Spring 3-20-2018

The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness

Maria Chiara Addis
M.C.Addis@edu.salford.ac.uk

Maria Kutar
m.kutar@salford.ac.uk

The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness

Chiara Addis
Salford Business School, Salford, UK
Email: M.C.Addis@edu.salford.ac.uk

Maria Kutar
Salford Business School, Salford, UK
Email: m.kutar@salford.ac.uk

Abstract

The GDPR will be enforceable in May 2018 and its impact is expected to be significant, both in Europe and outside Europe. To date, many UK organisations are still unaware of the new legislation, with most still focused on the first implementation stage. A high number of organisations are expected not to be GDPR compliant, and therefore potentially liable to high sanctions.
This paper draws upon research on the GDPR and organisations in the UK, carried out in 2017. The research intended to explore the relation between the GDPR and emerging technologies, and the impact of the new legislations on adopters of emerging technologies. The study aimed to understand knowledge, implementation and impact of the new legislation, its relation to emerging technologies and its future in the UK, particularly considering the impact of Brexit. The research results can help to understand the current state of awareness and implementation of the new data protection legislation in the UK.

Keywords: GDPR, Data Protection, Information Systems, Emerging Technologies, European Union, Brexit

1, Introduction

The European General Data Protection Regulation (GDPR)[1] is the new legislation on Data Protection becoming enforceable across the European Union in May 2018. The GDPR strengthens the protection of personal data of individuals in the European Union and simplifies data law within the European Union. The coincides with a time at which Emerging Technologies (such as Cloud Computing, Big Data, The Internet

[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, 2016)

of Things, AI, VR/AR) are producing an enormous amount of data, and the implications for Data Protection are significant but unclear. The impact of the GDPR on European and Non-European organisations is significant. However, to date many organisations are still unaware of the new legislation and its complexity, while others are still focusing on the first implementation stage. A high number of organisations are expected not to be GDPR compliant, and thus potentially exposed to the new high sanctions introduced.

This paper focuses on UK organisations, explores the Regulations' impact and their relation to emerging technologies, and how UK organisations foresee the future of Data Protection, especially considering the uncertainty created by the Brexit Referendum.

2. GDPR – The Context

The GDPR was adopted in April 2016 after four years of discussions. It will become enforceable on 25 May 2018 providing uniform Data Protection within the European Union, and it will constitute the first update of Data Protection regulations since the Data Protection Act/DPA 1998 (Gov.UK, 1998), which enabled the 1995 EU Data Protection Directive (Directive 95/46/EC of the European Parliament, 1995), to be enacted in the UK. The GDPR is expected to have an impact on both data security and business outcomes. Its implementation may be expensive and time consuming where organisations need to implement solutions for preventing attacks, analysing and responding rapidly to breaches, although the cost will be dependent on the current levels of organisational compliance with data protection legislation According to global research conducted by Dell Software (2016), Digital/IT companies were lacking a general awareness about the GDPR: 97% of companies did not have a plan to prepare for GDPR, and only 9% of IT and business professionals were confident that they would be fully ready in May 2018.

A recent survey conducted by the international law firm Paul Hastings and published by Computer Week (Ashford, 2018) suggests that more than 90% of the US and UK companies believe they will be compliant in May 2018. However, the same survey shows other worrying data. Only 39% of the UK companies and 47% of companies

in the States have GDPR projects in place, with only a third getting specific support from third parties with their GDPR implementation.

2.1 GDPR – The Essentials

The GDPR formalises some concepts already developed through the courts and provides higher accountability and transparency (Kolah & Foss). While many concepts in the GDPR are similar to the existing UK Data Protection Act, others constitute a significant improvement (ICO, 2016). In this section we outline the areas of change against current legislation.

Global reach

The new Data Protection legislation will have a global application. It applies to entities and subjects based in the EU, and to entities based outside the UE that handle EU citizens and residents' data (Art.3). Therefore, Non-EU organisations that process data of individuals who are in the European Union, and do business in Europe must comply with the new regulation.

Definition of Personal Data

Under Article 4.1 …any information related to an identified or identifiable (living) natural person ('data subject') ...who can be identified, directly or indirectly…by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The definition includes digital footprints, such as IP addresses and cookies, which are extremely important for location based marketing and data security.

Under Article 9 the definition of Sensitive Personal Data (special categories of personal data) is also expanded, with the inclusion of Genetic and Biometric data. Recital 51, for example, prescribes that the processing of photographs should not systematically be considered processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in

specific cases set out in this Regulation (e.g where it is in a member states' public interest).

