Will Compliance with the New EU General Data Protection Regulation Lead to Better Cloud Security?

Bob Duncan
Business School
University of Aberdeen, UK
Email: bobduncan@abdn.ac.uk

***Abstract*—The EU General Data Protection Regulation (GDPR) came into effect across the EU on 25th May 2018. It will certainly be the case that a great many companies will be inadequately prepared for this significant event. While a great many companies who use traditional in-house distributed systems are likely to have a hard enough job trying to comply with this new regulation, those who use any form of cloud computing face a particularly difficult additional challenge, namely the Cloud Forensic Problem. It is not enough that cloud use presents a far more challenging environment, but that the cloud forensic problem presents a far more difficult barrier to achieving compliance. This problem arises due to the fact that all computing systems are constantly under serious attack, but once an attacker gains a foothold in a cloud system and becomes an intruder, there is very little to prevent the intruder from helping themselves to any manner of data covered by the GDPR, either by viewing it, modifying it, deleting it or ex-filtrating it from the victim system. Worse, there is nothing to prevent the intruder from gaining sufficient privileges to then completely delete all trace of their incursion, possibly deleting far more records than they need to in the process. We address exactly what the requirements of EU GDPR compliance are, consider whether this can be done without resolving the Cloud Forensic Problem, and propose some approaches to mitigate this problem, and possibly the massive potential fines that could then be levied. We then consider whether the new EU GDPR will provide enough incentive for cloud users, and cloud service providers to get together to develop a much higher standard of cloud security which is both stronger than at present, and can deal with the Cloud Forensic Problem.**

Keywords–EU GDPR; Compliance; Cloud computing; cloud forensic problem.

I. INTRODUCTION

In [1], we considered the potential implications for cloud users in light of the cloud forensic problem for the then forthcoming EU GDPR compliance. We observed that during the drafting process of the regulation, one of the really useful componenents of the regulation was the requirement to report a breach within 72 hours of its occurrence. This brought a huge amount of effort to bear by corporates, desperate to ensure they would be able to comply. These efforts were reflected in the security breach reports, where it was apparent that the time between breach and discovery was reducing year on year. This could only be a good thing for all companies, and in particular cloud users.

Sadly, as a result of some intense lobbying, this component was somewhat watered down to a requirement to report within 72 hours of discovering the occurrence of a breach. As a direct result of this change, many companies instantly stopped working on this element of improving security, and again this too was reflected in the security breach reports, where the time between breach and discovery rocketed back to 2012 levels.

The EU General Data Protection Regulation (GDPR) [2], came into effect on 25th May 2018, and is likely to present one of the greatest compliance challenges faced by companies across the globe. Every company that trades anywhere on earth, should they deal with even a single EU resident, must ensure they are compliant with the EU GDPR. If that company suffers a security breach and the records of any EU citizen are compromised, then the jurisdiction of the GDPR will extend globally, and that company may be pursued and fined significant sums of money.

Achieving information security is a big enough challenge for companies who use conventional distributed network systems, but once companies start using cloud systems, the challenge increases exponentially. There are many reasons for this, mostly arising from the complexity of the additional relationships, and agendas, of different participant companies involved in cloud systems. Much research has been carried out to attempt to resolve these problems e.g., [3], [4], [5], [6], [7].

The most challenging, and as yet, unresolved issue is the cloud forensic problem, otherwise known as "The elephant in the room." Pretty much everyone knows about it, yet nobody is prepared to discuss it, let along try to resolve the problem, due to the difficulty of the challenge it presents. The new EU GDPR means that heads can no longer be left in the sand. This will not present an acceptable defence.

If any company using cloud is unable to resolve the cloud forensic problem, we suggest this will present such a fundamental issue that it will be impossible for that company to comply with this new regulation. As far back as 2011 and in subsequent years [8], [9], [10], [11], a great deal of research was focussed on trying to resolve this issue, yet it is clear from looking at regulatory fines for breaches that the message is not getting though.

In 2012, Verizon estimated that a total of 174 million data records were compromised [12]. By 2017, this had increased to an estimated 2 billion records lost or compromised in the first half of 2017 alone [13]. Yahoo disclosed a 1 billion compromised account breach in the 2013 attacks, yet when Verizon were in the process of taking over Yahoo last year and performing their due diligence, it turned out that **ALL 3 billion accounts** had been compromised [14], representing the biggest hack of all time.

In Section II, we look in some detail at the EU GDPR and consider the implications of non-compliance for any company that falls under its jurisdiction. In Section III, we identify what

the Cloud Forensic Problem is, and address why it is such a challenging problem to overcome. In Section IV, we ask whether it is possible to attain compliance without addressing the cloud forensic problem. In Section V, we address the minimum requirements necessary to achieve compliance. In Section VII, we look at what achieving the minimum requirements will allow us to do. In Section VIII, we consider the attitude of the regulator based on recently reported opinions made publicly by the regulator. In Section IX, we consider the likely attitude of corporate cloud users in response to these opinions. In Section X, we ask whether compliance with the GDPR might ever improve cloud security. In Section XI, we consider the limitations of this work, and in Section XII, we discuss our conclusions.

II. The EU General Data Protection Regulation

Why should companies be concerned about compliance with the EU GDPR [15]? Perhaps suffering a serious cyber breach leading to non-compliance, and resulting in a potential maximum fine of the greater of €20million or 4% of global turnover might serve to gain their attention. We should therefore take a good close look at the detail of the regulation.

The Article 29 Working Party [16] was set up by the European Commission under the terms of Article 29 of the Data Protection Directive in 1996, and its main stated missions are to:

- Provide expert advice to the States regarding data protection;
- Promote the consistent application of the Data Protection Directive in all EU state members, as well as Norway, Liechtenstein and Iceland;
- Give to the Commission an opinion on community laws (first pillar) affecting the right to protection of personal data;
- Make recommendations to the public on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community.

