COMPUTER LAW & SECURITY REVIEW 33 (2017) 458–469

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities

Apostolos Malatras [a], *Ignacio Sanchez* [a,*], *Laurent Beslay* [a], *Iwen Coisel* [a], *Ioannis Vakalis* [a], *Giuseppe D'Acquisto* [b], *Manuel Garcia Sanchez* [c], *Matthieu Grall* [d], *Marit Hansen* [e], *Vasilios Zorkadis* [f]

[a] *European Commission, Joint Research Centre (JRC), Italy*
[b] *Italian Data Protection Authority (Garante), Italy*
[c] *Spanish Agency of Data Protection (AEPD), Spain*
[d] *French Data Protection Authority (CNIL), France*
[e] *Data Protection Authority Schleswig-Holstein (ULD), Germany*
[f] *Hellenic Data Protection Authority (HDPA), Greece*

Keywords:
Personal data breaches
Data protection
Cross-border
Pan-European
Privacy
Cyber-exercise
Cooperation
General Data Protection Regulation

A B S T R A C T

The emergence of frequent personal data breaches of a cross-border and even pan-European dimension coupled with the current lack of harmonized and systematic approaches to tackle them have motivated the need for further research leading to possible improvement of those cooperation challenges. In this respect, we report here on the organization, execution and analysis of the 1st Pan-European Personal Data Breaches Exercise that was conducted at the end of 2015 by the Directorate-General Joint Research Centre in collaboration with the Directorate-General for Justice and Consumers of the European Commission and the Data Protection Authorities of seven EU Member States. This cyber-exercise aimed at promoting and improving collaboration between Member States when cross-border incidents of personal data breaches occur, by serving as training exercise, mapping existing procedures and by helping identify best practices to handle such incidents. This scientific initiative constitutes a direct support of the recently adopted General Data Protection Regulation. Analysis of results led to some very interesting findings. In particular, communication issues were the ones that were highlighted as the most important ones. There is an evident lack of a global communication list of competent officers from Data Protection Authorities and this hinders cooperation. Moreover, there are no established current practices on handling such incidents and accordingly their management is still performed in an ad hoc manner. The outcome

* *Corresponding author.* European Commission, Joint Research Centre (JRC), Via Enrico Fermi 2749, 21027 Ispra, VA, Italy. Fax: +39 0332785145.
E-mail address: ignacio.sanchez@ec.europa.eu (I. Sanchez).

http://dx.doi.org/10.1016/j.clsr.2017.03.013

of the exercise illustrated the need for putting in place systematic procedures, as well as tools and frameworks to support communication and interaction between all interested stakeholders.

1. Introduction

Pan-European personal data breaches refer to cases where personal data related to citizens from multiple EU Member States has been compromised. This type of data breaches could be the outcome of coordinated attacks originating from different Member States or it could also be the result of concentrated attacks towards multiple states. The distinguishing feature of such data breaches refers to their cross-border nature, which evidently increases significantly their complexity. The reason for this is the fact that multiple national authorities need to cooperate and coordinate their actions in order to address the breach in a consistent and homogeneous manner.

Cross-border incidents concerning personal data breaches are increasingly taking place nowadays, spurred by the high penetration of online, usually cloud-based services offered to citizens. Such services span across the borders of the various Member States and therefore it is not uncommon that the personal data of citizens of one Member State end up being stored in a data center located in another Member State. In the context of the EU, such events of pan-European dimension have been observed over the last years. The potentially sensitive nature of personal data involved, as well as the associated security and privacy risks in general, necessitate the prompt, effective and efficient handling of incidents of such nature. It is noteworthy that insufficient responses to data breaches have been recently highlighted by OWASP as being one of the top 10 privacy risks in 2016 (Open Web Application Security Project (OWASP), 2016). Whereas experience regarding national personal data breaches events can serve as a highly useful guideline, the cross-border element nonetheless introduces further complexity and other challenges due to the need for Data Protection Authorities (DPAs) from different Member States to collaborate and cooperate. In this respect, the Directorate-General Joint Research Centre (DG-JRC) of the European Commission planned and organized a simulation cyber-exercise with the clear aim to promote and improve collaboration between Member States when cross-border personal data breaches incidents occur. The cyber-exercise served accordingly as a training exercise for data protection officials, contributing towards mapping existing procedures and helped to identify best practices to handle such events.

The 1st Pan-European Personal Data Breaches Exercise was conducted at the end of 2015 by the JRC in collaboration with the Directorate-General for Justice and Consumers and the Data Protection Authorities of seven Member States (France, Germany, Greece, Ireland, Italy, Poland and Spain). It was the first exercise of this kind in Europe and it was timely conducted to explore these challenges in the context of Pan-European Personal Data Breaches as the new General Data Protection Regulation (GDPR) (EU Regulation, 2016) was adopted in May 2016. The GDPR, which will come into force two years after its adoption (May 2018), is built around the principle of risk management, not only from the point of view of personal data which are processed, but also for the cooperation between DPA aiming at mitigating the risks and possible damages of a Pan-European Personal Data Breach. This new Regulation extends the requirement for notification of personal data breaches to all data controllers (articles 33 and 34) and requires increased cooperation between Data Protection Authorities of European Member States (articles 60, 61 and 62). With the significant increase of cross-border incidents such as data breaches, this cyber-exercise constituted a solid illustrative example of possible initiatives promoting cooperation among Data Protection Authorities in order to facilitate an effective collaborative and coordinated response to such events.

A total of 20 data protection professionals were involved in the cyber exercise, which was powered up by a new version of the "EXITO Narrator" tool (EXITO Narrator Online Repository, 2016), developed by the JRC. The tool facilitated the proper flow of events and supported the technical dimension of the simulation, including reception of feedback, handling of simulated entities and provision of live simulated websites, social media feeds and email communications. The cyber exercise was coordinated from the European Crisis Management Laboratory at the JRC Ispra site in Italy. During the 8-hour simulation, more than 400 interactions between the participants were recorded.

The analysis of the exercise results provides valuable insight into the technical and organizational challenges that these types of incidents present to the European data protection community. The results of the exercise have already revealed the limitations of the current technical mechanisms used to cooperate in these situations and the need to develop new solutions to facilitate communication exchange. Challenging issues are mainly focused on the maintenance of a single point of contact list, communication issues, secure exchange of information, coordination procedures, applicable law and language issues.

The remainder of this paper is structured as follows. Section 2 discusses the inherent particularities of pan-European personal data breaches and examines some representative cases of such events. Section 3 details the experimental methodology that we undertook in designing and planning the cyber-exercise, whereas Section 4 discusses the exercise itself and how it was carried out. In Section 5, we review the findings that were observed based on the results of the cyber-exercise and propose a set of recommendations to address shortcomings in existing systems and processes. We conclude the paper in Section 6 by highlighting the current challenges and mapping the way forward to address them.