Consent

Where consent is given to collect, process and delete data it must be specific, informed, freely given, clear and affirmative (silence or pre-ticked boxes cannot be used to obtain consent, and that consent must be recorded and stored for audit purpose). Consent can be withdrawn at any time and it shall be as easy to withdraw as to give consent (Art 7).

Subject Access Requests (SAR)

Data Subjects can request access to personal data. There is a new , shorter deadline for organisations to respond (30 days and not 40) and it can be requested not only in writing.

Data Portability

A new right to have data exported onto a machine-readable format and transferred to another controller is introduced (Art 20).

Extended Right to be Forgotten

The right for Data Subjects to ask entities (both controllers and processors) to delete and destroy personal data is extended, and can be requested not only for search pages (as per Directive 95) but also in other cases, such as Facebook pages (Art 18). This right is not an absolute right but can be requested in specific case, for example when: the data was unlawfully processed, or retaining the data is no longer necessary (in relation to the original purpose), or this is necessary to comply with a legal obligation. Under the GDPR, the present of unwarranted and substantial damage or distress is not a necessary condition for exercising this right. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger. Data Subjects can also oppose the processing (where there is no overriding legitimate interest for continuing to do it) or withdraw their consent. (ICO, 2017, p 19)

Automated decisions, profiling and rights to explanation

GDPR introduces new requirements to provide greater transparency and more individual control. The GDPR introduces the definition of profiling (*Gathering information about an individual or group of individuals and analysing their characteristics or behaviour patterns in order to place them into a certain category or group, and/or to make predictions or assessments about their ability to perform a task; interests; or likely behaviour)*, new rights for data subjects and obligations for controllers (rights of explanation and the right to request human intervention).

Controller and Processor

Under the GDPR both have specific responsibilities, an expansion on the current situation.

Data Protection Officer (DPO)

The DPO is an independent GDPR role within an organisation to inform, advise and monitor compliance. Some organisations must have a data protection officer (DPO): if they are a public authority (except for courts acting in their judicial capacity); carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

Obligation to report breaches within 72 hours

Data breaches (e.g. cyberattacks or loss of company laptops or mobiles) must be reported within 72 hours after having become aware of it, both to Regulators and to individuals "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" (Art 33), or if "the data is anonymised or encrypted". If the organisation does not report a breach, this will result in a double fine (for breach and missing communication).

Data Protection Impact Assessments (DPIAs)

Organisations must perform a DPIA in order to understand the potential risks from processing data (Art 35). They are required in cases of:

-Systematic and extensive processing activities, including profiling, and in case of decisions that produce legal effects on individuals (Art 35 a)

-Large scale processing of special categories of data or personal data relation to criminal convictions or offences, including "processing a considerable amount of personal data at regional, national or supranational level…that affects a large number of individuals; and involves a high risk to rights and freedoms" (Recital 91).
-Large scale, systematic monitoring of public areas (i.e. through use of CCTV) (ICO, 2017)

Privacy by Design and by Default

Data protection needs to be taken into consideration from the beginning of any project (Art 25.1), and the controller must ensure that by default "only personal data which are necessary for each specific purpose of the processing are processed "(Art 25.2). By default, the highest privacy setting should be automatically applied to a new product, and by default, personal data should be kept only for the time necessary.

High Sanctions

Organisations are required to demonstrate how they are complying with the GDPR, and Data Protection authorities can assess how they are using personal data (audit). Administrative fines in the case of non-compliance have been massively increased. Regulators can impose:
-Fines up to €10m or up to 2% of the total worldwide annual turnover in case of minor breaches (Art 83.4).
-Fines up to €20m or up to 4% of the total worldwide annual turnover in case of major breaches (Art 83.5) and in case of non-compliance with an order by the supervisory authority.

It can be seen that under GDPR there are a number of additional requirements on organisations and some existing areas have been strengthened. In the following section we explore the impact of GDPR on emerging technologies.

3. Impact of the GDPR on Emerging Technologies

New technologies are creating increasing amounts of data (ICO, 2016) and the digital economy is growing. The European Union has been very active in both promoting Data-driven economy measures and protecting personal data of EU Citizens and

Residents (European Parliament, 2015). While legal obligations and responsibilities in traditional transactions are well defined (organisation as data processor, and customer as data controller), boundaries and responsibilities in non-traditional exchanges are less clear. The GDPR endeavours to clarify rights and protection of Personal Data in digital societies. In the rest of this section, we briefly sketch the main areas within Emerging Technologies on which the GDPR will have a major impact: Cloud Computing, Big Data, AI, The Internet of Things, VR/ AR.

