"It may be a pain in the backside but..." Insights into the resilience of business after GDPR

Gerard Buckley
University College London, UK
gerard.buckley.18@ucl.ac.uk

Tristan Caulfield
University College London, UK
t.caulfield@ucl.ac.uk

Ingolf Becker
University College London, UK
i.becker@ucl.ac.uk

ABSTRACT

The General Data Protection Regulation (GDPR) came into effect in May 2018 and is designed to safeguard European Union (EU) citizens' data privacy. The benefits of the regulation to consumers' rights and to regulators' powers are well known. The benefits to regulated businesses are less obvious and under-researched.

We conduct exploratory research into understanding the sociotechnical impacts and resilience of business in the face of a major new disruptive regulation. In particular, we investigate if GDPR is all pain and no gain. Using semi-structured interviews, we survey 14 senior-level executives responsible for business, finance, marketing, compliance and technology drawn from six companies in the UK and Ireland.

We find the threat of fines has focused the corporate mind and made business more privacy aware. Organisationally, it has created new power bases within companies to advocate GDPR. It has forced companies to modernise their platforms and indirectly benefited them with better risk management processes, information security infrastructure and up to date customer databases. Compliance, for some, is used as a reputational signal of trustworthiness.

Many implementation challenges remain. New business development and intra-company communication is more constrained. Regulation has increased costs and internal bureaucracy. Grey areas remain due to a lack of case law. Disgruntled customers and ex-employees weaponise Subject Access Requests (SAR) as a tool of retaliation. All small and medium-sized businesses in our sample see GDPR as overkill and overwhelming.

We conclude GDPR may be regarded as a pain by business but it has made it more careful with data. It created a short-term disruption that monopolised IT budgets in the run-up to GDPR and created a long-term disruption to company politics as Compliance and Information Security leverage the regulation for budget and control. The rising trend in the number of fines issued by national data protection regulators and the establishment of new case law will continue to reshape organisations.

CCS CONCEPTS

• **Security and privacy → Social aspects**; • **Social and professional topics → Governmental regulations**.

NSPW '22, October 24–27, 2022, North Conway, NH, USA

KEYWORDS

GDPR, General Data Protection Regulation, GDPR Business benefits, GDPR implementation challenges, Data protection

ACM Reference Format:
Gerard Buckley, Tristan Caulfield, and Ingolf Becker. 2022. "It may be a pain in the backside but..." Insights into the resilience of business after GDPR. In *New Security Paradigms Workshop (NSPW '22), October 24–27, 2022, North Conway, NH, USA.* ACM, New York, NY, USA, 14 pages. DOI: 10.1145/3584318.3584320

1 INTRODUCTION

Regulation has long suffered an image problem for being boring, bureaucratic and unnecessary. And while this can be true, regulation is a vital lever of government to achieve policy objectives. Governments regulate business to deliver better outcomes for the economy, the environment and society: for example to correct market failures, to protect people and wildlife from pollution and to safeguard citizens' privacy. The EU's GDPR is a good example of the latter and is a major disruptor in the context of data privacy and security.

Our focus is on the resilience of an overlooked stakeholder: business. Most attention has concentrated on the benefits of GDPR to the regulator in terms of stronger powers and to the consumer in terms of stronger privacy rights. However little research has tracked the benefits to business who, after all, have had to substantially modify their sociotechnical systems to operate it.

Academic literature, prior to the introduction of GDPR in May 2018, proposed a variety of potential GDPR benefits to business including better data management and analytics, brand enhancement and access to a level playing field. Since then, however, interest in the business perspective has waned and it lacks empirical follow-up data. Even recent studies [47, 4] rely on earlier papers and still speak in terms of potential opportunities and possible benefits.

While regulation is viewed by most as all stick and no carrot, the EU promoted and promotes the benefits of GDPR to business. Hence we are interested in exploring if there are benefits in reality and how they affect different groups or departments within an organisation.

For this reason, we employed a semi-structured interview technique to ask 14 senior executives in a range of companies what has been the actual impact of GDPR on them and across their organizations since 2018. We investigate:

RQ1: What are the perceived benefits of GDPR to business?
RQ2: Where are the effects of GDPR felt within a business?

After discussing the background to GDPR in Section 2, related literature in Section 3 and our methodology in Section 4, we analyse and discuss the findings in Sections 5 & 6. We show there are both

direct and indirect positive impacts on business from GDPR despite ongoing implementation issues.

We believe this is the first study to analyse the lived experience of GDPR by business since its introduction over three years ago and the first to identify how GDPR has changed the balance of power and decision making within organisations.

2 BACKGROUND

This section provides a quick recapitulation of what is the purpose of regulation, what are the fundamental principles behind formulating good regulation and how privacy and data protection regulation has developed over time. It summarises the GDPR, its objectives and the results of subsequent surveys by the EU on the success of its implementation. Since 2018, we note the dearth of assessment of the benefits to business of GDPR by the EU. We note a similar lack of follow-up by the professional advisory firms who were active commentators in 2017 & 18. Academic assessments follow in Section 3.

2.1 Why Regulate?

Regulation can generically be defined as a (set of) intervention(s) that either correct or enable a desired social and/or economic behaviour in response to public policy goals and objectives. In a narrow sense it can refer to a set of authoritative rules used alongside processes for monitoring and promoting compliance often referred to as traditional 'command and control' approaches. A broader interpretation of 'regulation' includes a range of interventions including market based instruments, etc, i.e. "all mechanisms of social control—including unintentional and non-state processes" [6, 7]. Thus, interventions may be used as alternatives, but more commonly as complementary activities, to traditional 'command and control' approaches. The mix is important because evidence suggests that SMEs for example "will only act when there is a specific requirement to do so" [58]. Regulation bridges the gap between an operator's self-interest and the interests of society [58].

Governments regulate business to guarantee minimum standards and protections. Left unchecked, the profit motive of business can lead to damaging behaviours that are detrimental to society e.g., price-fixing cartels, unsafe working conditions, abuses of consumers rights. While governments may also regulate the actions of individuals, public-sector or civil society organisations, our focus is on the regulation of business and data.

2.2 The Foundations of Good Regulations

Regulation brings both benefits and costs. It can stimulate ideas and can block their implementation. It can increase or reduce the risk of investing in new products and business models. It can determine how much funding is available for innovation and how much goes into tick-box compliance. It can influence consumer confidence and demand and determine whether firms enter or exit a market.

For this reason, most developed economies have policies, procedures and institutions to govern how regulations are developed, administered and reviewed. While approaches vary, such policies typically affirm the importance of openness, proportionality and fairness [59].

Openness demands transparency and participation in the policy design to ensure regulation serves the public interest and engages all the stakeholders that it affects or who hold an interest in it. Proportionality demands that the costs of compliance are commensurate with the benefits the regulation is intended to deliver. Fairness demands that regulatory decisions should be made on an objective, impartial and consistent basis, without conflict of interest, bias or improper influence. The theory is that this enables businesses to compete on a level playing field (LPF), and helps ensure that the best ideas, products and business models are those that succeed [16].

2.3 The Evolution of Data Regulation

The roots of GDPR can be traced back to two concepts – privacy and data protection.

Privacy is covered by Article 8 European Court of Human Rights (ECHR) – Right to respect for private and family life [31].

Data protection is covered by Article 8 of the Charter of Fundamental Rights of the European Union (CFR): Protection of personal data [19].

In Germany, personal data protection was linked to more expansive, more fundamental societal values. The term informational self-determination became key to understanding the German view of privacy after a constitutional case in 1983 ruled that "the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others." Norway, Sweden, France and the UK enshrined the right to data protection as a *sui generis* (in a class by itself) right, but they did not adopt the German concept of self-determination. They saw data as a valuable resource and subject to competing interests. For them, data protection aims to safeguard a just and reasonable equilibrium between the interests of the individuals and those of the community concerning the processing of personal data as enshrined in the 1980 OECD Privacy Guidelines, 1981 Convention 108 and 1995 Directive 95/46/EC [40, 29, 5].

GDPR (EU 2016/679) is a European Union Regulation that replaced and repealed the EU's 1995 Data Protection Directive (DPD, also known as Directive 95/46/EC. It talks to "the protection of individuals with regard to the processing of personal data and on the free movement of such data." This dual mandate explains the mix of prohibition and permission contained in GDPR. It is prohibitive because it says that personal data cannot be processed unless certain conditions are satisfied, which has echoes of informational self-determination and individual control. At the same time, it is permissive in that it says personal data can be processed provided certain conditions are satisfied. This dual mandate provides a balancing of interests, but it also underlies many of the critiques of the day to day operation of GDPR [55].

2.4 GDPR Objectives

GDPR came into force on 25 May 2018 [22], after which all organisations were required to be compliant. The UK GDPR, post-Brexit, was ruled as adequate by the EU in June 2021.

