SASIG-IAAC Masterclass- "Countdown to EU GDPR"- Discussion report

Organised by: The Security Awareness Special Interest Group and the Information Assurance Advisory Council (IAAC)

Hosted by: Aviva

Report written by:
Mindaugas Bazys, Rapporteur, IAAC

Friday, 27 January 2017
8:30am to 1:30pm

The report stems from an event run under Chatham House Rules. Consequently its content has not been attributed. Best effort has been made to represent the discussion and themes that emerged throughout the event. Please report any inaccuracies to info@iaac.org.uk. Our sincere thanks go to our hosts and speakers.

Abstract:
The session focused on the question of compliances with for the EU General Data Protection Regulation (GDPR). The looming deadline is 25th May 2018. The focus of the discussion was to establish how organisations can determine where they are and where they need to be. Several dimensions of preparing for the GDPR's arrival were highlighted as key challenges. These can be broadly split into three areas: Understanding and communicating the gravity of GDPR, implementing compliance in time and practical difficulties in ensuring compliance. This report breaks down these key areas of concern and highlights the practical steps which can be taken to mitigate against the challenges highlighted throughout the SASIG/IAAC Masterclass.

1. Understanding and communicating the gravity of GDPR

What emerged rapidly throughout the conversations was the need to ensure that an organisation's CEO/Board members take notice of, and put into action, a plan for GDPR. Described as the biggest single shake up of data legislation that there has ever been, conveying this warning can still be problematic when there are numerous challenges and tasks that command the attention of senior organisational staff members. To address this issue the general consensus was that firstly identifying the key elements of the GDPR of interest to senior people would do much to raise awareness of the scale of the task ahead to ensure compliance.

1.1 Non-compliance and infringements

First and foremost, perhaps the most striking element of the EU GDPR is the sheer weight of the penalties possible for non-compliance. This is very much the stick element to the legislation where non-compliance and infringements can carry administrative costs in excess of €20,000,000 or up to 4% of global annual turnover, whichever is higher. The comparison with the record £400,000 fine telecoms giant TalkTalk was handed in 2016 for failing to prevent its October data breach, the increased severity is clear. Putting forward the severity of the fines along with case studies illustrating the potential damage to overall profits was highlighted as a way to focus the attention at board level.

1.2 Joint liability between corporates and 3rd parties

GDPR distinguishes between those who process data and those who determine why the data is processed. A Processor processes personal data on behalf of a data controller . A Controller determines why and how personal data is processed. Both Processors and Controllers are within the scope of the regulation and both bear joint liability for infringements. Currently, a Controller bears all the risk, however post GDPR, a claimant can request the entire compensation from either party. While there is a claw back provision both parties, joint liability can impact contractual indemnities as well as one sided contractual positions.

1.3 Data Protection Officers

Key to the GDPR is accountability and being able to demonstrate compliance. Symbolic of this aim is the requirement to designate a Data Protection Officer (DPO) when the core activities of the controller or the processor involve "regular and systematic monitoring of data subjects on a large scale" or when the entity conducts large-scale processing of "special categories of personal data" (such as race or religious beliefs). The DPO should be an expert in data protection law and practice and they will advise the controller and processor their legal obligations as well as monitor compliance on all aspects of GDPR and other data protection laws.

Participants noted the operational impacts of implementing DPO's into organisations, such as the necessity for a team of DPO's if in an organisation with many subsidiaries that span across borders. Ensuring that the DPO has a direct line to the board was emphasised, as they have significant independence in the performance of their roles. Consequently, it may not be possible to bolt on the responsibilities to an existing senior staff member, such as head of cyber security, as there may be a conflict of interests. Combined with no limit on the length of their tenure the GDPR explicitly protects the DPO from dismissal or penalty for carrying out their duties. Coming to terms with the importance of this new role to compliance is crucial to planning for compliance.

2 Implementing Compliance in time:

Having attained a respect for the significance of the GDPR, the next key concern that emerged throughout the workshops was implementation in a timely manner - "how can I meet the extensive obligations by May 25th 2018?" It was felt that if one had not begun preparations for GDPR compliance by now it was starting to be too late. This is because for some ensuring compliance means root and branch changes, which for an international company is a complex task. Consequently, it is crucial that companies assess their policies to determine what neds to be done aginst a fast-approaching deadline. Two key areas for consideration are the training of staff and balancing resources alongside business as usual.

2.1 Training staff (particularly at lower levels)

A significant challenge for decision makers was preparing for the operational impact of the GDPR. For example, there was a need to provide staff members within organisations the training needed to ensure that personal data was handled safely. A typical scenario illustrates the potential risks found in failing to adequately train, particularly lower levels of staff.