3.1 Cloud Computing

The GDPR is quite prescriptive in relation to Cloud Computing, defining roles and responsibilities for Controller and Processor, outlining the content of the mandatory contract between the two (28.3), and regulating sub-contracting. The GDPR consider as Processors all kinds of cloud computing providers: Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS) and defines their obligations in relation to:

-Data destruction "…Processor must delete or return all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies…" (Art 28.3.g).

-Data Breaches, with processor to notify the Controller "without undue delay after becoming 'aware' of breach" (33.2).

-Security of Processing (Art 32) and record of processing activities (Art. 30.2).

The GDPR prescribes that controllers only use processors that can guarantee the technical and organisational measures to meet the GDPR's requirements (Art 28.1), and it regulates sub-contracting, prescribing that "The processor shall not engage another processor without prior specific or general written authorisation of the controller…" (Art 28.2).

The GDPR's compliance will be easier for the main players, as its requirements seem to be easily achievable by large organisations that can invest resources in technical and organisational changes, but will be more complicated for small organisations (Burton, 2016; Webber, 2016).

3.2 Big Data and Artificial Intelligence

According to existing data protection legislation under Directive 95/46, the processing and retention of personal data is only possible where it satisfies the concrete purpose of the original collection, and once this is done, data must be deleted. Re-processing data for a new purpose is allowed only if it is anonymised, compatible with the original purpose, and necessary to perform a contract, or is to comply with a legal obligation. Due to the existence of these constraints in Europe, some Big Data companies have tried to mitigate them asking consent on a wide purpose, keeping data for statistical purpose, or anonymising data (Mayer-Schönberger & Padova, 2015).

The principle of purpose limitation is retained by the GDPR (Art 5.b). However, the Regulation is more favourable to Big Data than the Directive, and seems to support innovation allowing some retention and re-use of data. Anonymous data are not subjected to the GDPR, but, for example, Art 89 prescribes appropriate safeguards, such as pseudonymization (Art 89.1) for processing scientific, historic or statistical purpose, and leaves the Member States to define the safeguards. Retention for statistical purposes is therefore still possible, and its applications are not rigidly defined by the GDPR, leaving to the Member States the competence to limit data subjects' rights for statistical purposes.

The GDPR recognises another important right for individuals. While they cannot refuse to be subjected to automatic processing, they have the right not to "be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her such as "performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements…" (Recital 71 and Art 22) and to require human intervention in the decision, with the exceptions of:

- Decisions authorised by the European Union or by the Member State (for example in case of tax evasion prevention) or necessary for entering or performing a contract between the parts
- Clear consent to the automated processing

Therefore, with Recital (71) the European Union recognises the right of European citizens to have clarification about decisions made through automated processing, a

new right that Goodman and Flaxman (2016) call “The Right of Explanation”. They argue that the GDPR “highlights the pressing importance of human interpretability in algorithm design” and forecasts “a pressing need for effective algorithms which can operate within this new legal framework”.

The need to have effective “decision making" algorithms is becoming a pressing issue, and the GDPR Right of Explanation is particularly important considering how algorithms work. Algorithms are generally aimed at finding patterns in large datasets, and such patterns are correlations and not causation. “The correlations identified by the algorithms point to some type of relation between different data but without necessarily providing an explanation as to what that relation is, nor whether there is a causal link between the data” (Kamarinou, Millard, & Singh, 2016, p 17).

Automated processing can produce negative consequences for Data Subjects as they can recreate, for example, patterns of discrimination (Crawford, 2016). If predictions are made by machine learning processes trained with biased algorithm, the result is what the European Data Protection Supervisor calls a “vicious circle of self-fulfilling prophecies…where the feedback the machine receives reinforces the bias present in the first place.” (European Data Protection Supervisor, 2016, p 4). For example, getting a loan would depend on postcode areas, and groups that are already oppressed and marginalised could be further discriminated against by the use of biased processes (Rhoen, 2016).

Barocas and Selbst (2016) add another level of analysis which gives rise to some concer, as the discriminatory decision would be more difficult to demonstrate (also in judicial proceedings) being the result of an (apparently unbiased) automated process and not a human choice. The authors highlight that this can produce the “perverse result of exacerbating existing inequalities by suggesting that historically disadvantaged groups actually deserve less favourable treatment” (Barocas & Selbst, 2016, p 674). However, not all algorithms and processes are biased, and if carefully created they can make decisions potentially more transparent than those made by humans (Goodman and Flaxman; Kamarinou, Millard, & Singh). The EU Institutions are aspiring to is to have automated processes based on algorithms that are more transparent, auditable and less discriminatory (ibidem).

