Data Protection and Tech Startups: The Need for Attention, Support, and Scrutiny

Norval, C.; Janssen, H.; Cobbe, J.; Singh, J.

DOI
10.1002/poi3.255

Publication date
2021

Document Version
Final published version

Published in
Policy and Internet

Received: 11 November 2019 | Accepted: 17 August 2020

DOI: 10.1002/poi3.255

RESEARCH ARTICLE

P&I Policy & Internet PSO WILEY

Data protection and tech startups: The need for attention, support, and scrutiny

Chris Norval | **Heleen Janssen** | **Jennifer Cobbe** | **Jatinder Singh**

Compliant and Accountable Systems Group, Department of Computer Science and Technology, University of Cambridge, Cambridge, UK

Correspondence

Chris Norval, Department of Computer Science and Technology, University of Cambridge, 15 JJ Thomson Ave., Cambridge CB3 0FD, UK.
Email: chris.norval@cl.cam.ac.uk

Funding information

Engineering and Physical Sciences Research Council, Grant/Award Numbers: EP/P024394/1, EP/R033501/1; Microsoft, Grant/Award Number: Microsoft Cloud Computing Research Centre (MCCRC)

Abstract

Though discussions of data protection have focused on the larger, more established organisations, start-ups also warrant attention. This is particularly so for tech startups, who are often innovating at the 'cutting-edge'—pushing the boundaries of technologies that typically lack established data protection best-practices. Initial decisions taken by startups could well have long-term impacts, and their actions may inform (for better or for worse) how particular technologies and the applications they support are implemented, deployed, and perceived for years to come. Ensuring that the innovations and practices of tech startups are sound, appropriate and acceptable should therefore be a high priority. This paper explores the attitudes and preparedness of tech startups to issues of data protection. We interviewed a series of UK-based emerging tech startups as the EU's General Data Protection Regulation (GDPR) came into effect, which revealed areas in which there is a disconnect between the approaches of the startups and the nature and requirements of the GDPR. We discuss the misconceptions and associated risks facing innovative tech startups and offer a number of considerations for the firms and supervisory authorities alike. In light of our discussions, and given what is at stake, we argue that more needs to be done to help ensure that emerging technologies and the practices of the companies that operate them better align with the regulatory obligations. We conclude that tech startups warrant increased attention,

support, and scrutiny to raise the standard of data protection for the benefit of us all.

KEYWORDS

compliance, data protection, data subject rights, emerging technology, General Data Protection Regulation (GDPR), privacy by design, supervisory authorities, tech-startups

INTRODUCTION

Reports of high-profile data misuse have placed data protection firmly in the spotlight (Isaak & Hanna, 2018). Data protection law is an important tool for scrutinising data-driven firms and holding them to account where harms occur or where requirements and expectations are not met. In such instances, authorities may investigate, and punitive actions may result. Naturally, compliance with such laws has become a high priority for many technology companies, given the threat of significant penalties for noncompliance and the growing public discourse on data-related issues. There is much data protection discussion that (rightly) focuses on the 'tech giants', such as Facebook and Google, and what these laws mean for the users of such services (e.g., see Houser & Voss, 2018). Comparatively, little attention is given to tech *startups*.

However, it will often be these startups that drive the development, commercialisation, and application of emerging data-driven technologies (artificial intelligence/machine learning [AI/ML], Internet of Things [IoT], blockchain, augmented/virtual reality, etc.). In this way, startups influence how new technologies come to be designed, deployed, perceived, and used—and can shape standard industry practices in the process. Yet they are often doing so with relatively constrained resources, limited expertise, and driven by their desire to disrupt and establish themselves in a marketplace. It follows that the practices of startups working at technology's 'cutting-edge'—who can rapidly grow and may become the 'next big thing'—can have significant data protection implications going forward. However, there is currently limited information about how companies in general, let alone emerging tech startups, are approaching data protection.

We, therefore, undertook a series of semistructured interviews with UK-based tech startups to explore the attitudes and opinions toward data protection laws before the EU's General Data Protection Regulation (GDPR) coming into force.[1]

We first use thematic analysis on the transcripts to identify a number of themes emerging from the interviews. We then use these themes as a guiding point for conducting a legally grounded analysis into the following research questions:

(i) How do tech startups perceive and approach the GDPR within their organisation?
(ii) What are the risks and implications of these approaches under the GDPR?
(iii) What are steps that can be taken by the startups, regulators, and policymakers to mitigate these risks and better support effective data protection practices?

These are important questions that will help shape our understanding of the challenges being faced by emerging tech startups with regard to data protection regulations. In turn, this can help in identifying ways of supporting technology startups in meeting their legal obligations. This can help reassure startups that their data protection efforts are sufficient and that their users' and customers' data are better protected.

Through our interviews, we find several challenges facing tech startups in meeting their data protection obligations. For example, firms often felt that it was unclear how, and in some cases, *if* their technology could be reconciled with the GDPR. We also observed startups questioning whether aspects of the GDPR applied to them, with some indicating complacency, by first waiting to see if and how the Regulation is enforced before acting. The rationale for this was a belief that regulators were more likely to focus on larger organisations rather than startups. We also noted instances where, in the rush to comply, startups were pursuing potentially unreliable sources of information regarding how their technologies could be reconciled with the GDPR. Our findings support an argument that tech startups need to be more proactive, not only with regard to their specific compliance obligations but also in understanding the broader aims and intentions of the GDPR. The results also indicate an urgent need for supporting firms—through guidance, advice, oversight, and technology—as they navigate the data protection landscape.

Data protection is an important concern; the GDPR has foundations in human rights,[2] and will help shape how technology organisations come to be seen by society more widely. Organisations must not be complacent, but rather properly account for their obligations. In light of our findings, we argue that *tech startups require increased attention* in terms of support, oversight, and regulatory enforcement, to help bring about a better, more accountable use of data-driven technology.

GDPR: A BRIEF INTRODUCTION

In May 2018, the European Union's (EU) GDPR (European Union, 2016) (GDPR) came into effect throughout the 28 member states. This binding legislative act applies to the processing of personal data: 'any information relating to an identified or identifiable natural person'.[3] The GDPR strengthens the rights of data subjects (those whose personal data is being processed)[4] while simultaneously reinforcing the responsibilities of data controllers (those responsible for determining the means and purposes of processing personal data).[5]

The GDPR places responsibilities on data controllers, including an obligation to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation'.[6] Supervisory Authorities—those responsible for enforcing the regulation, appointed by each member state—have the means for holding data controllers to account in the event of non-compliance. Organisations found to be in breach of the GDPR can face significant penalties, including fines of up to the greater of €20 m or 4% of annual global turnover, bans on processing,[7] among others—many of which could prove fatal for startups.

Principles and responsibilities

The GDPR is a principles-based regulation. Such regulations are defined by Black et al. (2007) as 'high-level, broadly stated rules or Principles to set the standards by which regulated firms must conduct business'. This is in contrast to prescriptive and detailed rules-based regulations, which can quickly become obsolete in dynamic contexts (Maxwell, 2015), such as those involving emerging technologies. The principles-based approach allows the GDPR to operate flexibly across sectors, business models, applications, and technology-specifics.

