General Data Protection Regulation (GDPR), Artificial Intelligence (AI) and UK organisations : a year of implementation of GDPR

Addis, C and Kutar, MS

General Data Protection Regulation (GDPR), Artificial Intelligence (AI) and UK Organisations: A year of implementation of GDPR

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 General Data Protection Regulation (GDPR) became enforceable in May 2018 and its impact is globally significant. Meanwhile, a growing number of organisations are increasingly adopting AI technologies. This paper explores the effects of the GDPR on UK companies adopting or using AI technologies. A survey of AI, Data Protection and technology experts is presented, the analysis of which provides some early insights into the praxis of GDPR and AI in operational contexts. Whilst a growing body of research focuses on AI ethics and the impact of algorithms, this project highlights other important concerns emerging from the introduction and use of AI technologies. The findings indicate that few organisations are fully compliant with the requirements of the GDPR, which is not unexpected given the novelty of the regulation and the complexity of the technology. Other elements which can impact compliance and innovation were less predictable. Therefore, we recommend adopting a holistic approach to the management of personal data and AI.

Keywords: GDPR, AI/ML, Data Protection, Management, Innovation

1.0 Introduction

The European General Data Protection Regulation[1] (GDPR) became enforceable in 2018, reinforcing the protection of personal data and creating new obligations for organisations. This coincides with a rapid increase in the use of Artificial Intelligence (AI) technologies and a surge of available data. The implications of the GDPR for organisations using AI are significant, due to newly introduced responsibilities, yet these remain unclear. This paper explores the GDPR's impact on organisations implementing or already using AI technologies, a year after becoming enforceable,

[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)

focusing on UK organisations. Awareness, practices and challenges faced by companies implementing the GDPR are explored through the experience of experts working for a variety of UK organisations, in most cases as consultants or legal advisors. Their expertise in Artificial Intelligence, Data Protection and Digital Innovation, and understanding of the many organisations with which they have worked, offer insights into the understanding, perception and implementation of the Regulation. In this paper we first of all provide an overview of the key changes introduced by the GDPR, with a particular focus on those which relate to AI technologies, and explain the data protection challenges arising from the implementation of AI technologies. We then introduce the study and present the results. The discussion explores the themes which emerged from the data. We consider compliance, risk and preventive data protection, and examine some of the specific findings regarding automated and augmented AI and the repurposing of data. Finally, we consider in the conclusions key recommendations for the practice of Data Protection for organisations utilising AI technologies.

2.0 GDPR and AI

2.1 GDPR

The General Data Protection Regulation (GDPR) is a milestone in the legal history of Data Protection. The GDPR created new obligations for organizations processing personal data, increased the protection of data subjects, and established a more cohesive data protection regime across the EU. Adopted after four year of discussion, the GDPR was necessary to modernise the legislation in order to protect the rights and freedoms of individuals in the context of the digital economy. It has influenced Data Protection legislation around the world, such as the California Consumer Privacy Act of 2018 (CCPA), the LGPD in Brazil (Raul, 2018), and the Washington Privacy Bill (Cesaratto, 2019).

The Regulation shifted the focus onto organisations, introducing new obligations and formalising some existing practises from courts and management. In the rest of this section we present the key changes introduced by the GDPR.

Personal Data

The definition is expanded to include any information that can identify a person, 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" (Art 4.1). Biometrics and digital identifications are therefore included within the expanded definition of personal data.

Controller and Processor

There are changes to the defined roles of controller and processor under the Regulation. The controller defines the purpose and means of processing (Art 4 (7)), and the processor processes personal data "on behalf" of the controller (Art 4 (8)). Processing is regulated by a written contract (Art 28.3). Controllers and processors must be able to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (Art 32.1). These measures include testing, confidentiality, security, integrity, availability and resilience of processing systems and services, pseudonymisation and encryption, ability to restore the availability and access to personal data in the case of physical or technical incident, and not enabling sub-processing without proper authorisation. In the current technology landscape, processors are often cloud providers and vendors introducing AI into organisations.

Lawfulness of Processing and Consent

There are strengthened regulations around lawful processing and consent. Data can only be processed lawfully if at least one of the following is in place (Art 6): Consent of the data subject; Necessary for a contract or to enter into a contract; Compliance with a legal obligation; Necessary to protect the vital interest of the data subject or another person; Necessary for the legitimate interest of the controller or a third party, when they are not overridden by "the interests or fundamental rights and freedoms of the data subject which require protection of personal data…" (Art 6.1(f)).

Consent is one of the lawful bases for processing personal data, and it must be freely given, specific (for that purpose), informed, unambiguous and affirmative. It can be withdrawn at any time, and it must be as easy to withdraw as to give consent (Art 7) – this is a considerable step on from earlier legislation.

Purpose Limitation

Processing is performed for a "specific, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes…" (Art 5.1 (b)). Further processing is possible in specific cases (archiving purposes in the public interest, scientific or historical research purposes or statistical purposes) and only if the new purpose is compatible with the original one ('purpose limitation'). Compatibility should be assessed taking into account the links between the 2 purposes (Art 6.4), the context of collection, the expectations of data subjects, nature of data, potential effect on data subjects, appropriate safeguards (such as encryption and pseudonymisation) (European Union Agency for Fundamental Rights, 2018).