Unlike its predecessor, GDPR is an EU Regulation and not a Directive. This means it has binding force in every member state

and there is no discretion over how it is transposed into national law.

The primary purpose of GDPR is to define standardised data protection laws for all member countries across the European Union. In summary, it was intended to [23]:

- Increase privacy and extend data rights for EU residents.
- Help EU residents understand personal data use.
- Address the export of personal data outside of the EU.
- Give regulatory authorities greater powers to take action against organisations that breach the new data protection regulations.
- Simplify the regulatory environment for international business by unifying data protection regulations within the European Union (a.k.a. the level playing field).
- Require every new business process that uses personal data to abide by the GDPR data protection regulations and Privacy by Design rule.

It has strict rules such as the rights for data subjects to access their own data (known as SARs), to be forgotten and to expect affirmative consent. It applies to companies inside and outside the EU if they hold personal data belonging to EU citizens. And it has tight data breach notification requirements and hefty fines of up to four percent of an organisation's total worldwide annual turnover if found in violation [27].

GDPR is strong on the obligations of business. It makes no reference to any benefits to business.

2.5 GDPR Scorecard

The EU has commissioned a number of surveys since the GDPR was applied. We highlight three surveys here: the 2019 Eurobarometer, the 2019 SME Survey and the 2020 EU Self-Evaluation Report.

The 2019 EU Barometer 487a [20] found that:

- Over 66% of EU citizens have heard of GDPR, over 50% have heard of their rights under GDPR, and almost 60% have heard of their data regulator.
- A majority feel they have partial control over the information they provide online. Only 20% say they see the Terms & Conditions (T&C's) to the collection and use of their personal data online, and only 13% say they read privacy statements in full.

The 2019 GDPR Small Business Survey was run by Proton Technologies AG [28]. Part-funded by a EU Horizon Project, it found:

- Millions of small businesses still do not comply with the GDPR.
- Encryption technology is still not widely understood.
- Small businesses want to comply and have invested heavily on GDPR compliance.

On June 24, 2020, the European Commission (EC) submitted its first report on the evaluation and review of the GDPR to the European Parliament (EP) and Council [11]. The report is required under Article 97 of the GDPR and will be produced at four-year intervals going forward. In its report, the Commission concludes that generally the GDPR has successfully met its objectives, namely those of strengthening personal data protection and guaranteeing the free flow of personal data within the EU. It identified a number of areas for improvement, including:

- Fragmentation between member states: differential interpretation of discretionary details
- Uneven enforcement: different *"data protection cultures"*, different budgets & resources
- Unforeseen Issues with Emerging Technologies: AI, IoT or facial recognition
- Unused Potential of Data Portability Rights: to avoid unfair practices and lock-in effects
- Adequacy Decisions: Pending third country regimes such as South Korea and UK
- Extra-territorial Reach: *"This approach should be pursued more vigorously in order to send a clear message that the lack of an establishment in the EU does not relieve foreign operators of their responsibilities under the GDPR."*

Whilst this report is akin to the EC marking its own homework and not an impartial external assessment, it is still a useful checklist of where the EC sees shortcomings in GDPR.

2.6 Gap in GDPR Scorecard

Our search has revealed a significant gap in the assessment of GDPR. There seems to be no equivalent to the EC's four-yearly evaluation and review from the perspective of one important stakeholder: the regulated businesses that handle customer data.

In the run-up to GDPR going live in 2018, there was a flood of surveys, studies and benchmarking reports by IT vendors and professional services firms. Since then, they have dried up.

One exception is the EU Multistakeholder Expert Group. Set up in 2017, it assists with identifying the potential challenges in the application of the GDPR from the perspective of different stakeholders, and to contribute to the EC's evaluation of GDPR in 2020. It is composed of up to 27 members drawn from trade and business associations, NGO's, academics, legal practitioners and privacy advocates. It is quite technocratic. Their *"contribution addressed topics such as the impact of the GDPR on data subjects' rights, the conditions for a valid consent under Article 7(4) of the GDPR, the one-stop-shop mechanism, the principle of accountability and the risk-based approach, data protection officers' ('DPOs'), the relationship between controllers and processors, and the development of Standard Contractual Clauses for the transfer of personal data"* [21]. Benefits analysis is not part of its mandate.

One of the few non-EU follow up surveys was a survey by Deloitte's *"A new era for privacy: GDPR six months on"* [14]. The headline was that consumer awareness has risen and 48% of organisations had made "significant" investment to improve their compliance. In addition:

- 70% of organisations had increased staff focused on GDPR compliance.
- 92% of organisations claimed confidence in their ability to comply with GDPR in the long term. 65% of organisations felt they had enough resources to comply.
- 78% had invested in new data loss prevention and 71% in unstructured data scanning.

Another non-EU study is the annual implementation progress report that is published by Access Now, a digital rights group. In

their latest, *"Three Years Under The EU GDPR"* [18], they describe GDPR as *"nothing but hot air"* because of slow and weak enforcement by the Data Protection Authorities (DPA). The EU is criticised for under-resourcing its DPAs and failing to levy sufficient fines and sanctions on business. This presents the EU and its DPAs with a media communications challenge - satisfying consumer rights protection groups and, at the same time, selling the benefits of a level playing field and GDPR compliance to business.

3 LITERATURE REVIEW

There is no shortage of academic GDPR studies. A Google Scholar search of General Data Protection Regulation will yield circa 3 million hits. Limit the search to papers published after GDPR went live in 2018 however and interest drops precipitously. Search for papers that contain the two keywords "GDPR success" or "GDPR benefits" anywhere in the text yields less again. As we narrowed the search, we quickly reached zero hits for keyword combinations such as "GDPR business benefits" or "GDPR consumer benefits" or even "benefits of GDPR to business". The lack of curiosity about GDPR's benefits to business after 2018 is curious.

In this section, we review the plentiful literature on the implementation challenges of GDPR. We examine papers that contained the word pair "GDPR success" and "GDPR benefits" anywhere in their text as well any relevant papers from multiple rounds of backward and forward searches. Most of these do not talk to our topic because they are not interested in how GDPR might deliver value or return from a business perspective. The studies in Section 3.2 explore exclusively regulatory angles. Other papers discussing benefits in fact only consider drawbacks (Section 3.3).

The two papers [47, 4] that do explore positive aspects of GDPR to businesses rely mainly on pre-GDPR work. We conclude that given the newness of GDPR, there are still few scientific follow-up studies.

3.1 GDPR Implementation Challenges

Unlike benefits, there is a surfeit of studies on the challenges of GDPR. It is a complex regulation [25], it fails to specify technical solutions [53] and it involves subjectivity [2]. Compliance can be expensive [53, 1]. Companies may need extra administration staff and expert DPO staff [38], extra employee training and face difficulty recruiting and retaining these people [35]. Regulatory restrictions may impact an organisations performance [54] and persuade some to cut back their service offering in the EU to avoid it [3].

GDPR brings increased technical complexity [9, 17, 46]. Data portability [33] as well data consent, rectification and deletion processes will require technical and organisational investment [17]. Data erasure (aka the right to be forgotten) is seen as particularly problematic for bigger companies [12, 15]. System and process audits [17] and recruiting more cybersecurity professionals will require more investment. Clamping down on how personal data is handled may slow down the development and application of emerging technologies such as IoT and blockchain [37, 56].

3.2 Studies on GDPR Success

Unlike challenges, there is a dearth of research on success. Under "GDPR success", the most relevant literature has a regulator or regulatory success focus rather than any reference to business success. Thus, Oxford Analytica's appraisal of GDPR on its first anniversary [44] looked at key shortcomings such as ensuring the compliance of business beyond "big tech", concern that public awareness of the GDPR in smaller EU states will lag that in larger states and criticism of the Irish regulator if it failed to demonstrate a clearer commitment towards robust regulation. Sanders, in *"The GDPR One Year Later"* [49] suggests the key to the GDPR's success requires data protection officials and judges to seriously evaluate situations in which privacy and freedom of the press appear to conflict. Kessler in *"Data Protection in the Wake of the GDPR: California's Solution for Protecting 'the World's Most Valuable Resource'"* [34] argues that the United States should adopt a federal standard that offers consumers similarly strong protections as the GDPR.

3.3 Studies on GDPR Drawbacks

Despite searching for "GDPR benefits", the literature is about the dis-benefits of GDPR, albeit with more of a focus on businesses. *"The Economic Impact of the European Reform of Data Protection"* is a 2015 paper by M Ciriani [10] of the Regulatory Office of the giant French mobile phone operator Orange. She argued that the extraterritorial application of European law would promote a level playing field within the European market. However, with the exception of the GDPR's impact assessment conducted by the European Commission, she claimed the literature she had examined shows that the costs of GDPR's adoption might offset the efficiency gains. She expressed concern that increasing the administrative burden might not help improve the competitiveness of European digital service providers, such as her employer. Flexible ex-post effects-based accountability would help industry.

