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

ABSTRACT

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

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

* 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
0267-3649/© 2017 Apostolos Malatras, Ignacio Sanchez, Laurent Beslay, Iwen Coisel, Ioannis Vakalis; Giuseppe D’Acquisto; Manuel Garcia Sanchez; Matthieu Grall; Marit Hansen; Vasilios Zorkadis Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).
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.
2. Pan-European personal data breaches and the General Data Protection Regulation

The emergence and proliferation of cloud computing services and in general online services that are available to European citizens has greatly increased the security risks involved with personal data breaches. There have been many related security incidents lately and they serve to highlight the challenges that exist in regard to protecting private and personal data shared by European citizens. Moreover, data breaches that generally affect great numbers of people also have the adverse effect of diminishing the trust of citizens towards online services, thus directly impacting negatively on the promotion and growth of the EU Digital Single Market (DSM) strategy. The established shift towards large-scale, cross-border incidents of personal data breaches, where personal data belonging to citizens from several European Member States becomes compromised, further exacerbates the aforementioned security and privacy concerns.

It is important to clearly define the term Pan-European Personal Data Breach in order to solidly set the context and clarify any ambiguities that might emerge from the concerned legislation. In this respect, a Pan-European Personal Data Breach involves a breach related to personal data belonging to citizens (data subjects) from more than one EU Member State. This implies that there might exist data controllers located accordingly in more than one EU Member State, although this is not binding (e.g. one data controller might be in charge of data referring to data subjects from different EU Member States). The origin of the attack leading to the data breach or the location of its target is also irrespective for the breach to be classified as Pan-European. The sole criterion for a Personal Data Breach to be classified as Pan-European is for it to have affected citizens, i.e. data subjects, from multiple Member States.

Based on this definition, Case studies 1 and 2 describe two typical examples of pan-European personal data breaches that took place in the last years. While retaining anonymity of the data controller, the case studies serve to expose the challenges and issues that can be associated with pan-European personal data breaches nowadays. It becomes clear that handling of such incidents currently does not occur in a standardized and uniform manner. Moreover, the issue of the leading authority, and that of the inter-DPA communication channels are prominently challenging.

---

**Case study 1**

A notable data breach involved personal data including user credentials, bank account and credit card details of almost 1.5 million customers from a Member State, out of more than 70 million in total. The controller was not a telecom operator and it was established outside the EU territory. The local DPA was informed about the event by the press. The personal data affected by the incident were stored in a server located in a data centre in the US. The data controller notified the incident to the affected customers via a generic email and also through their website about a week after the discovery of the data breach. Also, a series of new technical and organisational security measures were announced, aimed at better protecting the violated systems such as moving the servers to a new location with stronger protection and implementing audit and alert functionalities; cryptographic safeguards were strengthened and a post of Chief Information Security Officer was established. Taking into account the type of data controller and the fact that it was not established in the EU, no formal case was initiated by the local Authority. Another European DPA however initiated an action vis-à-vis the national branch of the controller. Contacts were set up between the two DPAs and exchange of information took place in the months after the security incident to take stock of the progress made in implementing the relevant security commitments.

---

**Case study 2**

Another incident of a personal data breach affected more than 30,000 customers in a Member State (MS), involving user data (names, telephone numbers, email accounts) for billing purposes and website access credentials. The controller was established in another MS. The local DPA was informed about the incident neither by the national branch of the controller nor via the official notification channel, but the case was spotted on a website dealing with security related issues. A letter was sent by the local DPA to the national DPA (the “lead” DPA) of the MS where the controller was headquartered, signaling the case and asking for details concerning the personal data (if any) of involved local citizens, and a request for information on the incident was issued to the national branch of the company. The controller replied to the local DPA reporting on the number of local citizens involved, the type of personal data involved and giving a description of how the incident was generated. At the specific request of the local DPA, the controller informed the customers of the data breach by email and provided a link to a website where further details could be found (in the customers’ national language) along with instructions to restore their passwords. The company, consisting in the implementation of a new VPN and the refreshment of all system administrator accounts, adopted additional security measures internally. The controller also provided the local DPA with the contact details of the officials who were dealing with the case for the “lead” DPA. The measures were considered as adequate by the local DPA, even if no inter-DPA contacts were ever established and the case was handled without coordination between the two DPAs.
Effectively responding to personal data breaches incidents requires a multidisciplinary and multifaceted approach (technical, policy, regulatory, financial and social aspects) involving all the concerned stakeholders, namely the data subject, the data controller and the data protection supervisory authorities. Coordination, collective information sharing, and decision-making are primary to the successful handling of personal data breaches incidents. In particular, cross-border personal data breaches incidents bear a series of additional challenges when considering the operations and techniques that need to be put in place to handle and address them. The current EU legislation (Commission Regulation 611/2013 (EU Regulation, 2013)) requires that “competent national authorities should cooperate in cases of personal data breaches having a cross-border dimension”.