During the time it has been active, the Article 29 Working Party has overseen the evolution of the GDPR, and has seen thousands of amendments proposed. One of the best proposals was the requirement to report all breaches ". . . within 72 hours of the breach occurring", which would have had the impact of ensuring that all organisations would give security top priority in order to achieve compliance. However, following much lobbying, this was watered down to ". . . within 72 hours of discovery of a breach." This rather took the urgency away from organisations, since many companies now took the view that until the breach happened, they would still be in compliance, resulting in many abandoning all efforts to improve security further.

Sadly, the impact of this change has been reflected in cyber breach reports. The global average time for all companies between breach and discovery in 2012 was an average of 6 months[17][18]. This had improved to just under 4 weeks by 2016 [19] — still far short of what is needed to understand what has been going on with the intruders while they were undiscovered. While this was a marked improvement over the intervening years, once the relaxation of the regulation took place, a great many companies immediately stopped working on security, taking the view that there would be no need to improve security as they would not be in breach of GDPR compliance until after a breach actually occurred. This rather short sighted view resulted in the time between breach and discovery reverting towards 2012 levels [20]. As Verizon [13] succinctly put it, "Apparently, it is not only The Eagles that are destined for a long stay at the hotel. The hackers continue to be checked in indefinitely as well. Breach timelines continue to paint a rather dismal picture — with time-to-compromise being only seconds, time-to-exfiltration taking days, and times to discovery and containment staying firmly in the months camp." That will not exactly fill the regulator with confidence about any company's ability to achieve compliance.

On a more positive note, another key amendment involved broadening the scope of the regulation, from all organisations anywhere in the EU, to any organisation anywhere in the globe, which stores privately identifiable information relating to any individual resident anywhere in the EU. This will certainly get the attention of far more organisations than would have been the case had it been an EU only requirement.

In the next three subsections, we have a look at how the GDPR seeks to streamline activities for both organisations and data subjects; how the GDPR will use enforcement mechanisms to ensure compliance; and what happens in the event of a data breach.

A. The Streamlining Goals of the GDPR

1) For Organisations: The idea for organisations is to streamline compliance by providing:

A single set of rules which would apply anywhere in the EU and by using the One Stop Shop approach, covered by Articles 46 to 55 of the GDPR, this would make for a streamlined approach for all organisations, whether based inside or outside the EU.

2) For Data Subjects: The idea for data subjects is to make the whole process for them much simpler by providing:

- Right of Access (under Article 15) - which gives data subjects the right to access their personal data held by any company subject to compliance with the GDPR;
- Right to Erasure (under Article 17) - which gives data subjects the right to have erasure carried out on certain data held by organisations about the data subject on any one of a number of grounds including non-compliance with article 6.1 (lawfulness) that includes a case (f) where the legitimate interests of the controller is overridden by the interests or fundamental rights and freedoms of the data subject;
- Data Portability (under Article 20) - data subjects have certain rights to data portability (particularly in the case of social media accounts), whereby a person shall be able to transfer their personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller;
- Data Protection by Design and by Default (under Article 25) - seeks to ensure that all data subjects can expect privacy by design and by default, that has been designed into the development of business

processes for products and services. This requires that privacy settings must be set at a high level by default and that technical and procedural measures should be taken care of by the controller in order to make sure that the processing, throughout the whole processing lifecycle, complies with the regulation. A report by the European Union Agency for Network and Information Security (ENISA) [21], elaborates on what needs to be done to achieve privacy and data protection by design. It specifies that encryption and decryption operations must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if any privacy is to be achieved. Furthermore, it specifies that outsourced data storage on remote clouds is practical and relatively safe, as long as only the data owner, not the cloud service, holds the decryption keys;

- Consent by Data Subjects - data subjects must have given their consent for data about them to be processed, thus providing a lawful basis for processing.

3) A Lawful Basis for Processing: The data subject must have given consent which must be explicit for data collected and the purposes data is used for (Article 7; defined in Article 4). Data controllers must be able to prove "consent" (opt-in) and consent may be withdrawn. Consent for children must be given by the child's parent or custodian, and must be verifiable (Article 8). Such consent to the processing of his, her or their personal data for one or more specific processing purposes, must be:

- necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- necessary for compliance with a legal obligation to which the controller is subject;
- necessary in order to protect the vital interests of the data subject or of another natural person;
- necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

B. Enforcement Mechanisms

- Appointing a Data Protection Officer - this person would be required for all data processor organisations, and a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. The appointment of a DPO within a large organization will be a challenge for the Board as well as for the individual concerned, due to the myriad governance and human factor issues that organisations and companies will need to address given the scope and nature of the appointment. In addition, the post holder will need to create their own support team and will also be responsible for their own continuing professional development as they need to be independent of the organization that employs them, effectively as a "mini-regulator";
- Ensuring Compliance with the GDPR, by checking that all the correct mechanisms are properly defined and in place, mainly through compliance demonstration, e.g, the data controller should implement measures which meet the principles of data protection by design and data protection by default. Such measures include the process of pseudonymising (Recital 78), i.e., by means of encryption, which process should be completed as soon as is practically possible.
- The GDPR seeks to provide Responsibility and Accountability by all parties involved in data processing, with expanded notice requirements covering retention time for personal data, and contact information for data controller and data protection officer. Automated decision-making for individuals, including algorithmic means of profiling (Article 22), which is regarded as contestable, similar to the Data Protection Directive (Article 15), receive particular attention. The expectation is that all actors involved in the whole process of data processing will behave responsibly and will be fully accountable for their actions. Data Protection Impact Assessments (Article 35) have to be conducted when specific risks occur to the rights and freedoms of data subjects. Risk assessment and mitigation is required and prior approval of the Data Protection Authorities (DPA) is required for high risks. Data Protection Officers (Articles 3739) are to ensure compliance within organizations.

