Novel EU Legal Requirements in Big Data Security

Big Data – Big Security Headaches?

by **Jasmien César and Julien Debussche**, the authors are associates at the law firm Bird & Bird LLP, Brussels, toreador@twobirds.com

Abstract: This paper aims to provide an overview of the new legal requirements related to security and breach notification imposed on businesses in the European Union and to demonstrate their pertinence for big data service providers. In addition, it lays down practical recommendations for the implementation of those requirements into the internal security strategies of big data service providers.

Keywords: Big data; security; breach notification; legal obligations

Recommended citation: Jasmien César and Julien Debussche, Novel EU Legal Requirements in Big Data Security: Big Data – Big Security Headaches?, 8 (2017) JIPITEC 79 para 1.

A. Security

1 As highlighted by the European Commission in its Communication "Towards a thriving data-driven economy", we currently observe a new industrial revolution driven by digital data, computation and automation.[1] Human activities, industrial processes, and research all engender the collection and processing of data in unprecedented proportions, triggering new products and services as well as new business processes and scientific methodologies.[2]

2 The resulting datasets, or "big data", are prone to security risks and incidents. In recent times, instruments have emerged to prevent or adequately respond to such risks, thereby imposing obligations on different actors in the data value cycle.

3 Such obligations not only derive from the General Data Protection Regulation (the GDPR), but also from other legislative instruments at both the European Union (EU) and national level. The advent of the (minimal harmonisation) Network Information Security Directive (the NIS Directive, also known as the Cyber-security Directive) has multiplied the requirements relating to security and cyber-security.

I. Requirements under the General Data Protection Regulation

4 For most big data analytics, it cannot be excluded that a processing of personal data will take place. In such case, the requirements relating to security under the GDPR will apply.

5 The obligations under the GDPR in relation to security are closely linked to those under the NIS Directive examined below, and are in line with best practices applicable to information society systems that require adequate protection of assets.

1 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a thriving data-driven economy", 2 July 2014, COM(2014) 442 final.

2 Ibid.

1. Data Governance Obligations

6 Under the GDPR, any organisation must implement a wide range of measures to reduce the risk of non-compliance with the GDPR and to prove that it takes data governance seriously. Such measures create significant operational obligations and costs.

7 A general obligation is imposed upon data controllers* to adopt technical and organisational measures to meet the requirements set in the GDPR and to be able to demonstrate that they have done so (Article 24 of the GDPR). Operating a regular audit programme, implementing privacy-by-design measures, running a Privacy Impact Assessment, appointing a Data Protection Officer, etc. are all measures considered to be in line with the data governance obligations, including the security-related requirements. Such measures must be reviewed and updated on a regular basis, taking into account the changing circumstances (Article 24(1) of the GDPR).

8 Furthermore, it shall be considered that the GDPR imposes a high duty of care upon data controllers in selecting their personal data processing service providers, which will require procurement processes and request for tender documents to be regularly assessed, in particular on the security aspects (Article 28 of the GDPR).

9 Adherence by the data controller or processor to an approved code of conduct or certification mechanism may feature as an element to demonstrate compliance with such data governance obligations (Articles 24(3) and 28(5) of the GDPR).

2. Security of Data Processing

10 The GDPR requires data controllers and processors to implement "technical and organisational measures to ensure a level of security appropriate to the risk" (Article 32 of the GDPR).

11 Such measures shall take into account the following elements:

- the state of the art;
- the costs of implementation;
- the nature, scope, context, and purposes of the processing; and
- the risk of varying likelihood and severity for the rights and freedoms of natural persons.

12 In assessing the appropriate level of security, account shall be taken in particular of the risks presented by the processing, notably from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed (Article 32(2) of the GDPR).

13 In this respect, the GDPR provides the following specific suggestions for what types of security measures may be considered "appropriate to the risk" (Article 32(1) of the GDPR):

- the pseudonymisation and encryption of personal data;
- the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

14 The GDPR indicates that adherence to an approved code of conduct or certification mechanism may be used as an element to demonstrate compliance with the security requirements (Article 32(3) of the GDPR). Currently, such codes of conduct or certification mechanisms are not yet on the market. In the absence of such instruments, companies shall rely on best practices and guidance provided by the authorities and take into account the elements mentioned above.