Moreover, Article 2 paragraph 5 of the Regulation 611/2013 states that “where the personal data breach affects subscribers or individuals from Member States other than that of the competent national authority to which the personal data breach has been notified, the competent national authority shall inform the other national authorities concerned. To facilitate the application of this provision, the Commission shall create and maintain a list of the competent national authorities and the appropriate contact points”. This is indeed the case of Pan-European Personal Data Breaches, however the handling of such events in a coordinated and systematic manner is not addressed within the Regulation. On the contrary, the GDPR makes specific such provisions. In addition, whereas the current regulation applies only to certain type of service providers, i.e. telecommunication providers, the forthcoming EU data protection regulatory framework extends the scope of applicability.

Upon the occurrence and detection of a personal data breach, targeted reactive measures should be triggered in order to reduce the adverse impacts that the specific breach might have over the several actors involved, particularly the individuals whose personal data was affected. Accordingly, under the current legislation it is mandatory that the personal data breach be reported to the competent national authorities and in this respect, the content of the notification in the context of EU has been harmonized. Nonetheless, the existing practices in handling cross-border incidents of personal data breaches at a European level remain unchartered. Additionally, there exists the requirement to notify the individuals whose data has been breached should the breach be considered likely to adversely affect them. The latter condition makes it difficult to have a uniform handling of the personal data breach especially when cross-border incidents are considered, since the interpretation of the notion of “adverse effect” is left to each individual national authority.

The General Data Protection Regulation that was published in May 2016 aims to address such concerns. It extends the scope of data controller to consider all entities that handle personal data and not only to telecommunication providers. In this respect, the applicability of the new data protection regulation will be more comprehensive since nowadays it is widely accepted that personal data from citizens are not only handled by telecommunication providers, but also from many other types of service providers over the Internet. The data controller has the obligation to notify the supervisory authorities about the data breach and subject to specific requirements being met should extend this notification to the affected data subjects as well. These are defined in Articles 33 and 34 of the Regulation.

In terms of the cross-border nature of personal data breaches, one of the main objectives of GDPR is to lead to consistency of data protection in EU and this justifies the transition from a Directive to Regulation. The particularities of cross-border incidents of personal data breaches are addressed in several articles of the GDPR. The notion of a lead authority in case that a data controller is established in several Member States is introduced in Article 56 as “the supervisory authority of the main establishment or of the single establishment of the controller or processor”. Additionally, articles 60, 61 and 62 focus on the cooperation between supervisory authorities of different Member States when such a need arises, as for example would be the case of a pan-European personal data breach. The requirement of mutual assistance by sharing of information and that of joint operations are clearly highlighted in the GDPR. In Article 61 in particular, it is mentioned that “supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner and shall put in place measures for effective co-operation with one another”. It becomes therefore evident that works such as the one in the context of the Pan-European Personal Data Breaches Exercise (PEPDBE) are extremely timely in providing support to the DPAs to accommodate the novelities introduced by the GDPR.

From a more general point of view, cooperation between DPAs of EU Member States is a significant challenge that has attracted attention from practitioners and researchers alike (Hijmans, 2016). In particular, the EU-funded project PHAEDRA II (PHAEDRA) (Improving practical and helpful cooperation between Data Protection Authorities II) aims to improve cross-DPA communication with the goals of achieving consistency, exchange of information, and cooperation regarding enforcement actions. The case of Pan-European Personal Data Breaches and the GDPR that we discuss in this paper can evidently be considered within this perspective and as such, the work of PHAEDRA deliverables such as Galetta and Kloza (2016) and Dariusz and Anna (2014) is very important (Galetta et al., 2016). maps existing cooperation schemes and mechanisms in order to ascertain whether they can be generalised and applied in a wider context. Furthermore, the challenges and recommendations discussed in (Galetta and Kloza, 2016) are consistent with our findings, in particular regarding the need for specialized ICT platforms and for supporting translation services.

