Citi GPS

FRESH INSIGHTS

ePRIVACY AND DATA PROTECTION

Privacy Matters: Navigating the New World of Data Protection

Citi GPS: Global Perspectives & Solutions

May 2018

Authors

Catherine T O'Neill is a Director in the Media team covering agencies and media owners. She is based in London and started with Citi in August 2007. She has a BA degree in Sociology from Liverpool. Catherine previously worked at Deloitte from 2003 to 2007 as an auditor in the media sector. Prior to that Catherine worked at the market research agency Ipsos in the Ipsos Loyalty division from 2001 to 2003. In the Institutional Investor All Europe Research Team survey the team was placed 3rd. She is a qualified Chartered Accountant.

+44-20-7986-8053 | catherine.oneill@citi.com

Thomas A Singlehurst, CFA
Head of European Media Research Team

+44-20-7986-4051 | thomas.singlehurst@citi.com

Dan F Homan
European Retail and Apparel & Footwear Analyst

+44-20-7986-4112 | dan.homan@citi.com

Georgios Ierodiaconou
Head of European Telecoms Research

+44-20-7986-4086 |
georgios.ierodiaconou@citi.com

Mark May
U.S. Internet Analyst

+1-212-816-5564 | mark.may@citi.com

Expert Commentators

John Bowman
Senior Principal
Promontory
Financial Group, an
IBM Company

Jan Wittrodt
Senior Lead Data
& IT Law
Zalando

Ingvild Næss
Group Privacy Officer
Schibsted

Telefonica
Data Team

Alexander Hanff
Founder & CEO
Think Privacy

Sector Contributors:

Nick Coulter
Surendra Goyal, CFA
Asiya Merchant, CFA
Ashwin Shirvaikar, CFA
James A Shuck
Kyle Twomey
Ana Chkhikvadze
Ronit Ghose, CFA
Amit B Harchandani
Walter H Pritchard, CFA
Michael Rollins, CFA
Ed Steele
Alicia Yap, CFA
Alvin C Concepcion
Michael Goltsman, CFA
Josh Levin, CFA
Nicholas Jones
Ian Sealey, CFA
Jim Suva, CPA

ePRIVACY AND DATA PROTECTION

Privacy Matters: Navigating the New World of Data Protection

"*We've lost control of our personal data*", Sir Tim Berners-Lee, inventor of the World Wide Web, said in March 2017. The widespread collection of data has led to the rise of data asymmetry and, consequently, consumer trust is low. Some would argue that it has led to the prioritization of profit over privacy. Consumers believe cybersecurity and privacy risks are amongst the biggest risks facing society.[1] The ramifications should not be overlooked by corporates and investors.

In our first Citi GPS report on ePrivacy and Data Protection (Who Watches the Watchers?, March 2017), we highlighted that the focus on data privacy is on the rise and forthcoming changes to regulation in the European Union (this year), will fundamentally alter the risk/reward of using data and, with it, alter the perception of the long-term opportunity from data.

In this follow-up GPS report, with Europe's General Data Protection Regulation (GDPR) less than a month away, we consider how prepared consumers, corporates, and regulators are for the tightening regulatory landscape. More broadly, we consider what the potential implications could be as we move from an environment where organizations have become accustomed to untrammeled access to data, to one where data minimization and transparency presides, consumers are empowered to take more control of personal data, and organizations are forced to think carefully about their use of data. To investigate this we surveyed those involved in implementing the GDPR across a range of organizations and conducted a series of interviews with industry experts from Telefónica, Schibsted, Zalando, and specialist consultancies.

The majority of companies believe they will have to change how consumer data is used which brings with it rising costs (i.e., of compliance). Trust plays a fundamental role and unless consumers believe the value trade is beneficial, access to personal data could fall as consumers are prepared to use their enhanced rights. The application of the regulation (unintentionally) favors those closest to the consumer and large companies vs. small companies. Murky data supply chains are set to see a shakeout. Advertising funded models have been one of the key planks supporting the Internet's development and the online advertising industry appears to be right at the heart of the challenges that regulation presents. As one survey respondent commented: "*The range of plausible outcomes includes total destruction of the online ad ecosystem in Europe all the way to a minor blip*."

Companies claim to be well prepared for the EU regulation change. The 25th of May is D-Day, when the regulation will come into effect, but this is not going to be the end of the process. In fact, it may well be the start of a step change in the approach to data protection regulation globally. We worry corporates and investors are being complacent about the risks.

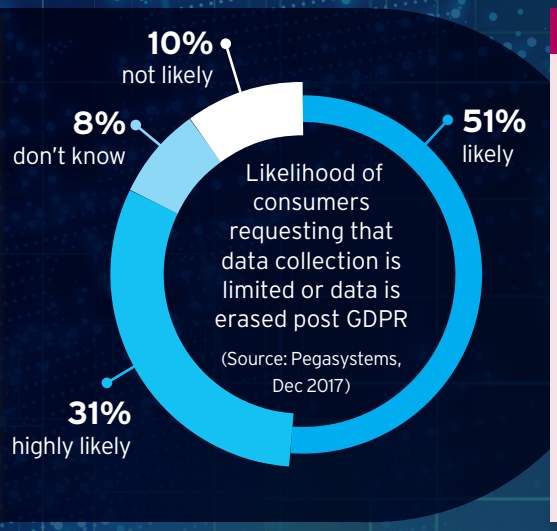
[1] PwC Protect.me Survey 2017.

How ready are we for GDPR?

Organizations have become used to virtually unhindered access to data but widespread data collection has led to consumer mistrust, lack of control over personal data and reluctance to share data. Consumers believe privacy is one of the biggest risks facing society; GDPR awareness is limited but appetite to exercise enhanced rights is high and willingness to consent is low.

21%
of EU consumers are **aware of GDPR**

Source: Pegasystems, Dec 2017



Only
21%
claim they **will provide consent** if asked to share browsing data to tailor offers

Source: Pagefair, Sept 2017

Only
14%
of EU consumers are happy to **share data with third parties**

Source: Symantec, State of Privacy 2015

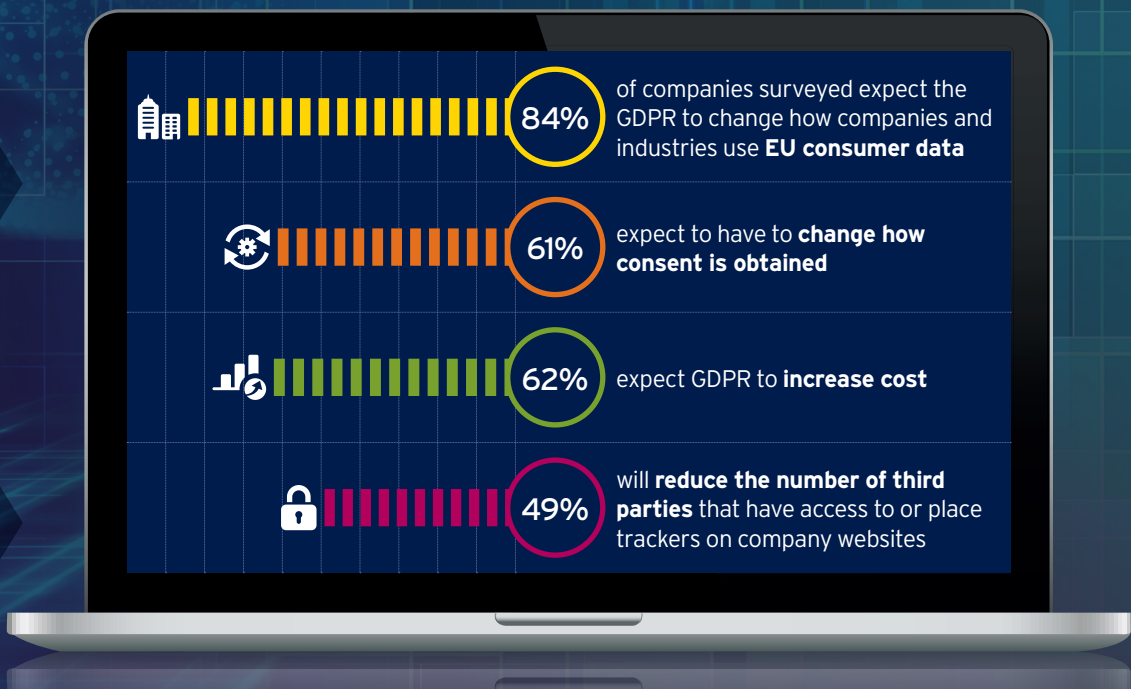
79%
of UK consumers **are not at all willing** to exchange personal data in return for **more personalized content** or **advertising**

Source: YouGov Omnibus Survey, Jan 2018

According to Citi's survey of corporates, preparation for GDPR is well underway and it will lead to a change in how EU consumer data is used

69%
of respondents claim to be **extremely or moderately prepared** for the GDPR

50%
of companies **won't be GDPR compliant** by the end of 2018 predicts Gartner



Regulatory change is expected to favor large companies with strong consumer relationships…But regulators are expected to actively enforce the GDPR and target symbolic cases

18% of respondents expect SMEs to get **weaker** due to GDPR

39% expect incumbent/large companies to get **stronger** due to GDPR

78% of companies expect authorities to very actively/ somewhat actively enforce the GDPR

"The range of plausible outcomes include a total destruction of the online ecosystem in Europe all the way to a minor blip. It's extremely hard to plan with that type of uncertainty. Further there is an irony that the regulation could actually help the largest players."

Source: Citi Research Survey

This could be just the start of a tightening of data protection regulation globally and within Europe. The draft ePrivacy Regulation could have a devastating impact on the online advertising industry

Only **5%** of consumers claim they would **accept all tracking** if browser settings become the gatekeeper

Source: Pagefair

Potential impact: **Up to 70%** reduction in European display advertising revenue;

Digital ad budgets cut by **1/3**

Source: IAB Europe/IHS Markit, WIK-Consult

What are companies saying about changing data protection regulation?

"I think that it really flips the script on what potentially will be a long term, broad reaching phenomenon in other regions, that will have industry-wide impact."

"Companies need almost surgical control of their data, and it seems like most are still using butter knives rather than scalpels."

"As a company that is heavily reliant on ad revenues, the ability to track and target users is vital to campaign performance. With targeting capabilities becoming far more limited, we will potentially see poor advertising performance, which could have a negative impact on ad revenue in the EU."

"It gives consumers the ability to better control their data sharing with the company and will allow us to be more focused on what consumers want."

Contents

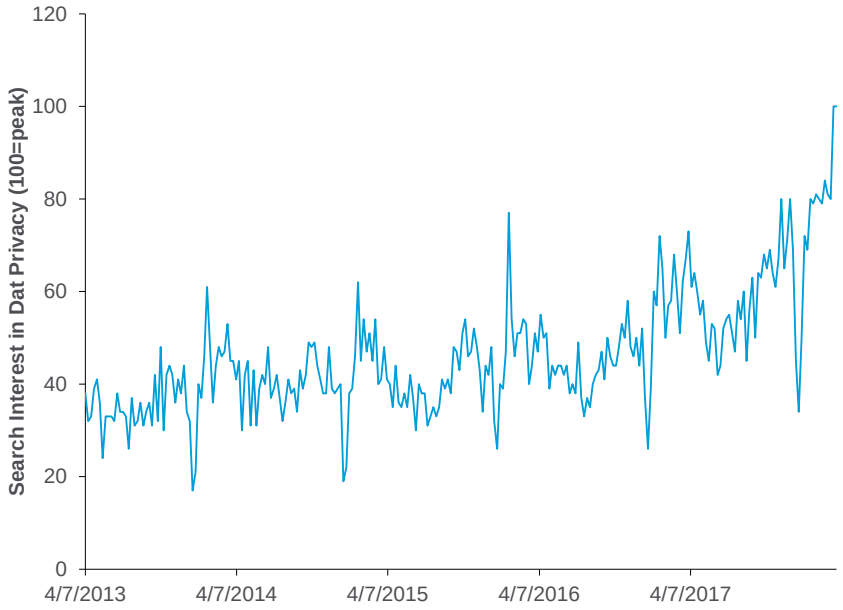
Executive Summary

Our first ePrivacy and data protection-focused Citi GPS report highlighted that pretty much everything we do as consumers online is tracked in some way, shape, or form.

Now for many consumers this will be part of an accepted value exchange whereby information is knowingly surrendered in return for a valued good or service. This said, most consumers may not fully appreciate how much of the data they generate is being collected and how this ends up being used (the recent Facebook/ Cambridge Analytica fallout perfectly highlights this).