II. Requirements under the Network Information Security Directive

1. Context

15 The NIS Directive was adopted on 6 July 2016 and entered into force in August 2016. From then on, EU Member States have 21 months to transpose the Directive into their national laws and 6 additional months to identify the providers of essential services subject to the Directive's requirements (Article 25 of the NIS Directive).

2. Scope of Application

16 The Directive imposes (online) security obligations on providers of two different types of services discussed below: essential and digital services.

a.) Essential Service

17 Article 5 of the NIS Directive defines an essential service as "a service essential for the maintenance of critical societal and/or economic activities depending on network & information systems, an incident to which would have significant disruptive effects on the service provision."

18 EU Member States have to identify the operators of essential services established on their territory within 27 months after entry into force of the Directive. Operators active in the following sectors may be included: energy, transport, banking, stock exchange, healthcare, utilities, and digital infrastructure (Annex II to the NIS Directive).

19 When determining the significance of a disruptive effect in order to identify operators of essential services, the EU Member States must consider the following factors (Article 6 of the NIS Directive):

- the number of users relying on the service concerned;
- the dependency of (one of) the sectors mentioned above regarding the service concerned;
- the impact incidents could have on economic and societal activities or public safety;
- the market share of the entity concerned;
- the geographic spread of the area that could be affected by an incident;
- the importance of the entity to maintain a sufficient level of the service, taking into account the availability of alternative means for the provision of that service;
- and any other appropriate sector-specific factor.

b.) Digital Service

20 A digital service is described as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" (Article 4(5) of the NIS Directive).

21 The NIS Directive covers three different types of digital services, which are defined as follows (Article 4 of the NIS Directive):

- Online marketplace: "a digital service that allows consumers and/or traders to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online market place".
- Online search engine: "a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found".
- Cloud computing service: "a digital service that enables access to a scalable and elastic pool of shareable computing resources" (See Fig. 1 below – Recital 17 of the NIS Directive).

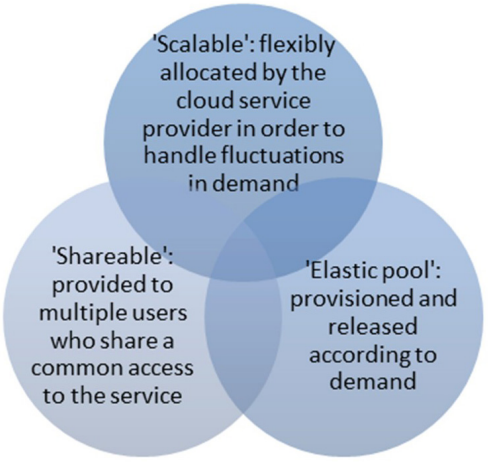

Figure 1: Definition of cloud computing service

22 In contrast to the operators of essential services, which are identified by each EU Member State, online businesses must self-assess whether they are targeted by the rules of the NIS Directive.

23 Considering the above, big data service providers may fall within the scope of the NIS Directive depending on the type of services they provide and the type of sector they are active in. It shall also be noted that, even though the NIS Directive only explicitly targets essential and digital service providers, suppliers to such providers may also be impacted by the obligations under the Directive due to flow down obligations.

3. Overview of New Rules

24 Given its nature as a Directive, the NIS Directive will need to be transposed into national law by the EU Member States. In the context of big data analytics, the essential and digital service providers and – where applicable – their suppliers will therefore need to comply with the transposing national law

in the EU Member State where they are established.

25 A digital service provider that is not established in the EU but providing services within the EU must appoint a representative. This representative will need to be established in one of the EU Member States where the digital services concerned are offered. In that case, the digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established (Article 18(2) of the NIS Directive).

26 Under the new rules intended to improve online security, the essential and digital service providers will notably have to (i) interact with new key actors; (ii) implement security measures; and (iii) notify security incidents.

a.) Interaction with New Key Actors

27 The NIS Directive requires EU Member States to designate several new actors with the aim of attaining a high common level of security of network and information systems within the EU (Article 1(1) of the NIS Directive).

28 Thus, each EU Member State has to designate one or more national competent authorities (NCAs) on the security of network and information systems, who shall monitor the application of the NIS Directive at the national level (Article 8(1) of the NIS Directive). Other key players coming onto the scene are the Computer Security Incident Response Teams (CSIRTs) (Article 9 of the NIS Directive). Interactions with such entities notably include the requirement to notify security incidents either to the NCAs or to the CSIRTs. The NCAs will have the necessary powers to urge essential and digital service providers to comply with their obligations under the NIS Directive (Articles 15 and 17 of the NIS Directive).