In practice, data controllers are required to comply with seven principles relating to the processing of personal data (Table 1). The 'Accountability' principle requires that the data controller 'shall be responsible for, and be able to demonstrate compliance with' the other

TABLE 1 The General Data Protection Regulation's seven key principles

Principle	Relevant Articles
Lawfulness, fairness & transparency: Personal data shall be processed lawfully, fairly and in a transparent manner.	Art 5(1)(a).
Purpose limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.	Art 5(1)(b).
Data minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.	Art 5(1)(c).
Accuracy: Personal data shall be accurate and, where necessary, kept up to date.	Art 5(1)(d).
Storage limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.	Art 5(1)(e).
Integrity and confidentiality: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	Art 5(1)(f).
Accountability: The controller shall be responsible for, and be able to demonstrate compliance.	Art 5(2).

principles. In other words, controllers must both be in a position to identify, operationalise and demonstrate to regulators how each of these principles is met.

The Regulation also provides data subjects with various rights, including those to access, rectify, and delete personal data held by a data controller. Similarly, organisations are responsible for implementing appropriate mechanisms to facilitate subjects exercising these rights, to fulfil their GDPR obligations. However, identifying the best means of implementation may not be trivial; for example, rights can have tensions with privacy and security concerns (Norval et al., 2018; Singh & Cobbe, 2019; Veale, Binns, & Ausloos, 2018).

The GDPR generally does not entail many detailed prescriptions of the particulars of what organisations need to do, in practice, to comply. Some, therefore, criticise the Regulation as lacking precision and clarity (Deloitte, 2018; Presthus et al., 2018; Sirur et al., 2018). For companies without legal expertise or even those without specific technical skills (such as cybersecurity expertise), it is not always immediately obvious how these principles and rights can be met within their organisations—a common theme raised by our interviewees.

Initial impact of the GDPR

In the run-up to and immediate aftermath of the Regulation's commencement, the GDPR was the subject of a number of large-scale surveys (Deloitte, 2018; IBM Institute for Business Value, 2018; ISACA, 2018; NetApp, 2018; SAS, 2018). These explored the readiness and attitudes to the Regulation across a broad range of sectors and organisation sizes (these mostly considered well-established organisations, and none focused specifically on tech startups). Despite the substantive similarities between the GDPR and the previous data protection regime—the Data Protection Directive (European Union, 1995)—these surveys suggested that a majority of companies did not expect to be GDPR compliant

by the commencement date. Deloitte (2018) reported that the three main reasons for this were the 'time left to achieve compliance', 'ambiguity of the GDPR text', and 'the difficulty of fulfilling some requirements', and that 62% of respondents were initially aiming for a 'risk-based, defensible' level of compliance. SAS (2018) found that 49% of respondents said GDPR would significantly impact their AI projects.

Sirur et al. (2018) conducted qualitative interviews with 12 organisations (a mix of small and medium enterprises [SMEs] and larger organisations—though not focusing on tech-startups per se), with a particular emphasis on cybersecurity. For most companies, it was found the largest nontechnical issue was in understanding the expectations of the GDPR, and how it could be implemented. The perceived 'qualitative' nature of the Regulation left some companies uncomfortable, and a lack of timely guidance from the Supervisory Authority left many unable to implement suitable measures for GDPR compliance. Their paper found a difference in language, tone, and perceptions in larger organisations and security-related SMEs when compared to non-security-related SMEs, with the former appearing more confident in approaching compliance. These findings corroborate that many companies have been struggling with their compliance obligations.

Compliance with the GDPR will be a requirement for all startups processing personal data, regardless of their sector or target customer base (B2B, B2C, or otherwise).[8] However, little research to date has specifically explored the impact on startups working with innovative and emerging technologies. This study is therefore timely, relevant, and, as we will discuss, has wider implications for the data protection landscape going forward.

A FOCUS ON TECH STARTUPS

Startups are broadly defined as organisations which are 'younger than 10 years'; 'feature (highly) innovative technologies and/or business models'; and 'have (strive for) significant employee and/or sales growth' (Kollmann et al., 2016). They are described as companies that 'work to solve a problem where the solution is not obvious and success is not guaranteed' (Robehmed, 2013), or that 'start from weak market and resource positions' (Katila et al., 2012).

Our focus here is on *tech startups*, companies that accord with the above definitions but that also work with developing and applying new technologies (AI/ML, blockchain, IoT, augmented/virtual reality, etc.). In the UK, the number of tech startups is rising at an average rate of one every hour (Prosser, 2018). However, relatively little attention has been given to how startups working at the forefront of emerging technologies approach data protection.

We argue that such startups require consideration. First, any organisation needs to consider how they will meet the GDPR's requirements; however, tech startups, as part of their innovation process, will often push technical and legal boundaries. This means there is likely to be a lack of prior knowledge, let alone guidance and best practice, over how to reconcile the technologies with data protection requirements. As a result, some startups may be willing to undertake (data protection) risks in their mission to 'disrupt' and gain market position.

Second, startups involved in technology innovation may work to inspire and define how technologies (and associated practices) are implemented and used by those that follow. Such startups are therefore standard bearers for their respective technologies—laying down markers which may remain ingrained for years to come. Their decisions, whether sound or questionable, have much potential for shaping industry practices going forward. And at the same time, they are particularly well-placed for accounting for data protection 'by design and by default'.[9]

Third, should these startups grow, the effects of their decisions, actions, and risks will be felt at scale. As we have seen, tech startups might eventually be acquired by large tech firms, whereas others may go on to become tech giants themselves. As such, it is important to deal with such issues *now*, rather than later. From a societal angle, it is better for the technology to align with data protection aims before and as it scales, to mitigate the prospect of large-scale data protection incidents. For organisations, it will likely be far more difficult and expensive to retrofit data protection into established systems, datasets and processes down the track—and retrofitting may be particularly challenging for startups given their lack of resources (Urquhart, 2019). It is therefore important that all necessary data protection considerations are actually undertaken, including by nascent organisations.

In short, the actions taken by tech startups have the potential for far-reaching implications on the wider data protection landscape, possibly with systemic consequences. Addressing issues sooner, rather than later, will play a key role in countering bad practices and misconceptions, for the betterment of data protection practices more widely. To explore possible ways forward, we undertook a series of interviews to improve understanding of factors such as how the startups perceived the impact of such laws; the compliance approaches that they are implementing; and ways in which they could be better assisted and challenged.

SURVEY METHOD

We conducted semi-structured interviews with technology startups about the impact of the GDPR on their organisations.

Recruitment

We invited a range of startups (as described in A FOCUS ON TECH STARTUPS) that were innovating with emerging technologies to participate in an interview about data protection (see Table 2).

These companies were identified from a variety of communities that startups frequent, including innovation and entrepreneur centres (which provide business-related guidance and support to startups), online technology communities for tech startups (e.g., 'meetup' groups), and 'tech cluster' network directories for a particular geographic region. Recruitment continued until the authors believed that thematic saturation of findings was occurring (O'Reilly & Parker, 2013), and this resulted in interviews with 15 organisations (self-selecting from a larger pool of 48 invitees in total).[10] Participating companies ranged from those in the prototyping and prelaunch phases to those with products/services having been recently introduced across a variety of industries and markets. Companies were typically small (e.g., less than 10 members of staff), and young (most were under 4-years old). Information about each of the participating companies is presented in Table 2.

