EDPS-ENISA Conference: Towards assessing the risk in personal data breaches

4 April 2019, Brussels

EDPS and ENISA organized a conference aiming to touch upon the current state of play in personal data breach notification, both from the perspectives of the regulators, as well as the data controllers/processors, while addressing the aspect of risk assessment.

This report provides the main points and key messages presented by speakers of the conference.

*****

Welcome messages

Wojciech Wiewiórowski, Assistant European Data Protection Supervisor

Mr. Wiewiórowski opened the conference, outlining that data protection laws are among those laws that European law has imported from the national solutions both from within Europe and without and stressing that there were several data breach notification systems that existed previously on a national level. Both GDPR and the Data Protection Regulation for EU Institutions (EDPR) have introduced the general system of data breach notification. Interestingly, Europe already had experience from sectoral solutions, most notably in the telecoms sector.

Mr. Wiewiórowski further focused on the aim of the conference on sharing and discussing experiences and issues encountered thus far from a very practical perspective, with a special emphasis on assessing the risks to the rights and freedoms of data subjects. To this end, the conference included speakers from European Commission DG JUSTICE who have experience with the legal scheme in GDPR, but also from DG CONNECT who have experiences with the telecoms sector and with the introduction of the NIS directive and the eIDAS Regulation. There will also be an opportunity to learn from national-level schemes, such as from the different Data Protection Authorities (DPAs).

Andreas Mitrakas, Head of Data Security and Standardization Unit, ENISA

Mr. Mitrakas presented ENISA's role in supporting capacity building at Member State level, encouraging cooperation on various levels such as cybersecurity exercises, and sharing expertise on cybersecurity. ENISA sees data protection as one of the areas of application of cybersecurity. But it also takes a broader inter-disciplinary view. To this end, ENISA has developed practical tools in cooperation with Member State authorities, for example a testing tool for data breach reporting. One of the core events of ENISA is the Annual Privacy Forum, which each year brings together research, policy and the private sector. The next edition in Rome will take place between 13 and 14 June 2019.

Mr. Mitrakas further focused on the recently adopted Cybersecurity Act, which gives another impetus to the works of ENISA, especially with a new role under the EU cybersecurity certification framework. ENISA has a great deal of experience work with conformity assessment bodies in terms of standardisation and follow up support. As ENISA moves into its new role in the EU cybersecurity certification framework, it will continue its cooperation with and support of Member States and the European Commission.

*****

Keynote Speech: Personal data breaches in the EU legal framework

Olivier Micol, Head of Data Protection Unit, European Commission - DG Justice

Mr. Micol started his speech with the observation that the issue of data breach should be examined at the juncture of Cybersecurity and the protection of personal data. Recently we have experienced several high-profile data breaches and the European Data Protection Board (EDPB) reported over 65.000 data breach notifications in 2018. Although, to be on the safe side, some operators might have reported some of these data breaches too zealously, the figures nevertheless indicate the importance of this issue.

Moreover, he noted that the requirements to notify data breaches take inspiration from other sectoral legislation, such as telecommunications, and that GDPR was inspired by the e-Privacy Directive. The idea was to integrate data breach notification into the data protection ecosystem. The Guidelines adopted by the European Data Protection Board on data breaches contributed to a harmonised understanding by stakeholders of the provisions governing data breaches.

Mr. Micol further stressed that the focus on data breach notification is to protect the individual – this is the first objective. It must reduce potential harm caused to the individual as also stated in recital 85 of GDPR, recital 61 of the Law Enforcement Directive and recital 61 of the Regulation 1725/2018 for EU institutions and bodies. This data breach notification system is linked to the overall concept of data security of article 32 GDPR. Importantly, the definition of a data breach is the same under GDPR, Regulation 1725/2018 and Law Enforcement Directive.