29 Furthermore, each EU Member State must select a national single point of contact, in order to facilitate the cross-border cooperation between the NCAs, the CSIRTs, and other relevant national authorities. If an EU Member State decides to designate only one NCA, that NCA will also perform the function of single point of contact (Article 8(3) of the NIS Directive).

b.) Implementation of Security Measures

30 The NIS Directive further requires operators of essential services and digital service providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the networks and information systems that they use for the provision of their services, and to prevent and minimise the impact of incidents affecting the security of such network and information systems (Articles 14 and 16 of the NIS Directive).

31 The security measures shall take into account the state of the art, to ensure a level of security of network and information systems that are adequate to the risk. Digital service providers must also consider the following specific elements when determining the appropriate security measures (Article 16(1) of the NIS Directive):

- the security of systems and facilities;
- incident handling;
- business continuity management;
- monitoring, auditing and testing;
- and compliance with international standards.

c.) Notification of Security Incidents

32 Under the NIS Directive, operators of essential services and digital service providers must notify the NCA or the CSIRT of incidents that have a significant impact on the continuity or provision of the services without undue delay (see Section A.II below for more details).

III. Security Standards

33 In addition to legal requirements on security, security standards indisputably have an important role to play in big data analytics. Moreover, relying on standards and certification schemes facilitates demonstrating compliance with legal requirements, including security requirements.

34 By relying on existing schemes, such as for instance the ISO/IEC 27000 series issued by the International Standards Organisation (the ISO) and the International Electrotechnical Commission (the IEC), big data service providers can demonstrate to the regulator and to their customers that their systems are adequate in terms of security.

35 Furthermore, several standards development organisations have created and are currently developing big data-specific standards. It is essential for any big data service provider to follow the evolutions in this respect closely.

IV. Security throughout the Data Value Cycle

36 The implementation of the abovementioned security measures can only make sense if they are implemented holistically, at all different stages of the data value cycle, to guarantee the continuity of services.[3] Fig. 2 aims to depict the data value cycle.[4]

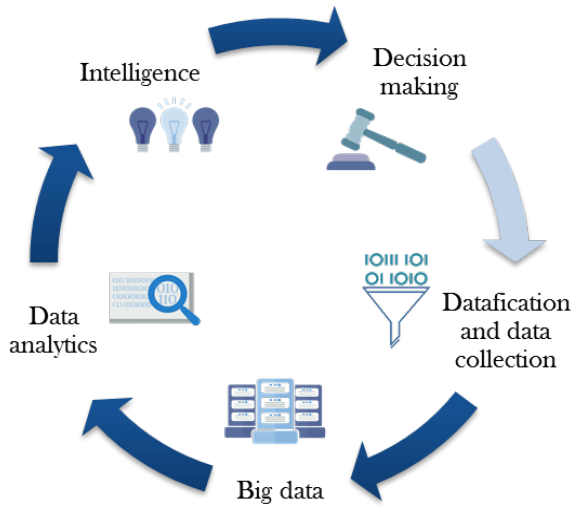

Figure 2: Data value cycle

37 Concretely, such a holistic approach entails that the following specific security issues and their possible mitigation measures ought to be considered throughout the different stages depicted above:[5]

Security issues	Mitigation measures
Integrity of the devices collecting data	Security testing procedures and audits, compliance with standards and certification mechanisms, access control and authentication.
Source validation	Encryption, security testing procedures and audits, risk assessment, source filtering, access control and authentication, monitoring and logging.
Infrastructure security	Security testing procedures and audits, compliance with standards and certification mechanisms, source filtering, access control and authentication, monitoring and logging.
Data security & secure data management	Encryption, security testing procedures and audits, access control and authentication, monitoring and logging.
Platform (e.g., cloud) security	Encryption, security testing procedures and audits, compliance with standards and certification mechanisms, risk assessment, access control and authentication, monitoring and logging.
Supply chain security	Security testing procedures and audits, compliance with standards and certification mechanisms, risk assessment.
Application software security	Security testing procedures and audits, compliance with standards and certification mechanisms, access control and authentication.
Interoperability of applications	Security testing procedures and audits, compliance with standards and certification mechanisms, access control and authentication.
Distributed denial-of-service attacks	Security testing procedures and audits, source filtering, monitoring and logging.
Unauthorised access	Encryption, security testing procedures and audits, compliance with standards and certification mechanisms, access control and authentication, monitoring and logging.