In the past year there have been several high profile instances of data breaches, leakages, and data being used in nefarious ways. This goes far beyond 'irritating' ads following you around the Internet. This has become a social and political area of debate. Interest in data privacy is at its peak.

Figure 1. Search Interest in Data Privacy Is at Its Peak



Source: Google

In the original GPS report we concluded that while the focus has been on the opportunities from the usage of big data, the challenges associated with ensuring adequate protection of personal data have been underplayed and underestimated. Europe's General Data Protection Regulation (GDPR), which comes into effect from the 25th of May 2018, represents one of the most significant events in ePrivacy/data protection regulatory history.

We won't outline the requirements of the GDPR here (as this was covered in the original Citi GPS report), but we believe the regulation is a game changer in terms of not only its scope and ambition, with the intention to increase transparency and consumer control over their own data at the core of it (privacy by design and privacy by default), but also the significant penalties for non-compliance (fine for non-compliance of up to 4% of global annual turnover).

It is extremely broad in its reach, impacting almost all sectors to a greater or lesser degree. It could also mark the start of more stringent data protection regulation.

In this follow-up GPS report we consider how prepared consumers, corporates, and regulators are for a tightening of the regulatory landscape. More broadly, we consider what the potential implications could be from a change in the behavior of consumers and corporates when it comes to personal data. The key questions we ask are:

- How will consumer behavior change as they gain more control over their personal data?
- How have companies been preparing for GDPR and what do they see as the challenges and opportunities?
- What is required when consent and legitimate interest are used as the bases for processing personal data?
- How will the use of personal data change and what are the longer-term implications?
- How actively will the regulators enforce GDPR and what is the risk of other regions following the EU's lead in tightening data protection regulation?
- What is the status of the proposed ePrivacy regulation and what are the potential implications if it comes into effect in its current form?

Roadmap to this Report

We break this report into six main sections. Going through each:

- In the first section we look at consumers' willingness to share different types of data for different purposes and **how consumers may use their enhanced rights when GDPR comes into effect**. The main conclusion is that consumers claim to be broadly unwilling to share data, reflecting a general mistrust of corporates (especially online platforms and marketing-related businesses) and an unclear value exchange (especially with third parties). The awareness of GDPR seems to be low (at the moment) but the appetite to exercise new rights is high.
- In the second section we **analyze the results of a proprietary survey we conducted to understand how corporates are preparing for GDPR and what the implications could be from a change in the use of data**. The vast majority (84%) believe GDPR will impact the use of data. Companies may seem confident they are well prepared, but 75% have been preparing for less than a year and whether they will be compliant by the 25th of May is uncertain. Sentiment towards GDPR remains broadly negative — regulation lacking clarity, implementation of systems to manage the new requirements, and obtaining consent were all cited as the most challenging aspects. It is the latter challenge that could pose the greatest risk due to the reluctant stance of consumers (especially for personalized ads and recommendations).

- The third section looks at **how regulators might approach enforcement and whether other regions could follow Europe's lead in tightening data protection laws**. The majority of corporates expect the regulators to be active in their enforcement of GDPR and, even if the general view is that the maximum fine is unlikely to be issued in year one, the threat of a fine of 4% of global annual turnover should be enough to prompt companies to take the regulation seriously. While large companies may be advantaged (unintentionally) by the regulation on many levels, they are also likely to be watched much more closely by the regulator. There are signs that data protection regulation is being tightened across several regions.

- In the fourth section we **dig into consent and legitimate interest as bases for processing personal data and what it really means from a practical standpoint**. Both are areas that have caused a lot of confusion and led to wide ranging interpretations, but both bases favor those with existing (strong) relationships with customers. The need to provide an equivalent service, under the consent requirements, to those users who don't consent to the use of personal data could lead to the rise of paid access and incentive schemes. There may even be a 'loophole' that some will use to justify the collection of data for online advertising and recommendations as a legitimate purpose. The guidance on legitimate interest leaves it open to some level of interpretation and many will see it as preferable to going down the consent route but there will be a fine line between what is acceptable and what is deemed to be intrusive.

- Section five **outlines the proposed ePrivacy Regulation, the next steps and potential implications for online advertising**. Organizations' general awareness of the proposed regulation is below 50% but amongst tech companies it is much higher. The potential regulation could be watered down yet, but if this does not happen it could have a devastating impact on the online advertising industry and future innovation as consent becomes the be all and end all in being able to collect data (not just personal data) and legitimate interest is not an option (with fine levels the same as GDPR). Some industry studies estimate online advertising revenue could come down by a third and there could be up to a 70% cut to display advertising in Europe.

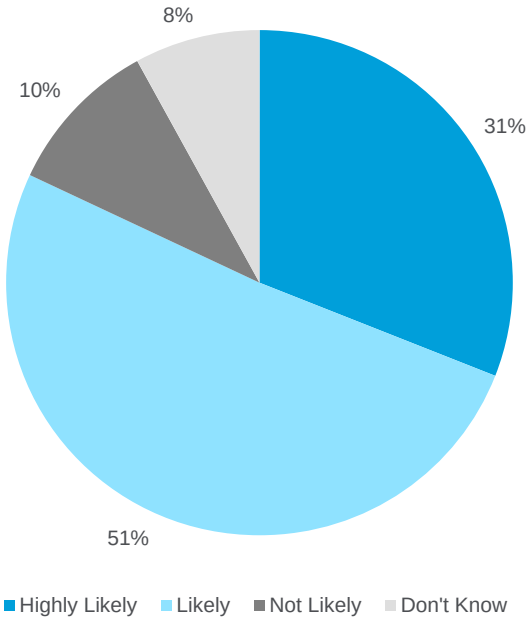
- In the sixth section we delve into many of these topics via **in-depth interviews with a number of experts in the privacy space across a range of industries**. It includes conversations with senior executives at Telefonica, Schibsted, and Zalando, as well as consultants (Promontory Financial Group, an IBM Company and Think Privacy).

Headline Conclusions

We reach seven main conclusions on the back of this work:

- **As of the 25th of May 2018 the majority of organizations will change how personal data is used in Europe (if not in other markets)**, prompted by the tightening of data protection regulation and a growing awareness amongst consumers (who will be in possession of enhanced rights) that the value exchange has increasingly tilted in the favor of organizations. The interpretation of the regulation will vary widely but those companies that are most transparent about their use of data, can demonstrate they are trusted custodians of data, and are offering clear benefits to consumers (in exchange for data) will be at an advantage in this changing environment. As consumers, we will see an increase in incentivization to consent e.g., coupons, loyalty points, and even paid access, as an alternative.

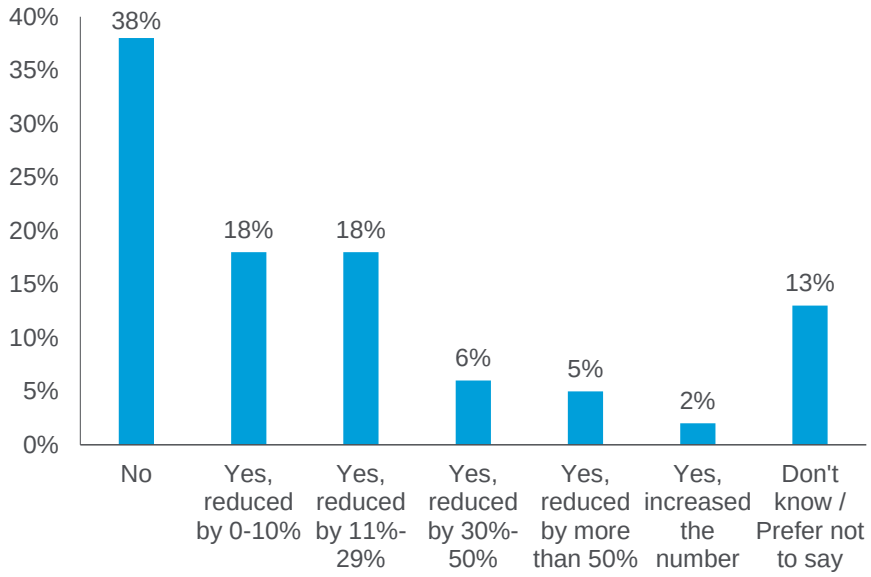
Figure 2. Likelihood of Consumers Requesting That Data is Limited or Erased Post GDPR



Source: Pegasystems (Dec 2017)

- There will certainly be **winners and losers.** Inevitably there will be a rise in Regulatory Technology (RegTech) businesses offering consumers tools to exercise their rights. A tightening regulatory environment appears to (unintentionally) favor large organizations vs. small and, in particular, large companies where their product or service is highly valued by customers. Third parties may suffer due to the lack of a direct relationship with consumers and also a reliance on publishers to obtain consent for access to personal data on their behalf. The regulation will increase paranoia about data leakages as the financial and reputational implications become much greater, and the value placed on first party data will increases. It could lead to a shakeout of some industries, and those operating as (non-essential) third-party suppliers in an overcrowded industry will be most vulnerable. This could be an opportunity for others to take share, consolidate or simply benefit from a less cluttered supply chain.

Figure 3. Change to the Number of Third Parties that Have Access to Place Trackers on Company Website



Source: Citi Research

- An unintended consequence of tighter regulation is that the **walls of the large tech operator's walled gardens could become even more impenetrable**, while at the same time their own access to large pools of data may barely alter. The ePrivacy Regulation, in particular, could push power further into the hands of the large online tech platforms under the proposal that browsers become the gatekeepers of privacy settings.

- The **online advertising industry is at the heart of it**. As one survey respondent remarked: "*The range of plausible outcomes include a total destruction of the online ad ecosystem in Europe all the way to a minor blip."* The industry has been vocal about the risks from GDPR and is even more concerned about the ePrivacy Regulation coming into effect in its current form. GDPR provides some wiggle room in the interpretation of consent and legitimate interest but this is not the case under the draft ePrivacy Regulation. Convincing consumers that there is a mutually beneficial trade in sharing data for personalized ads and recommendations could be tough. Online advertising is a $208.8 billion industry globally[2], equating to 40% of total global media spend, which has taken share from other media due to technology and tracking tools enabling more sophisticated ways of targeting consumers (with a heavy reliance on third party tracking and data). If large numbers of European consumers are unwilling to offer consent, choose to opt out, or exercise their new rights, it could reduce the pool of users available for targeted advertising. In the near term this could impact the effectiveness of online advertising (as anonymization and hashing data increases) and we could see the resurgence of direct mail. In the longer term, it may eliminate poor quality data (and wasted spend), enhance the value of data from trusted sources and accelerate the development of new approaches e.g. use of blockchain.

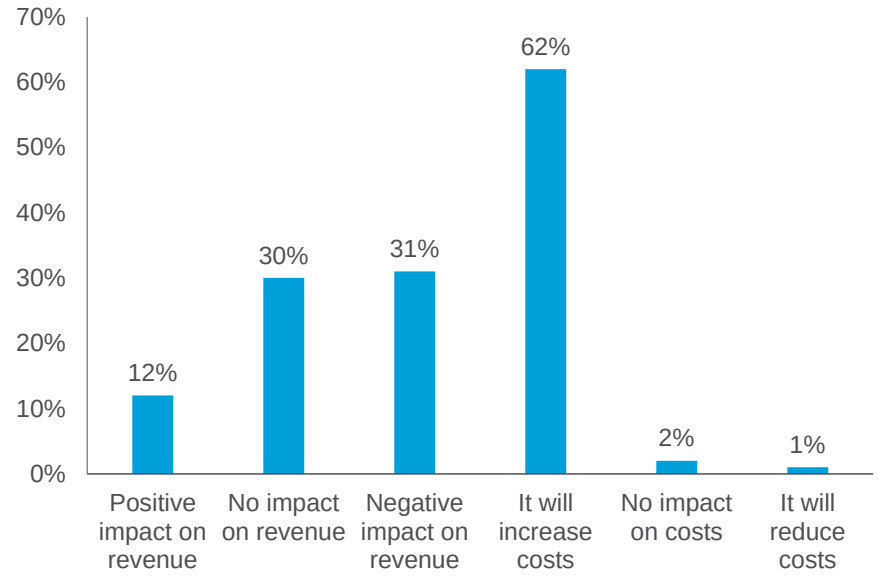
[2] Magna Global, 2017.

