European Journal of Privacy Law & Technologies



2018/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2018/1

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.

The contents of this Journal represent the views of the author only and are his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published online by G. Giappichelli in October 2019
www.ejplt.tatodpr.eu

SECTION III: USE CASES

Challenge Title: Compliance evaluation	
Use Case Author	Giancarlo Butti, Maria Cristina Gaeta, Suor Orsola Benincasa University of Naples
Topic	Legal area: Data Protection Law
Overview	Case Study The ACME bank has recently developed a new business line consisting of the direct offer of insurance products placed on behalf of a commercial partner. The signing of the policy documents takes place in the branch through the use of the FEA and the documents signed in this way are sent directly to substitutive storage with a third-party supplier that operates both on behalf of the bank and on behalf of the insurance company. The management process requires that all documents provided by customers are digitized for forwarding to the insurance company and that the original document is forwarded directly to the external service of the same company. Similarly, claims management takes place by collecting all the documents that are digitized directly in the branch office. The operations are carried out using a software application made available by the Company and branch operators access it through specific credentials issued by the latter.
1. Engage	
Big idea	Evaluate the compliance with the privacy regulation of a new service developed by the ACME company shortly before the entry into force of the GDPR.
Essential Question	Is it possible to define a verification plan to confirm full compliance with privacy regulation and criteria to guarantee it over time?
Initial resources	Provisions issued by the Italian Privacy Authority Authorityhttps://ico.org.uk/for-organisations/resources-and-support/audits/ https://www.dataprotection.ie/docimages/documents/GuidetoAuditProcessA ug2014.pdf
Guiding Ques-	Students divided into groups must identify the technical and organiza-

tions	tional aspects that need to be identified in order to proceed with a subsequent verification.
Reflections	The analysis can be inspired by the mapping of: • which stakeholders are involved in the data • what data are processed • if there are particular, judicial, biometric data ... • if data of minors are processed • who are the internal subjects who carry out the processing • which external parties participate in the treatment • it is necessary to map information flows • what are the IT tools used • what documents are used
Other notes	With the elements detected, it is advisable to draw the information flows both inside and outside the company.
2. Investigate	
Activity Description	After having identified the previously specified elements, the students must identify the requirements that must be put in place to be compliant with the regulations, as well as the related compliance criteria.
Resources	• General Data Protection Regulation • D.Lgs 196/03 • Article 29 Guidelines and EDPB • Provisions issued by the Italian Privacy Authority Authorityhttps://ico.org.uk/for-organisations/resources-and-support/audits/ https://www.dataprotection.ie/docimages/documents/GuidetoAuditProcessA ug2014.pdf
Synthesis	The students, divided into groups, must identify the elements that need to be tested.
Reflections	Students must identify the presence of: • Privacy Policy • Designations of authorized processing • Designation of external managers • Policies and procedures • Security measures in place
Other notes	The individual groups expose their results in order to define a shared set of elements to be tested, as well as the related compliance criteria.

3. Act	
Solution Prototypes	Students must develop a methodology for conducting the verification.
Solution	Students divided into groups must define in detail an audit plan that includes: • A list of the subjects within the company to be interviewed • The questionnaires to be submitted • The interview plan • Documents to be recovered
Implementation plan	Students share the material developed in order to define a single audit plan.
Evaluate	Students must verify that the defined plan includes all the elements to be tested and the related criteria for conformity assessment. In this regard, students should be divided into 2 separate groups. Each group must produce sample documentation (information, designation contracts ...) consistent with the content of the case analysed. The documentation produced will be analysed, according to the parameters defined in the audit plan, by the other group, in order to assess compliance.
Other notes	It is advisable to define audit report templates to be used to document the verification process carried out.
4. Reflection and documentation	
Case notes	The verification criteria developed should apply to any situation and not just to the case in question.