Table 1: Security issues and mitigation measures

38 In addition to applying mitigation measures internally, any company should ensure that safeguards are included in its contracts with, and can be enforced against, possible business partners.[6] Any such agreement should therefore contain specific information security obligations as well as the warranties, indemnity provisions, and limitations of liability related thereto. In order to ensure the enforceability of such clauses, the contract should also provide for audit rights.[7]

39 Furthermore, and inevitably, any agreement concluded for information security purposes should incorporate a comprehensive confidentiality clause.[8]

40 Better still, before entering into any business relations, an exhaustive due diligence of the envisaged business partner should be carried out, with a particular focus on information security.[9]

3 R Naydenov, D. Liveri, L. Dupre, E. Chalvatzi and C. Skouloudi, "Big data security - good practices and recommendations on the security of big data systems", (ENISA 2015).

4 OECD, "Data-driven innovation: big data for growth and well-being", (OECD Publishing 2015), <http://dx.doi.org/10.1787/9789264229358-en>.

5 R Naydenov, D. Liveri, L. Dupre, E. Chalvatzi and C. Skouloudi, "Big data security - good practices and recommendations on the security of big data systems", (ENISA 2015).

6 MR Overly, "Information security in vendor and business partner relationships" in JR Kalyvas and MR Overly (eds.), *Big Data: A Business and Legal Guide* (Auerbach Publications 2015).

7 Ibid.

8 Ibid.

9 Ibid.

V. Conclusion

41 Big data service providers must thoroughly and recurrently assess whether they are subject to security obligations under the GDPR and/or the NIS Directive.

42 In the affirmative, they shall integrate measures, at all different stages of the data value cycle:

- to ensure a level of security appropriate to the risks posed;
- enabling the on-going confidentiality, integrity, availability and resilience of systems and services (including those processing personal data);
- enabling the ability to restore the availability and access to data in a timely manner in the event of incidents;
- and to regularly test, assess and evaluate the effectiveness of security measures.

B. Breach-related Obligations

43 As an emerging technology, big data tends to rely on highly novel and high tech IT systems, which have had no or little time to fully mature into relatively secure techniques.[10] This not only renders big data systems vulnerable against external attacks, but also exposes it to potential unintentional data leaks.

44 The present Section focuses on the legal obligations that apply when data is thus compromised.

I. Preliminary Remark

45 Firstly, it should be noted that the legal concept of "data breach" does not coincide with the technical definition of "data breach".

46 As elaborated by E. Damiani in a big data context, there exist two sub-categories of threats on a technical level; i.e. (big) data breach and (big) data leak.[11] In this context, data breach refers to the theft of a data asset by intruding into the IT infrastructure, whereas data leak covers the disclosure of a data asset at a certain stage of its lifecycle.[12]

47 The legal notion of data breach however, encompasses both technical definitions of data breach and data leak. Indeed, data breach in a legal context does not necessarily entail the malicious behaviour of a third party, but is also established in case (personal) data is disclosed without interference of a threat actor – e.g., losing an unencrypted device.

48 Throughout this paper, we shall use the term "data breach" to refer to its legal interpretation.

II. Notification Obligation under the GDPR

1. Scope of the Obligation

49 The GDPR requires the notification of "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Articles 4(12) and 33 of the GDPR).

50 The table below provides an overview of the obligations imposed on the different actors involved.

Duty	Timing	Exemption
Data processor to notify data controller	Without undue delay after becoming aware of the data breach.	No exemptions mentioned in the GDPR, but the European Data Protection Board is tasked to issue guidelines on the particular circumstances in which a breach shall be notified.
Data controller to notify supervisory authority	Without undue delay and, where feasible, nolater than 72 hours after having become aware of the data breach.	Notification is not required if the breach is unlikely to result in a risk to the rights and freedoms of individuals.
Data controller to notify affected individuals (in close cooperation with the supervisory authority)	Without undue delay.	Notification is not required if: 1. The breach is unlikely to result in a high risk to the rights and freedoms of individuals; or 2. Appropriate technical and

10 E Damiani, C. A. Ardagna, F. Zavatarelli, E. Rekleitis (ed.) and L. Marinos, "Big data threat landscape and good practice guide", (ENISA 2016).

