IDPP

International journal for the
Data Protection Officer
Privacy Officer
Privacy Counsel

JOURNAL ADDRESSES

Personal data | Privacy | Data protection | Law, regulation and caselaw | The new DPO profession | Compliance | Independence and conflict | Resources | Records | GDPR | Ethics | Security incidents and notifications | Breach notification | Pre-problem solving | PbD/DPbD | Audits and assessment | Education, training and programmes | Solutions and systems | Resource update review |

ISSUE INCLUDES

2017 VOLUME 1 ISSUE 2

ie
Reinventing
Higher Education

MASTER IN GLOBAL CORPORATE COMPLIANCE

FORMAT	LENGTH	INTAKE	LOCATION
FULL-TIME/ PART-TIME	10 MONTHS/ 11 MONTHS	OCTOBER/ MARCH	MADRID

&

MASTER IN CYBERSECURITY

FORMAT	LENGTH	INTAKE	LOCATION	LANGUAGE
FULL-TIME	10 MONTHS	OCTOBER	MADRID	ENGLISH

www.ie.edu

International journal for the
Data Protection Officer
Privacy Officer
Privacy Counsel

Contents

Subscriptions
Subscriptions are available by contacting: lex@mydistillex.com.

Submissions
Submissions are invited and should be sent to lex@mydistillex.com.

Advertising
Advertising opportunities are available and requests should be sent to lex@mydistillex.com.

Disclaimer
The views expressed in the content submitted are those of the authors and do not necessarily reflect the views of the IDPOJ, its editors or publishers. Contributions and views contained in the journal are not intended as, and do not constitute, legal advice and are not a substitute for same.

Contact
IDPP, 7 Dunbo Hill, Howth, D13, Ireland. Contact: lex@mydistillex.com

Editorial

The current issues refers to

- Privacy By Design (PbD), the General Data Protection Regulation (GDPR) and fraud prevention tools;
- the GDPR and the implications and influence for data protection and privacy protection in Africa;
- the danger of using alerts including personal data to protect financial investors resulting from a new case in Spain;
- the massive Equifax data breach incident affecting 143 million individuals, and in particular the immediate and wider consequences for data protection professionals to consider.

The Privacy By Design (PbD) article focuses on the transparency requirements stipulated under the new GDPR and how these can act or assist as fraud prevention tools. PbD and DPbD are important toolsin an of themselves in ensuring appropriate protection for personal data, security and avoidance or risk activities.

The Data Protection Directive 1995 had a significant influence beyond the EU. The new GDPR will equally have effects beyond the EU, both in terms of practice, safety and the regulations of other countries. The next article considers the GDPR implications for data protection and privacy protections in Africa.

The penultimate article refers to a recent case in Spain. This article hightlights the case and refers to the danger of using alerts which include personal data to protect financial investors.

Data breaches are becoming more serious. The Equifax data breach article highlights the Equifax data breach and the lesson that data protection professionals must be aware of an increasingly wide number of interconnected issues, responsibilities and responses. It is increasingly evident that in particular circumstances, the responses (or lack of response)(and or delayed response) can further contribute to the problem event at hand. An inappropriate response can quickly escalate the problem. Worse still, this can be in a fully public manner with the full glare of media attention – and regulatory enquiries. The Equifax data breach is also a lesson on what should be done, what should not be done and the essential need that appropriate responses need to be timely and customer-centric.

Dr. Paul Lambert
editor

Privacy By Design (PbD) and Transparency Requirements Under the General Data Protection Regulation (GDPR) as Fraud Prevention Tools

John.E. Giannakakis, CIPP/E, CIPM. CFE, GDPR F+P,
Advocate, Partner, Co Head of Data Protection and Cybersecurity Practice Group at
Nikolinakos & Lardas LLP (www.nllaw.gr)

Background

On 14th of April 2016 the European Parliament adopted the new General Data Privacy Regulation ("GDPR") The GDPR is a Regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU). It also addresses export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR will come into effect on May 25th, 2018 it will replace the 1995 data protection directive ("Directive 95/46/EC").

The new Regulation contains a stricter set of provisions and requirements, including the adjustment of systems to secure "Privacy by Default" and "Privacy by Design", the appointment of Data Privacy Officer in specific cases, the requirement for keeping "Record of Processing Activities" for each legal entity employing over 250 employees or alternatively performing specific types of personal data processing the introduction of the 'Right to be Forgotten" (Article 17) amongst other requirements which broadens and explicitly codifies the right to be forgotten already contained in case law and states, among other things, the obligation to erase Data "without undue delay" if they are no longer necessary to be kept or if consent is withdrawn.

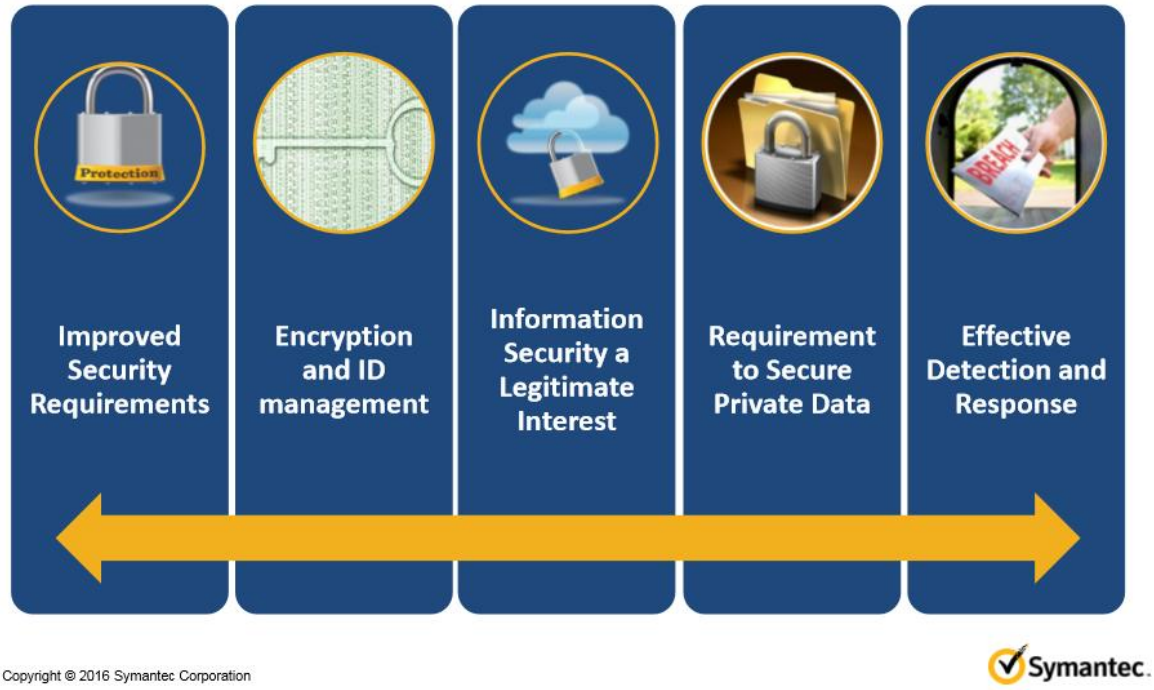
The most critical areas of the GDPR are its aligned and unified enforcement across EU countries, eliminating polyphony of the old regime, which applies at national level only as well as the data transfers both intragroup as well as to Companies outside EEA and Switzerland, as well to the US. GDPR, same as with the EU Data Protection Directive, (95/46/EC) has requirements for the transfer of data to countries outside the EU. Countries still must have an adequate level of protection. The US was not deemed to provide an adequate level of protection under the EU Data Protection Directive, and the solution of choice for most companies for cross-border data transfer was the Safe Harbor Arrangement. But Safe Harbor was invalidated earlier this year in the *Schrems* case.

Accountability & Transparency – Key Requirments Under the GDPR

Accountability made its formal debut in the field of international data protection more than 30 years ago, when it was adopted as a data protection principle in the Organization for Economic Cooperation and Development (OECD) Guidelines.[4] As of late, the policy discourse on the regulation of data protection has been rife with references to accountability. Most notably, in 2010, the Article 29 Data Protection Working Party issued an Opinion on the principle of accountability in which it elaborated upon the possibility of including a general provision on accountability in the revised Data Protection Directive.[5] The European Commission has also made a reference to the possibility of introducing a principle of accountability in its subsequent Communication outlining a strategy for modernising the EU data protection framework.[6] Within the context of these documents, the introduction of an accountability principle in the new General Data Protection Regulation as the sixth Data Protection Principle, not included in the Directive 95/46 is seen mainly as a way to help **ensure 'that data controllers put in place effective policies and mechanisms to ensure compliance with data protection rules'.** While this objective is in line with previous

iterations of the principle of accountability, important nuances exist among the various documents which have promulgated accountability as a data protection principle.

Articles 12 and 24 of the GDPR require from Data Processors and Data Controllers to "take appropriate measures to provide any information referred to in Articles 13 and 14and any communication under Articles 15 and 24 …….. in a concise**, transparent** …… "as well as implement appropriate technical and organizational measures to ensure and to **be able to demonstrate that processing is performed in accordance with the Regulation"** This newly introduced requirements transform the necessity of transparent processing and communication to data subject from a nice to have formality to a mandatory and demonstrable necessity for all Data Processors and Controllers as indicatively:



The accountability principle requires the demonstration of concrete, specific and demonstrable measures such as the implementation of Data Protection Policies, the introduction and inclusion of Privacy by Design to all Products and Services of each Processor/Controller encompassing Privacy from the design phase of the Product/Service throughout its life cycle , the introduction of Role based access to Personal Data, the preparation of Incident Response Plan and the upgrading of security to all systems with the use of variable techniques e.g. Data Masking, Data Encryption, Data Pseydonimization, etc to implement the requirement of Privacy by Design introduced by the GDPR.

What Type of Fraud Can be Prevented Through Data Privacy Compliance and Specifically Through Privacy by Design Implementation?

The implementation of good Data Management practices, to comply with the strict requirements of the Regulation is directly linked to the prevention of one of the most common and expanding types of "Insider Frauds" i.e. fraud committed by employees or people having access to proprietary information or Special Category Personal Data, namely, **"Identity Theft" one of the most common fraud types.**

Identity theft occurs when someone accesses another individual 's personal information (name, date of birth, SIN, PIN) and uses it to perform unauthorized financial activities in that individual's, accessing the other individual's bank accounts, writing cheques opening bank

accounts, or obtaining false loans. With the aforementioned personal data a thief can practically steal your identity.