Data Protection Officer (DPO)

The DPO is an expert who informs, advises and monitors GDPR compliance. The role is a requirement for some organisations, for example public authorities, and organisations who carry out large scale or regular and systematic monitoring of the behaviour of individuals, or large-scale processing that could lead to high risk, as in, for example, of special categories of data or data relating to criminal convictions and offences.

Privacy by Design and Privacy by Default

The GDPR makes obligatory the adoption of "privacy-enhancing technologies" (PETs), aiming at reducing the amount of personal data collected by organisations. These are proactive tools that prevent (Art 25.1) or reduce (Art 25.2) the amount of data processed, therefore reducing risks, and accountability of organisations.

Fairness

Data must be processed in a fair and transparent manner (Art 5.1 (a)) and it has been suggested that the "principle of fairness goes beyond transparency obligations and could also be linked to processing personal data in an ethical manner." (European Union Agency for Fundamental Rights, 2018, p119).

Accountability

Organisations have to demonstrate compliance with the Regulation principles (Art 5.2) and have to implement "appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this

Regulation" (Art 24.1). This requirement can be challenging for organisations using AI, especially for the use of opaque algorithms, particularly deep learning (Butterworth, 2018), and for the intelligibility of automated processes.

Transparency

In general, it is an obligation on the part of organisations to inform data subjects about how their data is used. This principle is particularly important in relation to AI, decisions made via automated processes, and it is embedded into some GDPR requirements:

a. The right of explanation/information. The right of individuals to have an explanation of the decision made by automated means;
b. The right to request human intervention, in the case of decisions which produce legal effects or similarly significant affects the data subjects (Art 22.3);
c. The right to refuse (in specific cases) a decision made only via automated processing.

The existence of a right of explanation has been the topic of "the algorithmic war stories" (Edwards & Veale, 2017, p 64), and of a lively debate amongst researchers and practitioners on the existence of the right (Goodman & Flaxman, 2016; Edwards and Veale, 2017; Selbst & Powles, 2017; Casey, Farhangi, & Vogl, 2018). This new obligation has been considered and explained very differently by researchers: a proper right; an obligation on organisations to provide meaningful information; an explanation of some type about the logic behind the decision.

Therefore, the principles of Fairness, Accountability and Transparency (FAT) create obligations for organisations processing personal data, and they must be present in any processing. Data must be processed in a fair and transparent manner (Art 5.1 (a)), controllers must demonstrate compliance, processing must not be performed in secret, and individuals should always be made aware of potential risks (European Union Agency for Fundamental Rights, 2018).

FAT compliance can be challenging for organisations using AI/ML as they can incur a higher degree of difficulty in demonstrating adherence to the principles, and people within organisations can possess different understanding and perception of concepts, obligations and processes.

2.2 Artificial Intelligence and Machine Learning

The growth in the use of AI that has occurred in the last few years can be attributed to the combination of an increase in available data, more powerful computing, and better algorithmic techniques (The Royal Society, 2017). AI is generally understood as the capacity of a machine to perform mental or physical tasks that are typical of humans. Its recent success is mainly due to the success of Machine Learning (ML), a specific area within AI which replicates a specific human cognitive capability: prediction.

As explained by Agrawal, Gans, and Goldfarb (2018), the capacity for guessing hidden or missing information is exactly at the core of the development of ML *"*Prediction is the key element in Machine Learning. Often misunderstood for a certain future forecast, "PREDICTION is the process of filling in missing information. Prediction takes information you have, often called 'data', and uses it to generate information you don't have.*"* (p24). Combining Computer Science with Statistics and Maths, ML is impacting upon other technologies and sectors where it is used to increase efficiency and production. In this paper we use the term AI to encompass both AI and ML, whilst noting the distinction between them. While the success of AI is obvious and inspiring, especially in Healthcare, its deployment and use can also produce some unpredictable and less desirable consequences. For instance, impacting upon Human Rights (e.g. Privacy and Data Protection) and producing long-term socio-economic changes.

Some examples of potential impacts related to Data Privacy are: reduction of privacy, misuse of personal data, reinforcement of patterns of discrimination already existing in societies, AI systems being used to influence and manipulate public discourse (Tufekci, 2017, 2018), and Malicious AI (Borgesius, 2018). Awareness of discriminations resulting from bias has emerged, and concerns over the illegitimate use of personal data are growing, e.g. around biased algorithms leading to discriminatory decisions, or lack of transparency in opaque algorithms or black boxes (particularly in deep learning). These concerns are now being discussed more frequently in various fields, and amongst academics, practitioners, and within the wider public (O'Neil, 2016; Crawford, 2017; Whittaker, 2019; Borgesius, 2018; IEEE, 2019).