Of particular interest is the recent work presented in (Barnard-Wills et al., 2016). The authors conducted a series of interviews with DPA experts and the European Data Protection Supervisor in order to register and highlight issues concerning coordination of DPA efforts across Europe in light of the forthcoming implementation of the GDPR. The authors analysed the results of the interviews and compiled a list of challenges and open issues, which are quite consistent with the findings of our work. We consider this work complementary to the one presented in this paper, since both study the same domain but from different standpoints. While the work presented in (Barnard-Wills et al., 2016) focused on identifying key points concerning cooperation between DPAs by means of analysing interviews and policies, we undertook a more practical approach. Accordingly, we set up a practical, large-scale
simulation exercise supported by appropriate ICT tools to assess relevant issues under realistic conditions. It is noteworthy that both standpoints reach similar conclusions.

3. Methodology

We set out to map current practices concerning the handling of pan-European personal data breaches events. We decided to conduct a large-scale simulation cyber-exercise that on one hand will map the current situation in the field and on the other hand will identify challenges and problematic areas. This type of simulated exercise has already been very useful in the past in similar dynamic and adaptive scenarios where many interactions between stakeholders take place (ENISA, 2011, 2012a). The 1st Pan-European Personal Data Breaches Exercise is a simulated event-driven exercise that aims to monitor currently established procedures, identify problematic areas and conduct analysis of the observed results to increase preparedness and mitigate prospective problems. Players and stakeholders are presented with a simulated incident of a personal data breach and are progressively provided with information and updates on this incident. The aim of the exercise is to observe how players handle this information and the various events in a realistic manner (Hoffman et al., 2005). An important notion regarding the exercise is that of “event”. Events were instantiated during the exercise to spur actions on behalf of the involved actors. Examples of events included the disclosure of some piece of information, citizens’ requests, data breach notifications, data controller actions, etc. By simulating a series of realistic events, we were able to monitor the actions of the various stakeholders in handling a pan-European personal data breach according to existing practices.

To tackle this goal we adopted an iterative methodology, whereby the requirements analysis phase included the interested parties, namely the DPAs, and comprised a series of meetings to establish their needs and identify the current shortcomings. Our methodology is based on existing methodologies and recommendations on how to conduct simulated cyber-exercises and in particular Kick(2015) and Grance et al. (2006). The steps of the methodology are shown in Fig. 1.

Defining the objectives of the exercise was the first step. It is of paramount importance because it sets the scene for the entire exercise and allows all interested parties to agree upon the scope of the exercise and its expected outcomes. A preliminary workshop with all stakeholders was conducted in order to elicit their views on the exercise and focus on the issues that we intended to examine by means of the cyber-exercise. During this meeting, the focus of the exercise was pinpointed to be that of pan-European personal data breaches and the particular area of study was identified as that of establishing current practices and examining the interactions between DPAs when such events take place. During this workshop, we performed a group dynamics exercise to kick-start activities and to identify broad areas of interest and challenges concerning pan-European personal data breaches incidents. The aims of the initial workshop were twofold, namely to identify realistic pan-European personal data breach incidents for the forthcoming cyber-exercise and also to provide a preliminary look at the current practices and interactions among the several stakeholders.

The aforementioned workshop also served to fulfil the second step of our methodology, i.e. selecting the approach to follow in conducting the cyber-exercise. In the field of IT and network security, cyber-exercises have been extensively used to educate users, as well as to study possible attack and defence strategies in a constrained environment (Conklin, 2006). Broadly speaking, cyber-exercises can be classified at three different levels, namely technical, operational and strategic (ENISA, 2015). At the technical level, information security cyber-exercises deal with incident detection, investigation and mitigation, as well as the exchange of data and information, whereas at the operational level cooperation, coordination, crisis assessment and tactical analysis are the focus. Lastly, at the strategic level, strategic decision-making and high impact management of public interest are concerned. This hierarchy of the scope and functions of cyber-exercises can be seen in Fig. 2.