Sarah Shyy, in the self-explanatory *"The GDPR's Lose-Lose Dilemma: Minimal Benefits to Data Privacy & Significant Burdens on Business"* [50] argues that GDPR fails to promote consumer privacy because, in today's data collection practices, consumers are forced to accept an online company's privacy policy and data collection practices. Meanwhile, the GDPR has disadvantaged SMEs by imposing cost-prohibitive measures, hindering SMEs growth, and spurring SMEs to exit the market. Rather than copying the GDPR model, she argues US lawmakers should learn from the GDPR's failings and adopt regulation that is both more effective in protecting consumer privacy and less burdensome on businesses.

3.4 Studies on GDPR Benefits to Business

There are two academic papers [47, 4], published in 2019, that are relevant from a business perspective.

Poritskiy et al. ask what are the main benefits offered by GDPR for IT companies [47]. They surveyed 286 Portuguese IT companies that were partners of their educational institution on eight benefits (and nine challenges) drawn from a literature review. On closer reading, the benefits stem from opinion pieces that pre-date the introduction of GDPR rather than empirical research.

They concluded the two most significant benefits were trust (consumer confidence) and legal clarification. These two benefits chime with two of their sources, Bilyk [17] and White [57]. The Bilyk study references a blog on theappsolutions.com website credited to a different author and the White study appears to reference a (now)

broken link to a GDPR news report. Another two of the eight benefits of GDPR, better decision-making and better risk-assessment, are also credited to Bilyk. Two more of the eight benefits, increased security of products / services and increased quality of documentation, are credited to Krikke et al. [36] which appear to reference brochure-style content on the site of the law firm Stibbe.com. Another benefit, create new competitive advantages, is credited to Dellie [13] which references a blog on the ITASCA.org site. Two further benefits, minimisation of the collected personal data and improved data management processes, are credited to Fimin [24] which references an article in Forbes magazine by the CEO of cybersecurity firm. The eight benefits surveyed in the questionnaire may indeed be real but the cited evidence behind them is not based on any qualitative or quantitative data.

In the second paper, Teixeira et al. [4] conducted a systematic literature review to identify the critical success factors that contribute to the implementation of GDPR. One of the research questions was *"What are the benefits of complying with GDPR?"*

Their review identified four potential areas of benefit: proper data management, use of data analytics, cost reduction and an increase in reputation and competitiveness.

Regarding data management, Lopes and Oliveira view GDPR as an opportunity for companies to document their processes and procedures [39]. Presthus et al. sees it as an opportunity to cleanse and audit personal data to cap any liability to abuse of personal data [48] and similarly, Skendžić et al. view GDPR as an opportunity to bring data consistency across the organisation [51].

Better data management enables better data analytics. Garber argue data-driven insights will help inform companies optimise their business processes and identify new business development opportunities [26]. Enhanced data management will lower costs by eliminating surplus data, redundant data and, thus, data storage costs [41, 8, 45]. O'Brien reports it could reduce costs by up to 2.3B EUR per annum according to estimates by the European Commission [42]. Beckett postulates that GDPR compliance and safe data governance skills may enhance a company's trustworthiness and generate new business and new customers [8]. Tikkinen-Piri et al. argue the adoption of GDPR may give a competitive advantage to organisations [53]. Garber and Miglicco believe compliance may also boost an organisations' performance by improving operational efficiency [26, 41].

The first paper [47] is a quantitative survey of GDPR dimensions based mainly on pre-GDPR literature. The second [4] is a systematic review of historic literature regarding GDPR success factors. Both look to the future and talk in terms of potential barriers and enablers. The former admits it does not explore implementation challenges nor company specifics and the latter admits it is unable to identify or present practical outcomes.

3.5 Motivation

Given GDPR is a relatively recent regulation, there are still few scientific follow-up studies. Neither of the two 2019 papers [47, 4] nor our review here were able to identify or substantiate specific benefits to business of implementing GDPR. Hence our research aim is to obtain information on the actual impacts of GDPR on business and how those effects are felt within and across the organisation.

4 METHODOLOGY

Due to the newness of the issue and the absence of reliable data, we decided to take an exploratory qualitative research approach and use thematic analysis on semi-structured interviews.

4.1 Data Collection and Analysis

Data was collected via a series of semi-structured one-to-one interviews with business executives who work in companies that handle customer data. The study covered a range of small, medium, and large companies to maximise the sample's representativeness. It deliberately targeted senior and middle-management executives drawn from across the various functions within an organisation to get as holistic a perspective as possible. It included two Chief Executive Officers (CEO), three Managing Directors (MD), one Chief Marketing Officer (CMO), one Chief Information Officer (CIO), one Chief Information Security Officer (CISO), one Finance Director (FD), three senior legal departmental heads and two marketing executives drawn from public relations (PR) and digital marketing analytics.

The interviews were conducted over Microsoft Teams in April and May 2021 during one of the Covid lockdowns across Europe. Ironically, this situation probably made it easier to access senior executives and made the conversations more relaxed as they were speaking from home rather than if the interview had been arranged in an office context pre-Covid. The interviews lasted, on average an hour and ranged between 35 and 90 minutes. The interviewees (9 male, 5 female) were aged between their early 30's and early 50's.

The interviews had a mix of open and closed questions. The open questions preceded the closed questions. The agenda for the open questions was very straightforward, namely asking executives what were the advantages and disadvantages of GDPR, based on their experience of it, within their companies. The agenda for the closed questions was developed by drawing on the literature review and capturing the predicted benefits and challenges. These were used as a checklist to ensure all the talking points were covered if they did not come up unprompted in response to the initial open questions. The interviewer's aide memoire can be found in Appendix A.

After conducting the first few interviews, we decided to add extra open questions at the end because we found participants had warmed to the subject by then and naturally opened up about how they would improve GDPR or how life would be different if GDPR had never happened.

One author conducted all the interviews to maintain consistency. The interviews were recorded and a report was written immediately after each meeting to summarise the main points. The research team reflected on the findings after each interview to identify common themes and resolve differences in interpretation. This initially caused the interview framework to be revised marginally.

The interviews were transcribed using automated transcription software and manually edited for correctness. This was followed by inductive thematic coding by the primary researcher based on the transcripts. This approach for analysing qualitative evaluation data [52] condenses raw data text into brief themes, which can be used to develop a model or theory about the underlying structure of experiences evident in the data. The codes in this research were initially generated from the literature review and expanded as the

interviews unfolded. Each code was manually transformed into a post-it note and clustered on a whiteboard to generate themes. This manual approach allowed us to easily iterate the analysis, and it facilitated cross-checking with the other researchers. We experienced a dramatic reduction in new themes after only a few interviews, in line with previous research [30]. We felt that saturation had been achieved after 14 interviews.

4.2 Sample Characteristics

It is difficult to recruit business people to dedicate time to an interview at the best of times. It is doubly difficult if the target is senior management and if the topic is a commercially sensitive matter. The interviewees were selected using convenience sampling. By networking through friends of friends and warm referrals, 14 senior executives agreed to be interviewed across six companies based in the UK and Ireland (which is in the EU). No attempt was made to reflect a representative group of practitioners based on EU geographic coverage. There was a conscious attempt, however, to diversify the sample away from solely IT or GDPR practitioners. The company classification is based on the number of employees [43] and shown in Table 1.

P1 was the owner-manager and sole employee of a technology solutions integrator with a turnover <£750K. It operated in the UK only. P2 to P5 were the senior management team of a small publisher with circa 30 staff that published specialist magazines for the UK and overseas markets. P5 and P6 worked at the HQ of a light engineering manufacturer with circa 100 staff. It exported to mainland Europe. P7 and P8 belonged to a global drinks company and were based in the Irish subsidiary. P9 and P10 worked at the UK HQ of an international legal practice with offices in Europe, Asia and the USA. The country practices are all independent practices under a common brand. P11 to P14 worked at the London-based global HQ for a banking and asset management company. The CISO and CMO held global responsibility.

4.3 Ethical Considerations

The authors' departmental Research Ethics Committee approved this study. It is designed to include pseudonymity, confidentiality and informed consent. The study does not identify individual participants. All identifiable information was stripped from the transcripts and the recordings were subsequently deleted. Some quotes were altered or redacted to mask details. The participants were aware of the research's purpose, the researchers involved, and their role in it. Participants were not offered any compensation for participating.

5 FINDINGS & ANALYSIS

This study investigates if there are any beneficial impacts to business from GDPR and how they are distributed across the organisation.