Furthermore, Mr. Micol referred to three types of data breach: confidentiality, integrity and availability breaches. The three legislations (GDPR, Regulation 1725/2018, Law Enforcement Directive) aim to prevent breaches but also to react speedily and limit the harm of the breach once it occurs. The mechanisms to do so are the same in all three pieces of legislation: firstly, the notification by the data controller to the supervisory authority (or lead supervisory authority in case of cross-border processing), no later than 72 hours, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons; and secondly, when the breach is likely to result in a high risk to the data subject, the communication from data controller to data subjects which must take place without undue delay. The swiftness in submitting a notification must be adapted depending on the risk (e.g. immediate risk of identity theft) . The information to be provided is the same across all three legislations. The process is triggered when data controllers become aware of the breach (the EDPB guidelines refer to a reasonable degree of certainty). Data controllers must therefore have organizational measures in place to identify and assess breaches. The 72-hour deadline allows for a short period of investigation by the data controller to assess the risk of individuals. The absence of precise information should not be a barrier to the notification of a breach. When it is not possible for the data controller to provide all information at the same time, he can do it in phases, starting with the information at his disposal. In cases where a data processor is first to become aware of a breach, he must immediately inform the controller who will then assess the risk. The failure to notify a breach exposes the controller to sanctions, which can be severe.

Mr. Micol finally stated that it is vital for controllers to develop a response plan in line with the accountability principle. Data Protection Impact Assessments might help in this regard. The Data Protection Officer (DPO) must act as a contact point to Data Protection Authorities. He also mentioned that the provisions on personal data breaches could contribute to fighting ransomwares because GDPR requires organisations who have suffered a breach notify, which limits the value of ransomware blackmail.

*****

Panel Discussion I: 'Personal data breaches under GDPR and EDPR: experience gained so far'

The panel, moderated by Thomas Zerdick (EDPS), aimed at presenting various cases of data breach notifications of the GDPR and EDPR and providing valuable information on the challenges the supervisory authorities are facing. To this end, it aimed at presenting in depth recent cases of personal data breaches while discussing open issues and challenges in the field. Some interventions of panel participants are presented in the following.

Max Rozendaal (Dutch DPA)

The Dutch DPA has had a data breach notification system in place since 2016. Since the implementation of GDPR, the Dutch DPA has received between 2000 and 2300 data breach notifications per month (specific statistics were presented during the presentation). The top sectors that have experienced data reaches are the financial and medical sectors. While the majority of data breaches still occur due to human error, a significant amount are the result of hacking malware and phishing. The Dutch DPA has also noticed discrepancies between how data breaches are assessed by controllers and processors. There are also differences in assessment between data controllers and the DPA. The DPA tends to be more concerned regarding the severity of a data breach.

The notification system in the Netherlands is completed via an online notification form. It uses a traffic light system and automatic categorisation to assess the severity of a data breach. Regarding the severity of a breach, there is a balancing act between the quality and quantity of data at risk. For example, 57 million emails and names versus in-depth info of 5 people.

The UBER data breach of 2016 provides an interesting case study. The nature of data stolen was online identities, but they were encrypted with hashing algorithms, which made it difficult for the perpetrators to reverse. Importantly however, the hashing algorithms used may be reversible in the future so it is essential to note which algorithm was used in case it is breachable in the future, in which case the data subjects must then be notified. Furthermore, there is often a significant time delay between the breach of information and the notification of the breach to the DPA and circumstances can change in this period, which should be kept in mind.

As a final point, Mr. Rozendaal, stressed that the most important thing to remember when assessing the severity of a breach is to never underestimate the risk a data breach can pose to data subjects.

Giuseppe d'Acquisto (Italian DPA)

In terms of statistics, 74% of data breach notifications in Italy come from the public sector. However, this does not necessarily indicate that the public sector is more at risk, just that the public sector is more likely to notify the relevant authorities because there is more awareness and they fear sanctions less.

Hacking is one of the primary cause of data breaches in Italy. The reason for this might be that the implementation of GDPR has drawn the attention of "activist" hackers. Furthermore, human error is a very common reason for data breaches. Different sectors also experience different types of breaches. For example, the medical sector mostly experiences "old-school" non-digital breaches, whereas the government sector experiences more hacking-related breaches.

The majority of data breach notifications concern small-scale breaches, with 46% of data breaches affecting under fifty data subjects. Currently, two-thirds of data breach cases in Italy are still open for investigation, split between the IT and legal departments of the Italian DPA. Of these open cases, the majority are between three and six months old. The notification procedure creates a backlog of cases. The investigation procedure is slow even though the notification system is relatively fast. Over 90% of closed cases were closed within six months.

According to a 2018 Ponemon Institute report, 56% of businesses have suffered at least one security incident within the last year and according to the Italian National Statistics Bureau, there are four million businesses in Italy. Therefore, Mr. d'Acquisto pointed that around two million security incidents are expected in Italy every year. However, a conservative estimate counted only 2000 data breach notifications in one year in Italy. The Italian DPA is currently only dealing with the "peak of the iceberg", but the workload has increased since GDPR was implemented. The vast majority of incidents are due to negligence in the implementation of article 32 of GDPR.