Research design

Each startup provided a representative to take part in an hour-long, semi-structured interview about the impact of the (then) incoming GDPR on their organisations. These representatives were selected by the organisations themselves and were often the founder and/or the Chief Executive Officer or Chief Operating Officer of the startup in question (in many cases doubling as the organisation's Data Protection Officer). Interviewees were

TABLE 2 Summary information about each interviewed start-up

Interview	Focus of start-up	Market	Location	Age (years)
1	Wearable Tech	B2C	London	1–3
2	Wearable Tech	B2C	Cambridge	4–6
3	Blockchain	B2B	London	1–3
4	IoT Smart Home	B2C	London	1–3
5	AI Smart Assistant	B2B	London	1–3
6	Data-driven Design Consultancy	B2B	London	7–9
7	B2B SaaS	B2B	Edinburgh	4–6
8	Marketing Automation Agency	B2B	Cambridge	7–9
9	Medtech	B2G	Cambridge	1–3
10	AI Human Resources	B2B	London	1–3
11	GDPR Compliance Software Development	B2B	Milton Keynes	1–3
12	Blockchain and Analytics	B2B	Oxford	1–3
13	Data Science Consultancy	B2B	Brighton	4–6
14	IoT Smart Home	B2B	Suffolk	7–9
15	IoT Healthtech	B2C, B2G	Oxford	4–6

Abbreviations: AI/ML, artificial intelligence/machine learning; GDPR, General Data Protection Regulation; IOT, Internet of Things.

given information about the study in advance, which included a clarification that the researcher would not be able to provide GDPR-related advice or answers, and completed a consent form. Interviews took place either via VoIP, phone, or in-person between December 2017 and May 2018 (in the run-up to the GDPR's commencement) and were audio-recorded. The transcript of each interview was pseudonymised by the lead researcher and then sent to the interviewee, giving them an opportunity to review and further redact, clarify, or correct their answers. The authors received approval to conduct this study from their institutional ethical review board before any interactions with companies or interviews taking place.

Analysis

Interview transcripts were inductively coded using thematic analysis; relevant quotes from the transcript were assigned one or more themes, and the process of identifying, merging, and refining themes happened iteratively throughout the coding process (Braun & Clarke, 2006). Related themes were grouped and subcategorised together, resulting in a 'thematic map'[11]—a hierarchical tree-like structure which maps out the relationships between themes. A summary of our themes can be seen in Figure 1.

Using these themes as a guiding point, we then identified potential answers to the research questions (outlined in the Introduction) and conducted a legally-grounded analysis of these approaches against the GDPR, taking into account its supporting materials (e.g., recitals, resources from the ICO—the UK's Supervisory Authority). This led us to identify several interesting trends, potential risks, and wider considerations for how startups can be better supported with their GDPR commitments going forward, which we present in this paper.

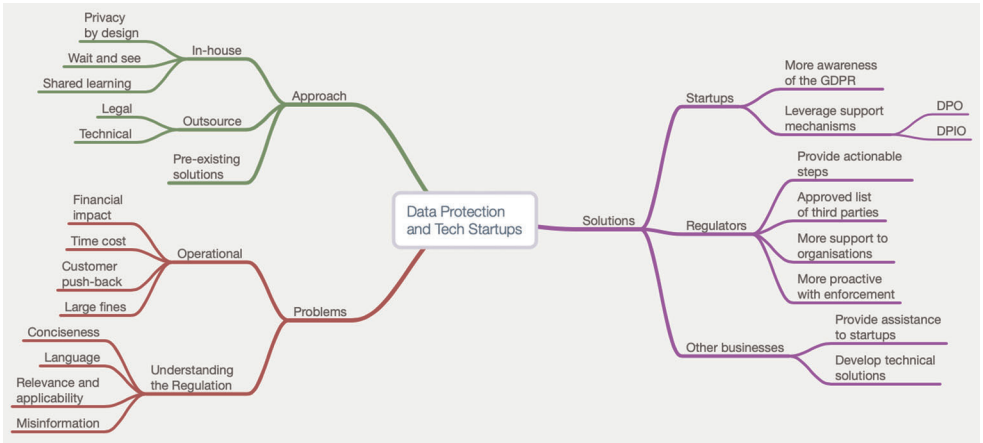

FIGURE 1 A summary of the themes emerging from the interviews

VIEWS OF THE STARTUPS

In line with RQ (i), we discussed the interviewees' opinions of the GDPR, and how they—as a startup—were approaching compliance. Their experiences led to several key insights, which we now discuss.

The principles-based approach of the GDPR was seen as particularly challenging for startups

The Regulation was repeatedly described by interviewees as 'vague' and 'open to interpretation', leaving many unsure of what was expected of them. There was a strong desire for Supervisory Authorities (and for the GDPR itself) to provide suitable, prescriptive guidance on how compliance could be achieved across industrial and application-specific contexts. Though any holistic approach towards this appears impractical given the broad range of sectors, applications and situations in which the GDPR applies, the frustration of participants was clear.

> It's there, and we have to comply with it, but as a small business, how do you do that? No one gives us that guide to say 'actually, you need to do this, this, and this'. (Company 1)

Company 11 commented that startups with limited resources were left 'struggling to even understand where to start'. They noted a 'huge skills shortage' with regard to data protection, making skilled people 'exceptionally expensive to recruit'. Interpreting the Regulation was seen as difficult (particularly for those with limited access to legal expertise), with Company 15 describing the GDPR as 'impossible to actually understand', and 'deliberately written for vagueness'. Even those who managed to develop compliance solutions were often unsure of whether they were legally sufficient:

> It's like there is this issue but no one tells you how to address it or what exactly it means. So if you offer a solution, you're not exactly sure if you're in the right or not. (Company 3)

Company 1 argued the GDPR should be summarised into clear and actionable steps. Many similar suggestions were raised, including desires for checklists or wizard-style support tools. However, others recognised that such an approach would conflict with the principles-based nature of the GDPR:

> You're going to have to decide what you do. So it's quite a shift in mindset for an organisation to understand. You can't just go 'tick, tick, tick, tick', and that's it done. (Company 11)

Interestingly, Company 11 suggested that startups should 'take responsibility for what they actually decide to do', and that guidance materials should provide startups 'the tools for them to make their own decisions'. This recognises that startups need more assistance in approaching the GDPR—understanding the need to achieve an informed, reasonable and defensible position, rather than assisting startups with their implementation specifics, as they request. This theme of startups needing to take more responsibility with regard to their data protection obligations was pressed further by Company 11, who noted that the GDPR wasn't actually that much of a step up from its predecessor, the Data Protection Act (European Union, 1995) (DPD), but that 'you have organisations that weren't compliant with the [DPD] in the first place'. This accorded with arguments that the DPD as it was 'interpreted, implemented and enforced' did 'not fully meet its stated objectives of protecting data subject's right to privacy with respect to their personal data' (Robinson et al., 2009).

Despite the challenges raised, the ambitions of the GDPR were perceived largely positive. Company 7 described implementing compliance as a 'massive pain', before reflecting that it was 'for the benefit of us all'. Another thought that forcing organisations to think about these issues would help steer good data protection practices going forward.

Some startups struggled to find necessary information from the UK's Data Protection Supervisory Authority

The startups expressed a range of views regarding the Information Commissioner's Office (ICO) and their guidance materials. Some praised the ICO as 'do[ing] a great job' (Company 9), producing guidance that is 'very explicit' (Company 15), and 'essential for [the startup's] comfort' (Company 7). However, though many had positive things to say about the ICO and its resources, there were also criticisms. The ICO's advisory materials were described as 'too vague for [being from] an official government body' (Company 3), 'a little open to interpretation' (Company 8), and 'late' (Company 15). Going further, Company 1 argued that by enforcing the GDPR without providing (what they saw as) adequate support, the ICO was 'actually trying to kill us [small businesses] rather than help us'.