Moreover, the growth of digital transformation and AI has considerable implications for Data Protection. The pace of digital innovation in digital business is rapid, and products are created in a shorter time to respond to market (Bughin, Catlin, Hirt, &

Willmott, 2018). Organizations are accepting greater risks: using data gathered from different sources (internal and external); working with external stakeholders (e.g. vendors and cloud providers) to implement and maintain AI systems; using 'out of the box' systems which can be subjected to fewer controls; underestimating the complexity of the full ML process (data to train algorithms, make predictions and learn).

The GDPR extends legislative protections in this area and the relevance of these for organisations is still in the emergent stages, due to the rapidly changing technology landscape and new elements of regulation. Research and application of AI technologies has grown considerably in the last few years and many organisations are moving into increasingly advanced digitalised activities with potentially low awareness of the associated risks. The interconnection of Data Protection and AI, especially in practice and management is therefore still new and underexplored. The research presented in this paper aims to contribute to the discourse in this emerging and important area.

3.0 The Project

The aim of this research is to provide insights into the implementation, compliance, and impact of the GDPR, on organizations implementing or using AI technologies, a year after the Regulation came into effect. The research presented here forms part of a wider project exploring how leaders and managers who are adopting and using AI technologies perceive, understand and apply the FAT principles, and how this may affect organizations. The project is ongoing, and the results presented and discussed below represent findings from the initial survey element of the work. It is anticipated the outcome of the wider project will provide guidance to support organisations in adopting AI technologies which are fair, transparent and accountable.

3.1 Study Overview: Participants and Question Themes

This study comprises a survey of experts in Data Protection and AI. Semi-structured interviews were the chosen method for this project and were used to understand perceptions, understandings and experiences of participants with relevant expertise. The nine participants included Privacy Lawyers, Data Protection Consultants, Technology Businesspeople, and ML experts. Semi-structured interviews were conducted between March and October 2019, with the data collection commencing 11

months after the introduction of the GDPR. Participants have experience in both private and public organizations across a range of sectors. Participants jointly had considerable expertise in Data Protection, AI, ML, and data technology management, and included individuals who were on national and international expert groups on AI and GDPR. They provided details of trends and information from their industries, and insights from the experience in their current and completed assignments.

The interview questions were based on GDPR and processes and aimed to elicit information on what organizations had done with regards to the new requirements introduced by the Regulation. In addition, questions were asked about AI, and the relationship to internal organisational processes. Seven interviews were conducted in person in locations around the UK, while two were conducted via Skype. Interviews were around one hour each and were recorded and transcribed prior to thematic analysis and coding using NVIVO.

4.0 Findings

In this section we present the key themes emerging from the interviews followed by discussion considering the overall messages and lessons that can be drawn.

a) Compliance with GDPR

There was a consistent view amongst participants that many organizations are not yet GDPR compliant. Many organisations were reported as having done the minimum to become complaint, or not having started at all, possibly as they were waiting for their competitors to have major data breach (P1). In contrast, others were described as adopting a cautious approach and taking the time to understand how to implement changes and develop processes that are GDPR compliant (P7). Many were said to be avoiding engaging in the debate around AI and GDPR due to the complexity of the technology or worries that this could impact their innovation (P4).

Differences appear to exist across sectors, and according to the maturity and size of organisations:

- Large organisations have invested resources in compliance (P7) and are looking strategically at GDPR (P6). This was also observed in a small number of smaller organisations which have a mature data culture (P6).
- Organizations in the regulated sector are reported to be more mature, confirming the gap that emerged in pre-GDPR research examining organisational preparation for the Regulation (Addis & Kutar, 2018). Finance and Large Technology sectors are in a more mature stage in relation to awareness and the application of good practices, such as the creation of working groups '*to make sure everybody is connecting on the same page*' (P4).
- Organizations in the public sector are generally more compliant, due to the sector being more regulated, and to some of the new GDPR requirements such as the use of Data Protection Impact Assessments (DPIA) having previously existed as requirements in the public sector.
- A lower degree of AI awareness and GDPR compliance was reported in the private sector, particularly and amongst medium and smaller companies and start-ups (P4). '*In some sectors AI is mainly using personal information and there is a little bit more of an understanding of the need for care*…' (P5). This seems to be particularly the case for recruitment in some start-ups, where Data Protection was not seen as an issue or not even on their radar (P5).

b) Risks

Risk awareness and risk management were mentioned as crucial factors in GDPR compliance. Large and high-profile organisations generally have a lower risk appetite, and they are taking advice on many aspects (e.g. security, data location and data access, P5). Large companies holding a vast amount of personal data are adopting a cautious approach before starting new initiatives and in pursuing current ones. A risk averse approach allows organisations to understand how the GDPR changes the way they operate (P7). Some organisations are managing their risks by strategically choosing the areas where there are fewer ambiguities and where some requirements can be more easily satisfied. Choosing and focusing on the areas where risks can be reduced with more confidence, such as data flows or data storage, for example seems to be a common strategy (P4). In other areas there are still uncertainties, e.g. around consent, and consent withdrawal from data used to train models (P4, P5):

'If we generate a machine learning model on personal information, but then, one of the data subjects say I want to be removed, does it mean that you have to retrain the whole model? So…there are a lot of interesting questions in this space and a lot of unknowns' nuances of those data protection questions applied to machine learning' (P4).