There exist many different types of cyber-exercises for information security (ENISA, 2012b), e.g. capture the flag (DefCon Capture The Flag Archive; Walden, 2005), cyber defence exercise (Conklin, 2006), full scale functional (Benzel, 2011; Liljenstam et al., 2005), serious games (Tesei et al., 2012) to name a few. Since the focus of this work was to map best practices for cooperation and coordination between DPAs and examine aspects of their interactions, such types of exercises were not considered as suitable to serve the desired purpose. Instead, we opted

![Fig. 1 – Methodology followed to design, set up and run the PEPDBE.](image-url)
for an event-driven, operational level game-based cyber-exercise (INCIBE, 2015). Game-based exercises describe a specific scenario and their goal is to explore the internal workings and the decision-making process that is involved, without exploiting real resources. Therefore, the approach that we adopted for the cyber-exercise is that of a distributed desktop exercise according to the terminology used for such exercises (ENISA, 2012b).

Having decided on the type of cyber-exercise and its objectives, we organized a second preparatory workshop with all interested stakeholders in order to define the scenario. This step of the methodology is very important since the scenario should be defined and constructed in such a manner to allow for all the objectives of the exercise to be met. This implies that the open issues and challenges that we wished to examine by means of the cyber-exercise needed to be part of the scenario in order for the stakeholders that participated in the exercise to be able to address them. A scenario definition was proposed to the DPAs that were part of the cyber-exercise and it was finalized after considering their fruitful feedback and deliberation over its distinct elements. The open challenges and issues that were unveiled during the preparatory workshop and subsequent stakeholder meetings served as requirements for the setup of the 1st Pan-European Personal Data Breaches Exercise. Accordingly, they were used to formally define and agree upon the simulation scenario, namely the mock-up pan-European personal data breach that the DPAs would collectively manage. In particular, some of the issues that we wished to study with PEPDBE involve the following:

- Current processes to handle pan-European personal data breaches;
- Communication protocols between DPAs;
- Communication between data controllers and DPAs;
- Sharing and exchange of information among DPAs;
- Notification of users subject to pan-European data breaches incidents;
- Designation of lead authority among DPAs;
- Handling of fragmented information from data controller due to the pan-European nature;
- Language/translation issues due to the pan-European nature of the considered incidents;
- Sources/channels of information utilized by DPAs in regards to personal data breaches incidents.

Considering these challenging issues, we designed a cyber-exercise to simulate a realistic undertaking of a pan-European personal data breach incident. We devised a scenario entailing elements that would trigger interactions between DPAs, data controllers and other stakeholders. A third workshop was organized to collectively agree with all stakeholders on the scope of the exercise (goals and limitations), to set the rules regarding the execution of the exercise and to perform a test run of the exercise. The scope of the exercise was limited to the monitoring of the handling of personal data breaches incident that are pan-European, i.e. more than one EU Member State is involved, and the goals included the mapping of current practices and the pinpointing of problematic areas. In terms of limitations, the simulated nature of the exercise imposed restrictions on how realistic the exercise itself would be. For example, simulated news websites were used as substitutes of real ones to spread information about the data breach and a constrained contact list was distributed to all participants to ensure that the exercise would remain confidential and not interfere with regular operational procedures of the participating parties.

During the test run of the exercise and in preparation for its actual execution, all participants were instructed to follow a set of rules of conduct. These rules were discussed and formalized during the third workshop. All involved stakeholders were asked to act as per their normal daily routines in their own offices and according to their current rules of conduct, i.e. they were responding to events according to their current established practices since this is an aspect that we wished to capture. Concerning the setup of the exercise, we distinguished between three roles, namely the exercise moderators,
Exercise moderators were in charge of executing the exercise. They managed the scenario and ensured that events were triggered when necessary, while additionally they assisted national moderators when needed and kept track of the proper execution of the exercise. It was their responsibility to cater for contingency measures in case of adversities and they were physically located at the headquarters of the exercise in the premises of JRC. The exercise moderators supervised the training of players and national moderators and provided them with related material. Moreover, during the exercise, they were sending event-related information to various actors and they were responding to players’ actions by assuming the role of various virtual actors, namely entities such as police authorities or affected citizens that were not physically part of the exercise. Lastly, exercise moderators were collecting feedback from all stakeholders after the finalization of the exercise.

National moderators were responsible for moderating the participation of their national DPA in the exercise and they were collocated with the exercise moderators. The moderators were members of the corresponding DPA and they acted like the rapporteurs of the exercise. They collected all the PEPDBE status reports that were submitted by players during the exercise. The moderators were also complementing status reports with their own comments and observations, since they were observing the players actions, decisions and procedures during the exercise. In addition, they were also in charge of handling problems that arose at the national level, e.g. communication issues with non-operational email addresses, and accordingly provided input to the exercise moderators. Finally, yet importantly, the national moderators completed the evaluation documents for their country and provided feedback on the PEPDBE and its results after its completion.