Yet, though there may be lessons for how the Supervisory Authorities can best support emerging tech startups, there were clear steps that the startups could have taken to better support themselves. In some instances, we observed participants criticising the absence of particular guidance that the ICO had, in fact, created guidance for. Such criticisms may, therefore, stem from the startups knowing where to look for advice and what was relevant for them. Company 11 as described this a challenge that many startups face:

> To even go on to the ICO's website in the first place, you need to understand that the ICO exists, and there isn't enough trying to bring this out into the public. (Company 11)

Largely, the startups wanted their Supervisory Authority to be a trustworthy source of timely, relevant and actionable advice for how data protection could be approached, implemented, and maintained in a broad variety of sectors. The ICO's resources were the main source of guidance for some of the startups—because 'they're the guys that are going to be enforcing it in the UK so what they say goes' (Company 8). However, this proximity to enforcement also led to wariness; Company 9 spoke of wanting to contact the ICO with data protection questions on multiple occasions but didn't for fear of 'opening a can of worms' by presenting the Supervisory Authority with their compliance issues. In all, the startups' opinions about the ICO and its resources were often multifaceted and complex.

Some viewed specific GDPR obligations as irrelevant to their organisation or irreconcilable with their tech

The startups repeatedly indicated that it was often unclear how their emerging and rapidly evolving technologies could be reconciled with certain requirements of the GDPR. This was particularly the case when discussing the GDPR's data subject rights. Though many of the startups saw implementing certain rights as trivial—such as the right of access (allowing the data subject to obtain access to their personal data)[12]—other rights were perceived to conflict with particular technologies. Some startups saw certain rights as irrelevant or non-applicable to their organisation, despite the GDPR making no such allowances.

The *right of erasure*[13] (which provides a mechanism for data subjects to have their personal data deleted by the data controller) was typically described as 'easy' (Companies 1, 4, 5). Though not all interviewees agreed. In particular, those working with blockchain technologies referred to perceived conflicts between the technology and the right of erasure (see Bacon et al., 2018). Company 3 described the right of erasure as the biggest GDPR challenge facing blockchain companies, because 'you cannot remove [the data], you need to find a way to make the data unavailable'. Company 12, argued that 'transparency is good; privacy is good; the two cannot coexist at the same time', referring to wider ongoing discussions about 'whether blockchains themselves can inherently ever be fully GDPR compliant'. However, such viewpoints appear misinformed; guidance produced by the CNIL—the French Supervisory Authority—has since outlined how blockchain implementations can be made GDPR compliant, offering 'concrete solutions to actors who wish to use it to process personal data', including for the right of erasure (CNIL, 2018). Nevertheless, despite this perceived conflict, these startups appeared undeterred from using blockchain technologies, though perhaps without the solutions put forward by the CNIL.

The right of erasure also introduced challenges for startups working with AI/ML. It was not clear how machine-learned models should account for the right of erasure (the data protection issues concerning what is encoded in models is topical; see Veale, Binns, & Edwards, 2018), and how it might affect the automated decisions being made. Further, the right of erasure is not absolute. Company 9 (a health-tech startup) discussed receiving legal advice on whether they could be exempt from such requests,[14] as they were not planning on allowing users (patients) to have their data deleted because they considered that their use of data was 'not the same as deciding that you don't want a gardening company to send you an e-mail anymore' (Company 9).

The *right to data portability*[15] (allowing subjects to obtain the personal data they have provided to the controller in a structured, commonly used, machine-readable format) was also considered easy to implement. However, some of the interviewees questioned the right's applicability. One startup didn't foresee a situation where they would be asked to facilitate the right because they considered themselves lacking direct competition (i.e., they foresaw nobody to whom the data might be transferred). Another described the right

to data portability as 'completely pointless', citing the challenges of data interoperability as a reason:

> What you're going to get is a huge CSV file full of data that's only meaningful to our system. (Company 15)

Overall, the aims of this right—to promote competition, consumer choice, and control over one's personal data—did not seem particularly well understood or appreciated.

Applicability of certain rights: For both the right of erasure and the right to data portability, some startups had—rightly or wrongly—deemed these to be irrelevant or non-applicable to their organisation. In some cases, the startups perceived challenges (or incompatibilities) in operationalising these obligations into their products (e.g., the blockchain example above). Yet, the GDPR generally obliges data controllers to comply with all of their rights and responsibilities, despite the challenges that may surface as a result. Though some exemptions to these obligations exist, the onus will be on the controller to demonstrate that nonfulfilment of a particular right is legitimate (perhaps a difficult undertaking, as exemptions are mostly related to compelling public interests[16]), with potentially significant consequences if incorrect.

If an organisation wrongly concludes that these obligations are not applicable, incidents of noncompliance, harms to data subjects, diminished trust, and regulatory repercussions may result. In instances where organisations find it difficult, or even impossible, to reconcile a particular technology with their data protection obligations, it is important that they consider whether the technology and its use are appropriate in their current form; in other words, to consider whether they should be doing what they're doing. Indeed, given that these startups are innovating with the technology itself, it is arguable that they are best-placed to look at how the technology could be made to align with data protection concerns—though it is important the approach taken is appropriate and does not itself introduce further risks to data protection (as has been observed by some approaches to dealing with access rights; Singh & Cobbe, 2019). There is a clear role for Supervisory Authorities to help ensure that such reconciliations are informed, and startups must ensure that they are active in seeking out such guidance for their chosen technology.

Startups recognised the GDPR's market implications

Startups are well-positioned to integrate data protection by design and by default (see in A FOCUS ON TECH STARTUPS) as they tend to build their new products and services. It follows that strong data protection was perceived by some interviewees as a possible competitive advantage—creating an opportunity to 'strengthen that [consumer] trust' (Company 13). Companies with good data protection practices were also thought to benefit from the increase in awareness of such issues:

> You don't need to explain the problems with the current way that companies handle data. That's become clear for everyone to see now. (Company 12)

However, one startup (Company 5) questioned whether going above and beyond the GDPR's strictly minimum requirements could be disadvantageous when competing against less-scrupulous organisations. In this case, the firm recognised that it was better from a data protection standpoint to do on-device processing (as opposed to transferring personal data to their own servers for processing), but that this would have cost implications. They also

noted that many of their competitors opted for the cheaper approach of server-side processing:

> It's a tough choice: Whether we want to make a product cheaper […] or we create a different kind of product which would be more expensive but which would do a much better job at user experience and data protection. (Company 5)

The Company ultimately opted for the more data protection-friendly approach. Though they believed that the increasing awareness of data protection issues would bring a competitive advantage, and thereby help mitigate the additional costs, they recognised that this decision was a business risk, 'because the price is a serious concern that consumers have'.

POTENTIAL IMPLICATIONS AND CONSEQUENCES

The previous section explored the startups' perceptions and approaches to the GDPR. We now explore RQ (ii), which relates to the risks and implications associated with these.

Input from data protection specialists were typically not part of the startups' ongoing compliance efforts

Expert (e.g., legal) advice was thought to be an effective way to gain reassurance and expertise regarding complex, GDPR-related questions—to 'make sure we get that right' (Company 7). However, though many interviewees had sought legal advice (and were largely positive about their experiences), it was described as 'too costly to be a regular thing' (Company 1). It also offered a (perhaps false) sense of security, with one startup wishing to 'put the onus on a lawyer':

> My tactic is to say 'well, I've spoken to someone that is a professional in this field and they've said it's OK'. You know, cover my own ass that way. (Company 1)

A few startups expressed a degree of distrust in those offering GDPR compliance consultancy services, mainly out of fear of paying for something that they didn't need. Company 15 described the idea of paying for advice as 'ridiculous', not believing that legal professionals 'actually know what they're talking about at the moment'. This accorded with the common perception among interviewees that it was unclear how the GDPR would be enforced.