- The **size of databases will probably fall, but the quality of the data may improve**. Longer term, if consumers feel there is transparency, choice, and a fair exchange on offer, then they may be more willing to share data. Although fear of (and a rising number of) data breaches could curb this willingness. Data mapping will drive companies to centralize and upgrade systems and security. Companies could eventually be in a stronger position to make better use of the data across areas such as product development, customer service, customer retention etc.

- The **regulators will undoubtedly want to make an example of a high profile company**. As outlined in our previous Citi GPS, the area of data protection has become a 'political football' and enforcement could be part of a broader tit for tat trade war. The heavy-handed approach to regulation in Europe could lead to some businesses exiting Europe or reducing investment and innovation in the region as the risks are too high. This may mean less choice for consumers.

- It will most certainly lead to an increase in costs (of compliance) but a bigger **risk is that data protection regulation not only becomes a more common feature worldwide but that rules similar to those laid out by GDPR become the norm**. Organizations could go from having untrammeled access to data to a world where there is much greater scrutiny over how data is used. If this scenario comes to fruition, it could have far reaching implications for the pace of growth in data heavy areas such as artificial intelligence and machine learning. As one survey respondent succinctly said: "*On the one hand everybody is speaking about industry 4.0 as well as IoT and on the other hand the limitations will grow and grow. From our point of view sometimes good knowledge and behavior should be enough than over-regulation*."

Figure 4. GDPR Impact on Revenue and/or Cost



Source: Citi Research

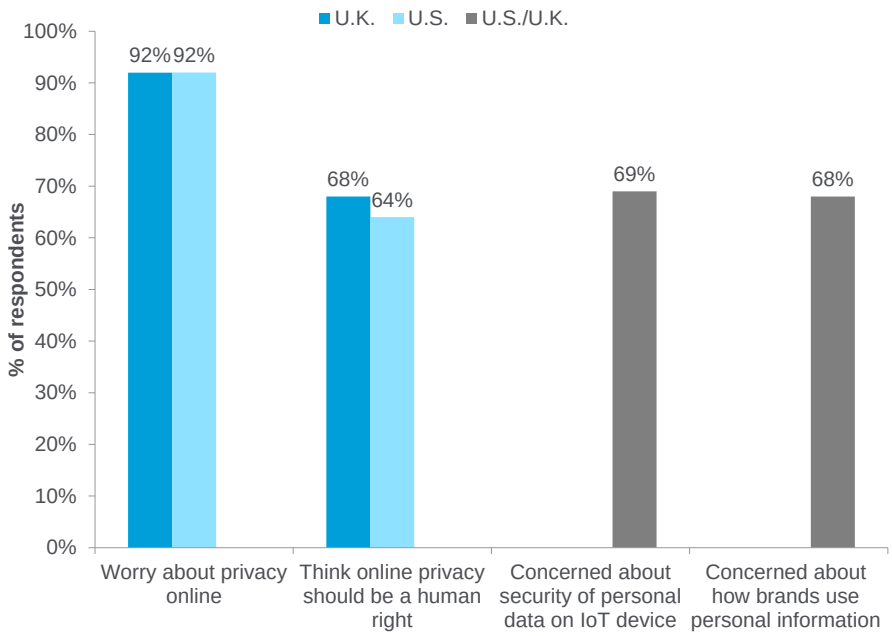
How Will Consumers' Change Their Behavior?

The main focus of this chapter is to assess how consumers intend to use their enhanced rights in relation to personal data when GDPR comes into effect and its implications on how the online ecosystem operates. We look at how consumers feel about data privacy, how they go about protecting their data now (particularly in the instance of a breach), their willingness to share different types of data for different purposes, and which rights consumers are most likely to exercise. The awareness of GDPR seems to be low (at the moment) but the appetite to exercise rights is high.

Data Privacy: Lack of Trust

It almost goes without saying that consumers claim to care about data privacy: "of course we do", is the obvious answer when the question is posed. In Figure 5 we show TrustE data from 2016 that simultaneously shows that general levels of concern about online privacy are high and the majority of U.S. and U.K. respondents see online privacy as a human right. At the same time, consumers are concerned specifically about security of data on Internet-of-Things (IoT) devices and how brands are using personal data.[3]

Figure 5. U.K. and U.S. Consumer Concerns About Privacy

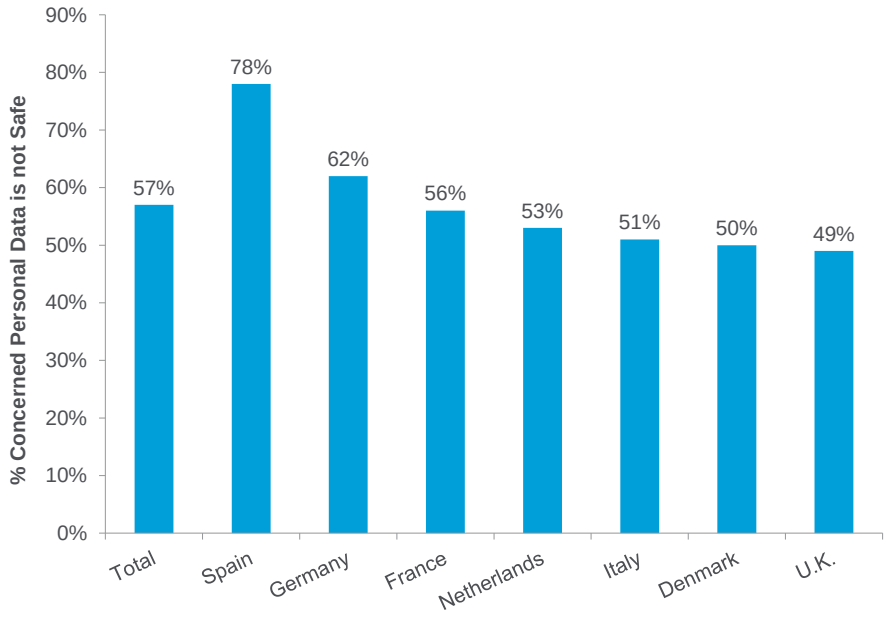


Source: TrustE; Gigya (2017 State of Consumer Privacy and Trust)

The headline numbers mask differences by culture and by industry. Survey work from Symantec shows that 57% of European consumers feel their personal information is not safe. There is a divergence by country — those in Spain are most concerned (78%), followed by Germany (62%). This compares to 49% that are concerned in the U.K.

[3] Gigya (2017 State of Consumer Privacy and Trust).

Figure 6. Level of Concern that Personal Information is Not Safe (by EU Country)

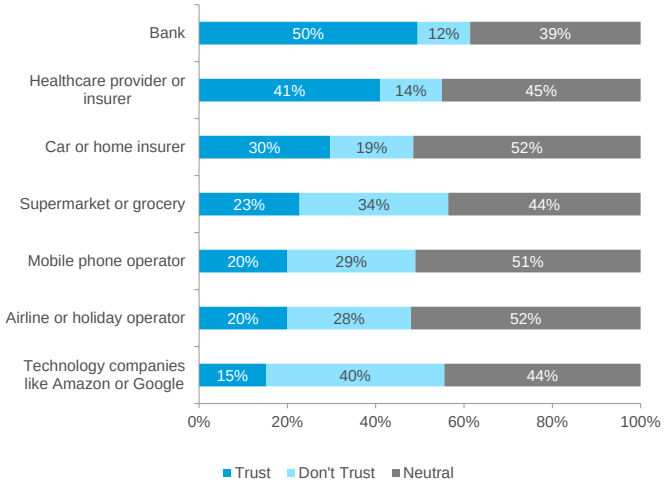


Source: Symantec (State of Privacy, 2015)

By industry, in general, consumers are more trusting of organizations where the service/product is one that is essential to pretty much all consumers, and access to personal data is critical to that service/product being delivered to consumers. For instance, there is a greater level of trust in providers of financial services and public sector entities. In the U.K., 50% of consumers claim to trust banks and 41% healthcare providers.[4] In the U.S., 42% and 39% claim to trust banks and healthcare providers, respectively.[5] There is a universal lack of trust in industries where it is less clear to consumers that providing access to personal data is necessarily needed (e.g. advertising/marketing and digital-related companies), which is probably underpinned by a lack of clear value exchange. In the U.K. only 15% of consumers trust technology companies like Google and Amazon, while 40% do not trust them. In the U.S. only 3% of consumers see marketing and advertising-related businesses as trustworthy. Other consumer-facing industries such as airlines, retailers, and telecoms also feature fairly low down the list of industries consumers trust.

[4] Oliver Wyman.
[5] PwC US Protect.me survey, 2017.

Figure 7. Level of Trust of Different Types of Organizations with Personal Data (U.K.)



Source: Oliver Wyman

Figure 8. Types of Business Consumers Trust Most (U.S.)

Source: PwC U.S. Protect.me Survey, 2017

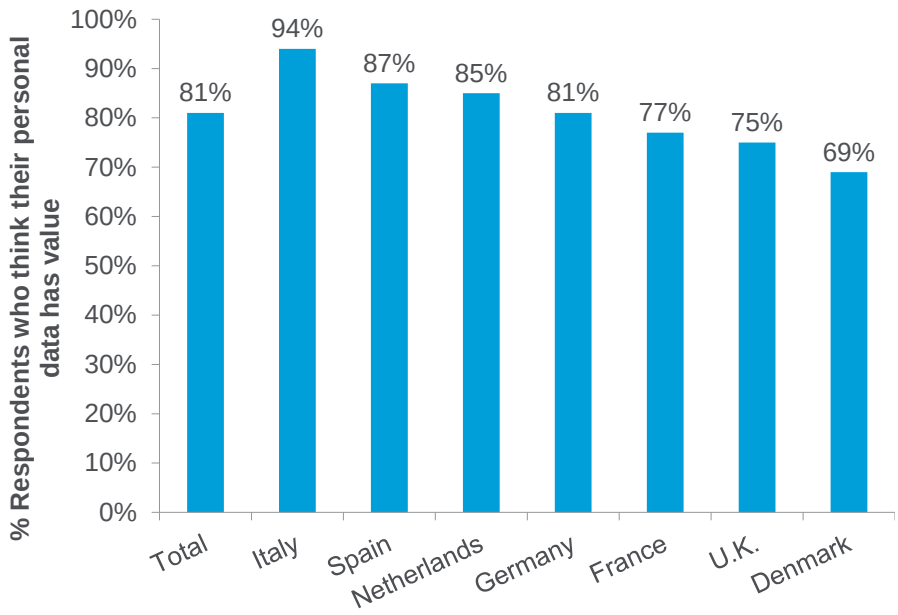
Value Exchange Is Unclear

So, why is there such a lack of trust amongst consumers when it comes to personal data? There are two reasons that regularly arise. One is that consumer willingness to trade data in exchange for goods and services is fairly low as the perceived benefit does not always outweigh the perceived risk from sharing the data. (According to one survey 46% of consumers believe they receive little benefit from sharing their information[6]). The other is that consumers feel they have limited control over their data. There are also varying degrees of willingness to share depending on what type of data is being handed over, whom with (first vs. third party) and for what purpose the data is being shared.

The Symantec survey highlights that 80% of European citizens believe their personal data has value, with Italian and Spanish consumers most of aware of the value of their personal data. The markets that are most concerned about data safety are also generally the markets that are more likely to place value on their data.

[6] Syzygy and Attest (survey of 2000 UK participants), April 2018.