C. In the event of a Data Breach

In the event of a data breach, under the GDPR, the Data Controller will be under a legal obligation to notify the Supervisory Authority without undue delay. The reporting of a data breach is not subject to any *de minimis* standard and must be reported to the Supervisory Authority within 72 hours after having become aware of the data breach (Article 33). Individuals have to be notified if adverse impact is determined (under Article 34), unless the data was encrypted. In addition, the data processor will have to notify the controller without undue delay after becoming aware of a personal data breach (under Article 33).

1) Sanctions: The following sanctions can be imposed:

- a warning in writing in cases of first and non-intentional non-compliance;
- regular periodic data protection audits;
- a fine of up to €10million or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, where there has been an infringement of the following provisions (Article 83, Paragraph 4[18]):
    - the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
    - the obligations of the certification body pursuant to Articles 42 and 43;

  - the obligations of the monitoring body pursuant to Article 41(4).
- a fine up to €20million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, where there has been an infringement of the following provisions: (Article 83, Paragraph 5 & 6[18]):
  - the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
  - the data subjects' rights pursuant to Articles 12 to 22;
  - the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
  - any obligations pursuant to Member State law adopted under Chapter IX;
  - non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

The above details provide the essence of what we need to know in order to understand what information will be required to be delivered in the event of breach, in order for the data processor to be compliant with the GDPR. In the next section, we will take a look at the Cloud Forensic Problem, and why it is such a difficult problem, not only from the security perspective, but also from the GDPR compliance problem.

III. The Cloud Forensic Problem (and Why it is Such a Difficult Problem)

All computer systems are continuously subject to attack, whether traditional distributed network systems or cloud systems, which are no exception. It is certainly the case that no system is immune to attack, and that is particularly true for cloud systems. During the past decade, a great many research papers have allowed a far greater level of security and privacy to be achieved in cloud systems. There have been many good papers produced on both security [22], [23], [24], [25], [3], [4], [26], [5], [6], [7], [27], [28] and privacy [29], [30], [31], [32], [33], [34], [35], [36], [37], [6], [38], [39], [40], [41], [42], [43], and a number of others have looked at better accountability as a means to meeting these ends [44], [45], [46], [47], [48], [49], [50], [31], [51], [52], [3], [4], [53], [54], [55], [38], [7], [56], [57], [58], [41], [59], [11], [60], [61], [62] However, despite all those efforts, no solutions have yet been found to address the cloud forensic problem.

As we have already stated, all computing systems are constantly under serious attack, but once an attacker gains a foothold in a cloud system and becomes an intruder, there is little to prevent the intruder from helping themselves to any amount of data covered by the GDPR, either by viewing it, modifying it, deleting it or ex-filtrating it from the victim system [63], [64], [65]. Worse, there is nothing to prevent the intruder from gaining sufficient privileges to then completely delete all trace of their incursion, possibly deleting far more records than they need to in the process, leading to further problems for business continuity.

Often, companies do not retain records of which database records have been accessed, nor by whom. This means that once a breach occurs, the ability of the company to be able to report which records have been accessed, copied, modified, deleted or ex-filtrated from the system becomes an impossible task. This results in non-compliance with the GDPR, meaning exposure to potentially punitive levels of fines.

This is often known as "The elephant in the room" in cloud circles. Pretty much everyone knows about it, yet nobody is prepared to discuss it, let alone try to resolve the problem, due to the difficulty of the challenge it presents. Make no mistake, this is a serious challenge to defend against, let alone overcome. However, not only is it a serious challenge for organisations using cloud, it also presents a major obstacle to compliance with the GDPR.

Once all trace of the intrusion has been deleted, there will be very little forensic trail left to follow, meaning many companies will be totally unaware that the intrusion has taken place, let alone understand what records have been accessed, modified, deleted or stolen. All too often, companies will believe they have retained a full forensic trail in their running instance, but often forget that without special measures being taken to save these records off-site [3], they will vanish when the instance is shut down.

Currently, in any cloud based system, there must be a complete and intact audit trail in order for the breached organisation to be able to tell which records have been accessed, modified, deleted or stolen. Where the audit trail and all forensic records have been deleted, there remains no physical means for any organisation to be able to tell which records have been accessed, modified, deleted or stolen, putting these organisations immediately in multiple breaches of the GDPR.

IV. Is it possible to achieve Compliance with the EU GDPR without addressing the Cloud Forensic Problem?

The short answer is, of course, it is not! For the reasons outlined in the previous section, we can see that there is nothing to prevent an intruder from destroying every scrap of forensic proof of their incursion into any current cloud system. It is clear that any form of forensic record or audit trail can not therefore be safely stored on any running cloud instance.

This means that the only safe method of storage of forensic data will be somewhere off-site from the running cloud instances. Clearly, the off-site storage must be highly secure, preferably stored in an append-only database, and should especially be held in encrypted format, with all encryption keys held elsewhere.

Doubtless some will say that as long as they are not breached, then they will not be in breach of the GDPR. While that may very well be true, how will they be able to tell whether they have or have not been breached, particularly in the circumstance where they have been breached, and the breach has been very well covered up. They will have no means of knowing, let alone proving the point. The regulator will be unlikely to accept this approach as an appropriate way to demonstrate a willingness to comply with the GDPR.

Let us suppose that a complaint is made to the regulator, the organisation will have no means of proving that the data has not been tampered with. Equally, if the breach has been extremely well covered up, they will neither have the means of complying with the requirement to: a) report the breach

within 72 hours, nor b) have any means of determining which records have been accessed, modified, deleted or stolen. Let us now suppose that the conversion of private data has yet to be encrypted, and worse, that the encryption and decryption keys are held on the cloud instance "for convenience". If we were to receive a request from any users whose data had just been compromised, we would be unable to comply with the request, meaning we would now be looking at multiple breaches, thus causing the fine level to escalate to the higher level, as outlined in Subsubsection II-C1.