According to a recent FBI survey conducted in 2015, the vast majority of identity thefts incidents is being performed by insiders having access to the proprietary information and misusing this access for obtaining illicit personal gain or in order to harm the Company/Employer by selling the proprietary information to a competitor or third party for their own gain or illicit benefits. Identity theft can take many forms spanning from unauthorized access to financial institution information from mailboxes, diverting emails from its intended recipients rummaging through trash or gaining access to workplace records.

How Can Companies Protect Themselves and Prevent Identity Theft?

Data Processors and Data Controllers i.e. Companies and Organizations can react by implementing a Compliance approach to the GDPR requirements. Indicatively by implementing role based access policy to databases containing personal and Special Category of Personal Data, allowing access only to specific employees whose roles interfaces with the stored proprietary personal information, by implementing random and frequent privacy compliance audits to key stakeholders and Departments within the Organization, by implementing strict Personal Data Retention and Deletion Policies, and audit against their actual implementation and by introducing state of the art security measures for databases and systems, upgraded firewalls, DLP programs, Data Masking, Data Encryption or Data Pseudonimization techniques as depicted in the following example.

Example of Pseudonimization Technique

Data Subject #	First Name	Last Name
1	Fred	Jones
2	Albert	Einstein
3	Erin	Brockovic
4	John	Lewis

Data Subject #	Sex	Age	Tel No	Addre ss 1	Address 2	Address 3	Post Code	
3	F	55	01234 567890	The House	Somewhere St	Anyplace	LL65 3NY	

Specifically “pseudonimization” of personal data explicitly referred in the Regulation as an ‘Risk Based Measure: and indicative approach to Privacy by Design requirement, allows Data Processors to process Personal Data, even for a different purpose than the one for which the Personal Data were originally collected and stored.

The combination of appropriate technical controls (pseudonimization, encryption, safe storage, digital forensics) with the implementation of Secure Data Management Practices and Data Protection Policies, can effectively prevent the misuse of Personal Data and other proprietary information by Insiders and minimize the incidents of identity theft within a Company, mainly performed by employees or persons misusing their access to this information for personal financial gain, or for purposes of revenge against their employer or gaining illicit benefits from competitors or third parties.

The random and mandatory security control – during or after the “exit interview” on a fired or exiting employee, and the forbiddance to take any type of portable devices, e.g. USB sticks, discs, flash disks etc if implemented on a larger scale could have prevented multiple identity theft cases while being in compliance with the new Data Protection European regime .

The adoption of simple and clear policies by Data Processors and Data Controllers as indicatively the introduction of a set of mandatory requirements applicable to all personnel e.g.:

- not to provide personal information such as credit cards, banking cards, PINs passwords, SIN and data of birth in response to any unsolicited request (including by email, website pop up or telephone unless the source is verified as a legitimate one;
- to promptly remove all mail from mailbox after delivery and not leaving mail lying around the workplace;
- not to respond to emails or telephone solicitations disguised as promotions or surveys offering instant awards or prizes;
- apply “Clear Desk Policy” to your electronic mailbox and not limited to your office;
- change your password regularly (e.g. once per month);
- apply two step verification to your PC or laptop;
- do not store sensitive personal information in flashes or USB sticks and other portable devices.

The compliance to the upcoming – strictest Data Protection Legislation in the world- as the new EU General Data Protection Regulation is considered to be -, does not impose additional financial or operational burden to Companies and Organizations – operating within EEA and worldwide. It encompasses a great opportunity to achieve competitive advantage, by implementing demonstrable Compliance Practices, and promoting the respect and value your Organization presents towards a valuable Corporate Asset i.e. Personal Data being entrusted to them by Employees, Customers, Peers, Authorities.

Moreover the implementation of the upgraded Security and Organizational Measures required by the Regulation can also upgrade fraud prevention and protect personal data and proprietary information from identity theft and other most common and frequent fraud schemes hence protecting and enhancing Corporate image and Reputation.

The GDPR Implications for Data Protection and Privacy Protection in Africa

Alex B. Makulilo*

Abstract

Africa and Europe have had relations for centuries. Mainly, the relationship between Africa and Europe is based on trade. A number of bilateral and multilateral trade agreements have been signed between the two parties. Concomitantly, policies that are designed by Europe to regulate the trading relations with Africa have had far reaching effect on the latter. This article offers preliminary assessment of the implications of the EU General Data Protection Regulation (GDPR) on privacy reforms in Africa.

Keywords: *Privacy, data protection, GDPR, reforms, Africa*

Introduction

The General Data Protection Regulation[1] is the new data protection regime in Europe. Its reform process was officially announced on 25 January 2012 and the Regulation was set to come into force two years after its publication. However, the adoption of GDPR took longer time than it was originally expected. On 8 April 2016 the GDPR was adopted after lengthy discussion and negotiations between the European Commission, the European Parliament and the Council of the European Union. Such deliberations took four years. The Regulation was published in the Official Journal of the European Union on 4 May 2016 and come into force 20 days later. However the GDPR effective date was postponed until 25 May 2018. The transition is meant to give EU member states time to align their laws and practices with the GDPR.[2]

The GDPR replaces Directive 95/46/EC and 28 national laws of EU member states. Although the review process that culminated to its adoption was officially launched in 2009, in reality the foundation of such process goes as far back as to numerous discussions, commissioned and non-commissioned reports, conference proceedings, commentaries by researchers, academics and practitioners, case law of the European Court of Justice, practices of national data supervisory authorities, etc between 1995 and 2009.[3] These sources provided clear signals that the Directive's revision was inevitable.

It is imperative to note that revision of the EU Directive came about after two decades of its adoption. Viviane Reding, the then Vice-President of European Commission, responsible for Justice, Fundamental rights and Citizenship had specifically pointed out three main trends as catalysts for EU data protection regulatory reforms: modern technologies, globalized data flows and access to personal data by law enforcement authorities.[4] Modern technologies

* Professor of Law and Technology, the Open University of Tanzania, e-mail: alex.makulilo@out.ac.tz

1 Regulation(EU) 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).

2 GDPR, Recital 171; Art.99.

3 See e.g., European Commission Justice's Studies, Decisions, Reports and Surveys, http://ec.europa.eu/justice/data-protection/document/index_en.htm; Article 29 Working Party on data Protection 1st, 2nd, 3rd, 4th, 5th ,6th , 7th ,8th ,9th ,10th ,11th ,12th and 13th Annual Reports, http://ec.europa.eu/justice/data-protection/article-29/documentation/annual-report/index_en.htm; Article 29 Working Party on Data Protection's Opinions, Working Documents and Recommendations (1997-2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

4 V. Reding, "The Upcoming Data Protection Reform for the European Union," *International Data Privacy Law* (2011)(1:1) pp.3-5, at p.3.

including the growth in mobile Internet devices, web-user generated contents, the outburst of social networking sites and above all the cloud computing technologies have been identified as new trends which postdate the Directive 95/46/EC. Because the latter law was adopted while the Internet was just at its embryonic stages in the 1990s, the recent technological developments especially in what have become known as the Internet of Things, cloud computing and Big Data analytics, have strained its operation. The modern technological developments have in turn increased globalised data flows at a 'rocketing' rate. Accordingly, globalization of technology has seen an increased role of third countries relating to data protection, and has also led to a steady increase in the processing of personal data of Europeans by companies and public authorities outside the European Union.[5] As a result, it has been difficult to precisely allocate responsibility, liability and accountability of various parties notably data controllers, processors as well as joint data controllers and processors. Also these cross-border flows of data to third countries have posed great challenges on how Europeans can enforce their data protection rights in non-EU jurisdictions. Besides these two trends, the growing appetite for personal data for reasons of public interest, in particular for public security matters, is also an important challenge for data protection.[6] While 'the collection and processing of personal information can be very valuable in order to secure important and legitimate public and public interests-if done in a way which fully respects the requirements of legality, necessity, and proportionality' its reverse may be disastrous to individuals'[7] control of their personal data.

The totality of the above trends exerted pressure to the need for revising the Directive. Such revision aimed at achieving the following objectives: strengthening the rights of data subjects; enhancing the internal market dimension; reinforcing data controllers' responsibility; revising the rules on police and judicial cooperation in criminal matters; improving, strengthening and streamline the current procedures for international transfers in the context of global dimension of data protection and providing better enforcement of data protection rules.[8]

The Key Elements of the EU GDPR

As a Regulation, the GDPR has a binding force upon EU/EEA member states and has direct effect upon them. The rationale for adopting a Regulation instead of a Directive (which has to be implemented or transposed by each member) is to achieve harmonization of the rules and practices. It is imperative to note that the GDPR permits member states to transpose many aspects into their domestic laws thereby questioning the overall aim of the Regulation of harmonisation and consistency in the law and practice.

Structurally, the EU General Data Protection Regulation is highly complex. It is a longer and more detailed text than the Directive. It has a preamble containing one hundred and sixty nine recitals. It contains eleven chapters with ninety nine Articles.

Like its predecessor, the EU General Data Protection Regulation is grounded on the same philosophical basis and objectives as the Directive. The philosophical underpinning of the GDPR is human rights and accordingly the twin objectives of the Regulation are to protect fundamental rights and freedoms of natural persons particularly their rights to protection of personal data and to ensure free flow of information within the European Union.[9]

---

5 ibid.

6 ibid.

7 ibid.

8 ibid, pp.3-5; see also, European Commission., "A Comprehensive Approach on Personal Data Protection in the European Union, COM (2010)609 final, Brussels, 4 November 2010, pp.1-19, at pp.5-16.