The players were members of DPAs from EU Member States that participated to the PEPDBE and they were located in the premises of their respective national DPAs. To achieve our goals, it was extremely important that during the exercise the players would handle the event as they would in their normal, day-to-day work procedures. This was communicated in advance to the players and with the assistance of the national moderators was enforced during the exercise. Players’ events mostly came in the form of an email, but also phone calls or even simulated websites were also used to communicate events. Contrary to the exercise and national moderators, the players were unaware of the scenario and responded to relevant events, as the scenario was unfolding. They reported to their national moderator any problems that occurred during the exercise and facilitated the latter in observing the execution of the exercise, e.g. by providing access to internal and external communications.

Players and national moderators were instructed to follow a policy of conduct in order to facilitate the exercise, the analysis of its results, as well as to avoid sharing any information, links or electronic communications records with anyone outside the scope of PEPDBE. All means of communications that were part of PEPDBE were tagged with a disclaimer to clearly state the simulated nature of the communication.

The actual exercise run was conducted in more than one location (namely the EC Joint Research Centre (JRC) at Ispra premises and the local sites of participating DPAs). The final step of the methodology that we followed consisted of the analysis and evaluation of the outcomes of the exercise. We report in the following on these aspects and propose a set of recommendations on improving the current state of handling of pan-European personal data breaches incidents, as well as proposing practical solutions to address the pinpointed issues.
4. Pan-European Personal Data Breaches Exercise

The JRC carried out the 1st Pan-European Personal Data Breaches Exercise in November 2015, in collaboration with the Directorate-General for Justice and Consumers and the Data Protection Authorities of seven European Member States. The cyber-exercise was 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 helping identify best practices to handle such incidents. The JRC in collaboration with the seven participating DPAs designed PEPDBE. It consisted of a live simulation, which recreated a realistic scenario where the personal data of millions of European citizens across several Member States are breached (in a simulated social network). In this scenario, agile and effective collaboration between Member States was required in order to respond and manage the situation in the best possible way.

4.1. Simulated scenario

Following a participatory approach that took into account the viewpoints of all stakeholders, we designed a simulation scenario that is representative of pan-European personal data breaches cases. Although some existing products and services, as well as actual pan-European incidents have inspired this scenario, we need to underline that the entities, products and services described as part of the scenario, as well as the scenario itself are completely fictional.

The data controller, namely the entity that suffers the data breach, refers to an instant messaging application with social media features specifically designed for mobile devices, with clients also available for desktop systems. The company offers services to all European Member States and it has a large and ethnographically diverse user base. The company has its headquarters in a Member State, the DPA of which participated in the cyber-exercise, but local subsidiaries also exist in the other participating Member States.

The scenario commences with an online posting of some personal information from customers of the data controller, but initially the leaked data cannot be associated to the data controller. Progressively all participating DPAs are made aware of the leaked data through various means such as citizen reports, online media and social networks or other bodies such as technical journalists, NGOs or privacy advocates, all of which were simulated by the exercise moderators. The motivation for this progressive spreading of the news was to examine the possible communications and interactions between DPAs at the beginning of a personal data breach when information is sparse and fragmented. Following the initial breaking news, a full-scale leak of breached personal data is posted online in a simulated forum and this is once again progressively disseminated to all DPAs. At this stage, it can be established that a pan-European personal data breach has occurred and the data controller can be identified. Simulated news websites were utilized to confirm the data breach and make it public knowledge.

Citizens were contacting their respective DPAs in order to gain information and support regarding the data breach or even to report unusual activities in their accounts. In doing so, we explored various means of communication to establish current practices and in addition we examined the possibility to support encrypted means of communications. During all these events we were monitoring the actions of the different DPAs in handling such requests, as well as any interaction that occurred between DPAs, e.g. asking for information. We also considered simulated police authorities asking DPAs for information to examine the potential penal aspects of a personal data breach and study how they are currently managed, as well as requests made by media for public statements to map the manner in which they are handled taking into account the pan-European nature of the event.