11 E Damiani, "Toward big data risk analysis", IEEE International Conference on Big Data (IEEE 2015), Santa Clara, CA, pp. 1905-1909.

12 E Damiani, C. A. Ardagna, F. Zavatarelli, E. Rekleitis (ed.) and L. Marinos, "Big data threat landscape and good practice guide", (ENISA 2016).

		organisational protection measures were in place at the time of the incident (e.g. data encryption); or 3. Measures have been taken subsequent to the incident, ensuring that the risk to the right and freedoms of individuals is unlikely to materialise; or 4. It would trigger disproportionate efforts. However, in this case, a public communication or similar measure to inform the public is required.

Table 2: Breach notification requirements under the GDPR

2. Notifications in Practice

51 The breach notification obligation under the GDPR evidently only applies in case of a breach of personal data. Therefore in the event of an incident, it is essential to carefully assess the nature of the data exposed. If such an assessment shows that no personal data has been affected, in principle no data breach notification is required under the GDPR. In this respect, it could reasonably be advocated that a breach of anonymised data or encrypted data – the key for which cannot be retrieved by a third party – does not need to be notified under the GDPR.

52 Therefore, appropriate technical and organisational measures should be implemented to be able to detect promptly whether a personal data breach has taken place and to immediately inform the supervisory authority and the individual if needed (Recital 87 of the GDPR). Such measures include the keeping of good logs, which facilitates a swift and efficient forensic investigation in case of an incident.

53 The personal data breach notification by the data controller to the supervisory authority must at least mention the following information (Article 33(3) of the GDPR):

i. The nature of the breach, including the categories and approximate number of individuals as well as personal data records affected;

ii. The name and contact details of the data protection officer or any other contact point that could provide more information;

iii. The likely consequences of the breach;

iv. The measures (proposed to be) taken by the data controller to address the breach, including any measures to mitigate its negative effects.

54 The communication to the affected individuals must detail in clear and plain language the nature of the personal data breach, recommendations to mitigate possible adverse effects, as well as the information listed under (ii), (iii) and (iv) above (Article 34(2) and Recital 86 of the GDPR).

55 In case it proves impossible to provide such information simultaneously within 72 hours, the GDPR allows providing such information in phases (Article 33(4) of the GDPR). However, the notification should indicate the reasons for the deferment, and the missing information should be provided without further undue delay (Recital 85 of the GDPR).

56 In line with the principle of accountability, the data controller must document any personal data breach as well as the corrective measures taken in order to allow the supervisory authority to assess compliance with the data breach notification obligations (Article 33(5) of the GDPR).

3. Sanctions

57 Under the GDPR, a company that does not comply with the data breach notification obligations may be liable to an administrative fine of up to 10,000,000 Euros or 2 per cent of its total worldwide annual turnover (Article 83(4) of the GDPR). Such a fine is entirely distinct from the affected individual's right to claim compensation for any material or non-material damage suffered as a result of an infringement of the data breach notification obligation (Article 82 of the GDPR).

III. Notification Obligation under the NIS Directive

1. Scope of the Obligation

58 Under the NIS Directive, operators of essential services and digital service providers must notify, without undue delay, to the NCA or the CSIRT incidents that have a significant impact on the continuity or provision of the services (Articles 14(3) and 16(3) of the NIS Directive).

59 As mentioned above, the NIS Directive is not directly applicable in the EU Member States but needs to be implemented in each national Member State law. It can therefore be expected that there will be a

difference in implementation of the security incident notification obligations between the different EU Member States.

2. Notification in Practice

60 The factors to be considered when determining whether the impact of an incident is significant are the following (Articles 14(4) and 16(4) of the NIS Directive):

Operators of essential services	Digital service providers
• the number of users affected by the incident; • the duration of the incident; • and the geographical spread of the incident.	• the number of users affected by the incident; • the duration of the incident; • the geographical spread of the incident; • the extent of the disruption of the service; • and the extent of the impact on economic and societal activities.

Table 3: Factors to determine the significance of an impact

61 In case an operator of essential services depends on a digital service provider for the provision of such essential services, any significant impact on the continuity of those services due to an incident affecting the digital service provider must be notified by that operator (Article 16(5) of the NIS Directive). The NIS Directive remains silent as to whether, in such circumstances, the digital service provider is obliged to notify such an incident to the operator of essential services. It is therefore to be expected (and highly recommended) that the operator of essential services would require such notification by the digital service provider contractually.