9 GDPR, Art 1.

Indeed the scope of the Regulation has remained the same as the Directive. It applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. As at its initial point, therefore, the GDPR applies to processing of personal data of natural person in both public and private sector regardless of the technology employed. This means both manual and automatic processing of personal data are covered by the Regulation. The GDPR does not apply to the processing of personal data in the course of an activity which falls outside the scope of the Union law; by a natural person in the course of a purely personal or household activity; and in the realm of national security and criminal law enforcement.[10]

The central element of the General Data Protection Regulation is its retention of the most basic principles of data protection in Directive 95/46/EC. However to make the GDPR stronger, additional elements have been introduced notably the transparency principle, clarification of the data minimization principle and establishment of a comprehensive responsibility and liability of the controller.[11] Moreover, the criteria of lawful processing have remained the same as in the Directive, only that the balance of interest criterion has to be applied. Also the Regulation clarifies conditions regarding re-purposing of the processing as well as conditions of consent with regard to processing of personal data.

The GDPR retains almost the same data subject rights as the Directive with few additional rights. The old rights have their scope been far clarified. The principle of transparency is at the root of the exercise of such rights. It is interesting to note in this regard that one of the new right introduced in the Regulation is 'the right to be forgotten' which simply mandates a data subject to direct the controller or processor, as the case may be, to erase and destroy completely any information relating to him or her, especially when its purpose or period required has expired or consent has been withdrawn.[12] The Court of Justice of the European Union(CJEU) had considered the right to be forgotten in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*[13] prior to the adoption of the GDPR. The court held that an Internet search engine operator is responsible for the processing that it carries out of personal information which appears on web pages published by third parties. Accordingly an Internet search engine must consider requests from individuals to remove links to freely accessible web pages resulting from a search on their name on the ground that the search results appear to be inadequate, irrelevant or no longer relevant or excessive in the light of the time that had elapsed.

The other right introduced by the GDPR is data portability which allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.[14]

The Regulation clarifies issues of controller and processor's obligations in data processing. Joint data controllers are also clarified in the GDPR. It is noteworthy that the Regulation introduces in clear terms the 'principle of accountability' as an obligation on the part of data controllers and processors. Controllers and processors are also obliged to carry out a data protection impact assessment prior to risky processing operation.[15] Also important to note is that the Regulation puts obligation on data controllers and processors to employ Data Protection Officers (DPO) whom will be required to possess knowledge on issues of data

10 GDPR, Art 2.
11 Explanatory Memorandum to the First Draft Proposal of the Regulation, p.8.
12 GDPR, Art 17.
13 Case C-131/12, Judgment of the Court (Grand Chamber), 13 May 2014.
14 GDPR, Art. 20.
15 GDPR, Art.35.

protection law and regulations.[16] The officer is required to discharge his or her duties with some levels of independence. There is also a requirement of data breach notification. The GDPR introduces a security breach communication framework for all data controllers regardless of the sector in which they operate. Notification obligations (to supervisory authorities and to data subjects) are triggered by accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.[17]

The general principles of transfer of personal data to third countries and international organizations are still maintained by the Regulation. The criteria and procedures for the adoption of an 'adequacy' decision by the Commission are based on Arts 25 and 26 of the Directive: rule of law, judicial redress and independent supervisory authority. However, the Regulation makes it clear that there is a possibility for the Commission to assess the level of protection afforded by a territory or a processing sector within a third country. Also binding corporate rules and standard contractual clauses are clearly spelt as means to be considered in the 'adequacy' assessment of data protection levels in third countries. It is also interesting to note that the in assessing the level of adequacy of protection, EU will take into account the third country's accession to the Council of Europe Convention of 28 January 1981 for the Automatic Processing of Personal Data and its Additional Protocol.[18]

Choice of law and jurisdiction rules have been radically changed in the Regulation. While in the Directive, these were based upon the 'territoriality principle' in the Regulation, such rules are based upon the 'country of origin' principle.

The Regulation clarifies a number of enforcement measures to be available for data subjects to enforce their rights. Sanctions and compensations have been enhanced. Previously the Directive did not clarify these issues as they were only left to the member states to provide them in their national data protection legislation.

Some definitions in the Directive have been taken out from the Regulation. Others have been retained by being complemented with additional elements in order to broaden their scope or to clarify them. In some instances, completely new definitions not part of the Directive have been introduced in the Regulation. Most of these definitions have been dealt with in such ways that they address the challenges of modern technologies.

The GDPR has also introduced a new concept not addressed in the Directive 95/46/EC. This is privacy by design and by default. It is noteworthy that privacy is not only regulated by legislation. There are other means that may help to protect privacy. Privacy by design and by default is one such other means. In this regulatory approach, privacy is considered as a fundamental component in the design and maintenance of information systems and mode of operation for each organisation. According to Art 25 of the GDPR, the data controller is required to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which necessary for each specific purpose of the processing are processed. This obligation relates to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

In terms of governance structure, the GDPR has replaced the Article 29 Working Party with the European Data Protection Board. Yet the Board is similarly composed of representatives (i.e. heads) of national supervisory authorities of each member state. Members of the Commission are no longer part of the Board, although they may attend its meetings, etc. The Regulation clarifies the independence of the Board, and describes its responsibilities and roles. Data protection regulators are provided just as in the Directive. A single lead

16 GDPR, Art.37.
17 GDPR, Arts. 33 & 34.
18 GDPR, Recital 106.

supervisory authority located in the Member State in which an organisation has its main establishment will regulate that organisation's compliance with the GDPR.

An Overview of Privacy Regulation in Africa

Although most constitutions of African states have provisions on the right to privacy, the concept of privacy and its regulation is relatively new. Currently most African countries still lack a comprehensive data protection legislation that is compliant to the international best standards, if not a data protection legislation at all. The first data protection legislation in the continent was adopted by Cape Verde in 2001. Currently there are 21 out of 55 African countries which have adopted such legislation.[19] There are similarly draft data privacy bills in various stages in many African countries.[20] It is imperative to note that the EU data protection framework has exerted influence in the data protection reforms in Africa. Partly, this is due to the existence of long time trading relations between Africa and Europe. Also the influence of Art 25 of the EU Data Protection Directive which restricts transfer of personal data from EU to third countries has played significant role of putting on Africa diplomatic pressure to enact such laws.[21] The assistance from European countries and agencies to Africa, have also catalysed the adoption of data privacy legislation. For example, in the Francophone Africa, the French data protection authority has provided support to many countries to enact data protection legislation.[22] Foreign and international agencies and organisation such as European Commission (EC) through the Support for Harmonization of the ICT Policies in Sub-Saharan Africa project (HIPSSA) and the United Nations Conference on Trade and Development (UNCTAD) have also have been instrumental in the evolution of data protection laws in the continent include.[23]

It is noteworthy that since the Directive was passed, approximately a period of 22 years to date, there is no African country that has received adequate certificate from the European Union. In 2010, there were attempts by four African countries namely Mauritius, Tunisia, Morocco and Burkina Faso to apply for adequacy from the European Union. However, the preliminary assessment showed that none of those countries complied with the European adequacy standard of data protection under Art 25 of the Directive.

Regional and sub-regional data privacy frameworks have also been developed and adopted over time. These include the African Union Convention on Cybersecurity and Personal Data Protection 2014, the Supplementary Act A/SA.1/01/10 on Personal Data Protection within Economic Community of West African States (ECOWAS), Southern African Development Community (SADC) Data Protection Model-Law 2012, East African Community (EAC) Legal Framework for Cyberlaws, (Phase I), 2008.[24] Of these, only the African Union Convention on Cybersecurity and Personal Data Protection as well as the Supplementary Act for ECOWAS are binding instruments. The rest are soft laws. It is noteworthy to point that the African Union Cybersecurity Convention is not yet in force for want of 15 ratifications by African states. Up to June 2017, only Senegal out of 55 countries had ratified this Convention.[25]

---

19 G. Greenleaf, "Global Table of Data Privacy Laws (As Known At 31 January, 2017)," *Privacy Laws & Business International Report* (2017)(No.145) pp.14-26.

20 ibid.

21 See, e.g. A.B. Makulilo, "Data Protection in North Africa: Tunisia and Morocco," in A.B. Makulilo, *African Data Privacy Laws* (Springer: Switzerland, 2016) pp. 27-44.

22 Lee A Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014) p.106.

23 A.B. Makulilo, "Data Protection and Law Reform in Africa: A Systematic or Flawed Process?" *International Journal of Technology Policy and Law* (2016)(2: 2/3/4) pp. 228-241.

24 For a critical analysis, see e.g. A.B. Makulilo, "Myth and Reality of Harmonisation of Data Privacy Policies in Africa," *Computer Law & Security Review* (2015)(31:1) pp. 78–89.

25 African Union., List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection,

Moreover, outside African, only two African countries notably Mauritius and Senegal have accessed to the Council of Europe Convention 108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol. Four more countries namely Morocco, Tunisia, Burkina Faso and Cape Verde have been invited by the Council of Europe to access to the Convention 108 and its Additional Protocol.

The Impact of EU GDPR on Africa

The implications of the GDPR on Africa cannot be fully drawn at this stage. This is because, the impact of a law does not only depend upon the textual analysis but also a vast array of factors-chiefly among them is sufficient practice of the law. Nonetheless, it is still possible to analyse certain implications of the GDPR at this moment.

First, the GDPR has a worldwide scope. Accordingly, it applies on Africa much the same as it does in Europe as long as African data controllers and processors have EU 'establishments' where personal data is processed 'in the context of the activities' of such an establishment. The term 'establishment' implies the effective and real exercise of activity through stable arrangements.[26] In *Weltimmo v NAIH*[27] the CJEU observed that the notion of 'establishment' is a broad and flexible concept that should not be confined to legal form. The presence of a single representative may be sufficient. Accordingly, an African data controller or processor who processes personal data of a data subject in the European Union under the umbrella of 'establishment' is subject to the ambit of the GDPR. More precisely, data controllers or processors in Africa not established in EU may still be subject of the GDPR if they process personal data of EU data subjects in connection with 'the offering of goods or services' or 'monitoring their behaviour'. Factors such as the use of language on websites which offer goods or services or currency generally used in one or more EU member states are relevant in ascertaining whether such a controller or processor which is not established in EU is actually offering goods or services or is monitoring behaviour of EU data subjects.[28] Mere accessibility of the controller's or processor's or intermediary's website in the Union, of an email address or of other contact details, or the use of language generally used in the third country where the controller is established, is not sufficient to ascertain offering of goods or services or monitoring of behaviour.[29] Thus, African data controllers and processors must comply with the requirements of the GDPR under those circumstances.