Accepting higher risks and dealing with any consequences that might arise seems to be a common strategy. Small start-ups have high-risk appetite, and they are essentially focusing on the quickest way to get products to market (P4, P5). They are reported as taking risks in areas such as data aggregation and data location, and having a smaller number of data scientists, considered important for risk awareness within small companies and start-ups:

'They themselves don't fully understand what they are doing, and they probably have a very high level of abstraction. They don't know which questions they should be asking, and do not understand the deeper level to be worried about, like biased algorithms'. (P4).

The growing practise of using open-source technology to create ML systems was referred to as an important factor in enabling small organisations to create AI systems.

'*…people are just interested in developing the technology, using it and getting the benefits from it, rather than taking that step back and thinking about all the implications…The whole ethics around it, transparency around it, I think people see it more as a barrier and they are reluctant to engage in that debate because that might stop them from getting the benefit' (P4).*

Those vendors who possess AI and GDPR competencies are investing in research. This was illustrated by P4, whose company is looking at a number of methods to reduce risks, such as techniques around anonymization, homomorphic encryption and differential privacy. Homomorphic encryption permits encryption leaving the possibility to operate on the data. Similarly, differential privacy allows operating on data without revealing the actual data. The increased knowledge coming from these new techniques was described as an improvement for both the organisation and its customers, and it can be seen that this demonstrates nuanced understanding of the GDPR and its underlying principles.

Other risks can result from incorrect assumptions and expectations: they can lead to underestimating risks, neglecting necessary checks and controls, or misunderstanding

responsibilities. A number of examples were provided. Some organisations were wrongly assuming other subjects or stakeholders to be in charge, or to be already dealing with Data Protection and security measures. In some cases, there are expectations that all checks are done in the cloud, or by the AI vendors implementing the AI technology. Misconceptions about the technology were reported, including an assumption that AI systems are able to self-learn as they are supposedly 'intelligent'. Within organisations there were incorrect assumptions that other departments are responsible for data (P1) and, in the legal sphere, that commercial confidentiality of information is riskier than personal confidentiality of information (P5).

c) Automated and Augmented AI Systems

Several participants raised the issue of potential risks arising from automated systems, such as the potential lack of control, intelligibility and accountability.

For example, P2 noted how understanding the correct prediction made by ML in healthcare can be challenging:

> *'...you don't know if the machine randomly got it wrong. You can look at how does the system behave on average…but for the individual, you don't know whether or not it's got it right or wrong, so there are some models that can tell you the confidence in their model'.*

The same participant discussed the relation between intelligibility vs performance: *'...so what happens in practice is that you can have a model that works very well, but you don't know how it works…'.* A lack of explainability in ML was more accepted in some situations and contexts (such as deep learning used to screen e-commerce reviews (P3), and less in other contexts. This lack of transparency is a challenge for the right of explanation / information, which requires organisations to provide a meaningful reason for decisions made by full automated systems. One of the participants expressed some concerns over the ability of AI systems able to provide organisations some meaningful explanation:

> *'The way that AI works it's completely different to the way a rational human brain sees, thinks…AI has not got contextual understanding of what's going on. So to explain decision-making, it's very difficult to say what AI is actually doing, in what counts in human terms as an explanation.' (P 5).*

However, individuals can request access to their data (via a Subject Access Request / SAR) to check whereas a product is using that information, as per the GDPR obligation

on the organisation *'...quite the extent to which that is appreciated, and or possible or feasible is a really and interesting tricky area...' (P5).* Decisions made by humans in the case of augmented AI were generally assumed to be less risky. Having a human in the loop was seen as an important factor in eliminating or lowering the risks associated with full automated processes. '*Human arbiters'* that '*should always have the possibility to step in and change the decision made by the machine'* (P1), are assumed to understand, intervene and correct in different moments of the process (P1, P3). A fully automated process is generally used when the benefit is on the end user (P3): *'Let's say when an Algorithm that is not necessarily explainable has been used, so typically if that involves the end person not to be impacted and decision is in their favour, usually it is automated, where the risk for the business is seems to be low'*. When at the end the person does not get what expected, that decision usually goes to a human. Therefore, while some organizations are cautious or aware of taking risks, others appear to be making the wrong assumptions or lacking the necessary knowledge or specific information to understand the Data Protection risks associated with the use of these technologies.

d) Lawful Bases of Processing and Business Models

According to the principle of Accountability, organisations must be able to demonstrate the lawfulness of processing. Those organisations using AI/ML for their innovation were not believed to be carefully thinking about their lawful bases (P 5). The same participant firmly believed organisations *can* lawfully use AI/ML. When implemented carefully, the GDPR was seen as a mean to protect vendors using the technology to develop their products, providing they could demonstrate that the balance between theirs and individuals' interests was carefully considered.