An added inconvenience would arise where the company had elected not to use encryption (or had used encryption, but left the encryption and decryption keys on the cloud instance). While encryption is not mandatory, in the case where it is not used, in the event of a breach, the company must communicate with all customers whose data may have been compromised. Where they are unable to tell whose data has or has not been compromised, they would need to write to every single customer to be in compliance. This could prompt a flood of requests from these customers to enquire about specifically which records of theirs were compromised. The company would be unable to provide this information, and would then enter into a case of multiple breaches of the GDPR, leading to the possibility of multiple large fines for non-compliance.

V. The Minimum Requirements to Achieve Compliance with the GDPR

We have seen that to do nothing would not be a viable option as far as GDPR compliance is concerned. Attacks will continue unabated. We must therefore be prepared and armed with whatever tools we can develop to ensure we achieve as high a level of compliance as we possibly can.

We therefore need to consider what the absolute minimum technical requirement might be to attain our objective of GDPR compliance. We know that under the GDPR the organisation must be able to:

- provide a Right of Access (under Article 15) to personal data by data subject, if requested;
- provide the means to comply with a Right to Erasure (under Article 17) by data subject, subject to the appropriate grounds being met;
- provide privacy by design;
- in the event of a data breach, report the breach to the Supervisory Authority within 72 hours after having become aware of the data breach (Article 33). The breach must also be reported to the controller without undue delay after becoming aware of a personal data breach;
- in the event of a data breach, notify the data subject if adverse impact is determined (under Article 34), unless the data was encrypted;

In the case of the first requirement, we would require to ensure the provenance and veracity of the contents of the database. In the case of the second requirement, if appropriate, the same provision would apply.

In the case of the third requirement, the cloud system must be designed in accordance with the recommendations of the Article 29 Working Party [66], which suggests the reports produced by ENISA should be followed. This report [67] specifies that encryption and decryption operations must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if any privacy is to be achieved. Furthermore, it specifies that outsourced data storage on remote clouds is practical and relatively safe, as long as only the data owner, not the cloud service, holds the decryption keys. ENISA have also produced a stream of other relevant reports, including a Cloud Risk report in 2009 [68], and recommendations for certification in 2017 [69].

In the case of the fourth requirement, we would require to ensure the provenance and veracity of the contents of the database. In the case of the fifth requirement, where the data is not yet encrypted, the same provision would also apply. However, it should be stressed that it will always be preferable to ensure data is encrypted before it leaves the control of the data owner.

It is clear that where no steps have been taken to ensure the cloud forensic problem has been mitigated, the organisation will fail on every count. Thus, as a minimum, we need to ensure the following steps are taken:

- all personal data should be encrypted, and this should be performed locally;
- the encryption and decryption keys should not be maintained on the cloud instance;
- a full audit trail of the entire database must be maintained off-site;
- full forensic records of all users having accessed the database and carried out any commands on the database must be collected and stored off-site.

VI. Architecture Changes Suggested

The starting position will be a conventional cloud instance containing everything needed to operate the system, including web based software, database software, intrusion detection software and anything else deemed to be appropriate.

A. The Bare Minimum

All database access requests, database logs, system logs and any other logs should be running on a separate high security system, away from the main cloud instance. This system should not have any conventional web interface, and the recording databases should be immutable, i.e. append only.

This approach will address the challenge of retaining a full forensic trail discussed in Section III.

B. The Improved Version

All database software should be removed from the cloud system and run on a highly secure system which is separate from both the main cloud instance and the forensic logging system. This ensures the complete separation of all data from software running on the main cloud instance.

Depending on the volume of transactional data, this system can run on a conventional distributed system, or a cloud system running only the database software or could be run across multiple virtualised machines.

VII. What will the Minimum Requirements Allow us to do?

Let us now assume that we have completed the bare minimum requirements. Can we now be sure that we can be compliant with the provisions of the GDPR? We must therefore look at each of the five reporting requirements in turn to establish whether we will be able to meet these requirements.

1) First, if a data subject serves us with a Right of Access request, can we respond in the affirmative? We are now sure that we hold the subject's data securely, in encrypted format in our database. Further, on the assumption that no breach has arisen, we can prove that the data has only been accessed by duly authorised persons because we have a complete forensic trail of everyone who has accessed the data records, and further that the data records have neither been modified, stolen nor deleted. We are therefore compliant on the first requirement;
2) Next, if a data subject serves us with a right to Erasure notice, can we comply with that request? Assuming the request can be legitimately carried out and is not prohibited by statute, then since we can correctly identify the private data held about the data subject, then there is no reason why we would be unable to delete the appropriate data as requested. Accordingly, we would be compliant on the second requirement;
3) Next, can we provide privacy by design? Our default design concept is to provide privacy by design through following the ENISA recommendations which suggest this be achieved by ensuring all private data is properly encrypted, that encryption and decryption keys are not stored on the running cloud instance, and that we retain a full and complete forensic record of all operations on the data held by the company;
4) In the event of a data breach, can we report the breach to the Supervisory Authority within 72 hours of discovery? In the case of a data breach, we will not only be able to notify the breach within 72 hours of discovery, we will actually be able to notify within 72 hours of the occurrence of the breach. In addition, since we will retain full forensic data and audit trails for the system, we will also be able to provide very precise details of which records were accessed and read, which might have been modified, with full details of what modifications were made, which records were deleted, and which records were exfiltrated from the system. Not only that, but we will be able to provide full details of how the perpetrators got into the system and where they forwarded any stolen records, which means we can identify precisely which records were compromised, thus ensuring we would be beyond fully compliant;
5) In the event of a data breach, would we be able to notify the data subject if adverse impact is determined (under Article 34)? In the event of a data breach, we would be able to identify every single record attacked, and identify every single data subject affected. Since the full records would already be encrypted, we would not be required to notify the data subjects, but would be fully capable of so doing. This would mean we would again be beyond fully compliant.

Thus, we can reasonably claim that we would be in a position to be fully compliant with all the requirements of the GDPR, thus providing an exceptionally high level of privacy on behalf of all data subjects. Thus, the level of exposure of data subjects would be extremely minimised, thus ensuring compliance with the regulation, and therefore the likelihood that we would be able to fully mitigate any penalty that would otherwise be applied by the regulator.