62 The notified NCA or CSIRT shall inform other Member States affected (Articles 14(5) and 16(6) of the NIS Directive). In this case, the NCA, the CSIRT, and the single point of contact shall ensure that the service provider's security and commercial interests are safeguarded and that the information provided remains confidential. The NCA or CSIRT may also decide – after consultation of the notifying operator – to inform the public, where such public awareness would be necessary to prevent or manage an incident (Articles 14(6) and 16(7) of the NIS Directive).

3. Sanctions

63 Essential or digital service providers that do not comply with the security incident notifications laid down by the national provisions adopted pursuant to the NIS Directive may be subject to a penalty, which is to be determined by each EU Member State at the national level. Pursuant to Article 21 of the NIS Directive, such penalties must be effective, proportionate and dissuasive.

IV. Conclusion

64 It is highly recommended for big data service providers to document the legal notification requirements applicable to them in a detailed manner, both at the EU and national level, in order to be able to comply with their notification obligations.

65 Big data service providers shall notify any security and/or data breach, which (i) has led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored, or otherwise processed; or (ii) may lead to a significant disruptive effect on the service provided by themselves or by their customers.

C. Internal Security Strategy

66 The question arises how big data service providers should fit the security and breach notification legal requirements examined in this paper within their internal security strategies.

67 Fig. 3 aims to provide some guidance in this respect. It sets out some of the main aspects to consider at each phase of the incident lifecycle: *i.e.*, pre-incident, during or immediately after the incident, and post-incident. For each phase, Fig. 3 recommends which practical steps to take in order to comply with the legal requirements examined in this paper.

68 Inevitably, an internal incident handling strategy like the one depicted in Fig. 3 can only achieve its purpose if it is constantly re-evaluated and updated in light of the changing circumstances and the new technological abilities. This goes hand in hand with the fact that the legal, statutory, and contractual requirements must be assessed and re-assessed at each step of each phase, in order to ensure full compliance.