In relation to right of explanation and accountability, in case of decisions made using Machine Learning technologies, an interesting point is made by Kamarinou, Millard, & Singh. If decisions are made using different sources this requirement can be difficult to meet in order to be compliant, and the point will be "open to interpretation and need to be resolved in the implementation and interpretation of the GDPR…" (Kerry, Blythe & Long, 2016).

3.3 The Internet of Things – IoT

"Bentham's panopticon is child's play compared to surveillance in a fully functioning IoT" (Wisman, 2012, p 7).

With an estimated 200 billion connected devices by 2020 (26 connected objects per person, Intel, 2016), the Internet of Things presents an exceptional challenge for personal data protection. The GDPR poses some challenges for the IoT, as noted by Finlay & Madigan (2016) and Edwards (2016) specifically with regards to:

Consent

As per GDPR, consent must be informed, unambiguous, given with a clear affirmative act (Recital 33), and demonstrable. Consent is the most challenging GDPR requirement to be met, as IoT ecosystems exist "a priori" and collect data from the environment independently by possible consent. "IoT devices usually…do not have means to display privacy notices and…devices are usually small, screen less or lack an input mechanism (a keyboard or a touch screen)" (Edwards, 2016, p 42).

Security

IoT is more susceptible to security breaches. Considering the rigid rule of Art 33 (breaches to be reported within 72 hours), organisations need to make sure they have everything set up to respond to a breach.

Many other elements of GDPR are of relevance to IoT; in particular the Right to be Forgotten, data portability and the right not to be subject to automated decisions. Other areas, like Privacy by Design and Privacy Impact Assessment will place specific requirements on IoT. Both requirements can be challenging. Some points made by Edwards are compelling:

1. Including Privacy by Design and PIAs in planning a IoT system, for example in smart cities, it is easier in new cities, (created with a top-down approach, such as Songdo in South Korea), than in already existent cities.
2. Designing IoT privacy should be done adopting a holistic approach, and involving other subjects (such as urban planners and architects).
3. Involving IoT vendors in creating Smart Cities has consequences for privacy and data protection. "While local governments may well feel they have the power and duty to control the final design but actual (though perhaps not legal) control may rest with private vendors or investors and their sub and sub sub providers in the Cloud." (Edwards, 2016, p 53).

Data protection is particularly relevant in relation to wearables technology, as this is one of the most powerful technologies able to collect data. Wearables use the Internet of Things ecosystem to collect and transfer data, and considering its growing popularity, data protection becomes particularly relevant especially for health data collected via wearables. The GDPR poses challenges for IoT environments and smart cities, and offers a new approach that take data protection and privacy from the start. Privacy by Design as the most important provision for the protection of personal data of individuals wearing personal devices (CMS Law Now, 2016).

Considering how personal data can be potentially accessed and personal privacy compromised in IoT ecosystems through for example, surveillance, sousveillance, and data driven economy, the challenges brought in by the GDPR are more than welcome.

3.4 Virtual Reality and Augmented Reality – VR/AR

The GDPR is also relevant for organisations using VR/AR technologies. Augmented Reality and Virtual Reality technologies are already applied in several sectors (such as Health, Entertainment, Defence, Education). As they are expected to grow in the next few years, concerns about Data protection and Privacy are huge.

Collecting data from locations where AR devices are placed, for example, can violate the privacy of individuals who are in those spaces and who have not given their consent. "AR automatically passes information about persons that the user sees, there

could be anything seen from social media, criminal record, and marital status" (Roesner et al, 2014, p.154).

In order to limit data violations, Brimsted (2016) for example suggests that "The processing of facial images, location and real-time data should be compliant prior to such activities taking place. This is just as relevant for start-ups as longer established businesses." This last point about company size is particularly important as the perception seems to be that the GDPR is relevant only for large companies.
Tozer and Mee (2016) analyse different aspects:
-The moments when personal info is collected in virtual reality environments: registration to access the service, and individuals' interaction in the virtual space, preferences, location are all of interest when considering IoT applications. Considering the GDPR's fines, VR/AR hardware, software and content providers must evaluate very carefully the potential legal consequences deriving from a not compliant data collection, data sharing, or location tracking in AR and VR environments are huge (Dentons, 2017).

4. Study Overview: Participants and Question Themes

The organisations identified for inclusion in the study were operating in various sectors (both public and private), and were chosen for being amongst adopters of emerging technologies. 50 potential participants (Senior Managers and Data Protection experts) were contacted for interview.