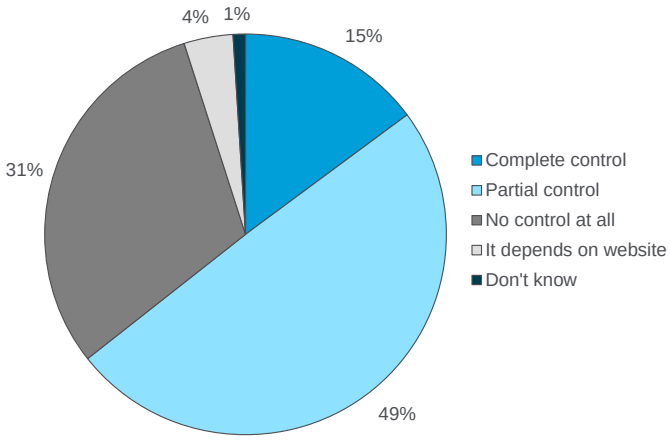
Figure 9. Consumers Think Their Personal Data Has Value



Source: Symantec (State of Privacy, 2015)

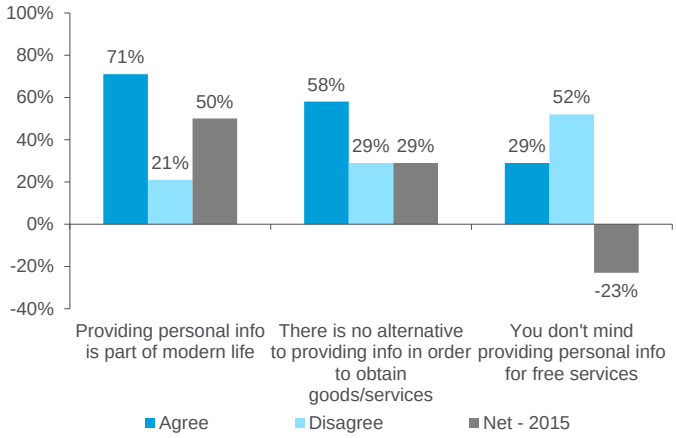
The limited control consumers feel they have over their data fosters a lack of trust. We see it as no coincidence that the industries least trusted are those that have built their businesses on the ability to harvest and utilize consumer data. This is where the data asymmetry is most apparent, yet consumers feel powerless to address it. Consumers accept that providing personal information is part of modern day life but are reluctant (if not sometimes completely unaware) participants in the data exchange.

Figure 10. How Much Control Do You Feel You Have Over the Information You Provide Online?



Source: Eurobarometer 2015

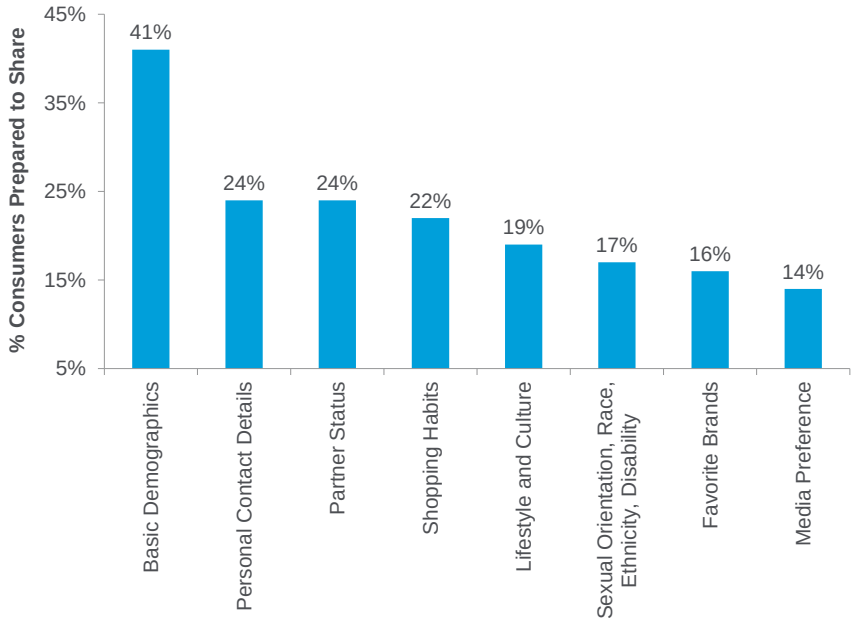
Figure 11. Attitudes to Sharing Data — Level of Agreement/ Disagreement with Statements



Source: Eurobarometer 2015

Willingness to share any type of data is relatively low — only 41% of U.K. consumers are prepared to share basic demographics such as age, gender, and social economic group, which is data that is not necessarily deemed to be personal. There is much greater reluctance when it comes to more personal data. The willingness to share drops to 24% in relation to contact details (postcode, mobile number) and less than 20% for information such as interests, sexual orientation, brand, and media preference. While some of these types of data are not likely to be classified as sensitive personal data, e.g., newspaper preference, it is information that a consumer may deem that organizations do not need to know in order to provide products/services.

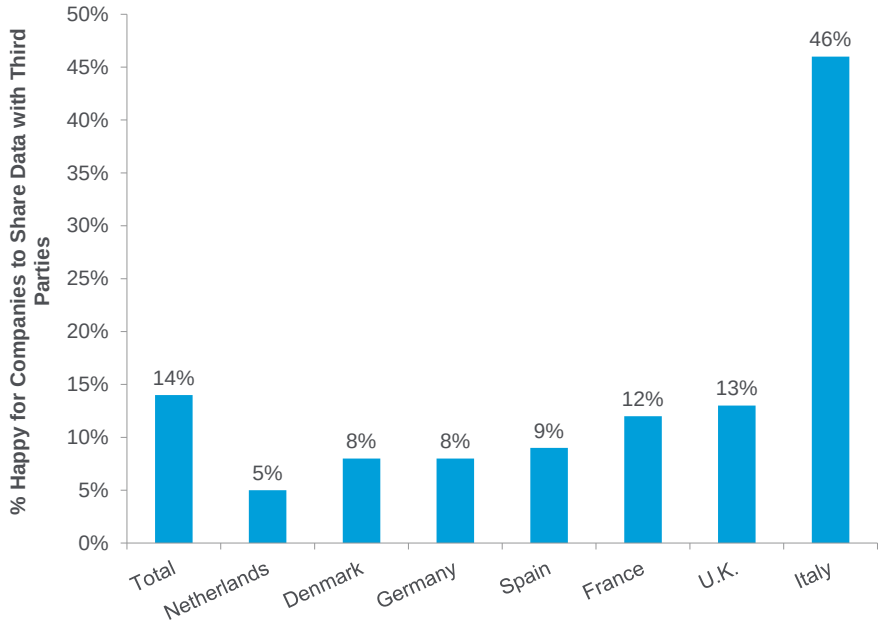
Figure 12. Information U.K. Consumers are Prepared to Share



Source: SAS (May 2017)

Persuading consumers to willingly share any data is not easy, but knowing whom it is being shared with will contribute to that decision. The lack of control and increase in public awareness of data breaches stokes fears of data falling into the wrong hands which is why it is going to be even harder for third parties to use data in the future. Only 14% of European consumers are happy for data to be shared with third parties. The Italians appear to be most relaxed about data being shared with third parties, which Symantec puts down to a higher proportion of Italians reading terms and conditions when buying products or services online (53% vs. average of 25% of EU consumers overall). GDPR will provide consumers with more transparency and control over data being shared with third parties and the risk, as this data shows, is that consumers will take the opportunity to limit sharing and third party access to data could diminish considerably.

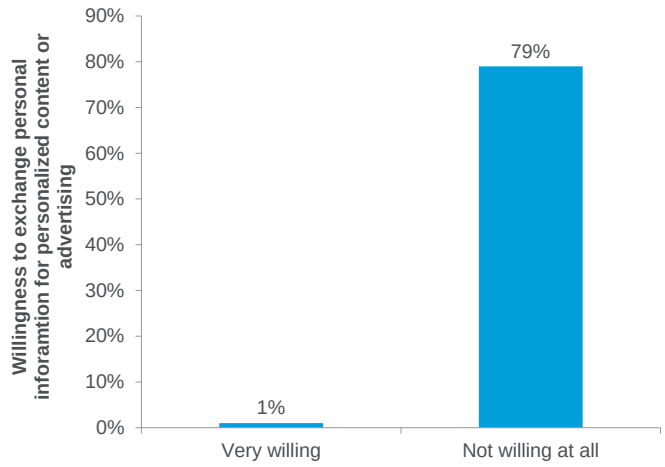
Figure 13. Percent of EU Consumers Happy for Companies to Share Data with Third Parties



Source: Symantec (State of Privacy, 2015)

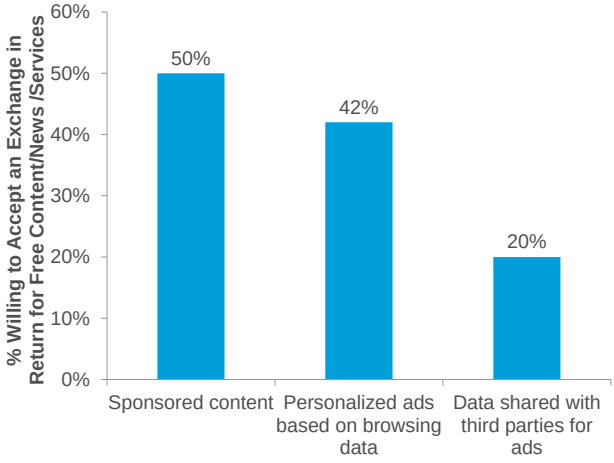
The tolerance level for data sharing for the purposes of personalized content or advertising appears to be low, and there is little difference between the regions. According to a YouGov survey conducted in January 2018, only 1% of U.K. consumers are 'very willing' to provide personal information in exchange for personalized content or advertising, and 79% are 'not willing' at all. The results of a survey run by GfK (on behalf of IAB Europe) shows a less extreme outcome, but still worrying for a heavily ad-funded Internet ecosystem. In the U.S., only 25% of consumers believe the risk of sharing personal data is worth personalized promotions, advertising, and coupons and only 18% believe the risk is worth it for product recommendations.

Figure 14. Willingness to Exchange Personal Information in Return for More Personalized Content or Advertising (U.K.)



Source: YouGov Omnibus Survey (Jan 2018)

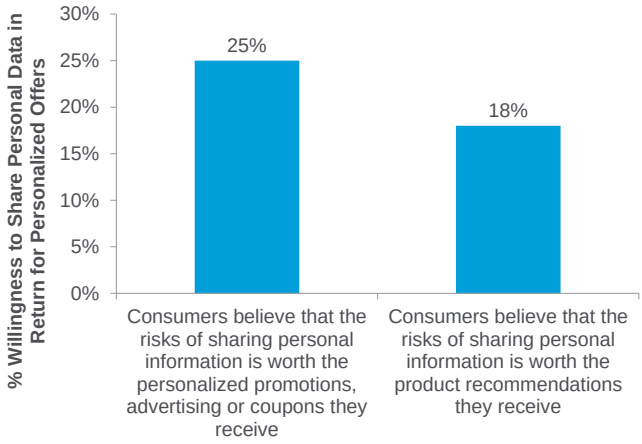
Figure 15. Percent of Consumers' Prepared to Accept The Following in Return for Free News/ Content/ Services (EU)



Source: GfK & IAB (July 2017

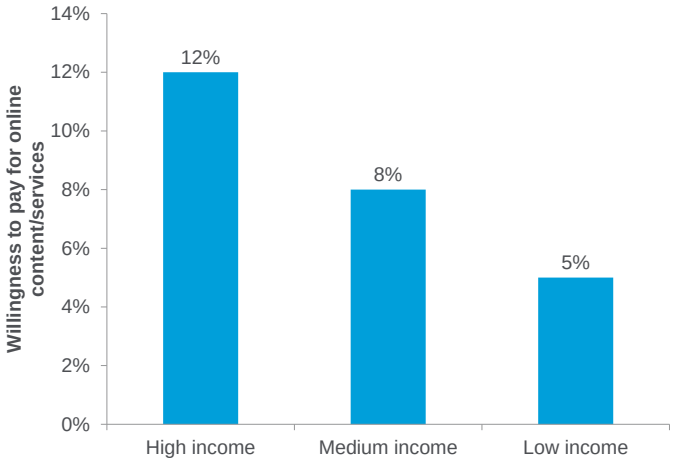
While consumers are not keen to provide personal data for more targeted ads, they have become used to receiving content and services for free so the propensity to pay for content online is low (across all income brackets). The GfK/IAB survey found that only 12% of Europeans with high incomes are willing to pay for online content and services. It drops down to 5% amongst those on a low income. Overall 92% said they would stop accessing their most used free news, content, or service site or app if it became paid access only.