The first is found in employees who are the first point of contact for customers. Post-GDPR, it is reasonable to expect an increase in the number of customers calling regarding the right to erasure, or the right to be forgotten. In this circumstance, an employee should be able to process the request and accurately determine the data which the company holds on an individual. Further complicating the matter is the that requests must be processed without undue delay and in any circumstance no longer than a month. Failure to do so can result in penalties, which if scaled up can pose a significant issue for decision makers, reaffirming the importance of training staff on the front line.

The second example relates to the data controller's obligation to notify a lead authority of data breaches within 72 hours, as well as informing the affected data subjects without undue delay. It is important to note that notification is not required if the breach is unlikely to risk the rights and freedoms of individuals. The first concern is the training of junior staff members to recognise the tell-tale signs of a data breach such as noticing an unusual program popping up on workstations or locked user accounts. Inadequately trained staff can delay the process of notifying senior staff across an organisation, which is particularly problematic in international organisations with an extensive structure, risking failure to adhere to GDPR breach notification obligations.

2.2 Balancing resources

The complexity of shifting a whole organisations behaviour combined with the upcoming deadline means that implementing, and more importantly sustaining, the changes will require a significant amount of resources. This presents a challenge when organisations are under pressure for the day-to-day pressures involving running the entity. Adequately balancing resources was highlighted as a challenge in managing the overall programme for change in terms of GDPR and needs to be built into any project or transformation plan.

3. Practical difficulties in ensuring compliance:

Discussants raised the issues of developing a well-functioning GDPR compliance plan, with concerns regarding how to benchmark the organisation and the practical difficulties such as identifying where data is stored. Grasping these key issues early promotes success in ensuring compliance.

3.1 Benchmarking the organisation

Assessing your current position was widely agreed as a crucial stepping stone toward compliance, with a GAP Analysis as an essential tool along the timeline to compliance. A GDPR Gap Analysis will identify specific areas of non-compliance within the organisation allowing for a targeted approach. Pivotal to an effective plan is understanding that there is no one size fits all solution, which can be directly applied to any organisation. For example, determining the nature of the data which your organisation holds will significantly impact the implications for complying with GDPR. Determining whether the data is of a sensitive nature such as home addresses, bank details and medical records is a critical step. This presents a challenge and the review process can be time-consuming.While a review process must be

thorough it is critical to avoid 'paralysis by analysis' as the looming deadline of GDPR is fast approaching.

3.2 Locating your organisation's data?

Finding out precisely where organisational data is stored was arguably the most important point of the day. Recent studies show that most organisations have an average of 52% 'dark data' -not knowing what data is held and where. This presents a significant problem in terms of complying with a regulation that focuses predominantly on data. Data can be in various locations and forms, for example, paper files which can date back several years. In addition, there may be numerous 3rd parties who may have had access to data, as well as employees taking data off site via electronic mobile devices or physical files. Key to the GDPR is accountability and with that comes the requirement for a visible audit trail. While there are technical tools available to reveal information about an organisation's data such as its location and content, complying with the GDPR will transform IT storage strategies. The fundamental importance of where the data is should not be overlooked.

3.3 Identifying how much of a practical problem erasing someone's data is

Referring to the right to erasure, or to be forgotten, erasing an individual's personal data becomes a significant challenge, particularly in absence of a clear understanding of where data is stored and its contents. Procedures for how personal data is corrected/deleted without undue delay will need to be created, as well as clear evidence that proves of your actions. Discussants recognised the logistical difficulty in potentially erasing someone's data, with the difficulty increasing the further back you go. Once again this may be more of an issue for certain organisations, for example those with an older IT structure or one with a wide variety of vendors. Adverse scrutiny tests will enable one to ascertain how difficult erasing someone's data is and will consequently highlight what success looks like.

4. Conclusion:

Several perspectives emerged in the general discussion, with wide considerations for the challenges that the EU GDPR brings about. Overall the main challenges are fully comprehending the significance of the GDPR, understanding the practical challenges that compliance may bring as well as implementing changes in time. This report has sought to further detail the challenges that decision makers face, as well as begin to introduce what can be done to mitigate against the challenges. Following on from this report, follow up workshops hosted by IAAC and SASIG will allow participants to monitor their progress, as well as share information and experiences regarding the journey toward complying with the GDPR next year.

Bibliography:

Horgan, Alan (2016) 'Q and A: What do business and the IT personnel need to do to be ready for EU GDPR?', available at: http://tech.newstatesman.com/enterprise-it/q-business-personnel-need-ready-eu-gdpr [Last accessed: 06/02/17]

Pearce, Mark (2016) 'The EU General Data Protection Regulation (GDPR): it's time to get serious about data protection', available at: http://www.paconsulting.com/our-thinking/eu-gdpr-its-time-to-get-serious-about-data-protection/ [Last accessed: 06/02/17]