Another significant remark was related to lawful bases of processing in automated decision-making. Relying only on consent can be risky for organisations. Asking for individuals' consent can be difficult prior to processing, and post processing, data subjects can withdraw consent (P5). Therefore, organisations should consider other lawful bases for justifying their processing, such as contract or legitimate interest, as long as that processing ought to be the only necessary means to achieve that purpose. P5 raised an interesting point, noticing how the 'necessity' was often dependent on the understanding of the concept:

'If your business model works by high volume decision making based on algorithms, does this in itself mean that the decision making is necessary? On a strict view the answer is no. On a more kind of open view, the answer is maybe, maybe it is, depending on where you give other safeguards within your process.' (P5).

Considering the growing interest in digital transformation, this point is particularly relevant at the current time. More organisations are choosing digital strategies which can modify or change their business models towards a more digital core and progressive developments towards more automated business process models are expected. Will this always create a 'necessity of processing' for digital businesses? Might this make the legitimate interest a default legal justification which will exonerate organisations from looking for another legal basis?

e) GDPR Requirements and AI

The GDPR requirements related to AI are not seen as easily achievable at this early stage of the use of the technology (P1, P3, P4). The sector and maturity of organizations are key factors in satisfying GDPR requirements. Internal cooperation and exchange between teams dealing with IT and data (such as data scientists), and those dealing with Data Protection (such as DPO and Information Governance managers) are also particularly important. Having Data Protection and data teams working together is more common in the public sector, this is likely to be due to the fact organisations are more used to performing DPIAs. In fact, whilst DPIAs are seen as a new GDPR requirement, they are not new in the UK, as they have been used for a long time within organisations operating in the public sector.

f) DPIAs and Privacy by Design

Not many organizations were reported to be performing Data Protection Impact Assessments (DPIAs) or using Privacy by Design (PbD) as these preventive activities were seen as *'luxury'*(P5) or '*a philosophy…very difficult to tie up*' (P6). Many organisations are reported to be thinking a little about PbD, with this mainly considered for specific issues, and not treated as a preventive and ongoing activity (P5). It is not yet clear if organizations starting to deploy or using AI/ML are performing DPIAs, or if vendors selling the technology are performing them, something considered particularly desirable and important by P5 (an expert in privacy law). The same

participant highlighted the importance of DPIAs for organisations and the lack of awareness of a valuable tool: '*I do not think that organisations necessary recognise how useful Data Protection Impact Assessment can be (*P5). In contrast, some organisations in the public sectors were reported to perform too many DPIAs (P6), and it was suggested that this was happening in the case of low risk situations where it is not a GDPR requirement. While this was not seen as negative per se, it was noted that the resources used for DPIAs could be employed for other activities.

The increased role of the DPO is another key GDPR element whose impact varies across sectors. Some organisations have concerns about the DPOs' power, and this was mainly reported in the public sector. Organisations '…*do not like it. In the private sector I have not encountered that so much. They know the DPO is an adviser, and they think of them as a lawyer and often appoint a lawyer. Those who have appointed a DPO they understand it.'* (P6). And yet, having a DPO does not necessarily guarantee compliance as '*years of struggle in getting themselves [DPOs] consulted*' were foreseen for those occupying that role. When companies in the private sector take the figure of the DPO very seriously, those are usually large companies with a low appetite for risk.

g) Accountability and Fairness

Accountability is a new requirement, and organisations now have a clear obligation to demonstrate compliance. The understanding of the concept can vary. When linked to demonstrating compliance within the security area, it is often considered as one of the easiest GDPR requirements to satisfy, as it is in the case of data location, storage and access (P5). In other circumstances its meaning is less understood, and in the case of small organisations '…*not even on their radar'* (P5). Accountability can be particularly challenging for organisations using deep learning, black box algorithms and autonomous systems (P3), and also in the case of ML systems continuously learning without any human oversight or having a too high degree of autonomy (P4).

However, demonstrating compliance can also be challenging for other reasons. People's competencies, power and team interaction can all impact the capability to demonstrate compliance. For example, P3 recalled the case of a manager who, lacking specific competences on AI, was delegating other people in the team, but carrying on owning the responsibility. *'There is a wider debate on how much responsibility bosses have…if something goes wrong, how much responsible and accountable they are?'*

(P3). Such situations were considered particularly problematic, as they were seen as a sign that some managers were signing off documents without understanding the consequences. This was considered a clear indication that, in some situations, accountability was more dependent on company decisions than algorithmic intelligibility.

Fairness is another GDPR principle which can be strictly linked to or be directly influenced by decisions on data made by the business. For instance, P6 revealed a link between concerns on people making decisions, and increased data collection. The fear of stigmatising certain categories of people by collecting data only from a specific group, or the lack of clarity on specific purposes, can lead organisations to collect data from everybody, increasing the amount of data and the related risks associated to data compliance:

> *'people making these decisions are always worried…and they collect everything for not missing out…so, in relation to Data Protection, it is easier if you have a clear purpose…always easy to justify, but it still needs to be driven by the purpose, the benefit, rather than that there is a piece of software available…' P6*

The decisions made on data, for example the data to be used, are usually made by one person or a group of people in organisations. New problems can arise when the data increases and *'you don't know what we want to know…we don't know what we're going to do…and we are going to let the data teach us' (P6).* Furthermore, it was unclear where qualitative checks on data were being performed next to quantitative ones: *'We would get an answer to this question I suppose only if an individual would bring concerns…or if really one of the regulators would really get involved…I would be very interested to know' (P5).*