Figure 16. Willingness to Share Personal Information in Return for Personalized Offers/ Advertising/ Recommendations



Source: Consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014

Figure 17. Willingness to Pay for Content/ Services Online

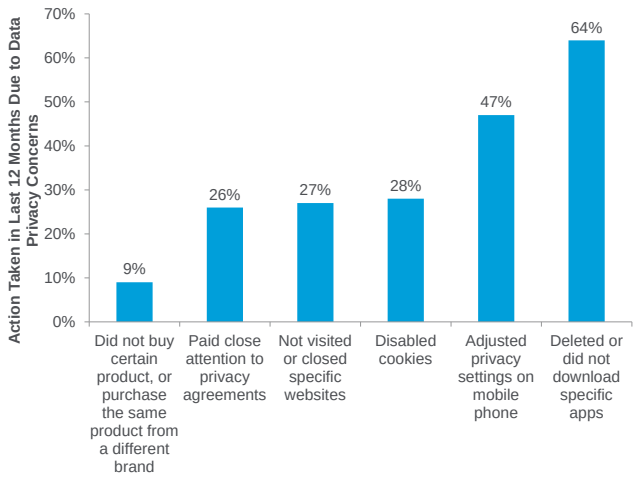


Source: GfK & IAB (July 2017)

Consumer Actions to Protect Data

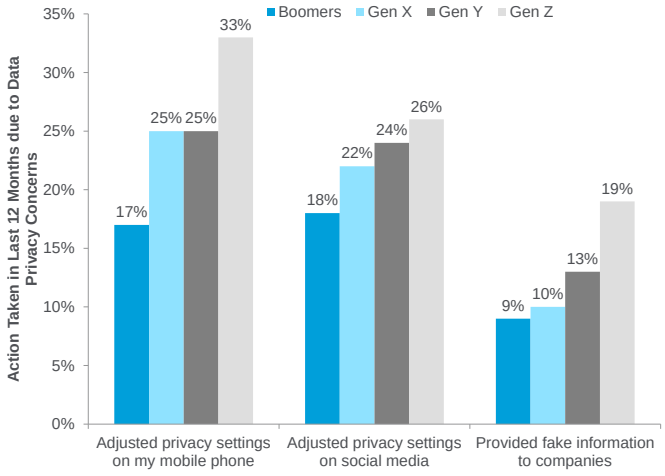
Consumers clearly feel constrained in their ability to control how personal data is used. At the same time, some consumers have adapted their behavior to reflect privacy concerns. According to a survey conducted by Deloitte/SSI, 64% of U.S. consumers have deleted or not downloaded apps due to privacy concerns, 47% have adjusted privacy settings on their mobile phone, and 28% have disabled cookies. The younger generation has been more active in adjusting privacy settings or even providing fake information than the older generations as they are likely to be more savvy technology users. We have also seen a rise in ad blocking over the past 2-3 years as well as a more proactive response from some of the browsers, e.g., Safari and Google, blocking certain cookies or types of online adverts. The motives vary between positioning as a guardian of consumer privacy and limiting the backlash against low quality, intrusive online advertising.

Figure 18. Action Taken in the Last 12 Months due to Data Privacy Concerns



Source: Deloitte/SSI 2016 consumer survey

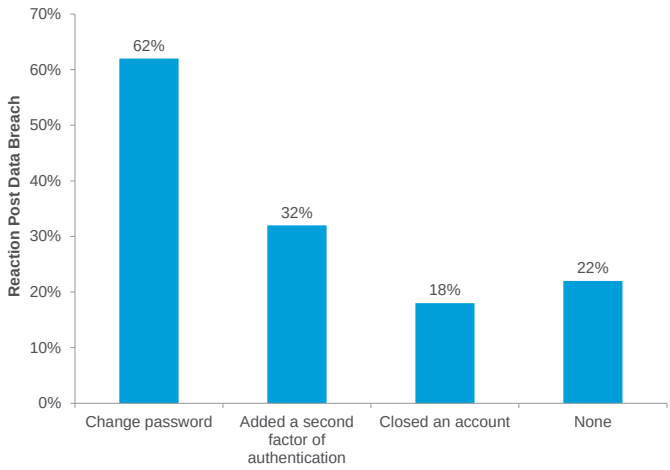
Figure 19. Action Taken in the Last 12 Months due to Data Privacy Concerns by Age Groups



Source: Deloitte/SSI 2016 consumer survey

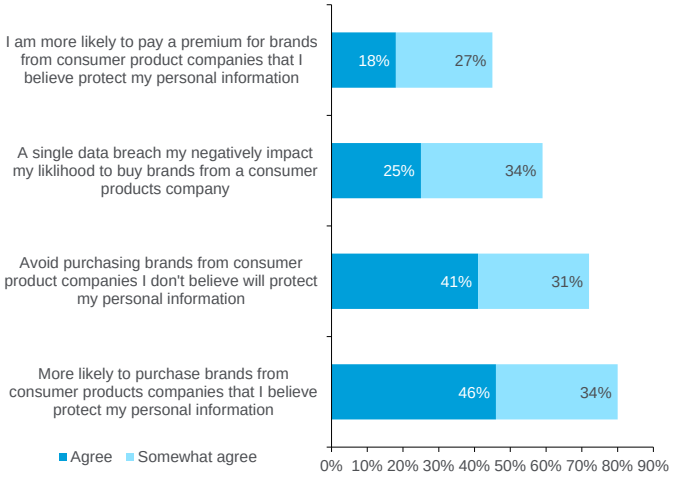
Following a breach, 62% of users changed their passwords while 22% did nothing. Of those surveyed, only 18% have closed the related account. Loyalty to, and engagement with, sites/brands that are deemed not to be trusted custodians of data could be disrupted. A survey by Deloitte suggests that a single data breach would negatively impact the likelihood of buying that brand again for 59% of consumers and 80% of consumers believe they are more likely to buy brands from companies that they believe protect personal information. In the eyes of consumers, taking the subject of protecting personal information seriously could provide a competitive advantage.

Figure 20. Action Taken Post Data Breach



Source: Gigya (2017 State of Consumer Privacy and Trust)

Figure 21. Consumers' Attitudes to Companies Based on Perception of Data Protection & Data Breaches



Source: Consumer product consumer and executive survey on data privacy and security, Deloitte LLP, August 2014

How Consumers May Exercise Their Rights

Through the myriad surveys of consumers on the topic of ePrivacy it is very easy to paint a bleak picture — lack of trust, lack of control, and lack of fair value exchange. However, there is clear evidence that what consumers say and what they actually do may vary depending on how inconvenient acting on an issue could be for them.

The recent (and still active) high profile example that provides insight into how consumers react when data has been used in ways that they had not expected is that of Facebook. It has been hauled over the coals in the press for how much data it has collected (including metadata from call logs and messages in some cases) and how the data is used/shared. None of what had occurred was necessarily illegal, but the issue was that consumers were clearly unaware of the extent of it. According to a survey from Toluna in the U.K., 53% of consumers said they trust Facebook less as a result of the Cambridge Analytica scandal but only 34% of users had updated their privacy settings on Facebook. In the U.K. only 5% of users claimed to have actually left Facebook[7] and in the U.S. the number is 10%.[8]

The imbalance between consumers and corporates when it comes to the collection and use of personal data is a key driver behind Europe tightening up regulation.

One way GDPR is trying to redress the balance is enhancing European consumer's rights in relation to personal data. Before we delve into the level of awareness of the GDPR amongst consumers and how consumers are likely to use their rights, here is a recap of what those rights will be.

The GDPR strengthens the rights of data subjects to object to processing of personal data, including an extension of some rights already present under the Data Protection Directive as well as the inclusion of new ones (rights to erasure and to data portability):

- **The Right to Object (Article 21):** Data Subjects now have an absolute right to object to processing for direct marketing purposes. More generally, the right to object is strengthened in several other areas when processing is not based on consent. A subject objection can only be overruled in cases where '*the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedom of the data subject.*' The onus is on controllers and processors, rather than individuals, to demonstrate their case in the event of conflict. This has the potential to be seriously disruptive, especially as processing has to be restricted immediately in the case of a complaint.

- **The Right to Exception from Automated Decision Making:** Under the GDPR, automated decision making on the basis of so called 'sensitive personal data' is only permitted if done on the basis of explicit consent and/or public interest.

- **The Right to Access your Data (Article 15):** Under the Directive the data subject could access confirmation of processing, data used, and purposes. The GDPR extends this to include additional information. The Recitals imply that companies will be required to make it relatively easy for subjects to access their data and, in some cases, controllers will have to provide remote access portals that will provide secure direct access for subjects to their data.

[7] Campaign, April 2018.
[8] Zerohedge (Techpinions), 13 April 2018.

Additionally, the GDPR also creates two new rights for consumers:

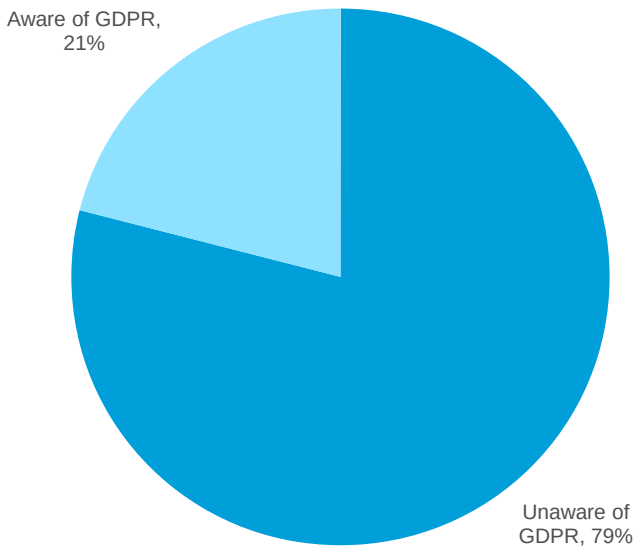
- **The Right to Erasure (Article 17):** 'Right to be Forgotten,' was initially brought to prominence in the 2014 case of Google Spain v AEPD and Mario Costeja González. The GDPR cements this right as a data subject can request all the data is deleted by a controller when personal data is no longer useful to the purpose it was initially collected and there is no longer a legal ground for processing and so forth. This is a particularly draconian restriction on controllers as they are forced to both delete data on their own servers and take 'all reasonable steps' to notify third parties of the erasure requirement, including those to whom they may have transferred/ sold the data.

- **The Right to Data Portability:** Data subjects must be able to transfer personal data from one controller to another, e.g., consumers with a music playlist on one platform should be able to retrieve it if they want to move platforms. The different technology platforms could make this complicated in practice.

Awareness of GDPR

The awareness of the GDPR is relatively low with only 21% of European consumers appearing to be aware of the upcoming regulation. The regulators have focused on guiding and educating business on implementation but there is clearly a lot of work to do to ensure consumers understand that in less than a month their rights, and ability to take control of personal data, will improve significantly. Companies are sending emails to consumers requesting consent to continue to market to them which should prompt an increase in awareness. We are likely to see privacy focused groups ramping up campaigns around the topic as well as provide tools that could make deletion requests or data portability requests much more straightforward.

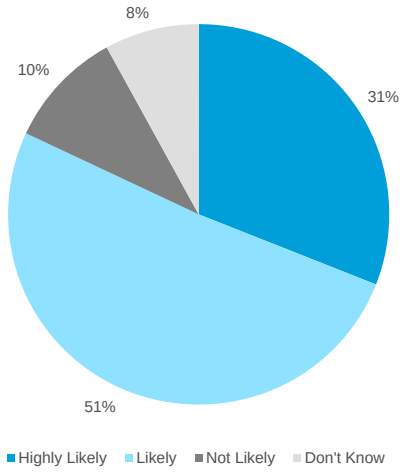
Figure 22. European Consumer Awareness of the GDPR



Source: Pegasystems (Dec 2017)

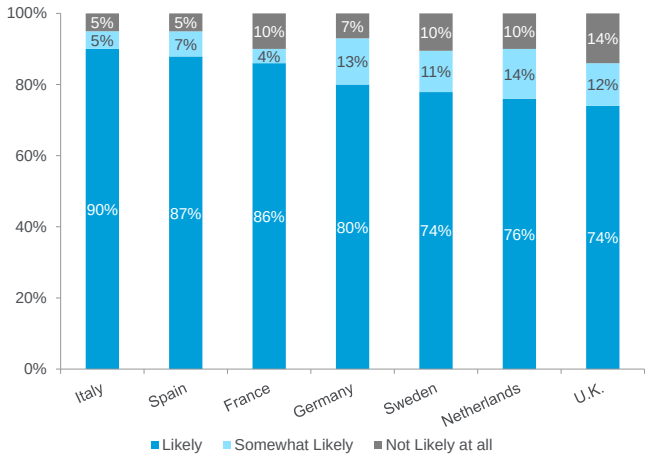
When respondents were informed of what their rights will be, over 80% stated that they are highly likely or likely to ask companies to limit or erase personal data once the GDPR comes into effect. Consumers in Italy and Spain are most likely to exercise their rights under the GDPR.