Contrast this position with the case where cloud users do not take these mitigatory steps. In every requirement - they would be non-compliant, thus exposing the enterprise to the full extent of penalties allowed, namely the greater of €20million or 4% of global turnover.

VIII. The Attitude of the Regulators

Since at the time of writing this article, barely three months has elapsed since the GDPR came into effect, there will not yet be a great deal of indication on what the attitude of the regulator to cyber breach events is likely to be. In spite of the short timescale that has elapsed, the UK Information Commissioner's Office (ICO) who are the UK GDPR regulator have seen complaints rise from 2,417 to 6,281 between 25 May and 3 July 2018 as compared with the same period from the previous year. On the plus side, they have increased staff by some 40% in anticipation of this significant increase in workload.

However, of a Reuters' survey of 24 of the authorities charged with carrying out the regulation of the GDPR who responded in early May, 2018, just weeks before the GDPR came into force, 17 responded that they did not yet have the necessary funding, or would initially lack the powers to fulfil their GDPR duties. Since many of these new powers have yet to be incorporated into their countries' laws, this is likely to result in a number of delays before any serious regulatory effort can be started. Many have said they will start by responding to complaints and investigate them on merit. Only a minority suggested they would proactively investigate whether companies were complying and make any attempts to sanction glaring non-compliance [70].

The expectation of the regulator will be that they would expect companies to take all reasonable steps to make their business compliant with the GDPR. However it is likely that where a company has not taken sufficient robust steps to prepare to achieve adequate levels of security, this will be regarded as a failure to take proper steps to safeguard the PII of users, and the company will be regarded as complicit in aiding the attackers to perpetrate their attack. This will likely ensure a much higher level of penalty will be applied. However, following a rather embarrassing leak, it became apparent that the European Commission is not itself GDPR compliant [71], and of course now claims that it is exempt.

In the event that any company chooses not to use encryption, or decides to leave the encryption and decryption keys on the running cloud instances, the company will again be found to be complicit in failing to achieve proper compliance. Again, resulting in a likely increase in the level of penalty applied, as well as a huge administrative burden for notifying customers on top of the penalty.

Some regulators have taken the view that they will investigate cyber breaches that arose before the GDPR came into effect. Others are clearly not yet ready to regulate properly yet. Some will investigate on receipt of a complaint. Others will clearly wish to be proactive in their approach. Time will tell how each will approach their job, and what the likely consequences will be for non compliance.

With currently 28 member states, and considerably more regulatory authorities granted power to regulate under the GDPR, it is also not yet fully clear just how the various regulators will act where breaches affect cloud customers from more than one EU country or area, nor how jurisdiction will be dealt with where a large corporate operates in multiple EU countries or areas within.

There is no doubt that is too early to speculate on how the many EU regulators will approach their regulatory duties, and how they might go about enforcing compliance with cloud users. In some respects, the fact that many of the regulators have neither the resources nor the legislative power to carry out their regulatory duties means that there will be an element of respite for cloud users. There is no doubt that a great many corporates will be only too happy to take full advantage of this situation to minimise the work they carry out on improving their security systems in order to provide a much better standard of privacy.

IX. The Attitude of Corporate Cloud Users

Judging by the content of the annual reports during the past decades of large corporates, who are not renowned for exhibiting highly transparent levels of disclosure, this is unlikely to provide a good source of information on successful cyber breaches. A great many corporate boardrooms fear the prospect of disclosure of problems and the likely knock on effect on the share price. While they are required to report cyber breaches within 72 hours of discovery, in the event that they have used cloud and the forensic and audit trails have been tampered with, it is unlikely that they will even report a cyber breach when it arises. Cleaerly there will be an element of moral hazard to take into account at board level. Why would they wish to create trouble for themselves, a potentially significant drop in their share price, and a potentially large fine when they wait a while, perhaps until the dividend has been declared and paid out (along with their bonuses) before considering publication of the cyber breach or reporting the cyber breach to the regulator. This could certainly present a serious moral hazard when there may be little direct forensic evidence as to the extent of the breach.

Equally, while many corporates publicly proclaim their desire to be compliant with the new EU GDPR, Calligo, in a recent survey of IT decision makers, it was discovered that 69% of them do not have the backing of their board to achieve GDPR compliance [72]. However, once something goes wrong, it is likely the large multinational corporates, accustomed to dealing with regulation and compliance issues, will actually do something about it. In time, they wil refuse to do business with suppliers unless they too seek GDPR compliance. This will likely mean an eventual flow through all industries that are required to be compliant.

This is often the way with large corporates. Do nothing if at all possible until something goes wrong, and then take whatever action is necessary to become compliant. Then make all your suppliers become compliant too. Of course, there are always a few who do the right thing right at the beginning. It would seem a very prudent approach. No action usually means the breach will hurt. Not to mention the consequences in lost business, business continuity impact, loss of share price, embarrassment, and punitive fines.

Given the likely obstacles faced by the various regulators in getting started with the job of regulation due to being under-resourced, and perhaps having no or insufficient legislative ability to carry out their regulatory tasks, many large corporates will be happy to take advantage of that situation by sitting on carrying out the necessary improvements until it becomes absolutely essential.

In that event, it is highly likely that attackers will be more than happy to take full advantage of this slacking off on tightening cyber security by having a field day with few obstacles to get in their way.

X. Will Compliance with the GDPR Lead to Better Cloud Security?

It is very clear that, particularly in some areas, it will take some considerable time for proper regulation to be properly implemented, perhaps even years. There is no doubt as all that as soon as some punitive level of fines is levied against cloud users, thus punishing all of society through higher costs being levied by the cloud users to cover this potential major in crease in their cost base, then more effort is likely to go into improving cloud security. It is just a pity that we end up punishing society in general, rather than the perpetrators of the crimes who are responsible for all this mayhem.