Potential biases in ML system were mentioned in relation to personal data used to assess individuals, such as the US criminal system where black people are considered to be more at risk of offending (P5). Describing a complex picture, with danger resulting from both input data (which may reflect systemic bias and social structures of discrimination) and the way machines are trained, P5 could see how biases can be present without awareness or knowledge of the organisations. Even though a greater awareness around identification and prevention of biases was reported in the last few years, it was not clear

if and how this was being translated into practice. Nevertheless, some organizations were reported requesting guidance on ethics:

> *'We want to be better at understanding if what we are doing is ethical…how you know that the algorithm is ethical when what it is doing is completely autonomous…there are morality questions…psychology…interdisciplinary research. There is a lot of unknown around what is considered to be good practice in this space' (Part 4).*

The access by developers to data held in controlled environments was raised as a potential issue by P2. *'…To train machine learning I need real data in a very controlled environment, with very limited access...When developers need access to that data, usually a specific environment is created for that purpose…. For less mature organisations that is a real eye-opener…' (*P2) After using it for training, developers are supposed to discharge the system created with the data pulled out from the master system. '*We may request the same data next time…and this can be challenging because we don't have the same training set ...to see how they both behave'* (P2). In similar situations, the number of staff looking at that data (and potentially sensitive data) can increase, and this seems to also happen when the system goes down, or when the company uses that data for '*improving the ability to provide the service' (P2)*. Similar cases advance further questions for an improvement of business processes.

h) New Purposes of Processing

AI is generally acquired for a specific purpose which increases efficiency, and in many cases is implemented without considering or understanding the implication for Data Protection. Often acquired for one purpose, AI is then used also for other purposes, which can result in unlawful and unfair outcomes.

> *'Technology always comes first, it's quick and easy to use. This system will allow you to do something simple, usually more efficiently. Once the system is there, they start to see patterns, and the uses start to present themselves. In the GDPR terms that is the other way around' (P6).*

The purpose of processing personal data is regarded as the preferred starting point of the process which leads to the acquisition of AI, as per GDPR. Therefore, starting from the need of the organisation and moving to the identification, acquisition and implementation of the technology which can best satisfy that need. The identification of the lawful basis for processing personal data, and its communication to data subjects,

should be done before the acquisition of the technology. However, this is not what is said to be happening in many cases. The business case is not the driver (as per GDPR logic) but the technology. Using the technology for additional purposes has massive implications for Data Protection (P6). For example, monitoring employees: *'Once the technology is there the uses occurred to people…so they don't even go into it with the intention of monitoring…' (P6).* The monitoring of both resources and people within organisations is increasing. For example, tracking business vehicles or employee access to premises, is often done using biometrics such as fingerprints, (P6), frequently used for pragmatic reasons. They were considered easy and reasonable when individuals are given alternative options such as entry codes to buildings. P6 envisaged a gradual increase of monitoring, inclusive of people and their performance. However, the participant noted that decisions based on data still tend to be made by people, and not by machines via automated decision processes (P6).

5 Discussion

The results have illustrated that there are gaps between current organisational approaches to Data Protection, the GDPR and best practice. In this section we discuss the key themes emerging from the data.

Compliance, Maturity and Risks

It is believed that few organisations are fully GDPR complaint, a year after the Regulation came into effect. However, participants reported an increased level of awareness in their activity, with more preventive thinking in this area, which indicates the positive effect of GDPR on organizational awareness. Many differences were reported according to sectors, size and maturity of organisations. More mature organisations have a good understanding of how to use privacy enhancing tools such as DPIA and DPO, and how to use the GDPR strategically, by connecting processes, teams and disciplines. For others the GDPR arguably translates into a cost that they may be unwilling or unable to pay, although this is a short-sighted approach given the potential risks involved. Mature organisations are in general aware of the risks, and of the general impact the GDPR has on processes, people and data. They are taking the time to understand its full implications and to choose effective compliance strategies. This

is important and indicates the organisational reach of effective approaches to GDPR, with effective compliance dependent on a nuanced understanding of its relation to the processes, people and data and ongoing consideration of data protection principles and requirements. A general low awareness or specific knowledge around GDPR and AI was described by various participants. Those more aware of GDPR and AI were reported investing on research to strengthen their compliance, improve the relationship with clients, and gain a competitive advantage. The lack of awareness is unsurprising given the relatively short time that the Regulation has been in effect and the immaturity of AI understanding outside of expert circles; although organisations are increasingly adopting the technologies, this does not necessarily translate into detailed understanding within organisations as illustrated by the findings above. This does present an urgent need for organisations adopting AI technologies to ensure that they have sufficient knowledge to understand the risks and their GDPR responsibilities. Related to this, some expectation also may lie with vendors and solution providers as well as customers, as they in many cases have greater understanding of the risks. Although the customers may have the responsibility for GDPR, there is a moral and also a business case for vendors to raise awareness of these responsibilities and associated risks. As stakeholders they should work together, although it is up to the organisation to educate itself, to provide resources and to own responsibility and accountability. Organisations should create new internal competencies, with hybrids roles in AI management, drawing on vendors resources to support their own organisational understanding. The GDPR is trying to regulate the relation between the two, and it is quite prescriptive. With the use of AI technologies, vendors often are gaining access to data and so the argument that they should also absorb some responsibility is compelling.