Figure 23. Likelihood of Consumers Requesting That Data Is Limited or Erased Post GDPR



Source: Pegasystems (Dec 2017)

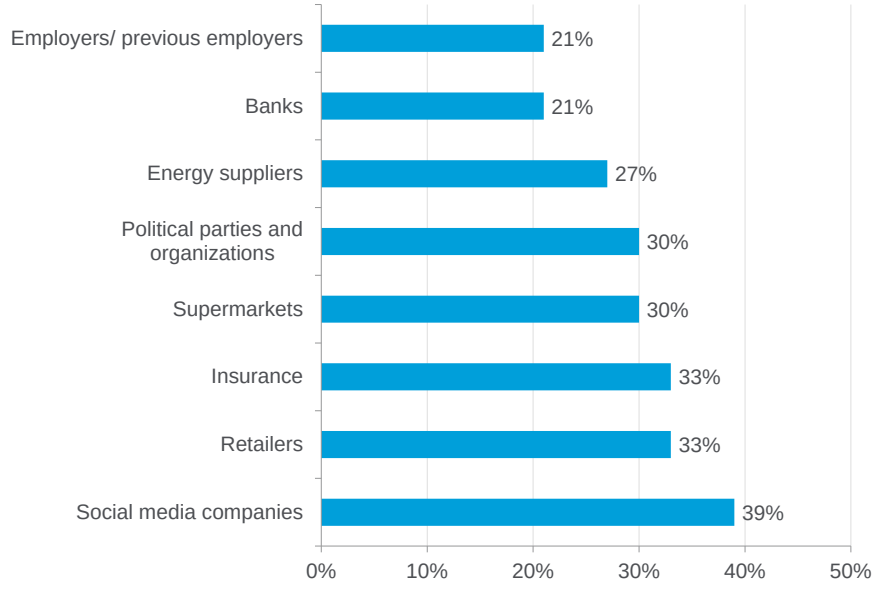
Figure 24. Countries Where Consumers Are Most Likely to Use GDPR Rights



Source: Pegasystems

Social media companies will likely receive the most requests for the erasure of data, followed by retailers.

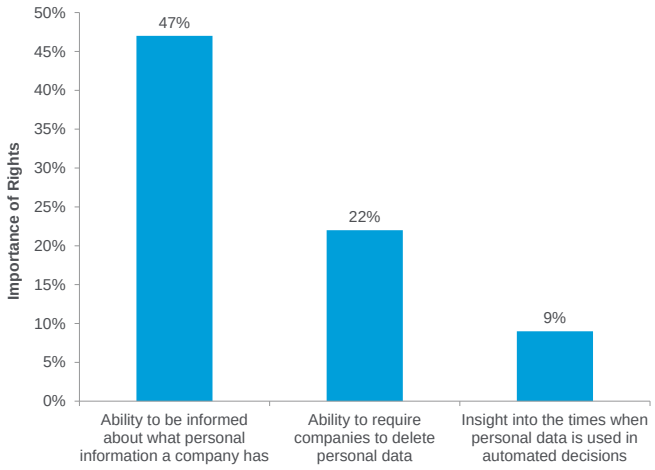
Figure 25. Percentage of Customers Who Will Request for Personal Data to Be Removed (by Company Type)



Source: SAS

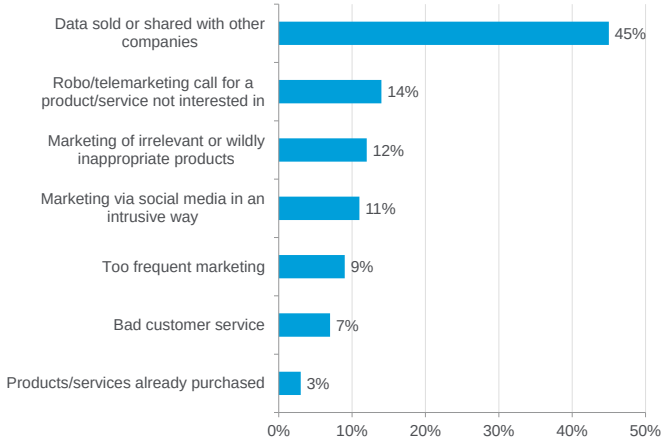
The “Right to Access Your Data” and the “Right to Erasure” are seen as the most important rights by European consumers. The most common reason given for wanting to exercise those particular rights is when data is sold or shared with other companies.

Figure 26. Top Consumer Rights Under GDPR



Source: Pegasystems

Figure 27. Main Reason to Access or Request Erasure of Data

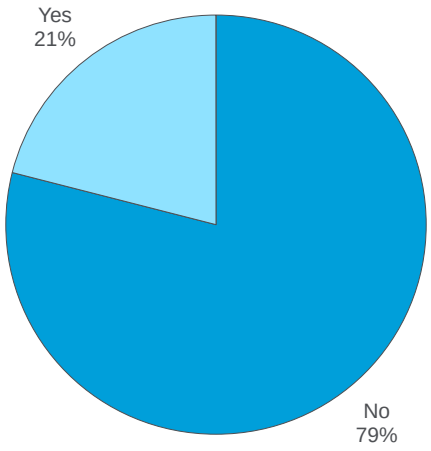


Source: Pegasystems

While not an enhanced right per se, the consent requirements for the use of personal data will be tightened under GDPR. Consent is still seen as an area where companies may use poetic license (whether access to a service/site can be made conditional upon obtaining consent, for example), and it is also the area which we flagged in the previous GPS that is deemed (by companies) to be one of the most challenging. The big unknown is how consumers will react when asked for consent for specific purposes.

The data earlier on the willingness of consumers to share or exchange data in return for free content, personalized ads etc. is worryingly low. A survey (of publishers and AdTech industry personnel) by Pagefair found that 79% of respondents would say no if a pop-up appears on a site requesting consent to share browsing habits to personalize offers (the message read: ‘We would like to share your browsing habits on our site with Brand Name and their analytics partners, to understand what offers may be of interest to you. This data will be deleted after 6 months. You can withdraw permission at any time.’). Not only could this mean databases will shrink significantly but it could mean a sharp halt to the untrammeled access that organizations have had to personal data.

Figure 28. Response to Pop-Up Message Requesting Consent for Sharing Browsing Habits



Source: Pagefair (Sept 2017)

Implications

The backdrop is consumers worry about the safety of personal data (more so in Spain vs. the U.K.) and there is a general mistrust of public and private handling of personal data in all industries, but especially online platforms and marketing-related businesses. The willingness to share personal data of any kind is less than 50% and it is much lower if the sharing request is with third parties, or the purpose is to use the data for personalized content and advertising as consumers do not believe benefits outweigh the risks of sharing the data.

The majority of consumers (81%) realize their data has value but they feel powerless to address the growing information asymmetry. While some consumers have adapted their behavior due to privacy concerns, it is not necessarily consistent. What consumers say they may do and what they actually do can vary if it is perceived there is no real alternative. This is one of the main reasons why the regulator has stepped in in Europe, to attempt to redress the balance and empower consumers to control their data without a detrimental impact on their ability to access services.

The consumer awareness of GDPR is low currently but this will probably change as the regulator, privacy groups and RegTech businesses push to increase awareness and tools come to market that make requests (deletion and data portability, for example) easy for consumers to enact. The biggest unknown for corporates is how consumers will react to GDPR. If the surveys are to be believed, there could be a seismic change coming. Trust is fundamental to the future of businesses online. The risk of a breach is not only financial (reflecting the fining power of regulators) but also reputational and operational as enhanced consumer rights may lead to a stronger backlash against companies not perceived to be dealing with it properly.

As the ease with which consumers can access data companies hold on them increases, it could prompt a realization that organizations potentially hold far more data than consumers appreciated. The risk is that this reinforces the current lack of trust that consumers feel which could lead to a significant reduction in their usage of a particular service. Inevitably, sites or products that consumers use less frequently are much easier to walk away from, while those that are embedded in our everyday lives are less easy to abandon.

Consent levels are likely to depend on how the request for consent is presented. If a third of U.K. shoppers claim they will request data is not used for marketing purposes[9] and only 21% claim they will consent to share browsing habits for personalized data, then companies need to be creative in their approach. It is clear that consumers need to understand and feel there is sufficient benefit from handing over data. This may be more difficult for the marketing industry to demonstrate and for those that don't have a direct relationship with consumers (especially third party tracking). Consumers could become much savvier about the value of their data and use it to shop around. For example, the right to data portability may make it much easier for consumers to move between services.

It is highly likely that databases shrink and the justification for holding onto data without a specific purpose becomes nigh on impossible. This means mindsets will need to change – data maximization as an approach will no longer be possible.

For all of the challenges and changes that could be prompted by a change in consumer behavior coupled with the regulatory requirements, there are some reasons for optimism longer term. Data quality could improve as those consumers who opt to provide personal data may be more engaged and conversion (to sales) may be higher. Data as an asset could increase in value. If companies can demonstrate that they can be trusted with consumer personal data, it could become a competitive advantage.

How companies approach this changing regulatory landscape could be extremely important for the outlook for their own future. It is this we turn to in the next chapter.

[9] SAS OnePoll study (May 2017).

How Corporates Are Preparing for GDPR

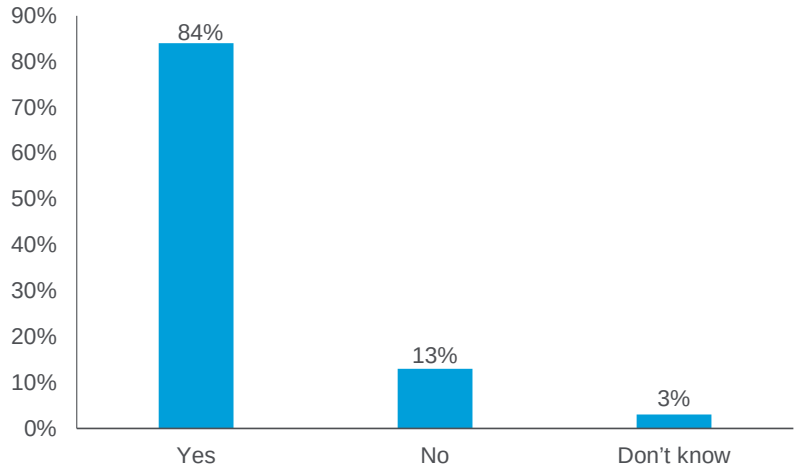
In this chapter we analyze the results of a survey we conducted in March 2018 of management/executives responsible for the GDPR implementation. The survey covered 100 companies across a range of sectors and seeks to understand how prepared companies feel they are for the GDPR, which areas are perceived to be most challenging and most supportive, the possible financial impact of the regulation, and how companies will change their use of consumer data in Europe.

Below we detail the main findings.

GDPR Will Impact How Data Is Used

An overwhelming number of respondents (84%) believe that the GDPR will impact the way their company and industry uses EU consumer data.

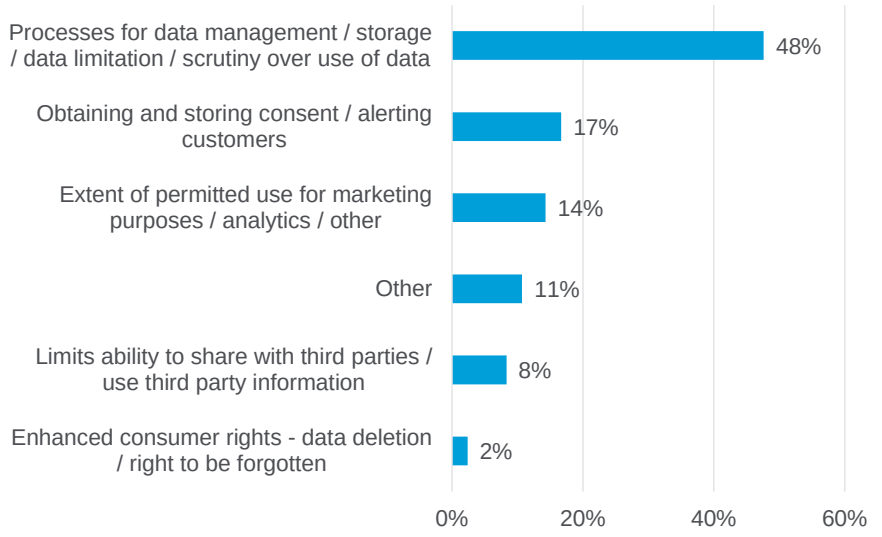
Figure 29. Will the GDPR Impact How Your Company and Industry Uses EU Consumer Data?



Source: Citi Research

The impact on the use of data will be broad reaching. Almost half of respondents refer to a change in data management processes (storage and security). The comments consistently refer to greater scrutiny and limitation of the use of data. Fourteen percent (14%) expect it to impact data in the use of marketing.