Initially, the data controller claimed to have no knowledge of a data breach that had affected it. In the course of the exercise, and after several DPAs contacted it, the data controller issued first a public statement acknowledging the existence of a data breach of personal nature and subsequently filed a data breach notification to the DPA where its headquarters were located. During the interactions between the DPAs and the data controller we explored issues pertaining to the language used and the possible need for translations. It has to be noted that the exercise moderators who had assumed this role simulated the data controller and all of its actions.

Subject to the personal data breach notification that was submitted by the data controller, the DPA to which it was submitted proceeded along with the standard procedures to the actions that are required by the existing legislation. In order to further study the impact of the cross-border nature of the event, the other participating DPAs were motivated to contact the one that had received the notification. For this purpose, simulated requests from citizens, journalists and other external bodies were triggered. In parallel, further information regarding the data breach were posted in the simulated news feeds and social networks to stress out the pan-European nature of the event and its significance and accordingly to monitor current practices of DPAs.

The simulated scenario was concluded with an updated formal notification submitted by the data controller, where the number of affected citizens and the wide geographical scope of the exercise were reported.

4.2. Running the exercise

This cyber-exercise in the domain of data protection was the first of its kind. A total of 20 data protection professionals were involved in the cyber exercise including both local and remote teams from each of the DPAs that participated to the initiative. The simulation was powered up by a new version of the web-based “EXITO Narrator” tool developed by the JRC (Benoist et al., 2012). Narrator is essentially a programmable finite state machine capable of simulating several scenarios. This tool facilitated the proper flow of events and managed 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. Fig. 4 illustrates the
number of communications exchanged between participants in relation to the different events of the scenario. It is evident that there are peaks in the number of monitored communications during events of high importance such as the breaking out of the news regarding the personal data breach and the notification by the data controller.

The “EXITO Narrator” tool was used by the exercise moderators to control the flow of the exercise and monitor received feedback, as well as by the national moderators to keep track of the execution flow of the cyber exercise and to provide feedback according to the actions and activities of their designated players. Players themselves did not have access to the simulation tool. It is a web-based exercise management tool specifically designed to drive high-level political cyber-exercises. It focuses on the story-telling aspect of the scenario presenting it to players as a synchronized sequence of media-rich briefings, to feed the decision making process. It also captures status reports that are submitted by its users in the form of contextual feedback. At any point, users can leave feedback on the exercise process, which will be accessible by the analysis team in the debrief phase. The initial version of “EXITO Narrator” featuring the described features was released in 2014 under the European Union Public Licence (EUPL) (EXITO Narrator Online Repository, 2016).

Furthermore, in order to provide to the players a more immersive experience during the simulation, we developed a new component called the Narrator Event Server (NES). This component brings an additional level of semblance to reality to the scenario by increasing its interactivity. In this respect, the NES provides emails from virtual entities and simulates virtual websites and dynamic services such as news, forums, RSS and social networks. By utilizing the NES it is possible to design a scenario in a way that the players are able to participate in the simulation in a more immersive manner without needing to access the web-based interface of the “EXITO Narrator” tool that is exclusively used by the moderators. This was the case of the simulation carried out in the Pan-European Personal Data Breaches Exercise, where the players interacted with the scenario exclusively through their working emails, websites and online services simulated by NES, to make the simulation as realistic as possible.

The scenario was mapped from its high-level description to a series of specific events in order to accommodate the event-driven nature of the simulation. Accordingly, the Master Scenario Event List (MSEL) was compiled, which details the different events that are defined in the “EXITO Narrator” tool and the time that they are expected to be triggered. There are two notions of time, namely the actual time during the exercise and the simulated time that refers to the simulated data breach. An important parameter involves the amount of time to be given to the DPAs to handle various events: given too short a time, proper responses will not be provided; too long a time will extend the duration of the exercise. In an attempt to strike a balance, we opted for a 10–15 minute slot for the handling of each event.

5. Findings and recommendations

The analysis of the exercise’s results provides valuable insight on the technical and organizational challenges that these types of incidents present to the European data protection community. The findings of the exercise have already revealed the limitations of the current technical mechanisms used for cooperation in these situations and the need to develop new solutions to facilitate communication exchange. Challenging issues are mainly focused on establishing a list of single point of contact, appropriate communication channels, secure exchange of information, coordination, applicable law, language and translation, and the need for additional cyber-exercise of this nature. In accordance to the findings of this 1st Pan-European Personal Data Breaches Exercise, a series of recommendations are proposed to address the identified existing challenging issues.
5.1.