A general lack of awareness and knowledge of the GDPR emerged early in the empirical phase of this research, impacting considerably on both on the number of final participants and on the scheduled research timetable. Some manifested an early interest in being involved in research on data protection, but not on a specific research project on the GDPR, others were not aware of the Regulation. Interviews were conducted in February and March 2017.

9 correspondents gave their contribution; this included lawyer specialists in Data Protection and Privacy, Academics, IT Project Managers, and amongst them authors of numerous articles, blogs and publications on Data Protection. The group

encompasses considerable expertise in data protection and comprises individuals working extensively with organisations on GDPR.

Questions were based on 5 main themes:

A. General knowledge of the GDPR. Questions were focused on understanding the level of awareness, knowledge, involvement of professional bodies, the informing of management, and the training of staff.
B. GDPR Implementation. Questions were aimed at understanding what organisations had done and planned to do to implement the Regulation.
C. GDPR impact on business operations, with question related to potential challenges and disruptions.
D. GDPR and Emerging Technologies. Questions were focused on understanding potential specific challenges for adopters and for data created/processed via Emerging Technologies
E. Future of Data Protection, with questions aimed at exploring perceptions and expectations for Data Protection, particularly considering the impact of Brexit.

The questions were a combination of closed and open ended which gave space for participants to expand and choose how to shape the answer according to their experience.

5. Results

The primary data analysis was carried out considering the 5 main themes:

General knowledge of the GDPR

Most of the participants agreed on the general lack of awareness. UK organisations were, in general, not well informed about the future changes in Data Protection, and in some cases not even aware of the new legislation due to be enforceable in May 2018. There were major differences in terms of organisation size and industry sector. Large organisations were more informed and up to date, as well as organisations operating in the regulated markets (such as the Financial and the Healthcare), and this was mainly due to the work done by Regulatory bodies. The Information Commissioner's Officer, professional networks, business organisations, and large consultancies were raising awareness via specific guidance and informative events (organised mainly in

London), with Lawyers, Data Privacy and Info Security professionals being the first to get informed.

Considering the low level of GDPR awareness among Executives it was not surprising that internal training for staff seemed to be still far ahead. Companies had not started training their staff, as they were planning to do it nearer the time of implementation (probably using third parties). Data protection training awareness is a must for all staff as, in general, most data breaches are internal and not due to external hacks. Delayed training seemed to be particularly risky, and even more so in this case considering GDPR complexity, its innovative requirements and high sanctions.

GDPR Implementation

The low level of awareness translated into a general low level of implementation, except for those organisations who were more advanced in terms of Data Protection. The regulated market was ahead, with big banks having already GDPR programmes in place, and other sectors (such as Insurance) following.

The organisations which were more GDPR- "advanced" were: evaluating the future implications of the Regulation; reviewing their current data in terms of location, quality, and usage; starting the recruitment of some key GDPR roles (such as Data Protection Officers, data privacy teams and IT Project and Programme managers). Others were showing mixed approach, with some businesses adjusting and reviewing how they collected their data, and some others waiting for more clarity before taking action. It also emerged that some organisations were unable to deal with the GDPR and were getting rid of their data completely or leaving the market.

GDPR impact on business operations (challenges and disruptions)

The GDPR was expected to be extremely challenging and disruptive for organisations, and to have a major impact on projects, Business as Usual, budget (for GDPR training and projects), and resources, with the recruitment of DPO and Data privacy specialists. Staff shortages were also expected after May/June 2017, when organisations were anticipated to realise the impact of the GDPR and to compete for resources.

The disruption was also projected on internal processes, which needed to be adapted to new GDPR requirements: new specifications for consent, data breaches' new deadline (72 hours), reduced processing time for subject access requests (30 days), protection of personal data from the beginning of the project/by design, GDPR training to reduce the chance of data breaches, and new processes for working with GDPR complaint third parties. Positive outcomes were also envisaged, with an increase of transparency and awareness seen as reasons for more business opportunities.

GDPR and Emerging Technologies

The GDPR was expected to impact on the implementation and popularity of Emerging Technologies, with organisations that are adopters of Cloud Computing, Big Data technologies, and Fintech and Data-driven Marketing industries particularly exposed.