Automated and Augmented AI systems

Intelligibility of AI Automated systems was reported as potentially problematic. A different degree of explainability in decisions made by Autonomous Systems was reported as more or less acceptable according to different sectors or cases. Augmented AI was generally seen as low risk, as having a human in the loop can improve or change the decisions made by AI. Specific problems that could arise from the interaction between human and machine were not mentioned by any participant. Potential issues

could however result from underestimating or ignoring specific risks in Human Machine Interaction (HMI), such as being over reliant on decisions made by AI or making biased decisions. Furthermore, the issue of the lawful bases of processing in automated systems, necessity of processing, and its connection to more automatized business models are all as yet poorly understood. These require clarifications via courts or national and EU Data Authorities, which will take time, especially for case law to develop. It would be helpful for the national and EU Data Authorities to provide guidance given the current void in this area.

Preventive Data Protection

Organisations do not appear to fully appreciate the strategic potential of "privacy-enhancing technologies" which in many cases are now obligatory under the GDPR, as strategic and preventive Data Protection tools. The case of DPIAs is emblematic of this gap. These are performed more than required in the public sector, often a sign of a tick-box culture resulting from external pressure and perceived obligations. Still missing from the private sector landscape, they are often completely ignored by small entities, usually the ones more focused on responding fast to market. DPIAs can be an important strategic instrument for organisations by providing times where staff with different expertise in the organisation come together and take the time to carefully examine new projects. By creating an obligation for exchanging information and fostering dialogue, DPIAs improve the organisational innovation process, becoming an important Information Management tool. This is particularly important in relation to AI, where the involvement of different disciplines and areas is highly recommended, for example, to reduce the risks of biases. While they may be perceived by some organisations as a 'luxury' or 'cost', DPIAs are an essential tool which encourage organisations to stop and think carefully about the impact, technical and otherwise, of their innovation. If used effectively, they are an important instrument for effective Preventive / a priori Data Protection. The use of DPIAs can create a space for organisations to pause, consider and evaluate proposals fully. This is especially important in digital transformation and enables a greater range of stakeholders to be included in the process which can not only reduce risk but also develop greater organisational knowledge and understanding.

Something similar emerged with regards to the DPO. The independent expert whose role is able to support organisations is not perceived as such. In the public sector, this

role is disliked for its alleged power. In the private sector, being completely absent or ignored by small ones, (many of whom are high risk entities) although sometimes adopted in low risk organisations. There is clearly some way to go in developing organisational awareness of the benefits of the DPO, unsurprising given that organisations are still more reactive than proactive in their approach to data protection, which is rarely considered as a strategic and competitive factor. For organisations adopting AI technologies the DPO is a potential ally and could mitigate the risk.

Accountability and Fairness

Data Protection is often conflated with security, and when this happens, Accountability is in general considered as an easy requirement to meet. When linked to explainability and intelligibility of ML, demonstrating compliance is a big source of concern for those more AI literate. While awareness around black boxes is growing, other elements that can impact the capacity of organisation to demonstrate compliance, such as power-knowledge and group dynamics, are less taken into account. This can be particularly problematic in organisations that have a clear accountability structure but use innovative technologies that are not completely understood by leaders and senior managers. Similarly, while awareness around biases in algorithms is growing, the praxis of Fairness can at times produce potentially opposite results for Data Protection, as seen in the case of the increased amount of personal data collected for fear of discrimination, which impacts on the principle of minimisation, data management and security, data retention and right to be forgotten.

Re-purpose

Identifying a new use for data processed via AI, once the technology is already implemented in organisations, was one of the most concerning elements emerged during the interviews. Identifying other purposes without a careful consideration of the lawful basis is risky, deeply problematic, and opposite to the GDPR approach. The extremely rapid pace of AI innovations, and their applications in very rapid market dynamics, where companies have to respond fast to market, reduce the time available for careful considerations of lawfulness. Furthermore, this has also an effect on power dynamics, as seen with monitoring, even when the final decision is made by humans.

Summary

In this study the analysis of findings has indicated that there are different approaches to compliance and risk which appear to be influenced by the type of organisation – in particular whether it is private sector or regulated sector (primarily public sector but also including some private sector domains such as finance). Within the private sector there are differences according to the size of the organisation. We have mapped this, including the innovation pace in Table 1 below

		Private Sector Organisations			Public and Regulated Sector Organisations
		Large	Medium / Small	Start-Ups	
Compliance	High				
	Medium				
	Low				
	Almost Absent				
Risk	High				
	Medium				
	Low				
Innovation Pace	High				
	Medium				
	Low				

Table 1: Compliance, risk and organisation type

6 Conclusion

The research presented in this paper provides insights into the implementation and compliance of the GDPR, a year after becoming enforceable. It is apparent that most organisations are not yet fully complaint with the Regulation. The findings show a low level of implementation and awareness, which seems result from the interplay of different reasons: technical and organisational, and both internal and external to organisations. With the exception of a few organisations that are using the GDPR strategically for their innovation, organisational awareness still requires improvement. Some of the GDPR requirements, such as DPIA, PbD and DPO, can become precious resources in innovation practices, not only to meet the required obligations, but to enhance organisational practices and strategic planning. Furthermore, reducing risk and

improving compliance is an urgent necessity given some of the complexities and challenges around AI.

