ISSN 2704-8012

European Journal of Privacy Law & Technologies

2019/2

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2019/2

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 Dicember 2019
www.ejplt.tatodpr.eu

Challenge Title: Vendor Risk Management and Data Protection Agreement negotiation	
Use Case Author	*Davide Borelli, Lucilla Gatt, Suor Orsola Benincasa University of Naples*
Topic	*Data Protection Law*
Overview	*'Ego' is an Italian cosmetic company headquartered in Milan. It focuses on hair colour, skin care, sun protection, make-up, perfume, and hair care. Its Head of Marketing, Jane, is currently working on a new web campaign to advertise Ego's brand new green tea mask: her plan is to create a website where people can purchase the new product or simply subscribe a newsletter to receive exclusive offers and the latest news on Ego's products.* *To run this campaign, Jane decides to use a Software as a Service (SaaS) solution named 'Bazaar', i.e., a US e-commerce platform for online stores and retail point-of- sale systems. As such, she contacts all the relevant internal stakeholders (i.e., Procurement, InfoSec, and Privacy) to get the new Vendor on boarded sooner.*
1. Engage	
Big idea	*Vendor Risk Management and Data Protection Agreement Negotiation.*
Essential Question	*How would you ensure that the use of third-party products, IT suppliers and service providers does not result in a potential business disruption or in any negative impact on business performance? How would you ensure that any third-party complies with the applicable data protection legislation? How would you make sure that a cross-border data transfer does not result in a material circumvention of the applicable privacy legislation?*
Initial resources	*1. A description of the web marketing campaign* *2. A brief Vendor Onboarding Process* *3. A Data Processing Agreement (DPA) Template* *4. Standard Contractual Clauses (SCC) Template*
Guiding Questions	*Acting as newly appointed Global Privacy Offices, the Students should try to update the existing Vendor Onboarding Process to include appropriate privacy controls and negotiate an ad hoc DPA and (where needed) SCCs.* • *What control would you put in place to ensure that every Vendor complies with the applicable data protection legislation?* • *Is there any sort of due diligence which might be carried out to*

	assess potential privacy risks? If so, what should be the content of such a due diligence? • *How would you negotiate a DPA? What are the main challenges? What would you focus on?* • *What if the processing activity results in a cross-border data transfer? What safeguards are you required to put in place to ensure that such a transfer does not result in a circumvention of the applicable legislation?*
Reflections	*Once the exercise is completed, the Students will be encouraged to reflect on the challenges of the vendor risk management from a privacy perspective. 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	*None.*
2. Investigate	
Activity Description	*Each Student is required to map out a process of investigation for answering the questions above.*
Resources	***Vendor Risk Management*** • *Guidance: A Practical Guide to Data Controller to Data Processor Contracts under GDPR (14 May 2018), available at http://gdprandyou.ie/wp- content/uploads/2018/05/Guidance-for-Data-Processing-Contracts-GDPR.pdf* • *What should be contained in a contract between a Data Controller and a Data Processor?, available a https://www.dataprotection.ie/docs/710-What- should-be-contained-in-a-contract-between-a-Data-Controller-and-a-Data- Processor/654.htm* • *ICO GDPR guidance: Contracts and liabilities between controllers and processors (13 September 2017), available at https://ico.org.uk/media/about- the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for- consultation-september-2017.pdf* • *Technical Note: Benefits of a new data protection agreement (7 June 2018), available at https://assets.publishing.service.gov.uk/government /uploads/system/upload s/attachment_data/file/714677/Data_Protect ion_Technical_Note.pdf* ***Cross-border Data Transfers*** • *The eighth data protection principle and international data transfers, available at https://ico.org.uk/media/for- organisations/documents/15 66/international_transfers_legal_guidance.pdf* • *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (30 May 2018), available at https://edpb.europa.eu/sites/edp*

	b/files/files/file1/edpb_guidelines_2_2018_ derogations_en.pdf • *Draft Guidelines on Article 49 of Regulation 2016/679 | WP 261 (12 February 2018), available at http://ec.europa.eu/newsroom/article 29/document.cfm?doc_id=49771* • *Adequacy Referential | WP 254 rev.01 (9 February 2018), available at http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49724* • *Data transfers abroad for outsourced data processing, available at https://www.edoeb.admin.ch/dokumentation/00153/00184/00189/index.ht ml?lang=en*
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 Vendor Onboarding Process, and* *(3) Their contractual strategy with 'Bazaar'.* *The proposal shall be shown to and discussed with the class. Afterwards, the groups shall engage 'Bazaar's Legal Counsel, Davide, to negotiate any necessary agreement on data protection. 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 Controller-Processor relationship* *2. What risk may be associate with the onboarding of new suppliers* *3. A brief explanation of how to conduct an audit/due diligence on a given supplier (and its products and services)* *4. An updated Vendor Onboarding Process* *5. A strategy for cross-border data transfers*

	6. A brief strategy to negotiate the contract with the supplier *7. 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 class. 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	*None.*
4. Reflection and documentation	
Case notes	*It can be developed in future by showing real onboarding procedures and let them assist a real contract negotiation.*