Secondly, the provisions on transfer of personal data to third countries incorporated in the Regulation have ramifications on legal reforms to third countries including Africa. Currently only 21 countries in Africa have data protection legislation in the EU style. Interestingly none of those countries have acquired adequacy certificate by EU. A preliminary assessment of four African data protection legislation (Mauritius, Morocco, Tunisia and Burkina Faso) by the European Union consultant in 2010 indicated that none is compliant to EU Directive on data protection.[30] As no adequacy decision has been made so far, African countries will have to pass through the hurdles of adequacy assessment under the GDPR. Although the criteria of assessment are almost similar, the GDPR establishes broader criteria. In contrast to the Directive, the adequacy assessment under the GDPR takes into account legal protections for human rights and fundamental freedoms. Since most African states have poor human

---

https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_.pdf.

26 GDPR, Recital 22.

27 C-230/14.

28 GDPR, Recital 23.

29 ibid.

30 For a critical analysis, see e.g., A.B. Makulilo, "Data Protection Regimes in Africa: Too Far From European 'Adequacy' Standard?" *Journal of International Data Privacy Law* (2013)(3:1) pp.42-50.

rights records or are dictatorial regimes,[31] this condition may be difficult to meet. Other criteria of assessment include access to transferred data by public authorities; existence and effective functioning of DPAs (majority of African DPAs are not established or fully operational)[32] and international commitments and other obligations in relation to the protection of personal data. Although majority of African countries are parties to the human rights treaties such as the Universal Declaration of Human Rights 1948, the International Covenant on Civil and Political Rights 1966; and the African Charter on Human and Peoples' Rights, it is likely that the EU will attach significant weight on the African Union Convention on Cybersecurity and Personal Data Protection 2014 in assessing international commitment and other obligations. The Cybersecurity Convention is the first and only binding treaty on data privacy outside Europe. Yet currently, out of 55 African countries only Senegal has ratified it. In this case this Convention is dormant since 15 ratifications are required to bring it into force.

Accession to the Council of Europe Convention 108 and its Additional Protocol will highly be considered by EU in the adequacy assessment. Recital 105 of the GDPR partly states: 'In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account' in assessing the level of adequacy of protection of personal data in the third country. As some African countries notably Mauritius and Senegal have successfully acceded to the Convention and its Protocol, they have an advantage of being positively considered by EU as meeting the adequacy standard under the GDPR subject to fulfilment of other criteria. It is also important to note that Tunisia, Morocco, Burkina Faso and Cape Verde have been invited by the Council of Europe to accede to the Convention 108 and its Additional Protocol. This is a positive move towards satisfying the adequacy standard under the GDPR.

It is also imperative to note that majority of data protection legislation in Africa does not provide expressly other possibilities of cross-border data transfer such as binding corporate rules and standard data protection clauses. As many African countries have not yet adopted comprehensive data protection legislation, these optional mechanisms will play significant role in the transfer of personal data from Europe to Africa. Accordingly, this may mean that law reform will be required to meet the criteria of Art 46 of the GDPR which deals with the transfer of personal data under appropriate safeguards.

Third, the GDPR has come up with new legal concepts such as privacy impact assessment, data portability, privacy by design and by default, the right to be forgotten, etc. Most of the concepts as well as new obligations to data controllers and processors in the GDPR which reflect the state of technology are not provided in the data protection laws of many African countries. This is due to the fact that some African countries adopted their data protection laws prior to the GDPR or the drafters of such pieces of laws did not go too far to ascertain the long term effect of the GDPR. This means that, law reform may be required to update such laws.

Lastly, it is imperative to note that companies in Africa that process EU personal data will have to comply with the GDPR. Breaches of personal data under the GDPR attract huge fines than those which are provided in the Directive. Accordingly, African data controllers and processors must as well make early preparations on how to comply with the GDPR so that they are not held responsible for data breaches.

Conclusion

31 See e.g., Human Rights Watch., "World Report 2017: Events of 2016" https://www.hrw.org/world-report/2017; Freedom House., "Freedom In the World 2017," https://freedomhouse.org/sites/default/files/FH_FIW_2017_Report_Final.pdf.

32 Makulilo (n 24).

An overview of the above discussion and analysis clearly show that the GDPR has significant impact on Africa. The most of important effect is on cross-border transfer of personal data. This triggers compliance by data controllers and processors in Africa to the requirements of the GDPR in the event they process personal data of data subject in the EU in the context of 'establishment' or offer goods and services to EU data subjects or monitor their behaviours. Compliance to EU data protection standards may mean that African countries have to revise their laws in line with the Regulation. Moreover, countries which have not yet adopted data protection legislation will have opportunity to consider the GDPR in their national laws. Finally, companies in Africa that process personal data of EU data subject will need to prepare for compliance with the GDPR.

The Danger of Using Alerts Including Personal Data to Protect Financial Investors

José M Baño Fos

Introduction

In today's world, any businessman would agree that building a good corporate brand and reputation is undoubtedly a key element to succeed. Yet, in certain professions, it is the personal reputation what is is quintessential in order to be able to carry a business activity successfully.

Even though doctors, lawyers or investment advisors, among many others, work more and more so under the umbrella of corporate brands that provide confidence to their actual or potential clients, it is undisputed that the trust and confidence that the clients generally require from these professionals is fundamentally based on personal relationships.

Thus, in these industries, it is mandatory for any professional to build a reputation as a trustworthy professional which is inherently linked to the name and surname of said individual.

This paper focuses on the financial services industry and the clash that it exists between providing accurate and transparent information to the investors with regards to any company or persona providing "dubious" investment services while respecting the personal data and, ultimately, the reputation of said professionals.

In particular, we will analyze the Spanish Exchange Commission's practice ("*Comisión Nacional del Mercado de Valores*" or "CNMV") of publishing information with regards to firms and natural persons allegedly carrying out investment services without the proper regulatory authorization and the personal data protection concerns that this behavior raises, showing how in our opinion the Spanish Supervisory Authority is currently infringing the EU Data Protection Regulation.

Moreover, this paper provides a very good working case scenario for the study of the interplay between administrative law and data protection regulation.

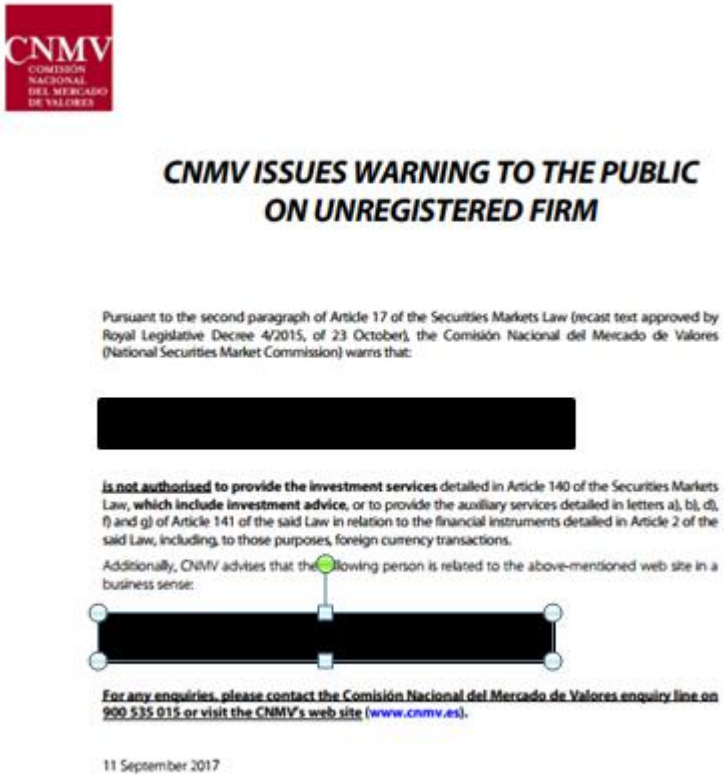
The CNMV's Practice

According to the mandate contained in Article 17 of the Spanish Securities Law ("*Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores*"), the Spanish Securities Supervisor - the CNMV - considers that it is its duty to inform the general public of any companies providing "investment services" without having previously obtained the proper authorization.

This entitles the CNMV, according to its own interpretation of the law (see section 3 below), to publish periodic alerts on companies suspect to be providing investment services without the adequate authorization and the natural persons related or associated with said companies.

The format in which the CNMV publishes these reports - which generally are replicated by the Spanish business newspapers – is the following: the CNMV informs that Company X is not authorized to provide investment services and then it specifies particularly which services is not authorized to perform (i.e. which specific service it thinks it is performing unlawfully) and subsequently provides the name/s and surname(s of those individuals that it

considers associated or connected to that Company. Let's see an example. The following is an extract of the alert published on September 11, 2017[33]:



CNMV ISSUES WARNING TO THE PUBLIC ON UNREGISTERED FIRM

Pursuant to the second paragraph of Article 17 of the Securities Markets Law (recast text approved by Royal Legislative Decree 4/2015, of 23 October), the Comisión Nacional del Mercado de Valores (National Securities Market Commission) warns that:

[redacted]

is not authorised to provide the investment services detailed in Article 140 of the Securities Markets Law, **which include investment advice,** or to provide the auxiliary services detailed in letters a), b), d), f) and g) of Article 141 of the said Law in relation to the financial instruments detailed in Article 2 of the said Law, including, to those purposes, foreign currency transactions.

Additionally, CNMV advises that the following person is related to the above-mentioned web site in a business sense:

[redacted]

For any enquiries, please contact the Comisión Nacional del Mercado de Valores enquiry line on 900 535 015 or visit the CNMV's web site (www.cnmv.es).

11 September 2017

We have deleted the company's information and the personal data of the individual - even though the information is currently available on the CNMV's website and accessible through research engines - for several reasons; the first one being that we do not want to be sued if Company X is able to show in Court that it did never carry out said investment activities in Spain.

Indeed, one of the most interesting aspects of these alerts is that as any good TV advertisement in reality it carries two different messages for the reader. The subliminal message is evident: "*we have learnt that Company X is providing investment services and they are not authorized to do so, so beware, because someone has already been ripped off*." The literal message yet is different and more nuanced: "*just for your knowledge, Company X is not authorized to carry this business activity because it does not hold the adequate authorization*".