Addressing the lack of single point of contact list

The lack of an established communication list among DPAs as far as the competent officers in charge of pan-European personal data breaches are concerned greatly hinders cooperation between DPAs. As it stands, personal contacts and ad hoc means of setting up communication channels are being used and it can be clearly stated that such an approach, far from being efficient, undermines efforts towards effectively responding to and handling of cross-border incidents of personal data breaches.

In this respect, we propose the development of an EU-wide single point of contact list. A single point of contact communication list involving competent officers, i.e. officers having expertise on personal data breaches, of the DPAs of all European Member States needs to be established. The list must be constantly maintained and kept up to date, as well as be made accessible to all interested institutional stakeholders.

5.2.

Catering to the lack of technical means for the agile and reliable exchange of information

The widespread use of email nowadays to exchange information and to communicate in general raises major concern as observed during the exercise. The current state of the art of email systems suffers from delays, misconfigurations and reliability. There is therefore an evident need to support communication channels between interested stakeholders and in particular DPAs to facilitate the agile and reliable exchange of information.

Our main recommendation entails the development of a platform to support exchange of information in the handling of cross-border incidents of personal data breaches. In particular, an agile and reliable communication platform that will complement and potentially replace current email-based communication needs to be designed, implemented and deployed. The platform should have a diverse functionality that facilitates cooperation and coordination of actions of different DPAs. The platform could be used to ensure a smooth transition between the existing European Commissions Directive 95/46/EC (EU Directive, 1995) and the upcoming General Data Protection Regulation, as well as to avoid overlaps by means of keeping track of the various steps of the process, e.g. contacted headquarters or national branches of the data controller. Additionally, it could act as a checklist of good practices, such as ask the controller to provide alerts or warnings in different languages. Such a platform would also address the issue of the lack of a single contact list, since all involved stakeholders will have access to the same platform and thus become informed on all developments regarding pan-European personal data breaches incidents.

5.3.

Need to harmonize and facilitate the secure exchange of information

An issue that was underlined by the majority of the participants in the cyber-exercise concerned the need to securely and reliably exchange information. In many cases and due to the cross-border dimension of the pan-European personal data breaches incidents it is necessary for DPAs to exchange information regarding the incidents themselves, as well as concerning the handling of said incidents. This information is extremely sensitive and needs to be delivered in a timely and reliable manner. Nowadays there does not exist any harmonized and systematic means of secure exchange of information between DPAs, which is a major hindrance in the efficient and effective tackling of pan-European personal data breaches.

Provision of harmonized procedures and technical means for the secure exchange of information emerges therefore as a major objective. The secure and reliable platform that was mentioned before will also be used to facilitate secure exchange of information by ensuring the integrity, authenticity, confidentiality, availability and traceability of the transferred information. Data encryption techniques will be used to satisfy these requirements, as well as secure communication protocols. It is also very important to establish common harmonized procedures and protocols to perform secure exchange of information. The use of a dedicated platform with well-defined use cases will ensure that all stakeholders adopt such common procedures.

5.4.

Lack of harmonized procedures to support cooperation in the handling of cross-border incidents of personal data breaches

The Pan-European Personal Data Breaches Exercise highlighted that there are currently no established practices on handling pan-European personal data breaches incidents and accordingly their handling is performed in an ad hoc manner. Reaching consensus and responding to such events in a harmonized and uniform way are extremely challenging tasks, which are exacerbated by the fact that information regarding the events is often dispersed among different DPAs. Based on the experience gained by the cyber-exercise, with the support and contributions of the DPAs community the aim is to identify, design, and implement appropriate procedures to handle cross-border incidents of personal data breaches in a methodical and systematic manner.

Accordingly, we propose to promote the development of agreed systematic processes to harmonize the cooperative response to pan-European personal data breaches incidents. Well-defined, systematic, documented and methodical processes need to be put in place in order to harmonize and homogenize the handling of pan-European personal data breaches incidents. In particular, issues such as coordination and collaboration, leading authority designation, reaching consensus and sharing of information are of the utmost importance. These commonly agreed processes would have to be followed by all the stakeholders to manage effectively such incidents.

5.5.