In this section, an expansive definition of 'benefit' is taken because benefits in business come in many guises. Typically, companies will classify benefits as either direct or indirect. Direct benefits have a clear cause and effect relationship, whilst indirect benefits are less clear cut. A direct benefit will generate new revenue or reduce costs and is quantifiable. An indirect benefit, sometimes called a soft benefit, may be less tangible and defy direct measurement. Benefits may be planned or unanticipated. Benefits can also be in the eye of the beholder: what advantages one part of an organisation can disadvantage another. And finally, as discussed earlier in the section on regulation, what benefits a company may or may not benefit the consumer and society.

Table 1: The organisations and interviewees labelled P1–P14

Size	Sector	Job Title	Labels
Micro	Technology	MD	P1
Small	Publishing	CEO	P2
		MD	P3
		FD	P4
Medium	Manufacture	CEO	P5
		IT MD	P6
Large	Drinks	Legal	P7
		Marketing	P8
Large	Law	Legal	P9
		CIO	P10
Large	Bank	Legal	P11
		CISO	P12
		CMO	P13
		PR	P14

Our framework for discussion is based on themes that were generated by analysing and abstracting the interviews. The small sample size should be considered when judging the findings' generalisability. We will show that many of the impacts attributable to GDPR are a win-win for both business and the consumer/society.

Four positive direct impacts and two indirect impacts are identified; and while the primary focus of the research was benefits, we identify five challenges with implementing GDPR.

The participants were invited to suggest how GDPR could be made better. We review their feedback in the final section.

5.1 Direct Impacts

5.1.1 Privacy-Aware Mindset. All interviewees stressed the importance of protecting data and privacy. On closer questioning, the motivation became clear. It is driven by fear. GDPR fines focus the mind. For severe violations listed in Art. (5) GDPR, the fine framework can be up to €20 million or up to 4% of global turnover, whichever is the higher. A compliance officer put it succinctly: *"Data breaches […] gives everyone an incentive to listen […] the 4% […] is hanging over the heads of the board"* (P11).

The threat is felt by small and large players alike. The FD of an SME put the effect of a fine in a stark manner, *"we're running on fumes most of the time anyway, so any little thing could push us over the edge financially"* (P4). The CMO in one of the larger companies said,

> *"Data breaches and liability fines [...] We do simulated exercises around crises [...] and they always come down to a cyber hack and data leakage, and data is what we run our business by. So generically, it is the thing that keeps me awake at night the most, and it is the one thing that could blow our company up."* (P13)

GDPR has made executives more aware of data privacy both at a corporate and at a very personal level.

> *"We were very aware of its arrival [...] it approached us as something of a tidal wave of regulation because we knew that the sanctions against companies that failed to adhere were going to be quite stiff. And we also understood that it was important. We all have personal lives and know what it's like when we have interference and intervention and unnecessary and unsolicited approaches by organisations."* (P3)

GDPR has changed companies' data use behaviour. A marketer put GDPR's impact on spam as follows:

> *"As painful as it might be, fundamentally what it allows us to do is to understand our customers desired level of engagement with our company. [...][In the] wild west before GDPR came along [...] you didn't have to bother about things like marketing permissions and things like that.[...] [You used to] have a mass of customers; you used to contact them through whatever means whenever you wanted to, and some were more receptive to that than others."* (P13)

GDPR has changed corporate attitudes. As one executive observed *"It does put the whole of the organisation into a different mindset"* (P12). It has raised *"awareness within the business around personal data, the importance of protecting it and treating it in specific ways"*. (P7) It *"has led to a better understanding of why we hold data"* (P7). It stops people from hoarding data and gets rid of the *"just in case mentality"* (P9).

It has also *"raised awareness within the business from a cyber perspective [...] which has resulted in us procuring cyber insurance"* (P9). *"Security is tighter now [...] in terms of encryption [...] we've tightened down access"* (P7).

In sum, the threat of GDPR fines has made companies become more responsible. As one CEO put it, *"I suppose we just are a little bit more careful what we use the information for"* (P2). That is clearly a benefit to consumers and society and arguably helped business become a better corporate citizen.

5.1.2 Spur to Change. New regulation like GDPR may require companies to change their people, processes or technology. It depends on how close their model of operation was already in alignment with the new regulation. Suppose a company is forced to buy a new data system to satisfy GDPR and the new system delivers new efficiencies and cost-savings. In that case, it is difficult to argue that they are direct business benefits of GDPR. After all, the company could have used that same money for something more value generative such as new product development or expansion into new markets. However, if a company is forced to face up to longstanding issues that it knew had to be fixed or it would decline, and if GDPR is the spur to make that investment finally happen, then it is arguable that the spin-off benefits can be regarded as a direct benefit to business from GDPR.

Out of the six companies in the study, two made minimal changes to their IT infrastructure. One tweaked their data classification *"It was just about reconfiguring it"* (P10). One was created after 2018 and was designed from the outset with GDPR in mind, and the remaining two were spurred to make fundamental changes. In both cases, GDPR *"got us to shift change at a quicker rate than usual"* (P7).

One of the SMEs said the most significant benefit of GDPR was *"getting things in order"* (P4). *"We had enough spreadsheets to fit in a football field"* (P4). They moved everything onto the cloud, went paperless, slashed costs and reduced headcount by 2/3rd. In effect, GDPR meant *"driving the digitalisation and automation of a lot of systems [...] and the restructure of the organisation"* (P6).

In contrast, one of the larger companies had already concluded that data-driven marketing *"is the way of the future"* (P8). It used GDPR as an opportunity to centralise all country customer databases in global headquarters (GHQ), standardise the data input and output processes, tighten access control and upgrade information security. It required all customers to re-opt in as part of a campaign to be GDPR-ready. It programmed standards into the workflow to enforce GDPR principles such as data minimisation and data retention periods and made it apply worldwide. As an example, the company now has an automated rule that flags and deletes prospect data if they have not been *"touched"* (P8) after a year. It also serves as a feedback loop between country management and GHQ. Why have you neglected to contact these prospects? Did a mass campaign target the wrong market?

Did GDPR spur innovation? All six companies initially said no when asked directly and then gave examples that sounded curiously like a new service or marketplace. The technology SME had added a self-service facility so that clients could interrogate and edit their own details, i.e. a do-it-yourself SAR. The IT outsourcer's business had boomed as it raced to develop new services to respond to clients' GDPR-related demands. Likewise, the law firm had had to recruit extra staff to handle the GDPR workstreams, opened a new branch office in the US to advise local firms with interests in Europe and expanded a GDPR-compliant legal technology platform service to its clients who needed to pool and overview legal matters internationally. The bank noted it had seen the RegTech sector expand which meant it had a wider selection of GDPR compliance systems to choose from.

To sum up, GDPR made companies upgrade their IT, some superficially and some more fundamentally and, it has spurred growth of the GDPR support services industry.

5.1.3 Reputational Signal. Reputation management is about sending the right signal to the right stakeholder. Does GDPR compliance by a company, communicated via their public privacy policies and online cookie consent notices, enhance a company's brand and reputation? Do consumers trust it more? Interviewees tied themselves in knots considering this. Many started with a flat *"No"* or, slightly less dismissively, *"I don't think it is high up in people's minds [...] since the legislation is no longer a choice and we all have to be*

compliant" (P2) or *"it's a minimum standard"* (P3). The recognition *"it's a necessary element of doing business"* (P1) morphed into *"I think failure to do it can impact negatively"* (P7) and *"It is a hygiene factor. If you are not GDPR compliant, you've got a problem"* (P10).

The concept of hygiene factors dates to psychologist Frederick Herzberg's two-factor theory of worker motivation [32], which marketers later adopted to mean the basic set of values that customers expect to be in place for any business or service they consider purchasing. In mathematics, it would be described as a necessary but not sufficient condition. *"Everyone wants to see that you are obeying looking after your data"* (P4). When asked about trust, a lawyer said, *"The customer expectation is higher. I'd say expectation more so than trust is higher"* (P7). In contrast, a marketer said, *"People are looking for brand purpose. They're looking for brands with meaning. They're looking for a brand with authenticity. They're looking for brands that do the right thing"* (P8). Referring to marketing communication, another said, *"From a client point of view, they know that you are only sending them stuff that they want to receive"* (P14).

So, some companies regard GDPR merely as a box to be ticked and some regards it as a signal and trust builder. Some use it to send a signal of *"reassurance"* (P14) that the consumer will not be spammed. Some use it to say we care about your data, and you can trust us. In fact, one CISO believed that their ISO27001B certification was an indirect benefit to the customer because it tells the customer *"we actually take security seriously"* (P12). In an online world where service experience is relatively undifferentiated, reputation is a key differentiator and GDPR compliance may now be part of it. Half of the sample chose to regard it as a lever and half thought it was a hygiene factor at best.

5.1.4 Standardisation. Standardisation is often seen as a positive output from regulation. The theory is that technical standards facilitate faster economies of scale on the supply side and provide the comfort of mind to encourage more rapid take-up on the demand side. GDPR might seem an unlikely exemplar, but three cases came to light that delivered direct business benefits.