The contrast is striking; whereas the literal message carries no assessment, in theory it is just informing the public of objective data - Company X is not authorized to provide investment services and person Y is the owner/manager/etc. of said company – the reputational impact is evident. No professional mentioned in said alerts will be able to maintain a successful practice any longer regardless of whether it does actually require a regulatory authorization or not.

[33] These announcements are published both in Spanish and English and stored in an online base available to the general public at https://www.cnmv.es/portal/advertenciaslistado.aspx?tipoAdv=1

As one can imagine, the impact of these alerts is far reaching since it is not targeted exclusively to potential clients but also to financial institutions which as soon as they learn about the alert will close or freeze the bank accounts of Company X or person Y to limit the risk of being considered a facilitator of Company X or person Y investment services.

Interestingly enough, even if the consequences are evident and damaging, technically, under administrative law, the alert does not fit within the traditional definition of an administrative sanction,[34] which means that as a result the company or individual involved is not granted the opportunity to a hearing or any of the safeguards of an administrative adjudicative proceeding.[35]

In other words, the professional is cursed and its reputation severely damaged without providing him or her with the opportunity to rebut the Supervisor's findings at an administrative phase. So one might reasonably ask: is this conduct legal?

The Weak Legal Underpinnings of the CNMV's Behavior and Yet the Difficulty for the Citizen to Annul the Alert

As we have seen, the CNMV's alerts claim that the publication is carried under the mandate contained in Article 17, second paragraph, of the Spanish Securities Act. Let's look at the provision:

> "The Spanish Securities Commission will ensure the transparency of the securities markets, the correct price formation of its stocks and the protection of investors, in order to do so the Authority will foster the dissemination of all information necessary to achieve such ends (Unofficial translation)".
>
> "La Comisión Nacional del Mercado de Valores velará por la transparencia de los mercados de valores, la correcta formación de los precios en los mismos y la protección de los inversores, promoviendo la difusión de cuanta información sea necesaria para asegurar la consecución de esos fines (Official Spanish version)".

Even though, it seems obvious that the legal basis used by the Spanish Authority seeks precisely to avoid the hassle of making a difficult factual finding about the actual services provided by Company X in Spain,[36] confronted against the Administration's leviathan, the natural person is ultimately at very uneven bargaining position.

Given the traditional margin of discretion granted to regulatory authorities under administrative law,[37] the Authority could reasonably argue in Court that the mandate contained in Article 17 of the Spanish Securities Law is sufficient to publish said alerts and that only if the information turns out to be inaccurate, i.e. meaning that person Y is not in any way linked to Company X, the alert should be withdrawn.

---

34 de Moor-van Vugt, Adrienne, Administrative Sanctions in EU Law (March 31, 2012). Available at SSRN: https://ssrn.com/abstract=1992922 or http://dx.doi.org/10.2139/ssrn.1992922

35 Asimow, Michael, Five Models of Administrative Adjudication (September 26, 2014). Forthcoming Vol. 63, American Journal of Comparative Law (2015); Stanford Public Law Working Paper No. 2502210. Available at SSRN: https://ssrn.com/abstract=2502210 or http://dx.doi.org/10.2139/ssrn.2502210

36 See the press release published by the Authority on October 9, 2003 announcing the launching of these alerts.

37 Nicolaides, Phedon and Prezios, Nadir (2014) Discretion and Accountability: The ESMA Judgment and the Meroni Doctrine. Bruges European Economic Research (BEER) Papers 30/2014. [Policy Paper]. BACIGALUPO, Mariano, La discrecionalidad administrativa (estructura normativa, control judicial y límites constitucionales de su atribución), Marcial Pons, Madrid, 1997.

In other words, the fact that the alert does not contain false information and it is not technically a sanction limits considerably the possibilities for a citizen to obtain redress based on classic administrative law grounds. Interestingly, this unequal bargaining position levels up once personal data protection is brought into the discussion.

A Data Protection Analysis of the CNMV's Behavior

As it might seem obvious to the data protection expert, but not so much to the Spanish Authority, publishing the name and surname of a specific individual and linking it to a specific company whose record might be, to say the least, dubious, amounts to the processing of personal data.

This section seeks to answer two related questions. First, is the Authority processing personal data and, secondly, if so, is the Authority complying with EU Data Protection Regulation?

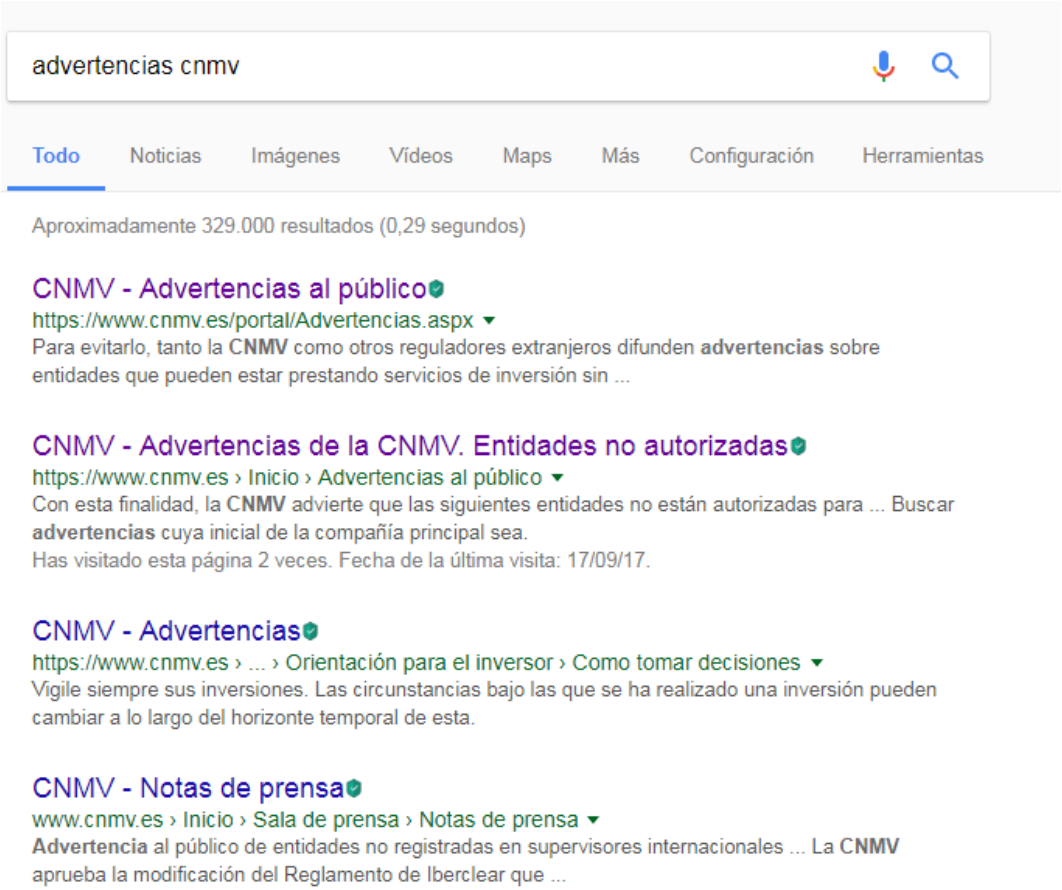
The processing of personal data

The EU Data Protection Regulation defines "personal data" as any information relating to an identified or identifiable natural person ('data subject') and defines an identifiable natural persona as one that can be identified by reference to a particular identifier such as his name. Evidently, the name and surname of a natural person is the easiest and more evident identifier and the company it works for, or it manages, or it controls, personal information relating to such individual.[38]

According to the Regulation, processing refers to the operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

As explained above, it seems evident the Authority processes personal data as it has built a database of companies which are suspicious of carrying investment activities without the adequate regulatory authorization and their shareholders, managers or related natural persons. This database is open to the public who can consult the information by company or natural person and is available also to search engines.

[38] See by analogy, the opinion of the Spanish Data Protection Agency nº0437/2010 regarding corporate email addresses available at https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2010-0437_Dato-de-correo-electr-oo-nico-de-empresa-de-los-trabajadores.-Cesi-oo- n-a-sindicatos.pdf (last accessed September 18, 2017).



In our opinion, this understanding is fully consistent with the ECJ's analysis on *Lindqvist*[39] given the use of the CNMV's website as a channel to access said information:

> "The term 'personal data' used in Article 3(1) of Directive 95/46 covers, according to the definition in Article 2(a) thereof, 'any information relating to an identified or identifiable natural person'. The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies. According to the definition in Article 2(b) of Directive 95/46, the term 'processing' of such data used in Article 3(1) covers 'any operation or set of operations which is performed upon personal data, whether or not by automatic means'. That provision gives several examples of such operations, including disclosure by transmission, dissemination or otherwise making data available. It follows that the operation of loading personal data on an internet page must be considered to be such processing. It remains to be determined whether such processing is 'wholly or partly by automatic means. In that connection, **placing information on an internet page entails, under current technical and computer procedures, the operation of loading that page onto a server and the operations necessary to make that page accessible to people who are connected to the internet. Such operations are performed, at least in part, automatically**."

The fact that part of this information can be in the public domain, for example, if the main shareholder's name shows on the alert and one can access the information on the public realm, for example if it is available on the Country Company's Registry, does not change the fact that the Authority is creating a specific database with a specific bias and impact and therefore is liable for the personal data processed in the course of such activity.

39 C-101/01, *Lindquist*, 6.11.2003.

Particularly, taking into consideration that the CNMV certainly facilitates finding such information which might not be so easily accessible. Indeed, this does not seem too far a stretch of the interpretation of the former Data Protection Directive by the ECJ in the famous *Mario Costeja* case[40] regarding the right to be forgotten and the role of search engines as facilitators of the accumulation of personal information regarding a particular individual:

> "Indeed, since the inclusion in the list of results, displayed following a search made on the basis of a person's name, of a web page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page."

Given all these elements it is time to try to answer the second question: is the processing of said information compatible with the EU Data Protection Regulation?

The infringement of the EU Data Protection Regulation: the MiFID Directive as an example of the adequate balance when issuing public alerts regarding investment services

Article 6 of the Data Protection Regulation sets out the different scenarios under which personal data processing can be considered lawful. Out of the different alternatives, the CNMV's behavior could potentially fall under, at least, two of them. Headings 6.1.c) "*processing is necessary for compliance with a legal obligation to which the controller is subject*" or (e) "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*".