Ultimately, the decision to seek specialist advice falls on the organisations, and some of the startups remained unable or unwilling to make it an ongoing part of their GDPR compliance efforts. Though organisations may find themselves able to implement compliance measures without the need for outside guidance, it is important that the solutions that they put in place are informed. Otherwise, there appears a risk that haphazard approaches, misconceptions and complacency could become commonplace.

Information about the GDPR was being shared among peers in their networks, raising questions of accuracy

Several interviewees turned to their business networks and peers for guidance on their compliance-related questions. Company 4, for example, was part of one such community

which had shared GDPR-related resources and organised a talk on compliance. Company 10 spoke of receiving compliance advice from their customers, and providing similar advice to other companies:

> They'll ask us 'What does it actually mean? What is your opinion and interpretation of it?' And I'll say, more or less, what I think it is. (Company 10)

The interviewees reported that there was often a lack of consensus amongst those providing guidance materials (e.g., regulators, consultancy services, online newsletters)—some having 'a slightly different interpretation of some of the details' (Company 10), which left those consulting them 'confused'. Many startups were turning to their network of contacts for sectorial or technology-specific advice—Company 14 spoke of starting online discussions to 'get a round robin of answers' from those within their sector.

While turning to others operating in similar spaces may appear an effective way to gain GDPR-related insights, the information may not necessarily be accurate. Company 10 commented that 'everyone is just asking everyone, and there's a lot of hearsay'. Companies were said to be writing about the GDPR—a 'hot topic' (Company 8)—to drive traffic to their websites. Naturally, this may pose risks, given that some writing about the GDPR appear not to be coming from an informed position. Company 15 had attended GDPR workshops and seminars where they recognised incorrect information being distributed. When probing further as to whether they believed misinformation was being shared, they responded:

> Massively. Massively so. […] People will realise that they've probably spent a lot of time and effort on things that weren't necessary. (Company 15)

Startups may be acting upon (and further spreading) inaccurate information without being aware of its veracity (such as with the blockchain example outlined earlier (in VIEWS OF THE STARTUPS). Following advice from unofficial sources could, therefore, be a risk, lulling organisations into a false sense of security. It also lessens the effectiveness of the data protection regulations themselves, causing a potential 'race to the bottom' with startups turning to other organisations that may be taking a misguided approach, with broader implications and risks to data subjects and society.

There are, of course, positives in organisations attempting to better understand these issues to improve practices, and in working together; indeed, not all advice will be misguided or misinformed. Nevertheless, the responsibility for compliance ultimately falls to each data controller, which entails verifying guidance received from others. Supervisory Authorities should act to counter misinformation (e.g., see the ICO's 'GDPR myths' blog series: ICO, 2019b), and may wish to explore more involved means of engagement, support and enforcement (as we will discuss) to help innovative tech startups with their GDPR obligations.

The prospect of large fines, particularly for unintentional noncompliance, dominated concerns

The GDPR greatly increases the maximum fines that can be levied for breaching data protection obligations. Perhaps due to the significant media attention given to financial penalties, fines were a recurring point of concern for many of the startups.

> There's all these enormous fines being thrown around, so everyone's very, very worried about it. (Company 10)

The focus on the size of fines was despite their maximum only likely being applied in severe or exceptional circumstances. One described the prospect of being fined as 'eye watering; you'd be out of business' (Company 9). Company 7 commented on being 'on the hook for quite a severe fine if things go wrong'. However, these fears largely concerned being found unintentionally in breach (as opposed to actively trying to shirk the law). This was Company 3's 'biggest fear', and was reflected by others:

> The concern is that we don't meet the compliance [requirements], there is a problem, and then we get the fine that might come. (Company 7)

There appeared little awareness of other penalties beyond fines, which can include potential orders to cease further data processing.[17] This is interesting because the other penalties should also be of concern for startups, who often generate little turnover, but where, for example, an order to cease their data processing operations could prove fatal to the organisation itself.

A recurring example of concern was the prospect of cyberattacks, which were described as 'frightening, terrifying, and unpredictable' (Company 9), and thought impossible to completely prevent, thereby exposing the organisation to (liability-related) risk. Company 14 believed that cybersecurity attacks were the biggest problem IoT companies face with regard to the GDPR. Yet, though security was a key point raised by many interviewees, security aspects are only one component of a larger set of GDPR-related obligations and responsibilities. The focus predominately on penalties relating to security considerations, at the expense of other obligations, may, therefore, be misplaced.

Some startups would 'wait-and-see' how the GDPR was enforced

Despite concerns over large fines, some interviewees suggested that startups would 'do a minimum and let's wait and see' (Company 10). That is, some organisations may do little or just that perceived as absolutely necessary until it was clearer how the GDPR would be enforced, who is being fined, and what measures are deemed appropriate. As these aspects become more widely understood, these startups would then adapt, to 'make sure that where other firms may have stumbled, we don't' (Company 3).

> If it's enforced strictly, it'll really make people look at it. It will be if there are big cases, where people actually get fined. That's typically when you'll actually see a reaction. (Company 10)

Several startups indicated that they believed the Supervisory Authorities were more likely to go after large organisations in the first instance, rather than startups like them—thereby encouraging this 'wait and see' approach. The larger organisations were thought to divert attention and scrutiny away from smaller organisations, and their repercussions for questionable data protection practices served as an indicator of impermissible behaviour for the startups:

> There will be some test cases fairly early on when some big players, you know the Facebooks or the Googles, get picked up on something and people will learn what you can and can't do in the eyes of the law. (Company 8)

These viewpoints reflect media reports that indicate, for example, that 'the [ICO's] focus would be on big companies', when enforcing the GDPR (Espiner, 2018). It seemed that

some smaller organisations expected to be able to 'fly under the radar' of the Supervisory Authorities, and able to act with a degree of impunity:

> I'm guessing [the GDPR is] not going to make much difference to anyone other than maybe big local authorities or people who are in the public eye […] They'll be the people who are most paranoid and actually following it. (Company 14)

Nevertheless, the obligations of the GDPR apply to all data controllers, regardless of their organisational size. Given the potential for startups to share strategies and mirror approaches taken by their peers (as discussed above), there is a risk that complacency could spread across organisations, impacting the industry as a whole. And further, the embedding of poor data protection practices within an organisation may mean that, as the organisation grows, the effect of such may be widely felt and harder to correct. Supervisory Authorities should therefore look to make it clear that such smaller companies not only can, but will be scrutinised and investigated. It is important to counter any perceived notions that smaller companies need not be concerned with enforcement and sanction, to prevent startups becoming complacent and bad practices becoming ingrained.

TAKING ACTION

The decisions and actions being taken by tech startups regarding personal data can have real and significant implications on individuals. RQ (iii) asks what steps can be taken by the startups, regulators, and policymakers to mitigate and manage data protection risks, and better support effective GDPR compliance. Towards this, we now present several considerations that these relevant stakeholders may wish to explore.

Startups have data protection obligations, which must be taken seriously

The GDPR is principles-based, meaning that organisations, including startups, must reconcile their practices with their regulatory obligations and reach a considered and defensible position. A common complaint was that GDPR-related guidance did not align with the technology or application area they worked with. That said, given these startups are pushing technological boundaries, it is arguable that it is they who are ideally placed to consider such issues, for example, undertaking data protection by design, as they work on developing and commercialising next-generation technology.