It is clear that every actor involved in the cloud ecosystem has a role to play in improving security, and therefore privacy too. There is no doubt that major cloud service providers are taking security much more seriously these days. It is equally clear that many large corporates are much less inclined to do so, unless pushed, and pushed hard, and that very much needs to change.

There is a clear need for greater accountability from all involved. It is also clear that there is a need to develop a better means of policing the use of computing resources with a view to tracking the real perpetrators of the crimes. Equally, we need to consider that many of the computing standards we are all familiar with today have been in existence for a great many decades, most of which were developed before the internet took off.

This means that there is undoubtedly scope to tighten up these standards significantly in the light of the need for greater accountability and a better understanding of how to pin responsibility on all bad actors.

There is little doubt that a huge amount of work will be involved by a great many people. However, the introduction of punitive levels of fines will likely help to accelerate this process. There is no doubt this will lead to better cloud security. The question is how long will it really take to reach an acceptable level of cloud security?

There is also little doubt that the GDPR will have far reaching consequences for other jurisdictions, particularly for the US, where existing legislation and regulation fails to go anywhere close to what the new EU GDPR is doing. This will doubtless lead to more change throughout the globe to bring

more and more legislation and regulation into alignment. Ultimately, this will be a good thing for society as a whole. For too long, criminals have skipped around the insular jurisdictional approach of many countries which has led to myriad loopholes being exploited by criminals who continue to perpetrate their seedy trade with impunity.

XI. Limitations and discussion

There are two very important tasks that must be performed in order not to limit the effectiveness of this approach. Since persistent storage in the cloud instance cannot retain data beyond its currently running lifetime [3], we must also make sure that all necessary logs and data are stored securely elsewhere. And as the default settings for virtually all database management software involves logging being turned off [63], we must ensure this function is turned on in all running cloud instances, again, with the data being stored securely elsewhere.

This prompts the question of what data we require to keep. In order to meet our regulatory compliance requirement, we need to understand the 5 W's — namely: Who is accessing our system? Where have they come from? What are they looking for? When is this happening? From this data, we should be able to infer the Why? Are they authorised to be in the system, to enter the system the way they have, to look at the data they are trying to access, and at the time they are trying to access it? Deducing the Why can give an indicator of anomalous behaviour.

Many database management software offers additional full audit trail capabilities. Each additional capability will require more and more storage resources. A balance will need to be found between the minimum requirement consistent with maintaining performance and a cost effective level of storage. The risk in not utilising all that is on offer, would be that this might compromise security, reducing the ability of the company to achieve compliance.

However, it is clear that a sensible precaution to mitigate this risk would be to encrypt all the data being held on all databases maintained within the system, ensuring that encryption/decryption keys are not stored on the cloud instances. While encryption is not mandatory, in the event of a breach where encryption is not used, the fine levied by the regulator is likely to be much higher as a consequence. Additionally, the company must personally notify every single customer whose PII is at risk, or was compromised in the course of the breach.

However, cloud users should also consider the fact that all actors in the cloud ecosystem should also be contributing towards resolving these issues, and that includes in particular the cloud service provider (CSP). There is undoubtedly a need for greater accountability from every actor in the ecosystem chain. Everyone needs to contribute to making cloud computing a much safer paradigm for the benefit of all actors, and hopefully to the detriment of all attackers too.

XII. Conclusion

The forthcoming GDPR will certainly present a serious wake up call to a great many companies operating around the globe if they find themselves falling under the jurisdiction of this new regulation. In this paper, we have considered whether it is possible to achieve regulatory compliance where any organisation is using cloud computing. Again, we reiterate that without suitable precautions being put in place, the answer is a resounding "No!".

We have outlined the key requirements from the regulation to which all organisations falling under its jurisdiction must comply. We have identified the currently unresolved "Cloud Forensic Problem" as presenting the largest obstacle to achieving compliance.

We have proposed how this challenging problem may be approached to ensure that cloud users can be fully compliant with this new regulation, with little more than being sensibly organised. Clearly, additional cost will require to be incurred, and there may be a small impact on latency, but these costs could significantly mitigate the possibility of a huge regulatory fine in the event of a breach. It is also likely that this approach will ensure faster discovery of the occurrence of a breach, thus minimising the potential impact on business continuity.

Perhaps we can look forward to the day when we can put the squeeze on attackers, or at least have the ability to track and identify them , thus allowing us to make them fully accountable for their insidious trade. There is little doubt that right now, we are all in it together, and thus we must all pull together in order to have any chance of succeeding against the overwhelming hordes of attackers who end up making many people's lives such a misery. It is time to get serious.

References

[1] B. Duncan, "Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing?" in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization, no. February. Barcelona, Spain: IARIA, 2018, pp. 1–6.

[2] EU, "EU General Data Protection Regulation (GDPR)," 2017. [Online]. Available: http://www.eugdpr.org/ [Last accessed: August 2018]

[3] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, B. S. Lee, and Q. Liang, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," Perspective, 2011, pp. 1–9.

[4] R. K. L. Ko, B. S. Lee, and S. Pearson, "Towards achieving accountability, auditability and trust in cloud computing," Communications in Computer and Information Science, vol. 193 CCIS, 2011, pp. 432–444.

[5] N. Papanikolaou, S. Pearson, and M. C. Mont, "Towards Natural-Language Understanding and Automated Enforcement of Privacy Rules and Regulations in the Cloud: Survey and Bibliography," Analysis, 2011, pp. 1–9.

[6] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services," Current, 2009, pp. 44–52.

[7] S. Pearson, "Toward accountability in the cloud," IEEE Internet Computing, vol. 15, no. 4, jul 2011, pp. 64–69.

[8] N. Papanikolaou, S. Pearson, M. C. Mont, and R. Ko, "A Toolkit for Automating Compliance in Cloud Computing Services," International Journal of Cloud Computing, vol. x, no. x, 2014, pp. 45–68.

[9] J. Singh and J. M. Bacon, "On middleware for emerging health services," Journal of Internet Services and Applications, vol. 5, no. 1, 2014, p. 6.