In order to assess, whether the broad power granted to the Authority under Article 17 of Spanish Securities Law to ensure transparency in the market is sufficient to meet the threshold set out by Article 6 of the EU Data Protection Regulation one must bear in mind the seminal judgment of the ECJ in the *Schecke* case.[41]

In that case, the ECJ ruled, on the one hand, that professional information could be encapsulated into the right to privacy enshrined in Article 7 of the Charter of Fundamental Rights of the EU as well as within the protection of personal data contained in Article 8 of the Charter[42] and that disclosure of such information could be considered lawful if (i) it arises out of a mandate contained in the law, (ii) which seeks to achieve an end of general public interest and (iii) provided that the interference on the right to privacy and personal data protection is proportionate the general interest pursued.[43]

Taking these elements into account it seems difficult to conclude that the Spanish Authority behavior is lawful under the terms of the EU Data Protection Regulation. The easiest way to understand why is drawing an analogy with the European Data Protection Supervisor Analysis of the MiFID Directive.

---

40 C-131/12, *Google Spain SL v AEPD (The DPA) & Mario Costeja Gonzalez*, 13.5.2014.

41 C-92/09 Volker *Und Markus Schecke GBR v Land Hessen, And C-93/09 Eifert v Land Hessen And Bundesanstalt Fur Landwirtschaft Und Ernahrung*, 9.11.2010.

42 *Para. 59 "It is of no relevance in this respect that the data published concerns activities of a professional nature (see Österreichischer Rundfunk and Others, paragraphs 73 and 74). The European Court of Human Rights has held on this point, with reference to the interpretation of Article 8 of the Convention, that the term 'private life' must not be interpreted restrictively and that 'there is no reason of principle to justify excluding activities of a professional … nature from the notion of "private life"' (see, inter alia, Amann v Switzerland, § 65, and Rotaru v Romania, § 43)."*

43 Paras. 65 to 74.

The MiFID Directive expressly grants under Article 70.6 supervisory Authorities such as the CNMV in Spain the power to publish a public statement after issuing a cease and desist decision or a fining decisions including the name and surname of the natural person/s involved.[44] Moreover, Article 71 of MiFID mandates that by default all decision shall be public unless the publication is considered disproportionate by the authority.[45]

Article 70.6 of the MiFID Directive has been transposed into Article 144, fourth paragraph, of the Spanish Securities Laws which grants the Authority has the power to issue cease and desist orders to companies operating without the adequate authorization and ultimate the power to fine such companies. In those cases, the Spanish Securities Law grants the authority the power to issue public alerts regarding such conduct. However, the cease and desist orders as well as the fines are subject to an administrative procedure that includes the right to a fair hearing.[46] Article 71 of the MiFID Directive on the other hand is to be found under Article 275 of the Spanish Securities Law. Yet as we have seen the Spanish Authority refers to a different provision when justifying its alerts.

The interplay between Article 70.6 and Article 71 is not easy to grasp as the European Data Protection Supervisor pointed out in its opinion on the original Commission's proposal.

> "Under Article 75(2)(a), the competent authorities already have, among their sanctioning powers, the power to issue a public statement indicating the person responsible and the nature of the breach (22). It is not clear how the publication obligation under Article 74 can be reconciled with the power to issue a public statement under Article 75(2)(a). The inclusion of the power to issue public statement in Article 75(2)(a) demonstrates that the publication is in itself a real sanction, which should be assessed on a case by case basis in light of the proportionality criteria enshrined in Article 76 (23)."[47]

---

44 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU Text with EEA relevance (MiFID II): "*In the cases of infringements referred to in paragraphs 3, 4 and 5, Member States shall, in conformity with national law, provide that competent authorities have the power to take and impose at least the following administrative sanctions and measures: (a) a public statement, which indicates the natural or legal person and the nature of the infringement in accordance with Article 71.*"

45 "*Member States shall provide that competent authorities publish any decision imposing an administrative sanction or measure for infringements of Regulation (EU) No 600/2014 or of the national provisions adopted in the implementation of this Directive on their official websites without undue delay after the person on whom the sanction was imposed has been informed of that decision. The publication shall include at least information on the type and nature of the infringement and the identity of the persons responsible. That obligation does not apply to decisions imposing measures that are of an investigatory nature.*

46 "*Será competente para la formulación de los requerimientos y para la imposición de las multas a que se refiere el apartado anterior la Comisión Nacional del Mercado de Valores que también podrá hacer advertencias públicas respecto a la existencia de esta conducta. Los requerimientos se formularán previa audiencia de la persona o entidad interesada y las multas se impondrán con arreglo al procedimiento previsto en esta ley*."

47 Eventhough, the numbering of the Articles changed the content is essentially the same and the Supervisor pointed out at the time. See the Opinion of the European Data Protection Supervisor on the Commission proposals for a Directive of the European Parliament and of the Council on markets in financial instruments repealing Directive 2004/39/EC of the European Parliament and of the Council, and for a Regulation of the European Parliament and of the Council on markets in financial instruments and amending Regulation on OTC derivatives, central counterparties and trade repositories (2012/C 147/01), available at https://edps.europa.eu/sites/edp/files/publication/12-02-10_financial_instruments_en.pdf (last accessed September 18, 2017).

The European Data Protection Supervisor went as far as to consider the publication of a public warning an administrative sanction on itself and thus subject to the principle of proportionality[48] and due process. Even though such a finding might be a bit of an over generalization it is true that in those cases that the publication is ancillary to the fine or cease order, thus it benefits from the guarantees of such proceedings.

Probably, as a result of EDPS report, the Commission's original proposal[49] was amended considerably to include the following particular limitation on the publication of personal data, under Article 71, paragraph 1, second indent of the MiFID Directive:

> "However, where the publication of the identity of the legal persons or of the personal data of the natural persons is considered by the competent authority to be disproportionate following a case-by-case assessment conducted on the proportionality of the publication of such data, or where publication jeopardises the stability of financial markets or an on-going investigation, Member States shall ensure that competent authorities shall either: L 173/460 Official Journal of the European Union 12.6.2014 EN (a) defer the publication of the decision to impose the sanction or measure until the moment where the reasons for nonpublication cease to exist; (b) publish the decision to impose the sanction or measure on an anonymous basis in a manner which complies with national law, if such anonymous publication ensures an effective protection of the personal data concerned; (c) not publish the decision to impose a sanction or measure at all in the event that the options set out in points (a) and (b) are considered to be insufficient to ensure: (i) that the stability of financial markets would not be put in jeopardy; (ii) the proportionality of the publication of such decisions with regard to measures which are deemed to be of a minor nature."

This shows that even after an entire administrative procedure with all the due guarantees foreseen in the Charter of Fundamental Rights of the European Union, the Authorities need to undertake a case by case analysis prior to the publication of any personal information. This also includes the obligation that the information remains accurate, as Article 5.1.d) of the Data Protection Regulation requires, in other words, the Authority shall publish all information relating to the possible litigation that might ensue afterwards. Article 71, second paragraph:

> "Where the decision to impose a sanction or measure is subject to appeal before the relevant judicial or other authorities, competent authorities shall also publish, immediately, on their official website such information and any subsequent information on the outcome of such appeal. Moreover, any decision annulling a previous decision to impose a sanction or a measure shall also be published".

Evidently, the powers of the Spanish Securities Supervisor are not limited by the content of the MiFID directive, yet this analysis shows that the Directive drafted when the Data Protection Directive was still in force had to reach a balance between ensuring transparency and protection personal data that following the Schenke ruling required not only the acknowledgment of such a general interest in a specific legal provision and an ongoing balancing of the different interest at stake through the principle of proportionality[50] but also a

---

48 The conflicting interests between the right to privacy and the right to data protection, on the one hand, and the need to enhance market transparency, on the other, had already been identified by the impact assessment report on the Commission's proposal with regards to whistle blowing and the recording of client orders but the impact assessment did not carry out any analysis of the compatibility of the publication of sanctions with personal data protection, as the EDPS report cleverly pointed out.

49 http://ec.europa.eu/internal_market/securities/docs/isd/mifid/COM_2011_656_en.pdf (Last accessed September 18, 2017).

50 Tridimas, *The General Principles of EU Law* (2nd edn, Oxford University Press, 2006).

procedure with all due guarantees under Article 41 of the EU Charter of Fundamental Rights.[51]

Thus, the entire assessment collapses once the Authority does not even grant those minimum guarantees. In other words, Articles 6.1.c and e of the Data Protection Regulation require not only that the task is carried out in the general interest and foreseen in a legal provision but also that is undertaken in accordance with the legal system which means, in our case, that no statement with a reputational impact on a natural person can be made without a proper administrative proceeding preceding such statement. Otherwise the legal provision entitling the Authority to process the personal data will not have been properly applied.

This very same conclusion is reached through a different reasoning if one focuses on the Regulation's requirement of accuracy on the processing of personal data (Article 5.1 EU Data Protection Regulation), if the key element for publication is the duty to warn, there must be sufficient evidence of an actual investment services activity prior to issuing the warning, otherwise there is no sense in the publication, yet if the Authority can issue the warning without a formal administrative proceeding reaching that decision, then how is it possible for the Courts to review and determine the accuracy of the information?

Conclusion

Ultimately the conclusion of this paper is quite straightforward: the Spanish Securities Supervisor infringes the EU Data Protection Regulation.

From a purely subjective consumer based point of view, is not difficult to understand the Authority. If the Authority receives a complaint from a disgruntled investor, it is easier to await to see if there are more complaints and check whether the company is registered to issue an alert than going through the procedure of opening a formal sanctioning investigation with the procedural guarantees that this requires. Particularly as this also allows the Authority to act more expediently avoiding that other "innocent" investors fall into the trap before it's too late as administrative proceedings tend to extend over time.

Yet, from a legal perspective, this coercive method of deterring illegal activities is troublesome as it allows the Authority to cause a serious impact on someone's professional reputation without even granting said person the right to a fair hearing. Moreover, it leaves the authority the opportunity to choose which infringements it seeks to pursue further, from others where it renders such announcement sufficiently effective. Not only so but allows it to threaten the companies or natural persons involved with the open of such an investigation in case they enquire about the publication of their alert.