In short, startups should be more proactive in their approaches to data protection. Generally, it seems they would benefit from becoming more aware of the aims and intentions of the GDPR, and more could be done to champion the Regulation as an opportunity to evaluate, consider, and implement processes to improve data protection practices. Should it not be clear how compliance can be achieved, advice should be sought (or other measures taken) to best ensure they can demonstrate their ability to meet their GDPR obligations.[18] If the appropriate actions are inherently unclear, there is a strong argument that firms should not proceed down a particular track until they have a clearer plan for dealing with the relevant data protection issues. This may involve adopting alternative technologies or technical approaches, for example—or perhaps rethink their aims altogether.

Startups can leverage the support mechanisms of the GDPR

The GDPR itself provides means aimed at supporting organisations through their compliance processes.

The Data Protection Impact Assessment (DPIA) is one such mechanism.[19] A DPIA is a process undertaken by a data controller to evaluate the impact and risks associated with processing personal data. It aims to serve as an early indicator for uncovering data protection issues and provides a means for response. DPIAs are mandated in certain circumstances,[20] and whenever a DPIA indicates that 'the processing would result in a high risk', organisations are obliged to consult the Supervisory Authority, who will then provide written advice within a given timeframe.[21] This does not preclude those who are not obliged to contact the Supervisory Authority to contact them for advice relating to a DPIA. DPIAs appear a useful mechanism for startups to explore the data protection implications regarding their technology, providing a mechanism in which they can receive external advice. DPIAs, where reported to Supervisory Authorities, may also assist those Authorities in keeping abreast of technological directions, and the resulting data protection implications.

The Data Protection Officer (DPO) is another support mechanism brought about by the GDPR.[22] DPOs are appointed by an organisation and act as an internal port of call for data protection guidance. They are responsible for advising the data controller about their GDPR obligations, monitoring compliance on an ongoing basis, and cooperating with the Supervisory Authority—among other responsibilities.[23] A DPO should be particularly well-placed to help startups with many of the points outlined in this paper (e.g., providing tech/sector/company-specific guidance, ongoing monitoring and assurance). Having such expertise readily available may help startups identify the risks associated with the use of their envisaged technologies, or in (previously unconsidered) areas of their organisation in need of attention.

DPOs appear particularly valuable for startups innovating with technology, as they can continually support the company with compliance and good practice throughout the product lifecycle: inception, design, implementation, and operation. Yet, we found most startups either did not see a DPO as applicable to their organisation, or they had appointed someone internally as a DPO (usually the interviewee), regardless of their data protection expertise or organisational independence. A DPO should be 'a person with expert knowledge of data protection law and practices',[24] and need not necessarily be from within that organisation. As such, external services offering DPOs maybe of particular interest to startups, by avoiding potential conflicts of interest by 'overloaded' team members, and enabling external oversight of a startup's often 'agile' nature.

Undertaking these measures: The GDPR outlines instances where appointing a DPO and/or conducting a DPIA are mandatory—though in practical terms, this requires the data controller to know enough about these measures to understand whether these conditions apply.[25] It follows that startups might not know they exist, let alone always be clear whether such measures would be appropriate. It may be that some might (rightly or wrongly) dismiss these measures outright—especially if they are perceived as an administrative burden. Nevertheless, even when not mandated, these measures can provide valuable ways forward, particularly for startups struggling to understand how GDPR compliance should be approached, and any associated costs may be negligible compared to those resulting from, for example, fines, sanctions, or where organisational data protections concerns affect future rounds of fundraising.

DPIAs and DPOs are mechanisms that not only provide support and guidance but also help data controllers indicate that they are taking appropriate technical and organisational measures.[26] As such, they may be an effective way forward for assisting startups with their compliance challenges. However, of course, this requires that the organisations are aware

of what these support mechanisms are, what they offer, how they are leveraged, when they must be undertaken, and the resources required.

Tech service providers might have a role to play

Organisations will often rely on a technology supply chain, for example, third-party (cloud) services or platforms, to provide their compute infrastructure, storage, security, and so forth (Cobbe et al., 2020). This is particularly so for startups; several interviewees spoke of the importance of using such services over purchasing/developing their own—a natural position, given the limited resources of startups, and the drive for rapid innovation.

Some interviewees suggested that these service providers and platforms can and should assist the consumers of such services (i.e., the startups) with their compliance processes. Given a tech startup's data might already be held by a cloud provider, the provider is well-placed to offer compliance-related tools and extensions to these services. Company 1 suggested that larger organisations could 'allocate a small percentage of their time to help small businesses'. It was also felt that using major platforms gave the startups reassurance, for instance with regard to cybersecurity—'because you want to pass on that onus on to them, and they are the ones that have the resources to put in place a very good authentication system' (Company 1).

These (cloud and other) services are often construed as data processors[27] (those who process personal data on behalf of a controller) (Millard, 2013). Though the GDPR already obliges data processors to assist in compliance,[28] the position (and misunderstandings as to where liabilities may fall) of providers that we observed from the interviews extend beyond that required by the law. Interestingly, this suggests a desire for some form of GDPR Compliance-as-a-Service (Kamarinou et al., 2018), the argument being that the service provider, by providing such infrastructure and by way of their significant resources, may be best-placed to deal with compliance-related issues. Of course, any such argument depends on the particulars of the application, service being offered, and the degree of control of the parties involved.

Moreover, there are questions of incentives; platforms may be hesitant to take on any associated liabilities, though they might consider doing so for a price. Platforms may also be motivated to take a more proactive role for reasons of reputation; data protection incidents occurring by those using their infrastructure could impact their business by negatively affecting the wider public perceptions of their organisation, and technology organisations more generally (i.e. avoiding a tech 'backlash'). Further, technology startups are regularly acquired by the same large organisations providing the supporting infrastructure and services, meaning those seeking to acquire startups potentially stand to benefit if better data protection practices are integrated from the start. In all, there appear to be opportunities and motivations for service providers, particularly those larger, to assist startups with their GDPR compliance commitments. Whether and how such a landscape develops, remains to be seen.

Startups warrant scrutiny and Supervisory Authorities should be proactive with enforcing the GDPR

Some interviewees believed that the ICO would focus their efforts on larger companies (rather than tech startups), or those operating egregiously. Not only have media reports supported this viewpoint by suggesting that the ICO's 'focus would be on big companies' (Espiner, 2018) but also the ICO itself has indicated that they would particularly focus on

those 'deliberately, persistently or negligently misusing data' (Espiner, 2018). The startups typically did not see themselves misbehaving, nor believed themselves of particular interest to the ICO, even if they were noncompliant in some aspects. Yet, though the GDPR sets out to avoid stifling the economic and social benefits of technology,[29] small and innovative tech startups should not expect to, nor be seen to be able to, act with impunity even where grey areas might exist.