The Italian DPA receives a large number of notifications due to negligence, which are either discarded because the risk assessment indicates that the risk to data subjects is low, or if it is high then the DPA will intervene with enforcement actions or investigations. When cases are discarded, there is poor accountability because it is the DPA that assesses the risk, not the controllers. When cases are investigated, the DPA can prescribe technical and organisational measures, which requires investment for the controller. It can also prescribe the communication of the data breach to the affected data subjects. Finally, it may also choose to impose fines on the data controllers.

According to Mr. d'Acquisto, the discarding of cases can have some negative consequences. Discarded cases require a workload with little societal benefit due to lack of accountability for data controllers. It is also unmanageable in a 'full iceberg' scenario where all data breaches are reported, as it is too time-consuming given current resources of the Italian DPA.

As a final point, Mr. d'Acquisto stressed that there is a shared public interest to report and solve data breach issues. This will aid to gain knowledge on unknown incidents and will increase trust in digital services. Notification is very useful to enhance trust and to protect individual's rights in the data economy, but it is less suited for discovering negligence. There is no need to re-invent the wheel, but we need to work on the notification interfaces. For notification we need trust between DPAs and controllers, as well as skilled authoritative DPOs. To discover negligence, we need to promote users' role and certification mechanisms, finding the right incentives for disclosure.

*****

Panel Discussion II: 'Personal data breaches management: processes and procedures'

The panel, moderated by Prokopios Drogkaris (ENISA), aimed at addressing the overall circle of personal data breach management with emphasis on the processes and procedures that should be in place for the prevention, detection, as well as mitigation of a personal data breach. To this end, it aimed at exploring current practices and practical examples, while discussing open issues and challenges in the field. Some interventions of panel participants are presented in the following.

Jo van Damme (European Court of Auditors)

The European Court of Auditors (ECA) has had a data breach framework since 2014. Every organisation will have data breaches and therefore must have internal procedures in place to be used by staff and externals working off-premises. Awareness of the data breach notification system was originally fairly low in the ECA, so they ran an awareness campaign for the data breach framework which significantly boosted awareness.

If an organisation or company uses external contractors, such as service providers, there must be clauses regarding data breaches integrated in the contract, which is uncommon at the moment. The ECA does not sign contracts without proper data breach clauses at the time being.

It is important that data controllers take responsibility for breaches and notify as fast as possible. Organisations must also have defined values of severity in place in advance, related to how many data subjects are concerned, what kind of data is at risk, and who the data is from. The ECA conducted training and simulated several scenarios, which means templates are already in place for dealing with breaches. It is imperative that an action plan is in place in the event of a data breach.

The Data Protection Officer (DPO) must also follow up and enact the action plan in a real-life scenario. At ECA the DPO has the ability to request to shut down the entire system if risk is high.

Rosa Barcelo (Squire Patton Boggs)

Ms. Barcelo in her speech presented some practical tips for dealing with data breaches

As a first point, from a practical point of view, 72 hours is a very short time period for the notification of a personal data breach. Unless companies are prepared, they will miss the notification deadline. Therefore, there should be an incident response plan in place which includes an instrument to establish the steps that must be taken when a breach happens and information on who is responsible (within the company) and which authorities must be notified.

If there is a cross-border breach, companies need to know which authorities to notify in each country. Thus, they should ascertain in advance which is their ‘lead authority’. They should also be familiar with the notification template of the lead authority .

Finally, it is worthwhile having forensic services, lawyers, and PR companies at the ready.

It is also vital that companies train for an incident and have contracts in place. As a processor has to notify the controller without undue delay, there should be guidelines documented in the data processing agreement so that there are no surprises for the controller.

Once a breach occurs, the first action to take is to try and contain the leak without accidentally creating a separate problem when trying to fix the current one. For example, in the event of a data breach, companies should avoid breaching data privacy laws by shipping information of the leak to another country for forensic analysis.

Giampierro Nanni (Symantec)

Symantec has vast experiences with the essential tools and processes for the prevention and handling of personal data breaches. Symantec divides these processes into four main points: prepare, protect, detect, and respond.