[10] J. Singh, J. Bacon, and D. Eyers, "Policy Enforcement Within Emerging Distributed, Event-based Systems," Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems - DEBS '14, 2014, pp. 246–255.

[11] J. Singh, J. Powles, T. Pasquier, and J. Bacon, "Data Flow Management and Compliance in Cloud Computing," Cloud Computing, no. Special Issue on Legal Clouds., 2015, pp. 1–12.

[12] Verizon, "2012 Data Breach Investigation Report: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service and Others," Tech. Rep., 2012. [Online]. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf [Last accessed: August 2018]

[13] Verizon, "Verizon Security Breach Report 2017," Tech. Rep., 2017.

[14] S. Khandelwal, "Its 3 Billion! Yes, Every Single Yahoo Account Was Hacked In 2013 Data Breach," 2017. [Online]. Available: https://thehackernews.com/2017/10/yahoo-email-hacked.html [Last accessed: August 2018]

[15] The European Parliament and The European Council, "General Data Protection Regulation," Official Journal of the European Union, vol. 2014, no. October 1995, 2016, pp. 20–30.

[16] EU, "Opinion 05/2012 on Cloud Computing (Data Protection)," 2012.

[17] PWC, "UK Information Security Breaches Survey - Technical Report 2012," PWC2012, Tech. Rep. April, 2012.

[18] Trustwave, "2012 Global Security Report," Tech. Rep., 2012.

[19] Verizon, "2016 Verizon Data Breach Report," Tech. Rep., 2016.

[20] Trustwave, "2017 Global Security Report," Trustwave, Tech. Rep., 2017.

[21] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Metayer, R. Tirtea, and S. Schiffner, Privacy and Data Protection by Design - from policy to engineering, 2015, no. December.

[22] M. Almorsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," 17th Asia-Pacific Software Engineering Conference (APSEC 2010) Cloud Workshop,Sydney, Australia, no. December, 2010, p. 7.

[23] M. Almorsy, J. Grundy, and I. Mller, "An analysis of the cloud computing security problem." The proc. of the 2010 Asia Pacific Cloud Work-shop Colocated with APSEC2010, Australia, 2010.

[24] V. Chang, Y. H. Kuo, and M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds," Future Generation Computer Systems, vol. 57, 2016, pp. 24–41.

[25] F. Doelitzscher, T. Ruebsamen, T. Karbe, M. Knahl, C. Reich, and N. Clarke, "Sun Behind Clouds - On Automatic Cloud Security Audits and a Cloud Audit Policy Language," International Journal on Advances in Networks and Services, vol. 6, no. 1, 2013, pp. 1–16.

[26] K. Lee, "Security Threats in Cloud Computing Environments," International Journal of Security and its Applications, vol. 6, no. 4, 2012, pp. 25–32.

[27] S. Ramgovind, M. Eloff, and E. Smith, "The Management of Security in Cloud Computing," in Information Security for South Africa (ISSA), 2010, 2010, pp. 1–7.

[28] H. Takabi, J. B. Joshi, and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security & Privacy Magazine, vol. 8, no. 6, nov 2010, pp. 24–31.

[29] S. Creese, P. Hopkins, S. Pearson, and Y. Shen, "Data Protection-Aware Design for Cloud Computing," Work, no. December, 2009, pp. 1–13.

[30] K. Hon, C. Millard, and I. Walden, "The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated ?" 2011.

[31] W. K. Hon, C. Millard, and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2," Legal Studies, no. 77, 2011, pp. 1–31.

[32] W. K. Hon, J. Hörnle, and C. Millard, "Data Protection Jurisdiction and Cloud Computing When are Cloud Users and Providers Subject to EU Data Protection Law?" Legal Studies, 2011, pp. 1–40.

[33] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, dec 2009, pp. 711–716.

[34] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," NIST, Tech. Rep., 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf [Last accessed: August 2018]

[35] H. Katzan Jr, "On The Privacy Of Cloud Computing," International Journal of Management and Information Systems, vol. 14, no. 2, 2011, pp. 1–12.

[36] W. K. Hon, C. Millard, J. Singh, I. Walden, and J. Crowcroft, "Policy, legal and regulatory implications of a Europe-only cloud," International Journal of Law and Information Technology, vol. 24, no. 3, 2016, pp. 251–278.

[37] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations," Natioinal Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. February, 2014. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [Last accessed: August 2018]

[38] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud," Computing, no. December, 2009, pp. 1–15.

[39] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," 2010 IEEE Second International Conference on Cloud Computing Technology and Science, nov 2010, pp. 693–702.

[40] S. Pearson, "Privacy, Security and Trust in Cloud Computing," in Privacy and Security for Cloud Computing. e: Springer, 2013, pp. 3–42.

[41] J. Prüfer, "How to govern the cloud? Characterizing the optimal enforcement institution that supports accountability in cloud computing," Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom, vol. 2, 2013, pp. 33–38.

[42] S. S. Shapiro, "Privacy by Design," Communications of the ACM, vol. 53, no. 6, jun 2010, p. 27.

[43] J. Singh, T. F. J. M. Pasquier, and J. Bacon, "Securing tags to control information flows within the Internet of Things," 2015 International Conference on Recent Advances in Internet of Things, RIoT 2015, 2015.

[44] EU, "Accountability for Cloud (A4Cloud)," 2018. [Online]. Available: http://a4cloud.eu/ [Last accessed: August 2018]

[45] C. A. Adams and R. Evans, "Accountability, Completeness, Credibility and the Audit Expectations Gap," JCC 14 Summer 2014, vol. 14, no. Summer, 2014, pp. 97–115.

[46] W. Benghabrit, H. Grall, J.-C. Royer, M. Sellami, M. Azraoui, K. Elkhiyaoui, M. Onen, A. S. D. Olivera, and K. Bernsmed, "A Cloud Accountability Policy Representation Framework," in CLOSER-4th International Conference on Cloud Computing and Services Science, 2014, pp. 489–498.