Figure 30. Main Ways in Which the Use of Consumer Data Will Alter



Source: Citi Research

Quotes on the Ways in Which the Use of Personal Data Will Change

"We cannot share consumer data with our suppliers anymore. Since we are a wholesaler for many brands, the brands are eager to get to know there customers. We need to be careful what we can share and what not."

"We will be more limited in the use of data, particularly for marketing purposes."

"We are getting the word out throughout the company to just take what you need and to be thoughtful about how you ingest, use, and delete data."

"According to the letter of the law — we must ensure that we are only analyzing and leveraging that which is permissible. It will, temporarily, cause internal strife and red tape, as we all are ensuring that we are following the new regulation."

"Since regulations are complex, the overall result will be reduced creativity and a more prudent approach to data collection and analysis."

"First related task will be to invest in a front-end marketing campaign in order to rebuild the database. Also use external agencies to help in the acquisition process. Anticipate more creativity needed to engage customers."

"Increases costs and complexity to obtain and use data. Increases barriers to entry for SMEs."

"We will have to use more intrusive alerts about anything involving customer data no matter how minor. Similar to the cookie notices, I'm not sure if this creates a better user experience."

"Ad targeting goes to context- or session-based."

"We currently rely heavily on the use of third-party cookies and first-party data that we collect on our own users. We use all of this data for ad targeting, and our fear is that without the ability to target in this manner, performance and as a result revenues, will start to fall."

"We will have limited possibility of using some online marketing tactics we used before, remarketing included. In affiliate marketing there will be limited transparency towards affiliate partners and it is questionable how this will unfold."

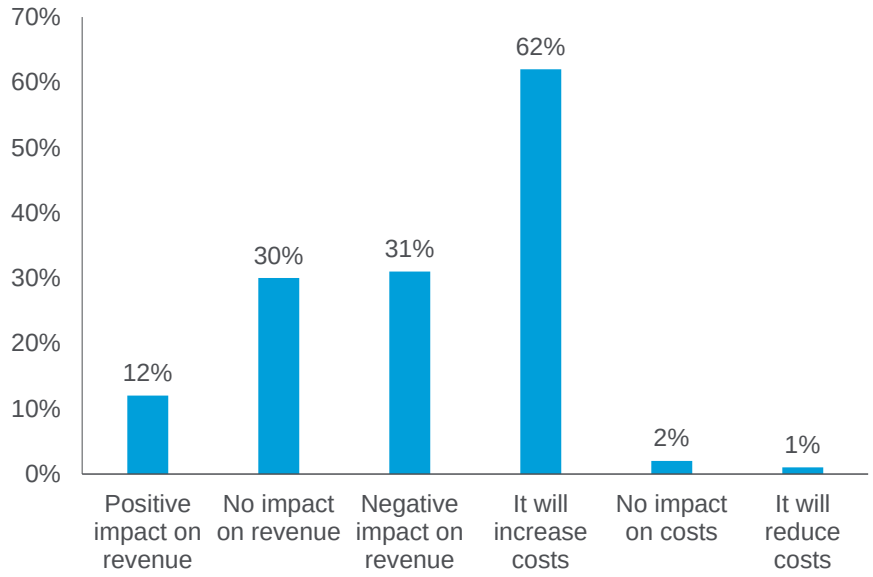
"More restricted access to data. Higher demand to delete archived data with respect to defined timelines."

"Digital initiatives (apps) are less likely to be launched as requirements increase."

Impact of the GDPR

The cost of preparing for the GDPR itself has been fairly immaterial (79% claim it has cost less than £5 million) but the ongoing financial impact of compliance with GDPR could be more meaningful. It is expected to lead to an increase in costs according to 62% of respondents, while only 2% of respondents claim there will be no cost impact. 31% of respondents believe it will have a negative impact on revenue and of those, 62% believe it will reduce revenue 0-5% and 27% believe revenue could fall 6-10%.

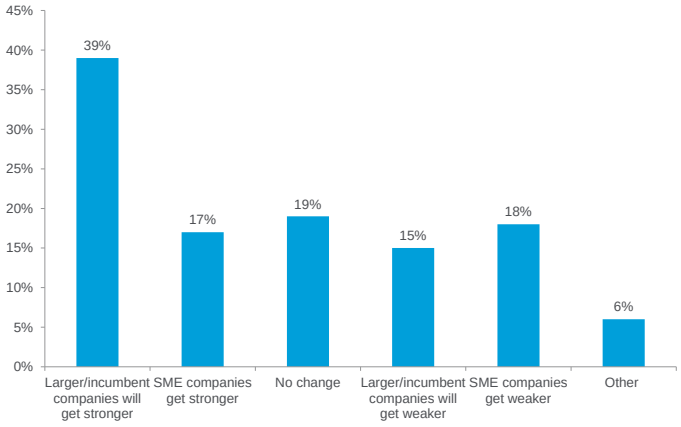
Figure 31. GDPR Impact on Revenue and/ or Cost



Source: Citi Research

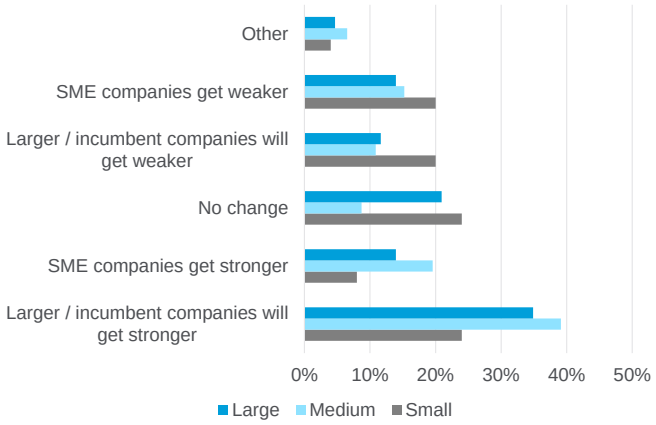
The competitive landscape is also expected to be disrupted by the GDPR. One of the commonly cited unintended consequences of the regulation is a strengthening of larger companies and our survey supports that view. Only 19% expect no change to the competitive landscape on the back of the EU's approach to data protection. While small companies seem to be less convinced that larger companies will get stronger, they are also not optimistic about the prospect of smaller companies getting stronger. They believe it is more likely that there will be no change or smaller companies will get weaker.

Figure 32. Impact on the Competitive Landscape due to the EU's Approach to Data Protection



Source: Citi Research

Figure 33. Impact on the Competitive Landscape due to the EU's Approach to Data Protection by Company Size

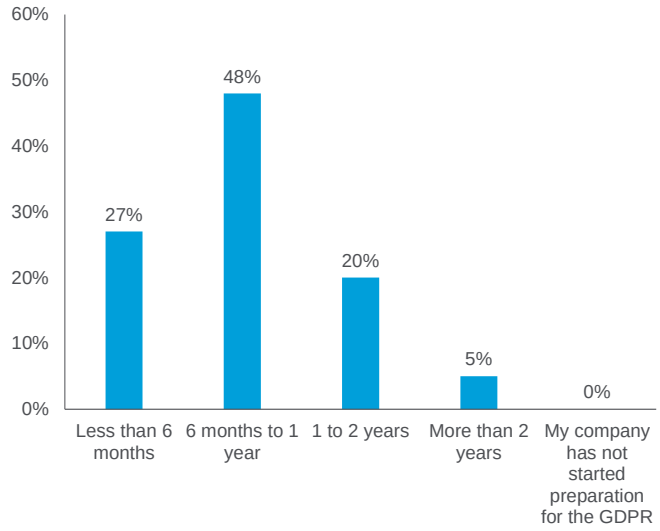


Source: Citi Research

Preparedness for GDPR

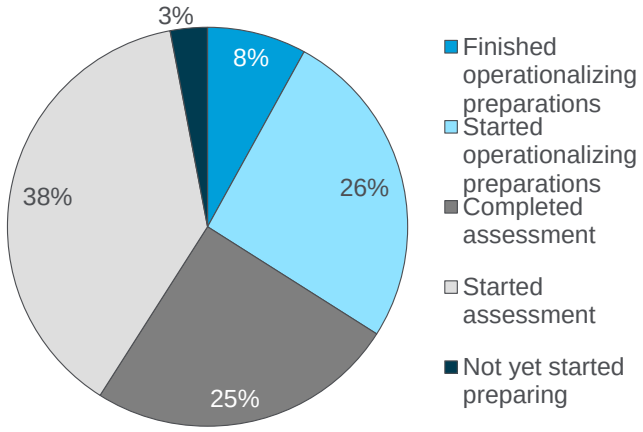
Despite the scale of the regulatory change, the majority of companies (75%) have only been preparing for GDPR for up to a year. The good news is that none of the companies surveyed have not started preparations, but only 5% have been preparing for over 2 years. A PwC survey suggests that (as of January) only 8% of companies have finished operationalizing preparations, and only 26% have started to operationalize preparations. The remainder are still in the assessment phase.

Figure 34. How Long Have Companies Been Preparing For GDPR



Source: Citi Research

Figure 35. Preparation Progress for GDPR (January 2018)

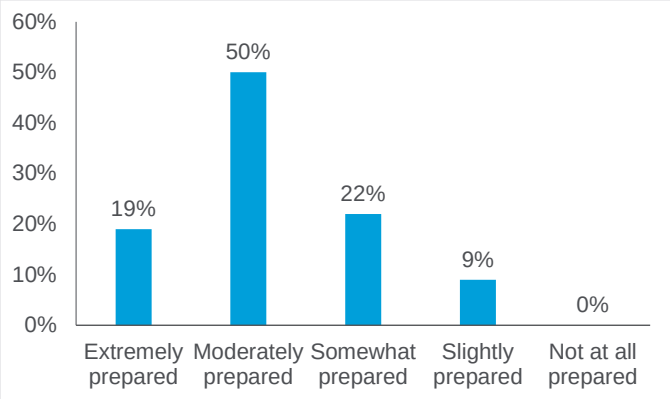


Source: PwC GDPR Pulse Survey (wave 3)

Sixty-nine percent (69%) companies claim to be extremely or moderately prepared for the GDPR and none claim not to be prepared at all. At a sector level, the tech sector appears to feel most prepared (92% extremely/ moderately prepared), which is not surprising given this sector is right at the heart of the data industry.

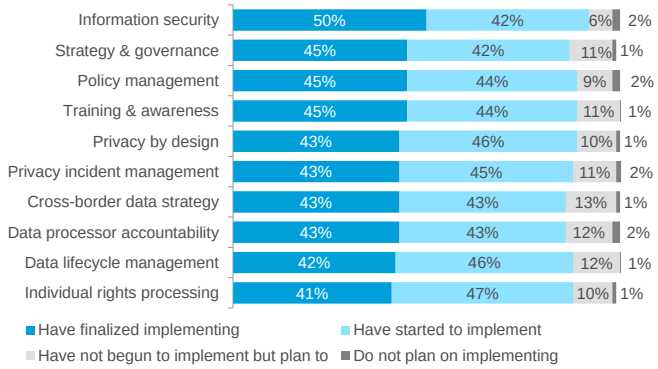
Given the fairly limited timeframe over which most companies have been preparing for the regulation, and the size of the task, it is a surprise that preparedness is so high. That said, this does not necessarily mean that companies are compliant — Gartner believes that by the end of 2018, 50% of companies will not be in full compliance. The PwC survey found that information security is the aspect companies appear to be most progressed with implementing, whereas there has been less progress in areas such as cross-border data strategy and data processor accountability.