Preparation requires appropriate risk assessment to identify threats and vulnerabilities in the system. All cases will be different, and no two organisations will have the same vulnerabilities. Recital 75 of GDPR outlines the risk of data and which data needs to be protected the most. It provides a good starting point for companies to know what needs to be done. Security against breaches must include some form of employee monitoring because the vast majority of data breaches occur through the end point.

There is a whole range of tools to protect against personal data loss and as such there is almost no excuse to not practice proper security methods. Nevertheless, even with proper security, this will not eliminate all risk of a data breach. Organisations should employ a zero-trust policy, that is to trust nobody and leave nothing to chance.

It is important that organisations have sophisticated detection capabilities. The ability to detect data breaches should cover multiple stakeholders and even extend to non-tech employees. This should involve continuous monitoring and pro-active event discovery. The shorter the detection time, the less sever the damage.

The response process should be well rehearsed, and the most important task is to contain the incident and then ensure the continuation of operations. Once an incident has been dealt with, it is essential to learn from the experience in order to mitigate the risk of future breaches.

Shadow IT & shadow data are a recipe for non-compliance and data subject risk. Shadow IT refers to unsanctioned apps in the cloud, accessed or downloaded, and used by the employees without knowledge of the IT department. On average, the number of apps run in a company’s cloud exceed a thousand. For example, an online PDF to Excel converter which requires users to upload and then download the processed file provides huge potential for infection and GDPR violations.

Agnieszka Wawrzyk (DG CONNECT)

DG CONNECT would like to share their experience implementing the NIS directive, which includes the security and notification requirements for Operators of Essential Services (OoES), and the Electronic Communications Code.

It is crucial to have some guidelines to the legal text of these directives to avoid confusion. For the implementation of the directives mentioned above, there were expert groups that came together regularly to discuss how the legal text could be translated into practical guidance. In the case of the NIS Directive, there is a regular sharing of experience and best practices to learn from each other across Member States. Member States work together with ENISA and DG CONNECT on the guidance to establish, for example, how to define a significant incident or how to measure its impact. One lesson learned was that the threshold for a ‘significant incident’ cannot be defined at the same level across all Member States because the parameters would not match from Germany to Malta for instance. Therefore, the threshold should be set at a national level. The guidance is a living document which can change over time. Following an incident, it is important to learn from it and to gather experiences from all Member States. The cooperation group is there for collaboration across Member States and the Directive does not define what the cooperation group should work on.

An example of such practical solutions was found for instance in a way to notify an incident. It was established that companies should be provided with at least two way to notify a security incident. If there is just an online form, this will be impossible in the case where the company loses internet or power, for example. Authorities must also ensure the confidentiality of the notification channel and include some form of authentication process to avoid fake notifications. As best practice, it was also found that authorities should send a confirmation message that it has received the breach notification. The notification process may occur in two stages: an initial notification with as much information as possible and then in the second stage a comprehensive report and analysis should be sent.

There can be a cross-border issue where information does not always flow between Member States. Member States discuss this issue in the Cooperation Group and working on ways to ensure coordinating and sharing information between competent authorities. Some are also working on a portal to report incidents or personal data breaches which the system then automatically sends to the competent authorities.

*****

Exchange of views with the EDPS

Giovanni Buttarelli, European Data Protection Supervisor

Mr. Buttarelli started his speech by stressing that there have been several recent high-profile data breaches, including Yahoo, Marriot International, Facebook and Uber, affecting billions of users. The constant risk of data breaches is significant. Since the first mandatory notifications of data breach were passed in California in 2002, these notification systems have spread across the world in response to increasing data security incidents. There are now 134 countries with data protection laws and there are only minor differences across countries for notifying data breaches. These obligations are here to stay.

According to Mr. Buttarelli, the risk of a data breach comes not only from a lack of security but also from the creativity of perpetrators of cybercrime, who are adapting and innovating. Therefore, security is an endless process. As, more and more data is processed and information about people becomes more comprehensive and precise, the damage caused by data breaches increases. The rate of cybersecurity issues is growing exponentially, and the complexity of cyber-attacks is rapidly evolving.

The EU is working towards building a cybersecure EU environment. As Mr. Buttareli outlined, in addition to cybersecurity measures and strategy, it should be clear to legislators and other actors that the risk of processing personal data must be limited. Security measures are an essential part of the solution but not the only one. It is also necessary to minimise the collection and processing of data, limit processing times, and make sure industry is considerate regarding the security breach system. To this end, Mr. Buttarelli stressed the need to maintain the existing legal safeguards. He further called for the EU legislators to complete their work on the e-Privacy Regulation by respecting GDPR and keeping security breaches as a key pillar. He stated that every additional day of delay, poses more risk of data breaches affecting companies and citizens, which can be devastating.