In the first case, a small and medium-sized enterprise (SME) that did a lot of business with the public sector described how time-consuming it used to be to bid for a new project because each *"organisation would write their own requirements around privacy"* (P1). Now GDPR has made responding to formal tenders for new business a quick box-ticking exercise instead.

In the second case, the drinks company standardised its customer database *"so for an international company we have a lot more consistency and assurance across the group"* (P7). It used to have to consult individual countries on the online and offline product packaging before every new product launch. Now GDPR means they can save time and say *"here is a policy and here is a language"* (P7).

In the third case, the banker liked the way GDPR neutralised a perceived weakness relative to more aggressive banks *"From a marketing perspective, the fact is that we all had different interpretations of what you can and can't do"* and approval sat with *"how strong our risk function was and [...] how militant it was. That is where oversight was"*. He felt *" you are at a competitive disadvantage with a stronger risk function."*(P12) but now *"it's good to know that all companies are legally bound by these GDPR rules"*.

The last example may also qualify as a demonstration of the benefit of a level playing field which the EU regularly messages as a benefit of EU-wide regulation in general. Not all respondents accepted this rationale behind GDPR and felt that the EU was *"trying to make it sound more for the companies but we all know it was for the consumer. They did it for people rather than the companies"* (P11).

5.2 Indirect Impacts

5.2.1 Powerful GDPR Advocates. Andrew Jackson, seventh president of the United States, is credited with the saying *"money is power"*. Within companies, this translates into budget is power, and nowhere is this more apparent than the power that GDPR has conferred on specific roles within companies to invest in compliance. One lawyer was quite frank: *"I am a boring lawyer, but I think the fact there's robust legal obligations has made business ensure compliance at a speedier rate than usual. [...] The level of fines makes for a great headline when you're running training and trying to get everyone's appreciation"* (P7).

GDPR has transformed the authority of the department responsible for it—usually Legal, Risk or Compliance—and made it an essential player in corporate data-related decision making: *"It has raised awareness of the compliance team. [...] People take compliance a lot more seriously"* (P9).

It may seem the main benefit of a beefed-up GDPR-legal resource is fine limitation. The lawyers cited other benefits such as reduced paper storage costs, greater awareness of the importance of cyber insurance, tighter scrutiny of third-party supplier contracts and more attention to where the data in the cloud resides to ensure the EU GDPR regime covers it.

5.2.2 Improved Data Management and Security. The other budgetary beneficiary is the IT department. One CISO (P12) believed GDPR *"did raise the bar for visibility of information security [...] in the past [...] it was regarded as a nice to have. [...] Not many companies actually had a security department"*. This CISO also thought that *"GDPR focused people's minds that if you let the data get out, then it could conceivably bring down the company"*. Another CISO (P10) described how they work with risk and compliance to document risk and list controls they had against those risks so that when they suffer a breach, an inevitability in their view, they can demonstrate to the regulator they had made a proportionate investment to meet their obligations to the spirit and letter of the legislation.

Thus, the budget has been invested in information security infrastructure, resilience, and eliminating single points of failure. Another focus is security awareness training for the workforce. The investment has resulted in streamlined processes, efficiencies and cost savings. It has motivated companies to take a holistic view of security rather than *"sticking the firewall in the way"* (P12). It has meant that the customer database is constantly cleansed and deduplicated to ensure client notification preferences are up to date, which in turn means the advertising is targeted at customer and prospective customers who are genuinely interested in the company's product or service. As one marketer put it, prior to cleaning up our data and duplicates, *"we used to have multiple versions of the truth"* (P13).

5.3 Challenges

5.3.1 New Business Development is Harder. A key part of new business development is identifying, qualifying and converting suspects into prospects and prospects into customers. A pipeline of leads is generated via a variety of means such as advertising, social media and email marketing campaigns.

The biggest drawback of GDPR for one SME was *"finding effective ways to find new customers"* (P1). He recounted how, before GDPR, their resellers made it a precondition that users had to agree to receive spam before their service was activated. Even though it has been against EU law to send unsolicited commercial emails or texts for almost 20 years, it seems to have taken the introduction of GDPR to get the message finally through to business because it changed the rules of consent and strengthened people's privacy rights.

Smaller companies felt GDPR had little effect on them since they were never great spenders on advertising in the first place. However, on exploring the application of the data minimisation principle, there was a dawning realisation by all the SMEs that it had affected them. In practice, they had stopped asking for more information than strictly required so that it could be used again in later campaigns. Previously, they used to periodically re-market to historic enquirers, ex-customers, or lapsed subscribers as a matter of routine.

Larger companies thought it had made their marketing more targeted and effective because they only communicated with genuinely engaged consumers who had already opted-in to receive marketing communications: *"GDPR forces us to categorise customers according to their wishes and to segment the communication we send them"* (P13).

The flip side for marketers is that it made it harder to build the brand if they were only allowed to talk to the *"converted"* (P8). It also made it harder for IT in large companies if they had multiple streams of leads (referrals from the parent company or associate companies, web enquires, responses to marketing campaigns, Facebook, Linkedin, Twitter, Google ads) because they had to deduplicate the customer to ensure their preferences were captured correctly and thereby avoid complaints about receiving unwanted marketing communications.

5.3.2 Direct & Indirect Costs. How companies experience the cost of regulation varies widely. One SME remarked he expected the costs to be more, but their only cost was the *"minimal"* ICO (UK Regulator) fee (P1). Another SME believed their costs had gone up because they had moved everything to GDPR-compliant cloud providers and assumed their transaction fees included a GDPR component. In general, apart from explicit GDPR-related costs such as cookie notice plug-ins, SMEs found it difficult to pinpoint additional costs.

Larger companies found it easier because they had made more extensive investments in systems, processes and manpower. One company estimated *"15% of our legal budget in the last year was probably on data protection"* (P7). Another put it at less than 5% (P10). In addition to direct costs, there were indirect opportunity costs. A Global IT Director described GDPR as *"stifling"* and *"distracting"* (P10). He complained that GDPR projects always trumped other innovative projects such as process automation. Another complained that they had lost business due to GDPR because it made the company so reluctant to share referrals or client information with associate companies in other EU countries.

Attitudes to the added expense vary depending on the department. Marketing sees it *"as an additional burden"* (P11). They complain *"they have no time and no budget for it"* (P11) and it makes their campaigns uncompetitive against players willing to sail closer to the wind. In contrast, IT see the bureaucracy as *"a cost worth bearing"* (P12) if it brings *"sensibility"* (P12) to an organisation.

5.3.3 Grey Areas of Law. Unsurprisingly, non-legal and legal interviewees had different perspectives on the state of the law. Most SME management did not have an opinion apart from a shared consciousness that they lacked in-house compliance knowledge. Some expressed worries about loose data hygiene by staff working from home. Some worried about SARs and how much disclosure was required. All thought they had outsourced responsibility for security under GDPR compliance to their GDPR outsourcers.

Participants who did have contact with GDPR complained simultaneously that GDPR was over-prescriptive and under-prescriptive. For example, some believed they should be trusted to use their professional judgement and take a risk-based approach to issues. Otherwise, *"GDPR is often like using a sledgehammer to crack nuts over things [...] put barriers where they otherwise wouldn't need to be"* (P9). Others wanted more precision about technical solutions and data retention periods. Despite their best efforts to be GDPR compliant, one marketer bemoaned, *"how transparent is transparent? [...] how much do you really have to spell it out [...] to be really clear enough"* (P8) after the Legal department had blocked their re-use of data collected during a campaign that had been designed to gather new leads.

A lawyer described the ambiguity that they experience whenever they suffer a data breach: *"I regularly go to external counsel to get their view and they never have a definitive answer. It is always from experience, or we'll have to wait and see"* (P7). Another lawyer described how they pore over ICO investigations to understand the decision-making and the findings that triggered the fines.

Some worried about GDPR in the UK after Brexit if there is a negative EU adequacy decision. One IT executive in a large company described it as *"utterly bonkers"* (P10) because *"the damage it would do to both the UK and European economy would be just politically unacceptable."* The executive also thought they'd have to have two platforms––UK and non-UK-—if the EU failed to find the UK was offering an adequate level of data protection.

5.3.4 The Data Audit Dividing Line. Data audits distinguish the big from the small. When asked about the impact of data audits on their business, one SME responded, *"What's a data audit"* (P1). Two other SMEs were uncertain and assumed their GDPR IT outsourcer had taken care of it. On follow-up, one of the IT Services companies confirmed they stored the data and advised their clients, but *"this is where it gets a little bit complicated [...] they need to know where the PII is themselves"* (P3).