While some of the issues relate to technical aspects, such as the low intelligibility of some ML models, or consent withdrawal of data used for ML models, others are more linked to organisational aspects. We have identified issues related to context, power within various stakeholders, and the lack of time and space for enhancing knowledge exchange and dialogue amongst different experts, all of which can impact compliance and innovation. The interplay of GDPR requirements and AI complexity require a new approach and multidisciplinary efforts for data protection issues to be effectively identified and managed as the technologies are adopted. We argue that such an approach requires:

- increased awareness and knowledge of both Data Protection and AI amongst leaders, senior managers and staff;
- increased awareness of power and organisational dynamics;
- active participation of stakeholders in different stages of innovation process.

An approach to innovation based on Information Systems Management, where the three core elements – people, technology and organisation – actively co-operate to innovation is urgently needed. In the next stage of this project, organisational case studies will be used to explore how these elements interact during the introduction of AI technologies, to provide a more detailed understanding so that guidance for organisations can be developed. The adoption of AI technologies is rapidly increasing and combined with the relative novelty of the GDPR and the ensuing areas of uncertainty, there is a real need for further research to inform organisations and practitioners and to develop the knowledge base.

References

Addis, M. C., & Kutar, M. (2018). The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness. Oxford, UK. Retrieved from https://www.ukais.org/resources/Documents/ukais 2018 proceedings papers/paper_39.pdf

Agrawal, A., Gans, J., & Goldfarb, A. (2018). Prediction machines: the simple economics of artificial intelligence. Harvard Business Press

Borgesius, F. J. Z. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. Retrieved from https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73

Bughin, J., Catlin, T., Hirt, M., & Willmott, P. (2018). Why digital strategies fail. McKinsey Quarterly. Retrieved from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/why-digital-strategies-fail

California State Legislature. California Consumer Privacy Act of 2018 CCPA (2018). Retrieved from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Casey, B., Farhangi, A., & Vogl, R. (2019). Rethinking Explainable Machines: The GDPR's Right to Explanation Debate and the Rise of Algorithmic Audits in Enterprise. Berkeley Tech. LJ, 34

Cesaratto, B. G. (2019). Washington State Considers Comprehensive Data Privacy Act to Protect Personal Information. Retrieved from https://www.natlawreview.com/article/washington-state-considers-comprehensive-data-privacy-act-to-protect-personal

Crawford, K. (2017). The Trouble with Bias - NIPS 2017 Keynote - Kate Crawford #NIPS2017. Retrieved from https://www.youtube.com/watch?v=fMym_BKWQzk

Edwards, L., & Veale, M. (2017). Slave to the Algorithm? Why a Right to Explanation is Probably Not the Remedy You are Looking for. SSRN Electronic Journal (Vol. 2017). https://doi.org/10.2139/ssrn.2972855

European Union Agency for Fundamental Rights. (2018). Handbook on European data protection law - 2018 edition. Retrieved from https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

Goodman, B., & Flaxman, S. (2016). European Union regulations on algorithmic decision-making and a “right to explanation,” (Whi), 26–30. https://doi.org/10.2139/ssrn.2903469

IEEE. (2019). Ethically Aligned Design. Retrieved from https://standards.ieee.org/industry-connections/ec/autonomous-systems.html

O’Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Broadway Books

Raul, A. C. (2018). The privacy, data protection and cybersecurity law review. Law Business Research Limited

Selbst, A., & Powles, J. (2017). Meaningful Information and the Right to Explanation. International Data Privacy Law, 7(4), 233. https://doi.org/10.1093/IDPL/IPX022

The European Parliament and the Council. 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, 59 Official Journal of the European Union (OJ) § (2016)

The Royal Society. (2017). Machine learning: the power and promise of computers that learn by example. https://doi.org/10.1126/scitranslmed.3002564

Tufekci, Z. (2017). We're building a dystopia just to make people click on ads. Retrieved from https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads/up-next

Tufekci, Z. (2018). Facebook's Surveillance Machine. The New York Times. Retrieved from https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-176analytica.html?rref=collection%2Fcolumn%2Fzeynep-tufekci&action=click&contentCollection=opinion&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=collection

Whittaker, M. (2019). @mer__edith testifying to @HouseScience: "while the cost of AI bias is borne by historically marginalized people, the benefits, from profit to efficiency, accrue primarily to those already in positions of power. This points to problems that go well beyond. Retrieved from https://twitter.com/AINowInstitute/status/1143987417864704000