The specificities of Emerging Technologies were mentioned by various participants. Data created/processed via emerging technologies produces huge challenges to Data Protection, especially in terms of: Data type, volume, velocity; Data purpose; Data ownership; Data location; Data flow, transfer and "interim steps" (For example, with regards to data encryption, or in the case of involvement of other parties, such as sub processors. In this case more clarity was required on data visibility, location, and the exact reason for their involvement); Data merging done with Big Data, the Internet of Things and Artificial Intelligence; Data Security (for both controller and processor).

Using data captured without clear consent (if not reliant on other lawful basis for processing) is unlawful according to the GDPR. Privacy by Design, privacy designed in from the beginning of the project is also a general obligation, prompting privacy notices available at the point of capture which is particularly interesting in the case of the Internet of Things.

Future of Data Protection

Data Breaches, reputation loss and increased awareness were highlighted. The future of Data Protection seemed to be expected to be one of non-compliance and data breaches. Numerous and massive data breaches were expected to create serious

consequences (such as reputational damages or loss of reputation in more serious cases), to affect the shareholders' trust, and to impact business continuity of many organisations. High sanctions following breaches were considered as potential causes for forcing many organisations out of business. The amount and complexity of data was predicted to increase, as well as the awareness of individuals, who will be more confused by the complexity of data but will request more protection for their personal data.

Even though more certainty was required for some parts of the Regulation (for example, in terms of jurisdiction), the GDPR was thought by participants to increase transparency, accountability and user trust, and was expected to influence other legislations in other Non-EU countries (in order to be able to carry on trading with the European Union).

The Brexit referendum created uncertainty on tge adoption of the GDPR, even though the UK was one of the EU Member States pushing for the creation and adoption of a new legislation on Data Protection. After a moment of ambiguity, the Government (guided by Theresa May) clarified that the UK was going to fully adopt the Regulation. The Regulation was expected by participants to be the main Data Protection legislation for the next few years, as creating a different UK Data Protection to repeal the GDPR was believed to be extremely costly for UK companies both in terms of new implementation costs and of trade with European partners. For example, a company only operating in the UK and processing the Personal Data of individuals in Europe, would be in any case subject to the GDPR, and therefore need to appoint a Representative within the European Union. Brexit was expected to create some issues, such as delays in GDPR implementation and more difficulties for UK companies in consolidating their position in Europe.

In March 2018 The UK is currently discussing the Data Protection Bill, the law that specifies some elements of the GDPR and this will be the UK data protection law after Brexit. At the time of writing the Data Protection Bill is still being discussed at the House of Lords, but it is expected to become law ahead of the May deadline for GDPR.

6. Discussion

The GDPR regulates how technologies create and process all personal data, and the protection offered was welcomed by most of the participants, as the amount of data collected, processed, shared, stored and re-used has increased dramatically.

The European Union is the most active political organisation in the world in protecting personal data of its citizens. It also recognises the importance of competition, international trade, and the enormous potentials deriving from Technology. The GDPR is the result of both interests, it recognises the potentials offered by Big Data and data-driven economy, and it strengths Data Protection of individuals.

New provisions (such as those on consent, Privacy by Design and by Default, Data Protection Impact Assessment, Right to be Forgotten, high sanctions), will have an impact on how emerging technologies will be utilised by organisations. Furthermore, the GDPR attributes the responsibility of protecting personal data to organisations.

Most organisations are now using Cloud Computing. The GDPR is quite prescriptive in relation to Cloud Computing/Processor (Art 27-30), clarifying: roles and responsibilities of controller and processor; content of their mandatory contract; responsibilities in the case of sub-contracting; data transfer across countries. Some of these points were mentioned by participants, and concerns were voiced particularly with regards to data ownership, data location, data merging, profiling, and, in general, to the GDPR readiness of Cloud Computing companies, also in relation to big Tech companies. For example, one participant mentioned the white paper published by Amazon Web Services which did not contain any reference to the GDPR.

Cloud Computing technologies, with their unlimited capacity and low costs, are closed linked to the diffusion of Big Data and AI. Enhanced algorithm analysis, availability of data from IoT, and data mining applications are some of the features of the Big Data revolution. The GDPR takes Big Data into consideration, and it is more favourable to Big Data than the current legislation, in allowing, for example, processing for scientific, historic or statistical purpose (Art 5). The GDPR leaves

Member States to define the safeguards, and the UK is defining them in practice in the Data Protection Bill.

The Regulation recognises also the right of individuals:

-To have some clarification about the decisions - the so called "The Right of Explanation" (Goodman and Flaxman, 2016). The GDPR "highlights the pressing importance of human interpretability in algorithm design" (ibidem, p 26) and forecasts "a pressing need for effective algorithms which can operate within this new legal framework" (p 26).