As we have seen, the possibilities for regular citizens to fight any abusive behavior by the Administration on this regard – think for example of a false complaint to the Authority – is very limited if circumscribed to the classic administrative grounds for appeal.

However, once data protection regulation is brought into place, the perspective changes completely and it is the Authority and not the individual the one bearing the burden of proof as to the need and accuracy of the publication.

---

[51] 26.10.2012 Official Journal of the European Union C 326/403 EN "*1. Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices and agencies of the Union. 2. This right includes: (a) the right of every person to be heard, before any individual measure which would affect him or her adversely is taken; (b) the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy; (c) the obligation of the administration to give reasons for its decisions*."

Ultimately, the nice paradox of this paper is that in order to protect the natural person one must resort to data protection regulation as classic administrative tools seem ill fitted to solve the sort of problems that the posting this warnings on the internet might have on personal/professional reputation. Nonetheless, in order to properly interpret and apply said specific regulation (the EU Data Protection Regulation), one must resort to classic administrative concepts such as the right to an independent and objective proceeding terminating with a properly reasoned decision.

This example thus nicely illustrates, in our opinion, the increasing interplay between data protection regulation and administrative law that is going to take place in the future.

José M Baño Fos
Attorney at Baño León, Madrid
Adjunct Professor IE University, Madrid

"Equifax Data Breach, 143 Million Only Tip of the Iceberg"

Dr. Paul Lambert

Introduction

Credit reporting agency Equifax has just been hit by a massive data breach due apparently to a data hack incident.[52] The information currently available indicate that the personal and financial data of 143 million individuals have been accessed by hackers.

Data breach issues are one of the most critical legal and practical issues which arise under the data protection regime for companies.[53] Data breach and data breach responses are and have been important.[54] However, the number of nuances and distinct issues within a data breach incident are increasing.[55] The Equifax data breach (2017) is a perfect example of this increasing complexity.

Crisis

Rupert Younger of the Oxford Centre for Corporate Reputation recently referred to the things which companies must do in a crisis.[56] These are referred to as:

- acknowledge and apologize;
- identify root cause of the crisis;
- make the necessary changes;
- ongoing evaluation of crisis response.

This is indeed appropriate in a data breach crisis. However, the above recommendations do not fully convey the complexity of crisis data events, such as the hurricane of data event issues being experienced by Equifax presently.

---

52 Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber, "Equifax Says Cyberattack May Have Affected 143 Million in the US," *New York Times*, 7 September 2017; "Equifax Says Data Breach Hit 143 Million," *BBC*, 8 September 2017; Olivia Solon, "Credit Firm Equifax Says 143m Americans' Social Security Numbers Exposed in Hack," *Guardian*, 8 September 2017; Craig Timberg, Elizabeth Dwoskin and Brian Fung, "Data of 143 Million Americans Exposed in Hack of Credit Reporting Agency Equifax," *Washington Post*, 8 September 2017; Craig Timberg and Elizabeth Dwoskin, "Hackers Access Database That Had Personal Data for 143 Million Americans From Credit Reporting Agency Equifax," *Washington Post*, 8 September 2017.

53 Generally note Lambert, *Essential Introduction to Understanding European Data Protection Rules* (Routlege Taylor and Francis); Jay, *Data Protection Law and Practice* (Sweet and Maxwell); Lambert, *A User's Guide to Data Protection* (Bloomsbury Professional); *Gringras, The Laws of the Internet* (Bloomsbury Professional).

54 Ronald W. Breaux, Emily Westridge Black and Timothy Newman, "A Guide to Data Protection and Breach Response," *Intellectual Property & Technology Law Journal* (2014)(26:8) 23.

55 Bradford C. Mank, "Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?" *Notre Dame Law Review* (2017)(92:3) 1323; Mary Ellen Callahan, "Once More Into the Breach," *Criminal Justice* (2017)(32:2) 20; Stephen A. Riga, "Two Breaches, Two Enforcement Actions, and a DDOS Attack: Data Security and the Rise of the Internet of Things," *Journal of Internet Law* (2017)(20:9) 3; Caleb A. Seeley, "Once More Unto the Breach: the Constitutional Right to Informational Privacy and the Privacy Act," *New York University Law Review* (2016)(91:5) 1355; John Reed Stark, "Top Cybersecurity Concerns for Every Director," *Corporate Governance Advisor* (2017)(25:2) 1.

56 Rupert Younger, "4 Things Companies Must Do In a PR Crisis," *CNN.com*, 1 September 2017.

New data breaches are increasing in detail, complexity and scale compared to the breaches of the past. On its face, the Equifax issue relates to a data breach event, a hack in particular. However, these are *not* the only aspects of crisis which the Data Protection Officer (DPO), Privacy Officer (PO), Privacy Counsel (PC), PR professionals, and others in Equifax need to consider and deal with.

Just some of these examples are outlined below.

Scale

This is no ordinary data breach event. The breach is reported as amounting to the data of at least 143 million individuals. This is large and significant by any scale. This scale translates into a massive response being needed by Equifax in order to inform, assist and protect the individuals concerned. The DPO, PO and or PC will be central in initiating, assisting and guiding these responses as appropriate.

Quality of Data

The nature and quality of the data is highly pertinent. The Equifax data are highly sensitive financial data, including financial details, social security numbers, driver licence numbers, name, address, etc. The sensitivity and financial nature of the breached data are important factors in escalating the responses needed.

Delay in Notifying Public

There was a clear delay in the company notifying the public and individual customers of the data breach.[57] It took five weeks from discovering the breach to notifying the public. This delay can have important implications and may be a factor in various investigations.

Unclear if Any Official Notification

It is unclear from reports if there were any official notifications of the data breach by the company, and if so, which regulators were notified.

Breach Becomes an International Concern

While legitimately the initial concern has been to the interest, expectations and rights of individuals in the US, concern has also quickly been expressed for foreign personal data also affected by the hacking. For example, Equifax has been advised to inform UK citizens if they too are at risk after the data breach event.[58]

Lack of Response and Then Poor Response

Equifax has been criticised for a lack of response and also when the response began, the inadequacy of that response.[59] The help website established was criticised and was less than functional for user concerns. It also initially redirected to existing services, and not the instant breach problem issues. These problems also extended to the call centre taking complaint and query calls. There were many reports of dropped calls, hours of call waiting, lack of knowledge and real informative assistance if and when a concerned individual was able to connect with a call centre individual. It is reported that there were no real information available, and apparently no proper scripts. The call centre personnel apparently had no ability to connect with live customer data to deal with queries.

Call Volume

---

57 Hayley Tsukayama, "Why Can It Take So Long For Companies to Reveal Their Data Breaches," *Washington Post*, 8 September 2017.

58 Alex Hern, "Equifax Told to Inform Britons Whether They Are at Risk After Data Breach," *Guardian*, 8 September 2017.

59 Olivia Solon, "Equifax Hack: Credit Monitoring Company Criticized for Poor Response," *Guardian*, 8 September 2017. Hamza Shaban, "People Have Been Signing Up For Equifax's Help Service. Here's What They Were Told," *Washington Post*, 9 September 2017.

There are reports, similar to the above, that the company was not able to deal with the volume of calls by naturally concerned individuals.[60]

Confusing Instructions

Some criticisms have been that the initial advice and instructions given by Equifax to concerned individuals has been confusing.[61]

Responsibility

There is a perception that Equifax is not properly seeking to address the problem, fix the problem, minimise and eliminate adverse effects to individuals, respond to individuals' concerns and the risks they are facing. There is also a perception that the company might even deliberately or inadvertently profit from the breach event, such as seeking to have individuals sign up to new or existing paid services, or to sign up for any services after a limited time free service – even victims of the data breach.[62]

Seeking to Avoid Responsibility and Liability

There are accusations that the company is deliberately seeking to cover itself off from legal (and ethical) responsibility to those affected, and whom are at risk of bad actors using their financial data for fraudulent purposes (fraud, identity theft, etc.). For example, there was a help website established by the company but some of the small print terms on it were understood by many to be an attempt to avoid and exclude liability and responsibility. On the help website a "small print … clause … prevented them from suing Equifax or entering into a class-action lawsuit."[63]

Risk to Individuals

Individuals whom are affected are open to the hackers, purchasers of the illicit data or other third parties seeking to use the stolen data for fraudulent purposes e.g. making false loan applications in the name of one of the individuals whose data was stolen from Equifax in the hack. These legitimate concerns are not, in the eyes of many, not adequately addressed by the company.[64]

Inadequate Response to the Risks to Individuals

Many individuals would feel that they are not being proactively advised of the full detail of the events that occurred and the impact and rick issues arising for them individually. Nor would they feel assured that they are advised adequately as to what steps (a) the company is taking, and (b) what steps individuals may take, to reduce the risks to them of fraud or other adverse effects arising. Nor might they feel that corrective steps or compensatory steps are being transparently being offered.

While the protection offered, turning the individual credit histories off for a period to counter fraudulent use of the stolen data, appears to be offered, it does not appear that this is proactively notified and explained on an individual basis. It appears that individuals themselves have to go and find the information. Where credit history turn-offs are offered,

---

60 Hamza Shaban, "People Have Been Signing Up For Equifax's Help Service. Here's What They Were Told," *Washington Post*, 9 September 2017.

61 Ron Lieber, "Equifax's Instructions Are Confusing. Here's What to Do Now," *New York Times*, 8 September 2017. Hamza Shaban, "People Have Been Signing Up For Equifax's Help Service. Here's What They Were Told," *Washington Post*, 9 September 2017.

62 Farhad Manjoo, "Seriously, Equifax? This Is a Breach No One Should Get Away With," *New York Times*, 8 September 2018. Hamza Shaban, "People Have Been Signing Up For Equifax's Help Service. Here's What They Were Told," *Washington Post*, 9 September 2017.

63 Olivia Solon, "Equifax Hack: Credit Monitoring Company Criticized for Poor Response," *Guardian*, 8 September 2017.

64 Brian Fung, "Equifax Finally Responds to Swirling Concerns Over Consumers' Legal Rights," *Washington Post*, 8 September 2017.

this might work with Equifax, but may not work with other agencies. Therefore, it is of limited effect and is not a full solution. It is also unclear what additional safeguards are being offered – and at what cost. Possibly any cost to individual victims, whether immediate or down the line, creates the wrong perception.