[47] K. Bernsmed, W. K. Hon, and C. Millard, "Deploying Medical Sensor Networks in the Cloud Accountability Obligations from a European Perspective," in Cloud Computing (CLOUD), 2014 IEEE 7th International Conference on. IEEE Comput. Soc, 2014, pp. 898–905.

[48] D. Butin, M. Chicote, and D. Le Métayer, "Log design for accountability," in Proceedings - IEEE CS Security and Privacy Workshops, SPW 2013, 2013.

[49] D. Catteddu, M. Felici, G. Hogben, A. Holcroft, E. Kosta, R. Leened, C. Millard, M. Niezen, D. Nunez, N. Papanikolaou, S. Pearson, D. Pradelles, C. Reed, C. Rong, J.-C. Royer, D. Stefanatou, and T. W. Wlodarczyk, "Towards a Model of Accountability for Cloud Computing Services," in International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC), 2013, pp. 21–30.

[50] A. Haeberlen, "A Case for the Accountable Cloud," ACM SIGOPS Operating Systems Review, vol. 44, no. 2, 2010, pp. 52–57.

[51] W. Hon, E. Kosta, C. Millard, and D. Stefanatou, "Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation," Queen Mary School of Law Legal Studies Research Paper, no. 172, 2014, pp. 1–54.

[52] K. L. R. Ko, P. Jagadpramana, and B. S. Lee, "Flogger: A File-Centric Logger for Monitoring File Access and Transfers within Cloud Computing Environments," Computing, 2011, pp. 1–8.

[53] T. Lynn, P. Healy, R. McClatchey, J. Morrison, C. Pahl, and B. Lee, "The Case for Cloud Service Trustmarks and Assurance-as-a-Service," in CLOSER 2013 - Proceedings of the 3rd International Conference on Cloud Computing and Services Science, 2013, pp. 110–115.

[54] N. Papanikolaou, S. Pearson, M. C. Mont, and R. K. L. Ko, "Towards Greater Accountability in Cloud Computing through Natural-Language Analysis and Automated Policy Enforcement," Engineering, 2011, pp. 1–4.

[55] N. Papanikolaou, T. Rübsamen, and C. Reich, "A Simulation Framework to Model Accountability Controls for Cloud Computing," CLOUD COMPUTING 2014, The Fifth International Conference on Cloud Computing, GRIDs, and Virtualization, no. c, 2014, pp. 12–19.

[56] S. Pearson, M. C. Mont, and G. Kounga, "Enhancing Accountability in the Cloud via Sticky Policies," in Secure and Trust Computing, Data Management, and Applications, 2011, pp. 146–155.

[57] S. Pearson, V. Tountopoulos, D. Catteddu, S. Mario, R. Molva, C. Reich, S. Fischer-Hubner, C. Millard, V. Lotz, M. G. Jaatun, R. Leenes, C. Rong,

and J. Lopez, "Accountability for Cloud and Other Future Internet Services," in CloudCom, 2012, pp. 629—-632.

[58] K. Bernsmed and S. Fischer-Hübner, "Secure IT Systems: 19th Nordic Conference, NordSec 2014 Tromsø, Norway, October 15-17, 2014 Proceedings," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8788, 2014, pp. 3–24.

[59] T. Ruebsamen and C. Reich, "Supporting Cloud Accountability by Collecting Evidence Using Audit Agents," in CloudCom 2013, 2013, pp. 185–190.

[60] A. Squicciarini, S. Sundareswaran, D. Lin, and S. Huang, "Promoting Distributed Accountability in the Cloud," in IEEE 4th International Conference on Cloud Computing Promoting, 2011, pp. 113–120.

[61] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," in IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 4, 2012, pp. 556–568.

[62] M. Theoharidou, N. Papanikolaou, S. Pearson, and D. Gritzalis, "Privacy risk, security, accountability in the cloud," in Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom, vol. 1, 2013, pp. 177–184.

[63] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail," in Cloud Computing 2016: The Seventh International Conference on Cloud Computing, GRIDs, and Virtualization, no. April. Rome: IEEE, 2016, pp. 125–130.

[64] G. Weir, A. Aßmuth, M. Whittington, and B. Duncan, "Cloud Accounting Systems, the Audit Trail, Forensics and the EU GDPR: How Hard Can It Be?" in The British Accounting and Finance Association: Scottish Area Group Annual Conference. Aberdeen: BAFA, 2017, p. 6.

[65] P. Tobin, M. McKeever, J. Blackledge, M. Whittington, and B. Duncan, "UK Financial Institutions Stand to Lose Billions in GDPR Fines: How can They Mitigate This?" in The British Accounting and Finance Association: Scottish Area Group Annual Conference, BAFA, Ed., Aberdeen, 2017, p. 6.

[66] EU, "Unleashing the Potential of Cloud Computing in Europe," 2012. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0271:FIN:EN:PDF

[67] ENISA, "Article 4 Technical Report," ENISA, Tech. Rep., 2011.

[68] ENISA, "Cloud Risk," ENISA, Tech. Rep., 2009. [Online]. Available: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment [Last accessed: August 2018]

[69] ENISA, "Recommendations on European Data Protection Certification," Tech. Rep., 2017.

[70] Reuters, "European regulators: We're not ready for new privacy law," 2018. [Online]. Available: https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X [Last accessed: August 2018]

[71] M. Murphy and B. Riley-Smith, "'Embarrassing' leak shows EU falls short of own GDPR data law," 2018. [Online]. Available: https://www.telegraph.co.uk/technology/2018/05/30/embarrassing-leak-shows-eu-falls-short-data-law/ [Last accessed: August 2018]

[72] V. Beckett, "Many businesses' attitudes to GDPR are 'bordering on negligent'," 2017. [Online]. Available: https://www.theglobaltreasurer.com/2017/10/13/many-businesses-attitudes-to-gdpr-are-bordering-on-negligent/%0A [Last accessed: August 2018]