We argue that Supervisory Authorities should therefore not shy away from monitoring and, where necessary, intervening (including imposing penalties and sanctions) on the behaviours of tech startups. Though one expects action against small companies which blatantly flout the law, a general sense of Supervisory Authorities failing to monitor or enforce against the infractions of startups risks lulling smaller companies into a false sense of security (i.e., that they can 'fly under the radar', that there is 'safety in numbers', etc.), resulting in them not taking their GDPR responsibilities sufficiently seriously. For reasons we have discussed, such viewpoints should be anathema and countered wherever possible. Of course, in the event of minor infractions, a nudge may well be a more appropriate way to correct behaviour than, say, a debilitating penalty. The GDPR provides a range of different investigative, corrective, and advisory powers that can be exercised—from issuing advice, issuing warnings, banning controllers from processing, and financial penalties.[30]

Supervisory authorities should also look to be the first (external) port of call for answers to questions, which can help counter GDPR compliance misinformation. One way forward is the ICO's proposed use of regulatory sandboxes as a means to supply companies with guidance (ICO, 2019c). A regulatory sandbox is a framework 'to allow small scale, live testing of innovations by private firms in a controlled environment (operating under a special exemption, allowance, or other limited, time-bound exception) under the regulators supervision' (Jenik & Lauer, 2017). Similar approaches have seen particular uptake by financial regulators in areas where new innovative techniques introduce complex questions, such as for blockchain-based companies (Cermeño, 2016). The ICO have also outlined Advisory Visits—an opportunity to apply for a 1-day visit from the ICO with the aim of gaining practical advice on how to improve data protection practices (ICO, 2019a).

Importantly, tech startups will need some knowledge and understanding that these support mechanisms exist, what they offer, that they are affordable (or free), and that it would help ensure that their decisions accord with the GDPR in an approachable and nonintimidating way. Supervisory Authorities may wish to directly target emerging tech startups to increase awareness of such mechanisms, and how they can and should be used. And again, the insights gained from greater interaction with such innovative organisations may help the Supervisory Authorities themselves to keep better abreast of the developments in emerging technologies—feeding back into their policy decisions, the guidance produced, and so on.

RESEARCH CONSIDERATIONS AND LIMITATIONS

As with any such research, it is important to consider how our findings may generalise beyond our sample of startups. Though our sample size was fairly limited; it was consistent with other qualitative undertakings in this topic (e.g., Sirur et al., 2018). Importantly, we observed consistency with many of the findings of the literature, such as the confusion and concern surrounding the steps required to actually implement the GDPR (Deloitte, 2018; Sirur et al., 2018).

Second, any research where participants opt-in from a larger population cannot discount the potential for selection bias (see Fiesler & Proferes, 2018), and our interviewees had consented to take part in these interviews (from a larger pool of invitees). Our organisations

were also fairly geographically homogeneous—most of which coming from London, a so-called 'tech cluster' (Silva, 2019)—and this may have implications for the challenges and opportunities facing tech startups (funding, infrastructure, investment, support, etc.). For example, our results indicated that compliance-related misinformation was being shared within communities, yet this is obviously highly dependent on the types of communities that a startup may find themselves in (e.g., tech cluster, average city, geographically remote); in this paper, many of the firms would be part of the same or similar clusters. Though beyond the scope of this study, further research which explores the differences between approaches to data protection by startups from a range of different communities and clusters may assist in building up a more nuanced picture. That said, given that a purpose of the GDPR is to harmonise the rules and its enforcement across the EU, it may be that similar effects occur across different areas.

We also acknowledge that attitudes and perspectives towards the GDPR will likely change over time, as it becomes clearer what is and is not deemed acceptable practice, how it is enforced, what the regulators focus on, and so forth. Yet, such progress often stems from initial work identifying such risks and arguing ways forward—as this paper sets out to do. Throughout this paper, we have outlined legally grounded discussion points and proposed potential ways forward for further consideration. In short, though we acknowledge limitations of our research and of our findings, we believe that this study contributes to an important topic; by reporting on our discussions with emerging tech startups, our aim is to bring about an improved understanding of what issues are being faced 'on the ground' and indicating how they might be addressed.

CONCLUDING REMARKS

Ensuring compliance with data protection obligations should be a key area of focus for technology companies processing personal data, regardless of their size. Much of the data protection discussion has focused on large firms or high-profile incidents, with comparatively little concerning innovative tech startups. We have argued that such startups warrant more attention; though tech startups can be innovators, trend-setters, and perhaps even the giants of tomorrow, our findings suggest that many struggle and misunderstand how compliance can be achieved. Failure to address such issues can have serious implications for the broader data protection landscape.

This study has explored the data protection issues and concerns being faced by startups working with emerging technologies. We found a series of common themes, which indicate that there are opportunities for startups to do more regarding their GDPR obligations. This includes being more proactive and recognising the existing mechanisms which might assist them in undertaking these tasks. It also appears there is a role for the Supervisory Authorities to provide more support, in terms of raising awareness, providing guidance, and in exploring the possibilities for other, more innovative support mechanisms; regulatory sandboxes representing a recent example. Moreover, and often less-discussed in a startup context, there appears the need for more scrutiny: Monitoring, intervening and taking actions to both prevent harm and deter. Timely interactions and intervention are required to ensure that startups are given the best opportunities to innovate within the boundaries of data protection regulations. We argue that such actions will assist in a more responsible use of personal data.

Our findings have also uncovered a number of areas in which future research could explore. One regards the practicalities of how those working with emerging technologies can best employ 'data protection by design'.[31] Such research could act to provide established best practices for those interested in using related technologies, and provide a baseline for

which less scrupulous organisations may be assessed. Also relevant is research that specifically focuses on the effectiveness of some of the intervention mechanisms we have discussed (in TAKING ACTIONS), as is that exploring whether and how the opinions of tech startups may have shifted now that the Regulation is in force.

In all, our work provides insight into the data protection attitudes and practices of tech startups. New startups will continue to be founded, and similar opinions and challenges will likely be faced as they attempt to navigate the regulatory landscape. As our work indicates, some might fall short of their obligations, or take a rather cavalier approach. This is important, not only because of the recent commencement of the GDPR but also because of the pipeline of relevant and related regulation under development. By drawing attention to some of these challenges, we outline ways forward for startups and Supervisory Authorities alike—thereby helping to bring about better and more accountable data-driven innovation.

ACKNOWLEDGEMENTS

We acknowledge the support of the Digital Catapult, the UK Engineering and Physical Sciences Research Council (EPSRC) through grant EP/P024394/1, and Microsoft, through the Microsoft Cloud Computing Research Centre.

ENDNOTES

[1]Though this study focuses on the EU's GDPR, similar data protection frameworks exist in many other countries (Greenleaf, 2017), meaning that the attitudes and challenges discussed here may also be relevant for other jurisdictions.

[2]GDPR, Recital 1.

[3]GDPR, Art 4(1).

[4]GDPR, Art 4(1).

[5]GDPR, Art 4(7).

[6]GDPR, Art 24(1).

[7]See GDPR, Chapter 8.

[8]There are only some limited exceptions where the GDPR will not apply (see Bird & Bird, 2020).

[9]GDPR, Art 25.

[10]Though we did not identify any obvious differences between those who opted to participate and those that did not, we recognise that any research involving self-selecting participants can have potential bias (Fiesler & Proferes, 2018; Norval & Henderson, 2019).

[11]Braun and Clarke (2006) define a thematic map as 'an overall conceptualisation of the data patterns, and the relationships between them'.

[12]GDPR, Art 15.

[13]GDPR, Art 17.

[14]See GDPR, Arts 17(3)(c) and 9(2)(h–i).

[15]GDPR, Art 20.

[16]GDPR, Arts 13(4), 14(5), 17(3), 20(3), 22(2) and 23.

[17]GDPR, Art 58(2).

[18]GDPR, Art 24.

[19]GDPR, Art 35.

[20]GDPR, Art 35(3).

[21]GDPR, Art 36(1-2) and Recitals 89–92.

[22]GDPR, Art 37-39 and Recital 97.

[23]GDPR, Art 39(1).

[24]GDPR, Recital 97.

