the german DPA (*Data Protection Atuhority*);
- *Handbook on European data protection law*, published by the *European Data Protection Supervisor*;
- Several documents provided by ENISA (*European Union Agency for Network and Information Security*) from its Data Protecion web page.

### Question P1.1

In this question each group will perform a short review of the Regulation (UE) 2016/679 (RGPD) or the ISO 27552 (*Security techniques - Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy management — Requirements and guidelines*) or the *Handbook on European data protection law*, in accordance with the following rules:

- If the group chooses the GDPR, it should review the following article of the regulation and write a short text (between 1/2 and 1 page A4) that reflects on how this regulation article can influence the development of the software. Note that the document has 173 initial recitals, some of which may be relevant to this reflection.
    - Article 5º - Groups 1, 5, 9, 13
    - Article 25º - Groups 2, 6, 10, 14
    - Article 32º - Groups 3, 7, 11
    - Section 4 (Data Protection Officer) - Groups 4, 8, 12
- If the group chooses the ISO 27552 draft, it should review the following section and write a short text (between 1/2 and 1 A4 page) that reflects on the implications that this point has on software development and / or operation.
    - 6.4 (*Human resource security*) e 6.5 (*Asset management*) - Groups 1, 5, 9, 13
    - 6.9 (*Operations Security*) - Groups 2, 6, 10, 14
    - 6.13 (*Information security incident management*) - Groups 3, 7, 11
    - 6.15 (*Compliance*) - Groups 4, 8, 12
- If the group chooses the *Handbook on European data protection law*, it should review the following section and write a short text (between 1/2 and 1 A4 page) reflecting on the implications of this subject for software development:
    - *Lawfulness, fairness and transparency of processing principles* - section 3.1 - Group 1, 13;
    - *Principle of purpose limitation* - section 3.2 - Group 2, 14;
    - *Data minimisation principle* - section 3.3 - Group 3;

- *Data accuracy principle* - section 3.4 - Group 4;
- *Storage limitation principle* - section 3.5 - Group 5;
- *Data security principle* - section 3.6 - Group 6;
- *Accountability principle* - section 3.7 - Group 7;
- *Right to be informed* - section 6.1.1 - Group 8;
- *Right to rectification* - section 6.1.2 - Group 9;
- *Right to erasure* - section 6.1.3 - Group 10;
- *Right to restriction of processing* - section 6.1.4 - Group 11;
- *Right to data portability* - section 6.1.5 - Group 12;

Note that the analysis should only be done to one of the documents, and the group should choose which one it prefers, according to the previous rules.

### Question P1.2

ENISA (European Union Agency for Network and Information Security) has done an excellent job in producing relevant documentation for data protection.

In the document [*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) analyze the *Pseudonymisation techniques* (section 3), and summarize them (between 1/2 and 1 page A4) - Groups 1, 2, 3, 4 or 5.

In the document [*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) analyze the *Data protection by default in practice* (section 3), and summarize them (between 1/2 and 1 page A4) - Groups 6, 7, 8, 9 ou 10.

In the document [*Privacy and Data Protection by Design – from policy to engineering*](Aula7/ENISA.Privacy and Data Protection by Design.pdf) analyze the eight strategies of *privacy design* (section 3.2), and summarize them (between 1/2 and 1 page A4) - Groups 11, 12, 13 ou 14.

### Experience 1.1

Table 1 of document [*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) identifies the most relevant web portals in promoting the use of tools that guarantee the privacy of the data (and / or the user).

Based on the web portals identified, carry out the following experiments:

- Use the Panopticlick tool from *Electronic Frontier Foundation* (EFF) to check if your browser is safe against *tracking* - https://panopticlick.eff.org/
- On *PRISM Break* check which applications to avoid and which ones you should prefer on your platform - https://prism-break.org/en/
- In *Security in-a-box* check the tactic to protect sensitive files on your computer - https://securityinabox.org/en/guide/secure-file-storage/
- Privacytools.io provides information on a broad set of privacy-preserving tools - https://www.privacytools.io/

### Question P1.3

*ARTICLE 29 DATA PROTECTION WORKING PARTY* published the *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*. These guidelines include the nine criteria that should be considered in order to assess whether the processing of personal data will result in a high risk - a DPIA should be performed whenever the processing meets two of these criteria.

1. Identify the nine criteria
2. Imagine that you are initiating a project that involves the use of personal data whose processing results in a high risk. Briefly explain the project and the processing, as well as the criteria that the processing satisfies.
3. Fill in the DPIA template.

### Question P1.4

CNIL (*Commission Nationale de l'Informatique et des Libertés*) provided an open-source tool to help with the *Data Protection Impact Assessment* (DPIA) at https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

1. Install the DPIA tool (available for Linux, Windows and MacOS) - https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
2. Use the DPIA tool for the project you explained in the previous question, briefly filling in all the required components.
3. At the end of the validation, go to the dashboard and choose the list presentation, select "Display PIA" and print to PDF file. Put it in your group space in github, as a response to this question.

## Engenharia de Segurança course - Project

You can use the rest of the class for the Engenharia de Segurança project.