-To refuse to be subject to decisions made only via automatic processing (such as profiling).

This clearly shows the importance placed by the GDPR on human interpretability in algorithm decision making. Both rights will be extremely useful for Data Subjects, and for those individuals and advocacy groups working on reducing existing inequalities, as they can be used to counteract the negative consequences caused by biased algorithms based on patterns of discriminations.

With regards to the Internet of Things and IoT ecosystems, the literature focused on some GDPR requirements, such as consent, security breaches and sanctions, Privacy by Design and Data Protection Impact Assessment/DPIA. Some participants expressed real concerns over possible surveillance through the IoT, and welcomed the future requirements, particularly with regards to consent and Privacy by Design.

7. Conclusions

Emerging Technologies are transforming how people live and work. Personal data is now the new oil, and new questions about power, agency and legitimacy arise. Legislations that protect individuals' personal data and regulate the digitalisation of "everything" are now needed more than ever, especially considering the data-driven economy and surveillance, as noted by participants. The European Union has been very active in promoting technology innovation and protecting personal data. The GDPR is a product of both these interests and at the same time a compromise between the two, increasing people's rights and providing rules for adopters of Emerging Technologies.

This research has shown that_UK organisations are not very aware of the coming Regulation. Most of them are not well informed about the future changes in Data Protection, with low level of knowledge also prevalent amongst Executives. Large organisations and organisations operating in the regulated market tend to be better informed and up to date, while others are still unaware. Training delivered by professional bodies and UK Regulators were slowly raising awareness; however, the lack of training for internal staff is particularly hazardous, considering the high chances of internal breaches and massive sanctions for non-compliance. Both the literature review and the expert interviews showed the prevalence of a low level of implementation with the exception of a few organisations, mainly in the regulated market, that have already GDPR programmes in place. Other organisations were waiting or exiting the market.

The implications for organisations are expected to be massive. The GDPR is an extremely complex piece of legislation, whose importance and effects have not yet been completely understood by most UK organisations. Moreover, another influential factor was the Brexit Referendum, because it led some organisations to believe, or hope, that the GDPR was not going to be adopted as a consequence of Brexit. Organisations had 2 years for becoming compliant before the enforcement date. One participant predicted a general panic from the end of 2017, and Laberis (2016) uses the term Tsunami to give us an idea of the massive turmoil to be expected regarding the non-compliance or delayed GDPR implementation in the future. According to the survey conducted by the international law firm Paul Hastings mentioned above, the Tsunami seems to be still far away in the minds of UK companies.

With regards to the research question addressing the specific impact of the GDPR on organisations who are adopters of Emerging Technologies, a surprising discovery was made in the early stages of the fieldwork, which had a profound impact on the research process. The lack of awareness was not only limited to the GDPR requirements but also to the usage of Emerging Technologies within organisations. A high number of organisations and professionals immediately ruled out the interview invitation on the basis that their organisations were not using any of the Emerging Technologies mentioned by the researcher. While this was understandable for some of

the more recent technologies, such as AI and VR/AR, it was surprising for more mature technologies, such Cloud Computing and Big Data, especially considering the high adoption rate of Cloud in the UK (90%). Therefore, the author found it easier to recruit Data Protection Experts working with various organisations, than Executives or Managers. For that reason, focusing the research only on adopters of Emerging Technologies was not possible due to time constrains. It turned out to be necessary to adopt a flexible approach and broaden the research question to focus on UK organisations in general and not only on adopters of Emerging Technologies.

The relationship between technologies and data protection is extremely fascinating. Rights can be enhanced or severely compromised, especially considering the most recent applications and potentials of AI. The role that Emerging Technologies will play in the future is exciting but also extremely worrying, which renders researching their implication on personal data and organisations necessary.

References

Ashford, W. (2018). Top UK and US firms still overestimating GDPR readiness. Retrieved 01.03.2018, from http://www.computerweekly.com/news/450432510/Top-UK-and-US-firms-still-overestimating-GDPR-readiness

Barocas, S. & Selbst, A. D. (2016). Big data's disparate impact. California Law Review, 104.