[25]GDPR Recitals 89, 90, 91, and 97 provide additional information.

[26]GDPR, Art 24(1).

[27]GDPR, Art 4(8).

[28]GDPR Art. 28.

[29]GDPR, Recitals 2, 6, and 7.

[30]GDPR, Art 58.

[31]GDPR, Art 25.

ORCID

Chris Norval http://orcid.org/0000-0002-4331-7863

REFERENCES

Bacon, J., Michels, J. D., Millard, C., & Singh, J. (2018). Blockchain demystified: A technical and legal introduction to distributed and centralized ledgers. *Richmond Journal of Law and Technology*, *25*(1), 1–106.

Bird & Bird. (2020). Derogations and special conditions. https://www.twobirds.com/%7E/media/pdfs/gdpr-pdfs/81–guide-to-the-gdpr–derogations-and-special-conditions.pdf

Black, J., Hopper, M., & Band, C. (2007). Making a success of principles-based regulation. *Law and Financial Markets Review*, *1*(3), 191–206.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Cermeño, J. S. (2016). *Blockchain in financial services: Regulatory landscape and future challenges for its commercial application*. BBVA Research. http://www.smallake.kr/wp-content/uploads/2017/01/WP_16-20.pdf

CNIL. (2018). Solutions for a responsible use of the blockchain in the context of personal data. https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf

Cobbe, J., Norval, C., & Singh, J. (2020). What lies beneath: Transparency in online service supply chains. *Journal of Cyber Policy*, *5*(1), 65–93. https://doi.org/10.1080/23738871.2020.1745860

Deloitte. (2018). *The time is now: The Deloitte General Data Protection Regulation benchmarking survey*. Deloitte LLP. https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/emea-gdpr-benchmarking-survey.pdf

Espiner, T. (2018, May 25). *GDPR: 'Don't panic!' Data watchdog tells firms*. BBC News. https://www.bbc.co.uk/news/business-44208456

European Union. (1995). 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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

European Union. (2016). 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). https://eur-lex.europa.eu/eli/reg/2016/679/oj

Fiesler, C., & Proferes, N. (2018). "Participant" perceptions of Twitter research ethics. *Social Media+Society*, *4*(1). https://doi.org/10.1177/2056305118763366

Greenleaf, G. (2017). 'European' data privacy standards implemented in laws outside Europe. *Privacy Laws & Business International Report*, *149*, 21–23.

Houser, K., & Voss, W. G. (2018). GDPR: The end of Google and Facebook or a new paradigm in data privacy? *Richmond Journal of Law and Technology*, *25*(1), 1–109.

IBM Institute for Business Value. (2018, May). *The end of the beginning: Unleashing the transformational power of GDPR*. IBM Corporation. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=86015886USEN

ICO. (2019a). Audits and advisory visits. https://ico.org.uk/for-organisations/resources-and-support/advisory-visits

ICO. (2019b). GDPR myths. https://ico.org.uk/about-the-ico/news-and-events/gdpr-myths/

ICO. (2019c). ICO's call for views on building a sandbox: Summary of responses and ICO comment. https://ico.org.uk/media/about-the-ico/consultations/2260322/201811-sandbox-call-for-views-analysis.pdf

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), 56–59.

ISACA. (2018, May). *GDPR: The end of the beginning*. ISACA. http://www.isaca.org/Knowledge-Center/Documents/2018-GDPR-Readiness-Survey-Report.pdf

Jenik, I., & Lauer, K. (2017, October). *Regulatory sandboxes and financial inclusion*. CGAP. https://www.cgap.org/sites/default/files/researches/documents/Working-Paper-Regulatory-Sandboxes-Oct-2017.pdf

Kamarinou, D., Millard, C., & Oldani, I. (2018). Compliance as a service. Queen Mary School of Law Legal Studies Research Paper No. 287/2018: 1–33.

Katila, R., Chen, E. L., & Piezunka, H. (2012). All the right moves: How entrepreneurial firms compete effectively. *Strategic Entrepreneurship Journal*, *6*(2), 116–132. https://doi.org/10.1002/sej.1130

Kollmann, T., Stöckmann, C., Hensellek, S., & Kensbock, J. (2016). *European startup monitor 2016*. Universität Duisburg-Essen Lehrstuhl für E-Business.

Maxwell, W. J. (2015). Principles-based regulation of personal data: The case of 'fair processing'. *International Data Privacy Law*, *5*(3), 205–216.

Millard, C. J. (2013). *Cloud computing law*. Oxford University Press.

NetApp. (2018, April). *NetApp GDPR survey: Gauging global awareness of business concerns*. NetApp, Inc. https://www.netapp.com/us/media/netapp-gdpr-survey-findings.pdf

Norval, C., & Henderson, T. (2019). Automating dynamic consent decisions for the processing of social media data in health research. *Journal of Empirical Research on Human Research Ethics*, *15*(3), 187–201. https://doi.org/10.1177/1556264619883715

Norval, C., Janssen, H., Cobbe, J., & Singh, J. (2018). *Reclaiming data: Overcoming app identification barriers for exercising data protection rights*. UbiComp '18.

O'Reilly, M., & Parker, N. (2013). 'Unsatisfactory saturation': A critical exploration of the notion of saturated sample sizes. *Qualitative Research*, *13*(2), 190–197. https://doi.org/10.1177/1468794112446106

Presthus, W., Sørum, H., & Andersen, L. R. (2018). GDPR compliance in Norwegian companies. *Proceedings from the Annual NOKOBIT Conference, Svalbard, Norway*, *26*(1), 1–15. https://ojs.bibsys.no/index.php/Nokobit/article/view/543

Prosser, D. (2018, April 6). UK technology startups hit all-time high. Forbes. https://www.forbes.com/sites/davidprosser/2018/04/06/uk-technology-start-ups-hit-all-time-high

Robehmed, N. (2013). Our thriving, global city is streaking ahead in the digital revolution. https://www.forbes.com/sites/natalierobehmed/2013/12/16/what-is-a-startup/

Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009). Review of the European data protection directive. https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf

SAS. (2018, May). GDPR: Most aren't ready—are you? SAS Institute Inc. https://www.sas.com/content/dam/SAS/en_us/doc/infographic/gdpr-109649.pdf

Silva, R. (2019). Our thriving, global city is streaking ahead in the digital revolution. https://www.standard.co.uk/comment/comment/our-thriving-global-city-is-streaking-ahead-in-the-digital-revolution-a4253231.html

Singh, J., & Cobbe, J. (2019). The security implications of data subject rights. *IEEE Security & Privacy*, *17*(6), 21–30. https://doi.org/10.1109/MSEC.2019.2914614

Sirur, S., Nurse, J. R., & Webb, H. (2018). Are we there yet?: Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*. https://doi.org/10.1145/3267357.3267368

Urquhart, L. (2019). In L. Edwards & E. Harbinja (Eds.), *White noise from the white goods? Privacy by design for ambient domestic computing*. Future Laq, EU.

Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. *International Data Privacy Law*, *8*(2), 105–123.

Veale, M., Binns, R., & Edwards, L. (2018). Algorithms that remember: Model inversion attacks and data protection law. *Philosophical Transactions of the Royal Society A: Mathematical Physical and Engineering Sciences*, *376*(2133), 1–15.

How to cite this article: Norval, C., Janssen, H., Cobbe, J., & Singh, J. (2021). Data protection and tech startups: The need for attention, support, and scrutiny. *Policy Internet*, 13, 278–299. https://doi.org/10.1002/poi3.255