Executives Leaving

In some instances a company executive or manager may end up defending the company, security and or the breach response. In many instances of data breach, some of the personnel involved from IT, technical services, data, security, management (including the Managing Director or CEO) have either been dismissed, resigned or reprimanded. This occurred in some of the Sony data breaches for example. In the Equifax case, John Peterson, a management consultant, who was affected by the breach says that "[t]his is a big deal, but the response has been underwhelming. I see no reason why the CEO shouldn't step down."[65]

Since the Equifax data breach crisis has developed at least two executives have left the company. Susan Mauldin, the Chief Security Officer, and David Webb, the Chief Information Officer, have now retired.[66] Subsequently the CEO did leave.

Calls for Regulation

There will be inevitable calls for more regulation of the credit reference sector. It is not easy for Equifax to deal with or counter these calls in a significant breach event such as has occurred.

Loopholes in Regulation

Many perceive that the type of organisation that Equifax is, in a sector which carrying associated significant risks for personal data and sensitive financial data, is one which is under-regulated. The comparison is made to the banking sector which is regulated. Yet, the credit agency sector does not appear to have the same level of regulation, safety and risk assessment.[67]

Individuals in the company potentially have to understand and possibly defend why there is a perception of loopholes or under-regulation for the company and the sector. Potentially they have to defend the sector and not just the company.

Part of the Pack, or Lone Wolf

In addition, other companies in the sector may feel that the company and the data breach event(s) are giving the sector a bad name. Does this create pressure for an errant company to put its hands up and distinguish itself from other companies in the sector whom may be messaging that they are better, reliable and ore secure? or that the sector does not need (more) regulation? Decisions have to be made as to whether the company is on its own, or part of the sectoral crowd.

Irony and Data Quality

Referring to the Equifax data breach, Comodo security expert Kenneth Geersis states that it "ironic, for cybercriminals to compromise the very companies that internet users rely on to

---

65 Olivia Solon, "Equifax Hack: Credit Monitoring Company Criticized For Poor Response," *Guardian*, 8 September 2017.

66 Dustin Volz and Diane Bartz, "Equifax Two Top Technology Executives Leave Company 'Effective Immediately,'" *Reuters.com*, 15 September 2017.

67 Tara Siegel Bernard and Stacy Cowley, "Equifax Hack Exposes Regulatory Gaps, Leaving Consumers Vulnerable," *New York Times*, 8 September 2017.

safeguard their identities and finances."[68] These are important issues which DPOs, POs and PCs cannot ignore.

Perception of Potential Self Interest, Insider Information and Insider Trading

Before the data breach was notified to the public, certain Equifax executives sold $1.8m of their shares in the company.[69]

A statement had to be issued by Equifax on the share sale issue. Ines Gutzmer, the Head of Corporate Communications for Equifax, stated that "The three executives who sold a small percentage of their Equifax shares on Tuesday, August 1, and Wednesday, August 2, had no knowledge that an intrusion had occurred at the time they sold their shares."[70] This issue, and the initial explanation, will no doubt receive greater scrutiny as matters advance. This may also include scrutiny from official regulators, including financial and stock exchange regulators.

Questions arise such as when the DPO, PO or PC was notified? were executives notified before the DPO, PO or PC, and if so how long was the delay in notifying the DPO, PO or PC?

Investor Relations

Investors, current and potential, are acutely aware of the data breach event once it has been announced, but are critically concerned with the impact on the company, revenues, profits, prospects, damage, cost, liability, litigation damages, official fines and penalties, and value of the company and of individual shares.

The shares in Equifax initially dropped 13-14 percent once the breach issue became public.[71] It then dropped 35 percent with predictions of a fifty percent drop.

Conclusion

Equifax is not just dealing with a neatly defined data breach crisis. The main hacking of sensitive financial and related personal data is significant. But there are also a host of related and follow on data crisis issues to be dealt with – short term, medium term and long term.

The relevant data protection professionals must be aware of an increasingly wide number of interconnected issues, responsibilities and responses. It is increasingly evident that in particular circumstances, the responses (or lack of response)(and or delayed response) can further contribute to the problem event at hand. An inappropriate response can quickly escalate the problem. Worse still, this can be in a fully public manner with the full glare of media attention – and regulatory enquiries.

Certainly in future, and potentially even now, the responses will become part of the consideration in official fines and penalties. Companies need to be aware that the GDPR in

---

68 Olivia Solon, "Equifax Hack: Credit Monitoring Company Criticized for Poor Response," *Guardian*, 8 September 2017.

69 "Before Notifying Public, Equifax Executives Sold $1.8m in Shares," subheading to Olivia Solon, "Credit Firm Equifax Says 143m Americans' Social Security Numbers Exposed in Hack," *Guardian*, 8 September 2017; "Company Executives Sold Stock After Breach Was Discovered," subheading in Craig Timberg, Elizabeth Dwoskin and Brian Fung, "Data Of 143 Million Americans Exposed in Hack of Credit Reporting Agency Equifax," *Washington Post*, 8 September 2017.

70 Olivia Solon, "Credit Firm Equifax Says 143m Americans' Social Security Numbers Exposed in Hack," *Guardian*, 8 September 2017.

71 ibid.

the EU as well as regulators in the US are constantly increasing the level of potential fines and penalties.

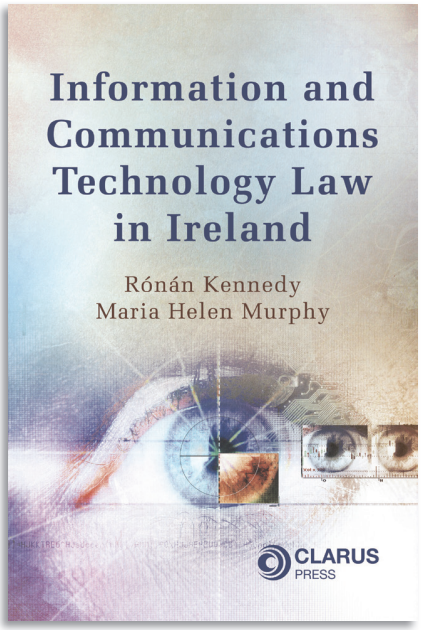
While this is a significant data breach because of the size but particularly because of the nature of the company involved (a financial credit rating agency), there are also other worrying data breaches above and beyond data breaches involving "normal" companies. Examples of these more serious data breach events include the data breach involving the SEC in the US and data breaches of certification/authorisation bodies.

The Equifax data breach is also a lesson on what should be done, what should not be done and the essential need that appropriate responses need to be timely and customer-centric.

International journal for the
Data Protection Officer
Privacy Officer
Privacy Counsel

Contact
Subscriptions and submissions should contact the
International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel at:

lex@mydistillex.com.



Information and Communications Technology Law in Ireland

Rónán Kennedy and Maria Helen Murphy

An up-to-date student textbook dealing with a range of IT Law issues.

Paperback €60

ISBN: 978-1-905536-96-2

Information and Communications Technology Law in Ireland

An up-to-date student textbook dealing with a range of IT Law issues.

Information and Communications Technology Law in Ireland considers the relationship between law and digital technology: both the way in which the development of information and communications technology (ICT) is shaped by legal rules, and the way in which ICT is changing how law is developed and implemented.

This book is designed to be accessible and is written in a practical style. Complex legal and technical material is explained in a clear and logical manner in order to aid understanding.

The book is divided into thematic sections including: contextualising the study of ICT and the law; private law implications of ICT (including intellectual property and online contracts); public law issues related to ICT (privacy, free speech, and computer crime), and the applications of ICT in legal practice. It also provides up-to-date information on key developing areas, including the General Data Protection Regulation, the Criminal Justice (Offences Relating to Information Systems) Act 2017 and crypto-currencies.

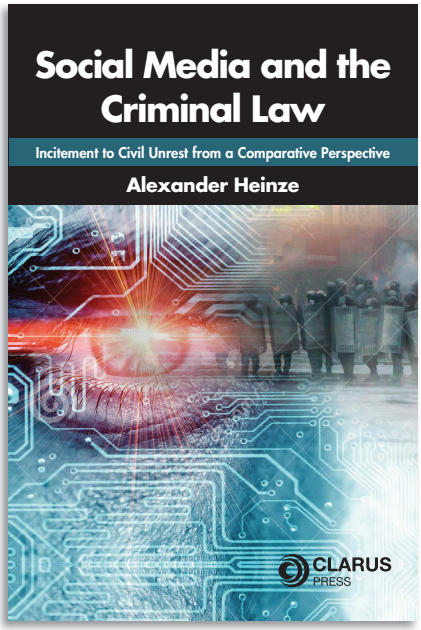
Social Media and the Criminal Law

Alexander Heinze

A unique work exploring social media and criminality.

Publishing 2018

ISBN: 978-1-911611-00-4



Social Media and the Criminal Law

A unique work exploring social media and criminality

Social Media and the Criminal Law is a new book which makes a cross-jurisdictional assessment as to whether the existing law is adequate for dealing with criminal conduct committed on social media sites in a manner that is compatible with human rights legislation and case law.

After defining the social media landscape, it both describes and analyses how social media expression is translated into criminal litigation. The author assesses how, in selected Common and Civil law jurisdictions, how laws traditionally governing particular types of expressive activity have converged in relation to criminal activity such as threats, hate speech, harassment, bullying, defamation, indecent images of children and terrorism.

This book's main focus is social media expression that plans and incites crimes, civil unrest and violent public protest and how this expression receives constitutional or human rights protection. Do human rights instruments protect people's messages, tweets, and Facebook posts that encourage an audience to protest? Can social media activity expose the average person to criminal liability when these protests turn violent? In an age where existing law can be seamlessly applied to new technologies and means of interaction, this book's comparative law approach to criminal activity on social media provides a much-needed analysis.

Clarus Press publishes a range of books and journals designed for both Irish and EU legal practitioners, academics and students.

CLARUS PRESS
www.claruspress.ie

Clarus Press Ltd,
Griffith Campus,
South Circular Road, Dublin 8

W: www.claruspress.ie
E: info@claruspress.ie
T: 01 415 0439

GDPR is not just a Privacy Protection Tool,

it is culture!

The DPO Academy

JOIN OUR GROUP
LinkedIn

www.dpoacademy.com