Brimsted, K. (2016). Virtual and augmented reality: time to update the legal handbook. Retrieved 31 December, 2016, from http://www.itproportal.com/features/virtual-and-augmented-reality-time-to-update-the-legal-handbook

Burton, G. (2016), GDPR may help Amazon, Google and Microsoft to dominate cloud computing, warns data protection lawyer, Retrieved 7 January, 2017, from http://www.computing.co.uk/ctg/news/2475110/gdpr-may-help-amazon-google-and-microsoft-to-dominate-cloud-computing-warns-data-protection-lawyer

CMS Law Now. (2016). mHealth – Wearables, technical innovation and Data Protection. Retrieved 01 February, 2017, from http://www.cms-lawnow.com/ealerts/2016/04/mhealth--wearables-technical-innovation-and-data-protection

Crawford, K. (2016). Artificial Intelligence's White Guy Problem. Retrieved 29 December, 2016, from http://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html?_r=2

Dell. (2016). GDPR: Perceptions and Readiness. A Global Survey of Data Privacy Professionals at companies with European Customers. Retrieved from http://www.eurocloud.fr/wp-content/uploads/2016/10/gdpr.pdf

Dentons. (2017). Virtual legality: Virtual Reality and Augmented Reality – Legal Issues. Retrieved from http://www.dentons.com/en/insights/articles/2017/february/20/~/media/ca3200046c7f4fe4a903c63fad09efac.ashx

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). Retrieved from EUR LEX http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

Edwards, L. (2016). Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective. Forthcoming European Data Protection Law Review (Lexxion)

European Data Protection Supervisor. (2016). Artificial Intelligence, Robotics, Privacy and Data Protection. Room Document for the 38th International Conference of Data Protection and Privacy Commissioners. Retrieved from https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/16-10-19_Marrakesh_AI_paper_EN.pdf

European Parliament. (2015). Big Data and smart devices and their impact on privacy. Retrieved December 14, 2016, from https://www.democraticmedia.org/sites/default/files/field/public/2015/ipol_stu2015536455_en.pdf

Finlay. F., & Madigan. R., (2016). GDPR and the Internet of Things: 5 Things You Need to Know. Retrieved 14 January, 2017, from http://www.lexology.com/library/detail.aspx?g=ba0b0d12-bae3-4e93-b832-85c15620b877

Goodman, B., & Flaxman, S. (2016). EU regulations on algorithmic decision-making and a "right to explanation". In ICML Workshop on Human Interpretability in Machine Learning (WHI 2016)

Gov.UK. Data Protection Act 1998 (1998). Retrieved from https://www.gov.uk/data-protection/the-data-protection-act

ICO. (2016). Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now. Retrieved from https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

ICO. (2017). Overview of the general data protection regulation (GDPR). Retrieved 30 January, 2017, from https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-4.pdf

Kamarinou, D., Millard, C., & Singh, J. (2016). Machine Learning with Personal Data. Retrieved 27 December, 2016, from https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2865811_code1175289.pdf?abstractid=2865811&mirid=1

Kerry, C., Blythe. F. & Long. W. (2016). How big will big data be under the GDPR?. IAPP. Retrieved 03 March, 2017, from https://iapp.org/news/a/how-big-will-big-data-be-under-the-gdpr/

Kolah, A., & Foss, B. (2015). Unlocking the power of data under the new EU general data protection regulation. Journal of Direct, Data and Digital Marketing Practice, 16(4), 270–274. doi:10.1057/dddmp.2015.20

Laberis. B. (2016). The Onrushing Tsunami Known as the GDPR. Retrieved 20 March, 2017, from https://securityintelligence.com/the-onrushing-tsunami-known-as-the-gdpr/

Mayer-Schönberger, V., & Padova, Y. (2016). Regime change? Enabling Big Data through Europe's new Data Protection Regulation. The Columbia Science and Technology Law Review (Vol.XVII). Retrieved from http://www.stlr.org/cite.cgi?volume=17&article=SchonbergerPadova

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). (2016). Retrieved from EUR LEX http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1481706421577&uri=CELEX:32016R0679

Rhoen, M. (2016). Beyond consent: improving data protection through consumer protection law. DOI: 10.14763/2016.1.404

Roesner, F. C., Denning, T., Kohno, T., Newell, B., & Calo, R. (2014). Augmented reality: Hard problems of law and policy. UbiComp 2014 - Adjunct Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 1283-1288.

Tozen, D., & Mee. D. (2016). VR: Not all legal plain sailing ahead, Retrieved 30 November, 2016, from http://www.gamesindustry.biz/articles/2016-09-06-vr-not-all-legal-plain-sailing-ahead

Webber. M. (2016). The GDPR's impact on the cloud service provider as a processor. Retrieved from http://www.fieldfisher.com/media/3993765/the-gdprs-impact-on-the-cloud-service-provider-as-a-processor-mark-webber-privacy-data-protection.pdf

Wisman, T. (2013). Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things. European Journal of Law and Technology, 4(2).