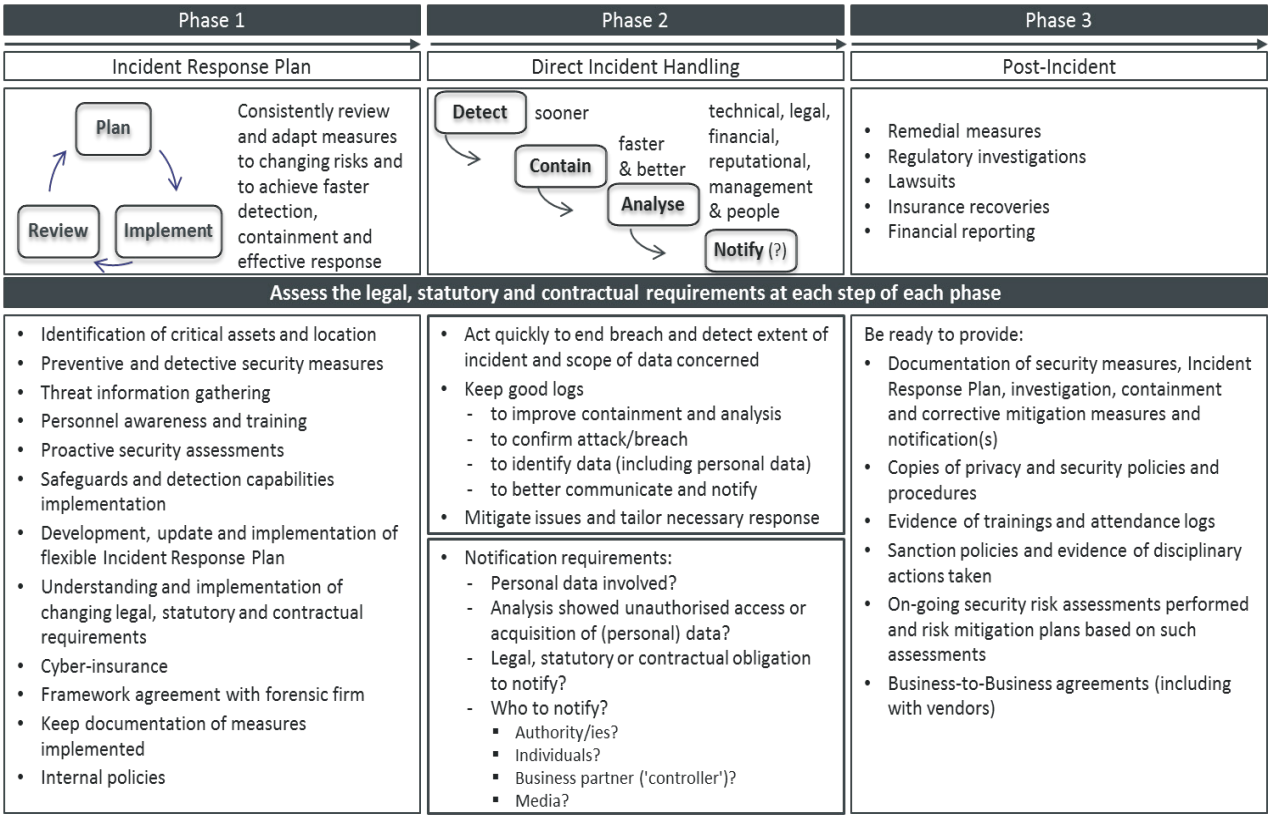

Figure 3: Incident Handling Diagram

References

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a thriving data-driven economy", 2 July 2014, COM(2014) 442 final.

[2] R Naydenov, D. Liveri, L. Dupre, E. Chalvatzi and C. Skouloudi, "Big data security - good practices and recommendations on the security of big data systems", (ENISA 2015).

[3] OECD, "Data-driven innovation: big data for growth and well-being", (OECD Publishing 2015), <http://dx.doi.org/10.1787/9789264229358-en>

[4] MR Overly, "Information security in vendor and business partner relationships" in JR Kalyvas and MR Overly (eds.), *Big Data: A Business and Legal Guide* (Auerbach Publications 2015).

[5] E Damiani, C. A. Ardagna, F. Zavatarelli, E. Rekleitis (ed.) and L. Marinos, "Big data threat landscape and good practice guide", (ENISA 2016).

[6] E Damiani, "Toward big data risk analysis", IEEE International Conference on Big Data (IEEE 2015), Santa Clara, CA, pp. 1905-1909.

[7] J. Ghent, "Digital risk management and data protection", (Innovation value institute, 2014)

[8] Desai, "Law and technology. Beyond location: data security in the 21st century", Communications of the ACM, vol. 56, pp. 34-36, January 2013, doi: 10.1145/2398356.2398368

[9] N. van Dijk, R. Gellert and K. Rommetveit, "A risk to a right? Beyond data protection risk assessments", Computer Law & Security Review: The International Journal of Technology Law and Practice (2015), doi: 10.1016/j.clsr.2015.12.017

[10] Kung and others, "PRIPARE: a new vision on engineering privac and security by design" (2014)

[11] Samaras, S. Daskapan, R. Ahmad and S. Ray, "An enterprise security architecture for accessing SaaS cloud services with BYOD" (2014), doi: 10.1109/ATNAC.2014.7020886

[12] Kosta and K. Stuurman, "Technical standards and the draft General Data Protection Regulation" in P. Delimatsis (ed), *The law, economics and politics of international standardization* (Cambridge University Press, 2016, forthcoming)

[13] Kennedy and C. Millard, "Data security and multi-factor authentication: analysis of requirements under EU law and in selected EU Member States" (2015)

[14] M. Dekker, D. Liveri and M. Lakka, "Cloud Security Incident Reporting – Framework for reporting about major cloud security incidents", (ENISA 2013)

[15] M. Dekker and D. Liveri, "Cloud Security Guide for SMEs – Cloud computing security risks and opportunities for SMEs", (ENISA 2015)

[16] Rijmen, D. De Cock, N. P. Smart and R. Tirtea, "Recommended cryptographic measures – Securing personal data", (ENISA 2013)

[17] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

[18] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1

[19] ISO/IEC 27000:2016 – Information technology, security techniques

* A data controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; a data processor is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (Article 4 of the GDPR).

This paper was written within the European Union TOREADOR project ("TrustwOrthy model-awaRE Analytics Data platfORm"). Granting authority: European Union. Call: H2020-ICT-2015. Topic: ICT-16-2015 (Big data - research). Type of action: RIA. Grant agreement no.: 688797, Starting date: 1st January 2016, Ending date: 31st December 2018.