Moreover, Mr. Buttarelli pointed that the mandatory notification of personal data breaches is of central importance, as is the risk assessment of these breaches. He mentioned that we cannot underestimate this risk or individuals may suffer avoidable damage, but if the risk is overestimated then there may be a waste of resources. It is important to find the right balance and remain resistant to bureaucratisation.

Mr. Buttarelli further focused on the need to find new working methods from all involved in the processing of personal data, as well as the supervising authorities. Processors and controllers should implement substantive dynamic procedures. They must try to refrain from bombarding DPAs with questions and notifying non-important breaches. Europe needs to achieve a new culture in complying with these regulations. Of course, mistakes are made, but controllers must look at the substance and take a human centric approach.

The EDPS will continue to actively support the EU institutions and operationally supervise how EU institutions comply with their obligations. It will also invest to develop new internal procedures. The

EDPS will continue to work with ENISA both bilaterally and via other networks such as the Annual Privacy Forum.

Finally, with regard to the Working Party 29 Guidelines, Mr. Buttarelli mentioned that the EDPB has endorsed the document and a recent technological subgroup has been mandated to develop this further. The EDPS has accepted to act as a rapporteur. The EDPS will work to foster a new culture and develop new tools.

*****

Panel Discussion III: 'Supporting data controllers on assessing the risk of a personal data breach'

The panel, moderated by Athena Bourka (ENISA), aimed at exploring the risk assessment process in the context of a personal data breach on the controllers' side. To this end, the focus was on existing guidelines, best practices and examples with regard to risk assessment in the context of a personal data breach, as well as lessons learned from specific cases. Some interventions of panel participants are presented in the following.

Dina Kampouraki (EDPS)

The EDPS has been helping EU bodies to comply with the legal framework surrounding data breaches. It understood the necessity of providing specific guidelines which were published in November 2018. These guidelines give practical guidance regarding how controllers can identify, mitigate, report, and inform data subjects of a data breach. The EDPS created an online tool for the notification of data breaches by the EU institutions. It took into consideration relevant security measures for the protection of the confidentiality of the received notifications applying encryption at the notification process and limiting the processing of information by the staff at the EDPS. In order to aid the European Institutions and Bodies to comply with the legal framework on the implementation of the obligation to notify data breaches, and to help in creating awareness and grow the expertise, the EDPS has been organising various case studies within the DPO network and various workshops with many European institutions.

Security incidents will happen daily and are unavoidable, and is crucial that the institutions are able to detect them in time and deal with them accordingly. The EDPS has published guidelines on security measures in order to ensure that the EU institutions and bodies are well prepared.

In the EDPS' experience thus far, from the data breach notifications that have been received, it was clear that controllers took the necessary measures to mitigate the risk and also additional measures to ensure that they canavoid similar events in the future. In addition to that the European institutions and bodies frequently reported data breaches to the EDPS even when there was no risk and there was no legal obligation to do so and they often notified data subjects when not needed.

A risk assessment on a data breach is a case-by-case issue and is a difficult process. It is related a lot to experience and expertise. The controllers have been using different methods or/and methodologies to measure the risk and there is no standard method. EDPS is using specific criteria to measure the risk that have been also used by the DPAs. These criteria may include the nature and volume of data, the category of data subjects and the sensitivity of the data at risk. Data protection impact assessments (DPIAs) are also important to feed decisions whether incidents are of high or medium risk. Usually data breaches related to processing activities that required a DPIA may be an indication of medium to high risk impact on the rights and freedoms of the individuals. In the EDPS guidelines12 practical examples are included to help controllers make the right decision regarding risk assessment.

EDPS has observed some additional difficulties in relation to comply with the legal obligations. For example problems were recorded relating with the obligation to notify the breach within the 72-hour deadline. This was due to controllers not having the ready procedures in place or not knowing whether to notify. Internal communication problems were also observed within a controllers processing environment.

EDPS is currently working with the EDPB to enhance the guidelines on the Personal Data Breach Notification and especially to the aspect of the risk assessment.