Difficulties in the interpretation of the applicable law

There was some ambiguity regarding which DPA would take the lead and contact the data controller of the company affected by the pan-European personal data breach and whether only the Member State where the company had its headquarters would be contacted or local subsidiaries would also be asked for information. This aspect highlighted some shortcomings of the current legislation that will be eventually addressed by the forthcoming General Data Protection Regulation (GDPR) proposed by the Commission in 2012 and recently adopted in May 2016, in particular with regard to articles 60, 61 and 62 on cooperation.
Therefore, better support for legislation should be provided. In light of the upcoming General Data Protection Regulation and taking into account the inter-DPA interactions in the context of pan-European personal data breaches, a task force of specialists needs to harmonize the process concerning the applicable laws. This task force can provide useful and concrete contributions to the forthcoming definition of the General Data Protection Regulation implementation measures.

5.6. Language issues

While language issues and the need to translate information due to the cross-border dimension of the events were pinpointed as important aspects, they were nevertheless adequately addressed during the cyber-exercise. It remains however, an open issue how to tackle this challenge in a homogeneous and systematic manner and not in an ad hoc fashion as it is currently the case.

We thus recommend increasing support for internationalization. Support needs to be provided to the community of DPAs to automate and harmonize translation services in order to avoid ambiguities that arise due to poor or incomplete current processes. The platform for the handling of pan-European personal data breaches should be equipped with translation tools to address this concern. The use of other means of translation services should be discouraged to hinder ambiguities. Moreover, because online translation tools may keep records of requests by users, the use of a dedicated translation tool for the platform would greatly promote confidentiality that is of paramount significance for the cooperation between DPAs.

5.7. Usefulness of the Pan-European Personal Data Breaches Exercise in promoting cooperation between DPAs

It was widely acknowledged by all the participants that the Pan-European Personal Data Breaches Exercise had a very positive outcome in terms of both the handling of events of such nature, but also in terms of promoting collaboration between DPAs. It served as an excellent training tool for DPAs to collectively address a challenging issue and to do so in a practical, hands-on manner.

Carrying out periodic Pan-European Personal Data Breaches Exercises including all DPAs is highly recommended. As attested by the feedback received from the participants, the cyber-exercise has been found to be very helpful in promoting cooperation between DPAs and as a vehicle to deliver training in the handling of pan-European personal data breaches. It is therefore proposed to conduct periodic cyber-exercises of this kind including DPAs from all European Member States. Moreover, in line with the other recommendations, future cyber-exercises can also explore the practical usage of the procedures and technical means that may be developed specifically to support cooperation.

6. Conclusions

We described in this paper our work on the planning, organization and conducting of the 1st Pan-European Personal Data Breaches Exercise, which was the first of its kind in the field of data protection. The particular challenges that arise when considering personal data breaches events of cross-border dimension require additional efforts on behalf of all involved stakeholders, as well as modifications of existing processes and incorporation of novel techniques and methodologies. The potentially sensitive nature of personal data involved, as well as the associated security and privacy risks, calls for the prompt, effective and efficient handling and management of incidents of such nature. Such incidents are becoming more and more common especially in the EU of 28 Member States moving towards a Digital Single Market, attributed to the proliferation of online, cloud-based, cross-border services offered to citizens that exchange and share personal data when using such services.

Current practices as applied to personal data breach events that are confined within a single state can evidently provide useful guidance in handling events of larger scale that are additionally cross-border. However, pan-European personal data breaches have significantly increased degree of complexity in terms of coordination, need to exchange information as well as legal concerns regarding responsibilities of Data Protection Authorities, i.e. who is leading the process and who is responsible for what. Distributed collaboration, coordination and reaching of consensus is a challenging task on its own and becomes even more challenging when the element of personal and potentially sensitive data and its protection is taken into account.

Building on this need and the currently established limitations, we planned and organized a simulation cyber-exercise with the clear aim of promoting and improving collaboration between Member States when cross-border incidents of personal data breaches occur. The cyber-exercise served accordingly as a training exercise for data protection officials and it greatly assisted in mapping existing procedures and helped to identify best practices to handle such events. The analysis of the cyber-exercise results provided valuable insight on the technical and organizational challenges that these types of incidents present to the European data protection community. The results of the exercise 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.

With cross-border incidents of data breaches becoming more and more common and with the increased need to promote harmonization, this cyber-exercise constituted an example of possible initiatives to promote cooperation among DPAs in order to facilitate an effective collaborative and coordinated response to such incidents. Accordingly, the next steps of this research effort aim to support the current and forthcoming EU Data Protection legislative framework with respect to the requirement of collaboration between European Data Protection Authorities in pan-European personal data breach events.

REFERENCES