Large companies approach it differently. They all do data audits. They find them time-consuming, but they appreciate they are *"a good thing"* (P7). One IT executive remarked, *"It may be a pain in the backside, but once you've done it once, then at least you know*

where everything is. […] And you will be able to follow data around your organisation" (P12). Another lawyer described how they had undergone two audits—-in-house and external-—and opined: *"I found the audits helpful […] you can leverage off […] and show the reports to the directors and say either look how well I am doing in this area […] or we scored low here"* (P7). Data audits are powerful tools in big business for building business cases for investment.

5.3.5 The Weaponisation of Subject Access Requests (SARs). One SME has never received a SAR. In another SME, the CEO had dealt with a handful personally. As companies scale up in size and customer base, satisfying SARs can become more challenging.

The CEO of a medium-sized company described vividly the pain of dealing with disgruntled customers who use SARs

> *"as a stick to beat us with. They'll put in a SAR […] just to be awkward. They're saying '[…] you have inconvenienced me, so now I'm going to inconvenience you.' Are they entitled to every internal email? They have rights to everything, but I'm saying, 'but why? Why should they?' [Perhaps] we'll do it offline [in future]."* (P2)

Larger companies described similar issues with customers and, even more problematic, ex-employees. Some companies found it difficult to differentiate between emails that plainly referred to the ex-employee and deserved to be released and those that mentioned the ex-employee in a performance report alongside other employees. *"we've had an employee one that was horrendous […]going through emails at what you can redact […] I've seen from an employer perspective and it's very much weaponized"* (P7). Other companies adopt a more proportionate response to SARs and require a precise aim.

Actioning the right to be erasure is also problematic *"the systems are not set up to make it easy to remove those people. It's not built into Microsoft systems. There is not a right to forget button that goes right across all your Microsoft systems files and folders"* (P12).

5.4 Suggested Improvements to GDPR

At the end of the interviews, people were asked for their ideas on how could GDPR be made better. There was a certain amount of special pleading and wishful thinking. Nevertheless, the feedback points to ways in which GDPR could be made more accepted and more effective in achieving its goals.

5.4.1 An SME-lite Version. All the SMEs felt GDPR was overkill for companies like them that hold truly little data compared to Big Data companies. One CEO queried why they should be held to the same standard as a medical institution that holds sensitive personal data. *"The rules I have to follow should not be the same ones as Goldman Sachs has to follow"* (P5). The desire for simplification is understandable. Unfortunately the rights-based nature of GDPR hardly lends itself to differential watering down of protections for customers of SMEs but not of big business. Nevertheless, in practice, the regulator could consider applying the same principles on SMEs in a more proportionate manner.

5.4.2 Reframe It. A marketer suggested the regulator should demystify and reframe the message. *"Less a pain in the arse type thing […] bring to the fore the real benefits […] in a more creative way"* (P8). This may seem an unusual demand, but marketing spin is not alien to the EU Regulators. After all, most GDPR updates since 2019 usually include references to the benefits of the level playing field (LPF) and the competitive advantage to business of compliance. However, these messages do not resonate with this sample of companies. The LPF is irrelevant to SMEs who are typically domestic in focus and not material for larger companies if they already have operations in other countries. NOne of the respondents believed GDPR conferred a competitive advantage to them within the EU (because everyone must abide by it) and some saw it as potentially a disadvantage in non-EU countries if the competition is not saddled with the same restraints.

5.4.3 Share It. The GDPR expert in the bank felt the UK Regulator failed to support big business. *"There is nothing to encourage people or companies to share best practice. There is not a forum […] or platform […] where the professionals can go and ask questions or share what works for them"* (P11). At the other end of the expertise spectrum, the CEO of a SME felt let down for different reasons *"I looked for checklists […] on government sites. Everyone is trying to get me to take a course to get a certificate in GDPR compliance"* (P5). All they wanted to know was *"what are the major things we should concentrate on"* (P5).

5.4.4 Clarify It. Most respondents thought GDPR had brought legal clarity to the situation. Article 6 of GDPR is clear about the six lawful bases for one to process (collect, store, use etc.) people's data. However, the legal practitioners still felt there was a need for clarity on the wording in some instances, e.g., co-processor, international data transfers. *"I did a Certificate in Data Protection Law […] and at one stage I was about as qualified as you could be, which was a bit of a joke, because I didn't know more than anybody else. You go to talk to a law firm [about a case]. They have more experience but it's not necessarily they know more […] until there is more case law"* (P7). Like the previous point about sharing learning, there seems a clear opportunity for the regulator to take a more proactive role in this area.

5.4.5 Loosen it. Some of the legal practitioners chafed against the rigidity of the rules. They argued that the regulator should allow a more commercial or risk-based approach of the rules for an informed professional such as happens with anti-money laundering. Questions remain about how this would work in practice including how such an approach is compatible with the fundamental rights character of data protection and how a risk-based approach could be made consistent. The other concern is the notion of risk itself and the risk thresholds (to the consumer?) that would need to be satisfied before GDPR could apply.

5.5 Counterfactual: What if GDPR didn't exist?

This counterfactual scenario was added to the agenda after it arose organically mid-way into the research. When asked what they would be doing differently with customer data if GDPR wasn't here today, the consensus was that they'd hold more data, hold it for longer, use it for multiple purposes and not worry so much about the security. *" I'd like to say it wouldn't be that different because we want to, […] from an ethical perspective, […] to put in these controls anyway, but I think that would be being a bit disingenuous. I'm sure that we just have a lot less control because we're not being forced to, so*

we just wouldn't. And. We would store data for a lot longer and we give a lot[…] more people access to the data" (P10). The lost freedom to proactively market to ex-customers or cross-sell to other customers in different subsidiaries of the bank was uppermost in the mind of the CMO *"Ultimately the scale of our marketing opportunity would be that much larger"* (P13) if GDPR didn't apply today.

6 DISCUSSION

6.1 The benefits of GDPR to business

Whilst one should be cautious generalizing from a small sample, our findings are drawn from broad-based conversations with senior and junior executives across the functional spectrum of organisations and they show that GDPR has had a common range of effects on business at large.

The threat of fines has changed the mindset of companies. In a world where data privacy is getting ever more important, GDPR has forced companies to catch up with their clients' desires and wishes to serve them only what they want to be served and use their data only in the way they want it to be used. It has forced companies to clean-up their act. This is a win-win for companies and society.

The threat of fines has changed the data infrastructure of companies. In a world where compliance projects trump non-compliance projects, GDPR has forced companies to modernise and upgrade their data management, data quality and information security. In possibly a one-off hit, GDPR has gifted companies a reason to invest in projects, such as rationalising legacy databases, that they knew were important but kept putting on the long finger. It has delivered many of the 'usual' benefits of an IT project directly to companies whose technology was sub-optimal and it has indirectly benefited companies whose technology was adequate but still required enhancements to meet the regulations.

Contrary to the common perception that regulation adds complexity, GDPR has delivered standardisation benefits by streamling processes in some situations cited in our research. It is also used by some companies to signal their privacy credentials in the belief it enhances their brand and reputation.

Our findings on benefits do not tally with many of the projected benefits in earlier literature. The area of agreement is around improved data management process [9, 24], use of analytics [26] and increased security [36]. There is some equivocal overlap in the area of reputational enhancement [8, 53]. We found some marketing participants shared the same belief. However, many of the other assertions such as improved consumer confidence [13] and trust [13, 17], legal clarification [17], competitive advantage [13] and cost reduction [45, 41, 8, 42] were not supported by our findings. The size of the GDPR fining system was well understood in advance, but the transformational effect it was going to have on corporate psychology was under appreciated.

6.2 The changing balance of power

Our findings show that the impacts of GDPR are felt differently within a business. It has created new power bases within companies. Depending on the industry, it will have a different name, but typically GDPR expertise sits in the Risk, Compliance or Legal department and the IT/IS or Information Security department. Both have enjoyed boosts to budgets and headcount. Suffering a high-profile data breach that could destroy a company's reputation and potentially suffering a big-ticket fine that could ruin a company's finances has meant that GDPR risk continues to be a board agenda item. This means both departments continue to be more involved with corporate-level data decision-making than before. It also means that Marketing has a high quality, more up-to-date database of customers and their communication preferences.

So, while Legal and IT may be winners, are there losers? Yes. There are direct and indirect losers. The most obvious are the executives spread across an organisation who championed projects that were delayed or killed in competition with higher priority GDPR initiatives. Less obvious are senior management. Their discretion was hemmed in pre-GDPR by the need to prioritise GDPR-readiness. Their discretion is now policed by Legal or IT departments who follow breach investigations zealously and remind them that GDPR compliance is an ongoing commitment. The indirect losers are the departments that have to handle the extra workload generated by GDPR compliance, e.g., Human Resources having to negotiate with disgruntled ex-employee SARs, Customer Service having to deal with dissatisfied customer SARs and Marketing having to constantly update customer notification preferences. A lawyer said *"I think if you were to ask a marketing person what are the benefits […] I think they might struggle to articulate some benefits"* (P7). Another lawyer characterised the perception of their role and GDPR, *"From a marketing perspective […] they see it as a stopper"* (P11).