EDPS is also aware that the DPO network must invest in developing awareness and training of staff among the EU Institutions and Bodies in order to detect breaches in time.

Nikolaos Fikatas (Fundamental Rights Agency)

Often, data controllers are familiar with risk issues but struggle to understand the concept of data protection, as they view it as a foreign concept even though it is not new. They consider it new due to the implementation of GDPR and the fines and reputational risk that come along with it. This explains some of the over-notification of unimportant data breaches. Controllers in the public sector prefer to notify the authorities because they think there is a risk and for transparency reasons. They also find it hard to find the balance between under and over reporting. There is a need for more clarity on when to notify and guidelines with examples and definitions.

Data management classification could be improved in order to better support the processes for internal risk management. Better mapping of the data that an organisation controls will facilitate easier understanding of the risk profile of the data. This mapping should be a made an integral part of processing operations in security plans.

The role of the DPO is very clear from the guidelines and regulations. The DPO must be informed when a data breach or security incident is detected and must also advise the controller on the data breach. The DPO must take responsibility before, during, and after a data breach.

Fernando Silva (Portuguese DPA)

Data controllers often see the obligation of data breach notification like reporting themselves to the police for speeding. On the other hand, the public perceives it as a transparency matter.

The workload for the DPAs is huge and much like the Italian DPA, the Portuguese DPA finds it hard to respond to every notification. It is important to implement mitigation methods after an incident is reported to limit the number of future notifications.

The supervising authorities carry out investigations sometimes because the public uses notifications as a way of complaining. In all cases, the DPA can support but cannot provide detailed advice to the controller.

The Portuguese DPA uses risk assessment criteria based on the ENISA methodology and its experience of similar cases based on volume, sensitivity and nature of data.

Since May 2018, the Portuguese DPA has received over 630 data breach notifications but fines have not been issued yet. In 2019, the DPA received 106 data breach notifications. A lot of breaches are not notified, particularly because many start-ups are not aware of GDPR and data breach notification obligations.

Patrick van Eecke (DLA Piper)

Since May 2018 and the implementation of GDPR, there has been a lot of uncertainty for companies regarding compliance with GDPR. DLA Piper conducted a survey that over the past 7 to 8 months, there have been over 60 000 data breach notifications across the EU but almost 50% of these happened in the Netherlands, Germany and the United Kingdom. This indicates that there is a lack of consistency when assessing the risk of data breaches which is a result of uncertainty in different countries. The biggest challenge is that the notification triggers are quite unclear, and in practice, a lot of the assessment appears to come down to the "gut feeling" of the data controller. There is no consistency or objectivity in the assessment.

There is a need for more clear objective criteria. Controllers often want a number risk-rating which they can then base their qualitative discussion on. DLA Piper created an automated decision-tree tool, based on ENISA and Article 29 Working Party guidelines, which produces a quantitative assessment of the risk for their clients. This quantitative assessment provides the groundwork then for a more in-depth qualitative discussion.

Erik Valgaeren (Stibbe)

There is often confusion at companies in the event of a data breach. The immediate actions that companies should carry out are to determine whether the breach is malicious or not, manage communications, contain the risk as much as possible, and finally take the strategic decision whether to restore service but then risk contaminating.

Fact finding is the next important step. But a lot of controllers do not have the capabilities to undertake the forensics aspect of this process. Therefore, it is sometimes wise to get assistance from external forensic experts or auditors.

In all cases, every action taken should be documented and logged. Other important data to collect concern: territorial aspects of the attack, nature of the data breach (human error, technology failure, malicious intent, etc.), data involved, categories/number of data subjects affected, time of the data breach.

*****

Closing Statements

Wojciech Wiewiórowski, Assistant European Data Protection Supervisor

Mr. Wiewiórowski outlined the need to use this discussion for further work in the field of personal data breaches. He also mentioned the necessity of comparative studies across the Member States regarding the ongoing actions at the various DPAs, DPOs, data controllers etc. He concluded that it is essential to continue to discuss and exchange examples on this topic.

Andreas Mitrakas, Head of Data Security and Standardization Unit, ENISA

Mr. Mitrakas stressed that better security measures will of course result in fewer breaches. However, when personal data breaches do occur, organisations must inform authorities. Perhaps the authorities can work on tagging data properly and streamline the reporting process in order to aid data controllers. He concluded that in the future 5G will exacerbate data security and privacy issues, so it is imperative that we get this right today.