European Journal of Privacy Law & Technologies

2019/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2019/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

Published Online by G. Giappichelli in June 2019
www.ejplt.tatodpr.eu

SECTION III: USE CASES

Challenge Title: Privacy by Design and by Default and Data Protection Impact Assessment (DPIA)	
Use Case Author	Davide Borelli, Lucilla Gatt, Suor Orsola Benincasa University of Naples
Topic	Pharmaceutical
Overview	Get Well Soon' is a leading pharmaceutical company co-headquartered in Italy and the United Kingdom. Amongst others, 'Get Well Soon' focuses on developing smart medical devices many of which can be remotely managed via ad hoc mobile apps. The Head of IT, Davide, is currently developing a new mobile app which links to a smart tooth-brush: any data collected via the use of such device is then processed in the backend and shown to users in an intelligible form. Davide has recently completed his mandatory GDPR training. Having learnt that by law privacy shall be baked into any project development lifecycle from the outset, he is now concerned that his new app, as well as any other app developed by his team is not fully compliant with the applicable data protection legislations. As such, he immediately contacts the Global Privacy Team of 'Get Well Soon' seeking for advice.
1. Engage	
Big idea	Privacy by Design and by Default and Data Protection Impact Assess-ment (DPIA)
Essential Question	What does 'Privacy by Design and by Default' mean in practice? How should it be implemented within an existing Project Management Methodology (PMM) and System Development Life Cycle (SDLC)? How would you spread accountability throughout the business?
Initial resources	1. A brief illustration of the 'Get Well Soon' company structure, and 2. A brief PMM process 3. A brief SDLC process

Guiding Questions	Acting as newly appointed Global Privacy Offices, the Students should try to design a privacy governance model and update the existing SDLC and PMM to bake-in privacy from the very outset. • What does 'Privacy by Design and by Default' means in theory? And in practice? • How would you organise the overall privacy structure at a central and local level? How would you raise awareness (and accountability) throughout the business? • How would you assess potential privacy risks? How would you create momentum for a wider and shared privacy accountability? How would promote a smoother change management process?
Reflections	Once the exercise is completed, the Students will be encouraged to reflect on the many meanings and applications of 'Privacy by Design and by Default' and its ontological mutability. The Students will also be encouraged to think about how a similar scenario could be tackled more effectively in future and to record any individual reflections on the exercise.
Other notes	
2. Investigate	
Activity Description	Each Student is required to map out a process of investigation for answering the questions above.
Resources	• Preliminary opinion 5/2018 on Privacy by Design (31/05/2018) of the European Data Protection Supervisor, available at https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf • Data protection by design and default (23 May 2018), available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ • Data Protection Measures by Design and By Default (March 2018), available at https://odpc.gg/wp-content/uploads/2018/05/DPByDesign.pdf • Guide, Software Development with Data Protection by Design and by Default (28 November 2017), available at https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/ • Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps (24 October 2012), available at https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_app_201210/

	• Privacy Enhancing Technologies: Evolution and State of the Art. A Community Approach to PETs Maturity Assessment (9 March 2017), available at https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art/at_download/fullReport **Data Protection Impact Assessment (DPIA)** • 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, WP248 (4 April 2017), available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 • Draft List of types of Data Processing Operations which require a Data Protection Impact Assessment (6 June 2018), available at https://www.dataprotection.ie/docimages/documents/DPIA%20for%20co nsultation.pdf • Data Protection Impact Assessments (15 May 2018), available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/ • Data Protection Impact Assessments (2018), available at_http://gdprandyou.ie/data-protection-impact-assessments-dpia/ **Internet of Things** • Big Data and Smart Devices and Their Impact on Privacy (21 September 2015), available at_http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPO L_STU(2015)536455_EN.pdf
Synthesis	In groups of 5, the Students are required to create a PowerPoint presentation which outlines: (1) Their findings on the topic, (2) How they would update the existing SDLC and PMM workflows, and (3) A Target Operating Model (TOM). The proposal shall be shown to and discussed with the Head of IT of 'Get Well Soon' who may challenge the proposed approaches. Each group shall evaluate the performance of the others and outline pros and cons of each suggested approach.
Reflections	The Students will be encouraged to reflect on the operational side of privacy and on how to foster awareness and accountability within the business. They will also be encouraged to think about how a similar scenario could be tackled more effectively in the future and record any individual reflections on the exercise.
Other notes	None.

3. Act	
Solution Prototypes	Each Group will provide a classroom style briefing to fellow students to explain the process and outcome of their investigations, and to disseminate the implications which flow from this. The above-mentioned briefing shall include the following 1. An explanation of the Privacy by Design principles 2. How to make them live in the real world (i.e., strategies, tactics, privacy patterns) 3. A brief explanation of what is a Data Protection Impact Assessment (DPIA) 4. A Target Operating model (TOM) proposal 5. An updated PMM and SDLC process 6. Pros and cons of the suggested approach The recommendations provided should aim to improve attitudes to data privacy and security, as well as awareness of the implications of breaches of the privacy laws and regulations. The proposal shall be shown to and discussed with the Head of IT of 'Get Well Soon' who may challenge the proposed approaches. Each group shall evaluate the performance of the others and outline pros and cons of each suggested approach.
Solution	The Students shall provide a solution or options for different solutions in the format suggested above.
Implementation plan	The Students shall provide a plan on how the solutions may be delivered, and how to foster a virtuous change management within the business.
Evaluate	The Students shall answer the following – 1. What are the strengths and weaknesses of the approach you have suggested? 2. How did you assessed the proposed trade-off between legal compliance and business needs? 3. What did you learn from this exercise? The Students will also be required to carry out a SWOT analysis on one of the suggested approaches.
Other notes	
4. Reflection and documentation	
Case notes	It can be developed in future by showing real SDLC and PMM processes and let the Students carry out a real Data Protection Impact Assessments (DPIAs).