A lasting legacy of GDPR is a shift of power. It has put non-commercial functions, which were hitherto regarded as support functions, at the heart of strategic decision-making. The long-term implications of this remain to be seen, but one can make some educated guesses. As GDPR beds down and regulators become more comfortable issuing fines (based on precedents in other EU countries), the influence of these groups will increase rather than decrease. Senior management will become exasperated with box-tickers and binary thinkers and may seek to recruit people with different skill sets and risk appetites. Conversely, if enforcement by regulators is timid and the threat landscape is perceived to be less draconian than expected, senior management may decide to game the system and put the box-tickers back in their box.

The introduction and operation of GDPR is not a rational application of a new data protection regulation. It is a benefit, a tool or a weapon of power whose promotion is contextualised by different groups within an organisation that have different aims and methods of leverage. Even actors, such as ex-salespeople who would normally rail against GDPR constraints, weaponise SARs to their own ends creating unintended consequences.

To the best of our knowledge, this disruptive change in power dynamics has not been anticipated in earlier information security literature.

6.3 Implementation issues remain

GDPR is not without its disadvantages. This was not the primary focus of our research but we identify a number of challenges. New business development and intra-company communication is more

constrained. Regulation has increased costs and internal bureaucracy. Grey areas remain due to a lack of case law. Disgruntled customers and employees weaponise SARs as a tool of retaliation.

Our findings on challenges tally with many of the issues identified in earlier literature. The complexity of GDPR, its lack of specificity, its subjectivity, the cost overhead, the difficulty recruiting and retaining expert staff and operationalising the right to erasure were all well anticipated. The restrictions on marketing were known in theory but the effect on new business development in practice was underappreciated. The chilling effect on intra-company communication does not appear in earlier literature. On the other hand, some hypothesised downsides, such as companies withdrawing services in the EU to avoid GDPR, did not ever come up in conversation.

When we asked our participants for ideas as to how to improve GDPR, we find that they believe that regulators should re-frame GDPR messaging to be more positive, sponsor forums to facilitate the sharing of learning and coping strategies, clarify policies and apply lighter standards on small business.

Existing literature does not consider getting business buy-in to GDPR. The emphasis is more on the punitive power of GDPR. In contrast, the literature has long recognised the need to simplify and clarify its requirements.

7 CONCLUSION

GDPR is a regulation that is designed to safeguard EU citizens' data privacy. The benefits to the consumer and the regulator and the downsides to business are relatively predictable. What we were interested in exploring however is whether there are any benefits of GDPR to business and how they might affect the different parts of an organisation. To our knowledge, nobody has looked at this from the perspective of business since GDPR came into effect in May 2018.

Using semi-structured interviews, we surveyed 14 senior executives responsible for business, finance, marketing, law or IT drawn from 6 small, medium and large companies in the UK and Ireland. We deliberately sampled beyond the IT department, which tends to be the typical target of GDPR surveys, to obtain a fuller picture.

We find the threat of large fines has focussed the minds of business and made it more privacy conscious. GDPR has gifted companies a reason to justify investment in modernising their data management processes and security. Companies have cleaner and more up-to-date customer databases. In the absence of GDPR, companies admit they would ask for more information than necessary, use it more frequently, hold it for longer and keep it less securely.

It has created new power bases within organisations that act as guardians or champions of privacy. Such in-house regulators will continue to enjoy influence on corporate decision making provided the regulators maintain a steady news flow on enforcement actions against offenders and data breaches.

We find that many implementation issues exist that would benefit from better communication, guidance and simplification by the EU and its regulatory arm.

In summary, GDPR may be a headache to business but it has made it more careful with data. Judged by that standard, GDPR has been a successful socio-technical regulation because it has made companies put their house in order to their own benefit and to the benefit of wider society.

7.1 Limitations

There was little empirical research to compare and contrast our findings. The study is based on a small sample size and may affect generalizability confidence. The participants do not have the same job profile in each company. This is partly due to smaller companies having general managers who hold multiple briefs and larger companies having executives who are responsible exclusively for a department such as technology or compliance.

7.2 Future Work

Future work could pursue several avenues. One could repeat the research with a larger sample population to support the generalisability of any findings; or repeat the research in other EU countries or industrial sectors and compare the differences; or analyse and compare how the power dynamics evolve within companies as the real risk of fines becomes clearer over time; or analyse the enforcement records of national regulators and the perceived compliance of industry in their jurisdiction. Alternatively one could review recent initiatives to make GDPR more proportionate in its application to SMEs whilst maintaining consistent protection of consumers' rights.

ACKNOWLEDGEMENT

We thank the anonymous reviewers, our shepherd Mark Burdon, and all attendees of NSPW '22 for their constructive feedback. Gerard Buckley is supported by UK EPSRC grant no. EP/S022503/1.

REFERENCES

[1] Maria Addis and Maria Kutar. 2018. The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness. *UK Academy for Information Systems Conference Proceedings 2018*.

[2] Sushant Agarwal. 2016. Towards dealing with GDPR uncertainty. In *11th IFIP Summer School on Privacy and Identity Management*, 1–7.

[3] Darcy W. E. Allen, Alastair Berg, Chris Berg, Brendan Markey-Towler, and Jason Potts. 2019. Some Economic Consequences of the GDPR. *Economics Bulletin*, 39, 2, 785–797. DOI: 10.2139/ssrn.3160404.

[4] Gonçalo Almeida Teixeira, Miguel Mira da Silva, and Ruben Pereira. 2019. The critical success factors of GDPR implementation: A systematic literature review. *Digital Policy, Regulation and Governance*, 21, 4, 402–418. DOI: 10.1108/DPRG-01-2019-0007.

[5] Ausloos, J. and IViR (FdR). 2020. *The Right to Erasure in EU Data Protection Law*. Publication Title: Oxford Data Protection and Privacy Law. Oxford University Press. DOI: 10.1093/oso/9780198847977.001.0001.

[6] Robert Baldwin, Martin Cave, and Martin Lodge. 2011. Regulation and the European Union. In *Understanding Regulation*. (2nd ed.). Oxford University Press, Oxford. ISBN: 978-0-19-957608-1. DOI: 10.1093/acprof:osobl/9780199576081.003.0019.

[7] Robert Baldwin, Martin Cave, and Martin Lodge. 2012. *Understanding regulation: theory, strategy, and practice*. (2nd ed ed.). Oxford University Press, New York. ISBN: 978-0-19-957608-1 978-0-19-957609-8.

[8] Phil Beckett. 2017. GDPR compliance: Your tech department's next big opportunity. *Computer fraud & security*, 2017, 5, 9–13. DOI: 10.1016/S1361-3723(17)30041-6.

[9] Colin J. Bennett. 2018. The European General Data Protection Regulation: An instrument for the globalization of privacy standards? *Ip*, 23, 2, 239–246. Soon Ae Chun, Nabil R. Adam, and Beth Noveck, (Eds.) DOI: 10.3233/IP-180002.

[10] Stephane Ciriani. 2015. The Economic Impact of the European Reform of Data Protection. *Communications & Strategies*, 97, 41–58, 1st quarter 2015.

[11] European Commission. 2020. Communication from the Commission to the European Parliament and the Council. (2020). DOI: 10.1163/2210-7975_HRD-4679-0058.

[12] Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, and Ignacio Sanchez. 2018. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer law & security review*, 34, 2, 193–203. DOI: 10.1016/j.clsr.2017.10.003.

[13] Laszlo Dellie. 2019. GDPR Compliance as a Competitive Advantage. ISACA. Retrieved May 28, 2021 from https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/gdpr-compliance-as-a-competitive-advantage.

[14] Deloitte. 2018. GDPR Six Months On. London, UK.

[15] Edward S. Dove. 2018. The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. *J law med ethics*, 46, 4, 1013–1030. DOI: 10.1177/1073110518822003.

[16] Dr John Paul Salter. 2020. What does a level playing field mean? (2020).

[17] Daria Dubrova. 2018. Challenges and Benefits of GDPR Implementation. The App Solutions. Retrieved Apr. 20, 2021 from https://theappsolutions.com/blog/development/gdpr-challenges-and-benefits/.

[18] Estelle Masse. 2021. Three Years Under GDPR. Tech. rep. Access Now.

[19] EU Agency for fundamental rights. 1981. Article 8 - Protection of personal data. (1981).

[20] European Commission. 2019. General Data Protection Regulation One Year On. Press Release IP/19/2956.

[21] European Commission, Directorate General for Justice and Consumers. 2020. EU: Multistakeholder Experts Group publishes contribution on GDPR evaluation. DataGuidance. Retrieved Apr. 8, 2021 from https://www.dataguidance.com/news/eu-multistakeholder-experts-group-publishes.

[22] European Parliament and of the Council. 2016. Regulation (EU) 2016/679. *Official Journal of the European Union*, 119, 1.

[23] European Union. 2022. General data protection regulation (GDPR). (2022).

[24] Michael Fimin. 2018. Council Post: Five Benefits GDPR Compliance Will Bring To Your Business. *Forbes*.

[25] Maria da Conceição Freitas and Miguel Mira da Silva. 2018. GDPR Compliance in SMEs: There is much to be done. *Journal of information systems engineering & management*, 3, 4. DOI: 10.20897/jisem/3941.

[26] Joe Garber. 2018. GDPR – compliance nightmare or business opportunity? *Computer fraud & security*, 2018, 6, 14–15. DOI: 10.1016/S1361-3723(18)30055-1.

[27] GDPR.EU. 2018. What are the GDPR Fines? (2018).

[28] GDPR.eu. 2019. GDPR Small Business Survey. Proton Technologies AG.

[29] Gloria González Fuster. 2014. The Materialisation of Data Protection in International Instruments. In *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Law, Governance and Technology Series. Gloria González Fuster, (Ed.) Springer International Publishing, Cham, 75–107. ISBN: 978-3-319-05023-2. DOI: 10.1007/978-3-319-05023-2_4.

[30] Greg Guest, Emily Namey, and Mario Chen. 2020. A simple method to assess and report thematic saturation in qualitative research. *PLOS ONE*, 15, 5, e0232076. DOI: 10.1371/journal.pone.0232076.

[31] Hemback Legal. 2022. Article 8 ECHR - Right to private life, family life, correspondence and home. (2022).

[32] Frederick Herzberg, Bernard Mausner, and Barbara Bloch Snyderman. 2017. *The Motivation to Work*. (1st ed.). Routledge. ISBN: 978-1-315-12482-7.

[33] Wang Kaushik. 2018. Data Privacy: Demystifying The GDPR. iSchool | Syracuse University. Retrieved June 21, 2021 from https://ischool-dev.syr.edu/data-privacy-demystifying-gdpr/.

[34] Joanna Kessler. 2019. Data Protection in the Wake of the GDPR: California's Solution for Protecting "the World's Most Valuable Resource" Notes. *S. cal. l. rev.*, 93, 1, 99–128.

[35] Javid Khan. 2018. The need for continuous compliance. *Network security*, 2018, 6, 14–15. DOI: 10.1016/S1353-4858(18)30057-6.

[36] Judica Krikke, Erik Valgaeren, and Gérald Origer. 2019. GDPR: What are the challenges? Stibbe. Retrieved May 30, 2021 from https://www.stibbe.com/en/expertise/practiceareas/data-protection/general-data-protection-regulation/what-are-the-challenges.

[37] He Li, Lu Yu, and Wu He. 2019. The Impact of GDPR on Global Technology Development. *Journal of global information technology management*, 22, 1, 1–6. DOI: 10.1080/1097198X.2019.1569186.

[38] Peter Lindgren. 2016. GDPR Regulation Impact on Different Business Models and Businesses. *Journal of Multi Business Model Innovation and Technology*, 4, 3, 241–254. DOI: 10.13052/jmbmit2245-456X.434.

[39] Isabel Maria Lopes and Pedro Oliveira. 2018. Implementation of the general data protection regulation: A survey in health clinics. In *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. DOI: 10.23919/CISTI.2018.8399156.

[40] Orla Lynskey. 2015. *The foundations of EU data protection law*. Oxford University Press.

[41] Gary Miglicco. 2018. GDPR is here and it is time to get serious. *Computer fraud & security*, 2018, 9, 9–12. DOI: 10.1016/S1361-3723(18)30085-X.

[42] Ralph O'Brien. 2016. Privacy and security: The new European data protection regulation and it's data breach notification requirements. *Business information review*, 33, 2, 81–84. DOI: 10.1177/0266382116650297.

[43] OECD. 2022. Entrepreneurship - Enterprises by business size. (2022).

[44] Oxford Analytica. 2019. Europe's national regulators hold key to GDPR success. *Emerald Expert Briefings*, oxan-db, oxan-db. DOI: 10.1108/OXAN-DB243916.

[45] Rob Perry. 2019. GDPR – project or permanent reality? *Computer fraud & security*, 2019, 1, 9–11. DOI: 10.1016/S1361-3723(19)30007-7.

[46] Eugenia Politou, Efthimios Alepis, and Constantinos Patsakis. 2018. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, 4, 1. DOI: 10.1093/cybsec/tyy001.

[47] Nazar Poritskiy, Flávio Oliveira, and Fernando Almeida. 2019. The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, 21, 5, 510–524. DOI: 10.1108/DPRG-05-2019-0039.

[48] Wanda Presthus, Hanne Sørum, and Linda Renate Andersen. 2018. GDPR Compliance in Norwegian Companies. In *Proceedings from the Annual NOKOBIT Conference*. Vol. 26. Nokobit, Svalbard, Norway.

[49] Amy Kristin Sanders. 2018. The GDPR One Year Later: Protecting Privacy or Preventing Access to Information Essays. *Tul. l. rev.*, 93, 5, 1229–1254.

[50] Sarah Shyy. 2020. The GDPR's Lose-Lose Dilemma: Minimal Benefits to Data Privacy & Significant Burdens on Business. *U.c. davis bus. l.j.*, 20, 2, 137–164.

[51] A. Skendžić, B. Kovačić, and E. Tijan. 2018. General data protection regulation — Protection of personal data in an organisation. In *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, Opatija, Croatia, 1370–1375. DOI: 10.23919/MIPRO.2018.8400247.

[52] David R. Thomas. 2006. A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*, 27, 2. DOI: 10.1177/1098214005283748.

[53] Christina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula. 2018. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer law & security review*, 34, 1, 134–153. DOI: 10.1016/j.clsr.2017.05.015.

[54] Erik van der Marel, Matthias Bauer, Hosuk Lee-Makiyama, and Bert Verschelde. 2016. A methodology to estimate the costs of data regulations. *International Economics*, 146, 12–39. DOI: 10.1016/j.inteco.2015.11.001.

[55] Michael Veale, Reuben Binns, and Jef Ausloos. 2018. When data protection by design and data subject rights clash. *International Data Privacy Law*, 8, 2, 105–123. DOI: 10.1093/idpl/ipy002.

[56] Nick Wallace and Daniel Castro. 2018. The Impact of the EU's New Data Protection Regulation on AI. Centre for Data Innovation.

[57] White, S. 2018. General data protection regulation and the trust of the consumer.

[58] David Williamson, Gary Lynch-Wood, and John Ramsay. 2006. Drivers of Environmental Behaviour in Manufacturing SMEs and the Implications for CSR. *Journal of Business Ethics*, 67, 3, 317–330. DOI: 10.1007/s10551-006-9187-1.

[59] World Economic Forum. 2020. Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators. (2020).

A INTERVIEW FRAMEWORK

Remind and reassure the interviewees that the conversation will abide by the university's ethics code and their contributions will be anonymized. Check they are comfortable with being recorded.

Part 1 Open questions
- Tell me about your job
- Industry sector & Size of company?
- What is your role, your title, your department?
- What does your company / department use customer data for? Describe

Part 2 Open questions
- Are you familiar with GDPR?
- How has it affected your day-to-day work / department / division / company?
- Biggest benefits?
- Biggest challenges?

Part 3 Raise topic areas if they haven't come up in answer to open questions. The benefits checklist is drawn from the academic literature review.
- Company's brand / reputation? Rationale?
- Customer trust level? How do you know?
- Legal certainty? Grey areas?
- Level playing field across Europe; Access to a bigger market for your company?
- GDPR compliance and competitive advantage in EU and in non-EU markets?
- Innovation? Have you seen new products / services?
- GDPR-led growth? Give examples. Investment incentive?
- Advertising? Changes post-GDPR? Targeting?
- GDPR-linked upgrades to internal systems and / or streamlined processes? Examples?
- Security now versus before?

Part 4 Raise topic areas if they haven't come up in answer to open questions. The challenges checklist is drawn from the academic literature review.
- Departmental impacts?
- Company-wide and / or market impacts?
- Compliance cost overheads?
- Data audit impacts?
- Data minimization impacts?
- Data security rigidities?
- Data breaches / Greater liabilities to fines?
- Accountability and governance - how does it work?
- Privacy rights - satisfying SAR's, right to correction and deletion?
- Impact of privacy-first processes on advertising / marketing / servicing customers?

Part 5 Open questions about the future of GDPR
- What makes good GDPR good?
- Any recommendation about how to improve it?
- What would the company be doing different today with data if GDPR did not exist?