Figure 36. Preparedness for the GDPR



Source: Citi Research

Figure 37. Preparation Across Various Elements of the GDPR



Source: PwC GDPR Pulse Survey (wave 3)

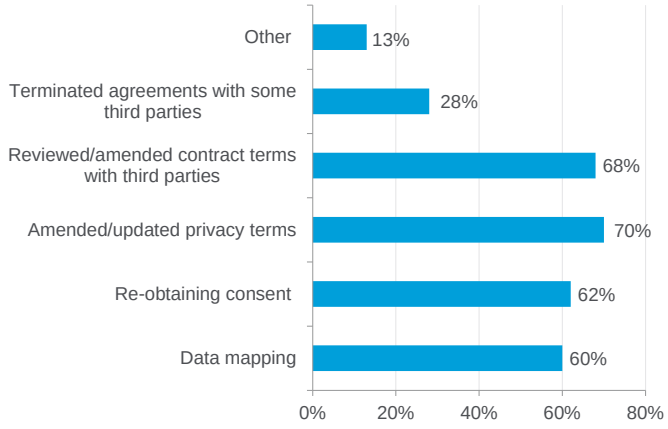
Actions Taken to Prepare

The key actions taken to prepare for the GDPR have focused on amending the privacy policy (70%) and reviewing contracts with third parties (68%). Large companies are much more likely to have taken these actions than small companies. Data mapping and re-obtaining consent for using data have also been undertaken by at least 60% of respondents. We are not surprised that 'Re-obtaining consent' is being actioned by a number of companies because, according to W8, up to 75% of customer data held within business' marketing databases could be obsolete if the GDPR is strictly applied.[10] Other actions include terminating agreements with some third parties (large companies 38% vs. small companies 13%), hiring consultants to help with privacy impact assessments, and internal training.

Retailers have focused on amending and updating privacy terms (86%), but less than half have re-obtained consent or reviewed third-party contracts. Technology companies are more likely to have conducted a data mapping exercise (75%) and amended privacy terms (83%). Advertising companies have focused on reviewing third-party contracts (91%), but little over a third have conducted a data mapping exercise.

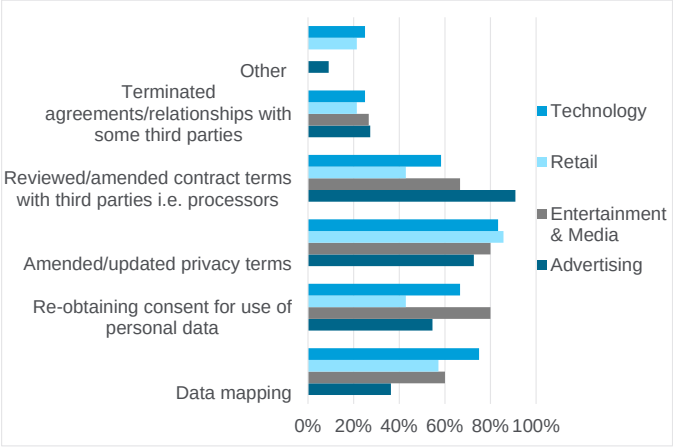
[10] www.decisionmarketing.co.uk (11 August 2017).

Figure 38. Actions Taken to Prepare for the GDPR



Source: Citi Research

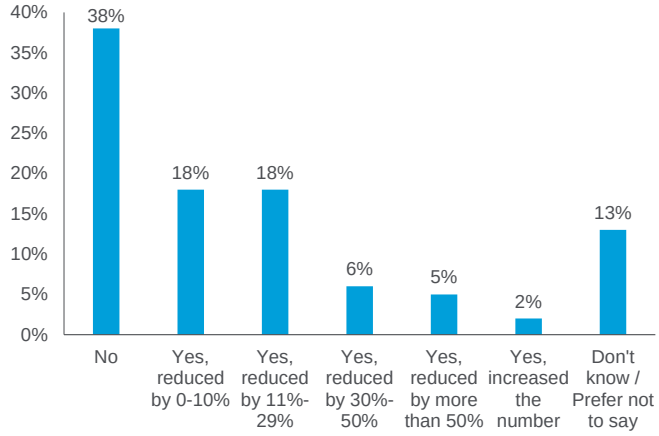
Figure 39. Actions Taken to Prepare for the GDPR by Sector



Source: Citi Research

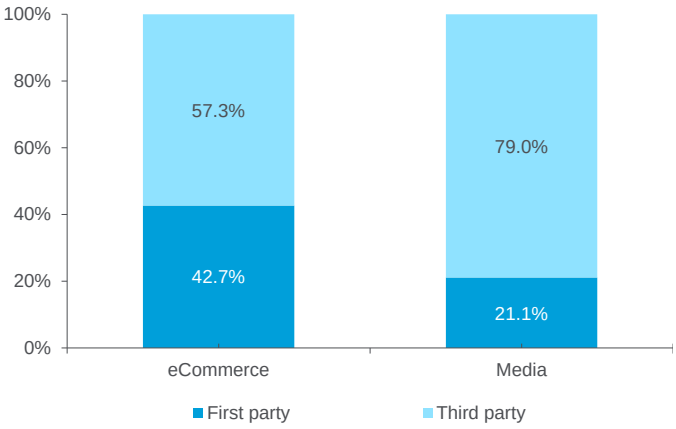
Delving further into third party related actions highlights the risks for suppliers. Only 38% of respondents claim not to have altered the number of third parties that have access to place trackers on their websites, and 36% have cut the number of third parties that have access to their website by up to 30%. The Article 29 Working Party data highlights the extent to which cookies placed on websites are from third parties. As GDPR introduces a much greater risk of non-compliance (in the form of heavy fines) many publishers will use the GDPR as an opportunity to clean up third-party trackers and access to their sites. We have already started to see the likes of Google and Facebook limiting the access afforded to third parties, which may lead to less transparency for businesses that rely on these platforms for marketing, commerce etc.

Figure 40. Change to the Number of Third Parties that Have Access to or Place Trackers on Company Website



Source: Citi Research

Figure 41. Cookie Types: First Party vs. Third Party

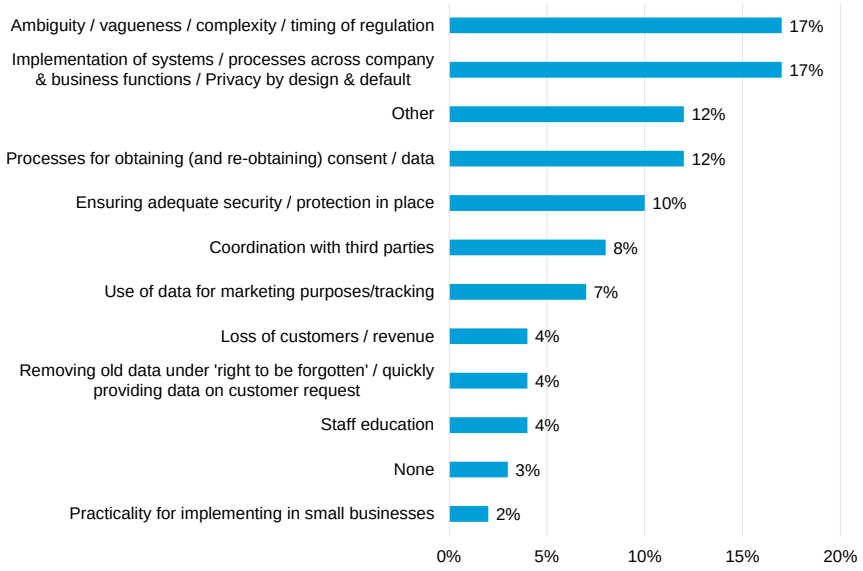


Source: Article 29 Working Party 14/EN, WP 229

Challenges and Opportunities

What stands out from the responses to the open question about which aspect of the GDPR is most challenging is frustration with how to apply the regulation. The regulation may be set in stone, but there is a lot of ambiguity about the application of it, and the more detailed guidance on key areas has been drip fed extremely slowly. The practicalities of applying it from a systems perspective, especially for those organizations where there may be multiple systems holding various types of data, is the other main challenge. Obtaining consent, managing third parties and impact on data used in marketing are also cited as challenges

Figure 42. Most Challenging Aspects of the GDPR



Source: Citi Research

Quotes Related to the Most Challenging Aspects of the GDPR

"As a media buying business, we regularly use cookie based data to target display advertising for clients. This and many other forms of intent signaling data will not be available post GDPR, restricting the media we can buy for our clients. In addition, clients will have less data to share with us to generate useful insight."

"Understanding how this can practically be applied in a small business cost effectively. Obtaining consent from long-established lists — people often simply don't read these types of emails and/or don't understand the significance 'I've already said yes otherwise I wouldn't be getting this email!' How to keep evidence of consent — bureaucratic record keeping — how do we realistically do this? Too complex for most small businesses to understand."

"As a company that is heavily reliant on ad revenues, the ability to track and target users is vital to campaign performance. With targeting capabilities becoming far more limited, we will potentially see poor advertising performance, which could have a negative impact on ad revenue in the EU."

"Privacy by default could lead to loss of income due to complexity for the users. We are a SaaS software firm so if the user is not using the application because of the complexity of the configuration of privacy, we will lose him."

"We are acting as a data processor for partners who have end-customers. The structure of our contracts is getting more complex and we need to take more risks into account."

"Loss of customers currently on loyalty program who will not renew opt in to allow us to market to them."

"On the one hand everybody is speaking about industry 4.0 as well as IoT and on the other hand the limitations will grow and grow. From our point of view sometimes good knowledge and behavior should be enough than over-regulation."

"The regulation is overreaching in its scope and does not seem to align with the practical requirements of our (and many) businesses. There is too much of a one-size-fits-all and there is limited room for flexibility. We appreciate the intentions and motivations, but the view is that the law itself is a little removed from the realities of daily business."

"The regulation is extremely vague. The range of plausible outcomes includes a total destruction of the online ad ecosystem in Europe all the way to a minor blip. It's extremely hard to plan with that type of uncertainty. Further, there is an irony that the regulation could actually help the largest players: Google and Facebook relative to independents."

"Data inventory mapping across corporate functions (finance, payroll, Human Resources, operations, marketing) was more challenging than first thought. The cloud operations were easier to inventory and comply with as it is regularly audited. All client contracts needed to be updated with standard contractual clauses and resigned. Consent needed to be obtained from all EU persons to collect and all 3rd parties needed to be provided with an updated contract. Any third parties not agreeing would need to be replaced."

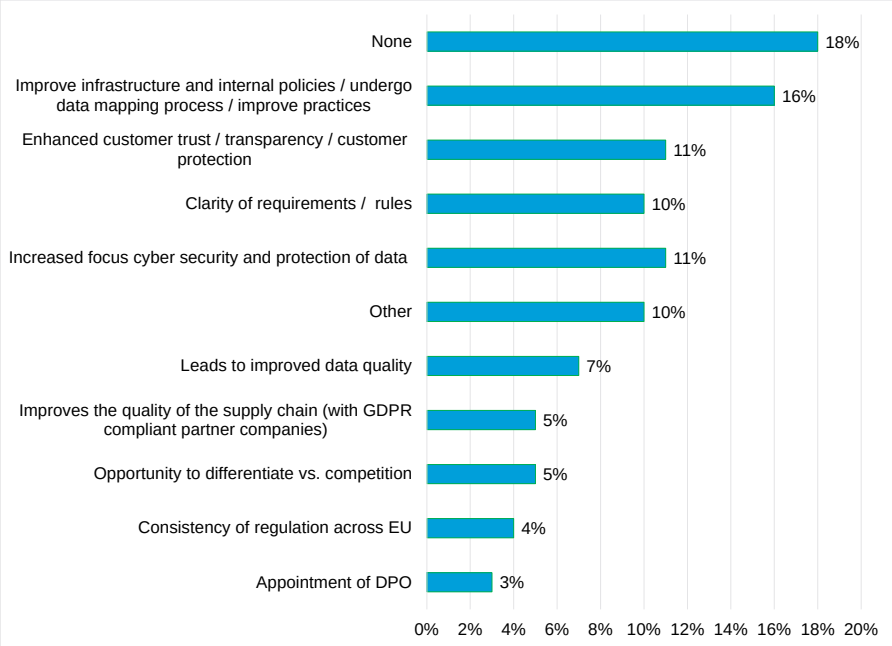
"Assure complete traceability — we have a lot of unstructured data where we have stored personal data right to be forgotten — from technology point of view we have issues to fulfil this demand. Some of aspects of GDPR regulative are still unclear — scope of work which should be done is still not clearly and completely defined."

"Communicating the rules of GDPR to the rest of the organization and ensuring it is treated as a priority"

"Companies need almost surgical control of their data, and it seems like most are still using butter knives rather than scalpels. We couldn't do this on our own."

The challenges are clearly perceived to outweigh the opportunities as 18% of respondents, when asked, could not identify anything helpful about the GDPR. Data mapping and improving data related processes are seen as the most beneficial aspect of the GDPR. The EC sees the 'one stop shop' approach, which harmonizes the regulation across Europe, as a major benefit to organizations, but corporates don't necessarily appear to agree as only 4% cite this as helpful.

Figure 43. Most Helpful Aspects of the GDPR



Source: Citi Research

Quotes related to the most helpful aspects of the GDPR

"Implementing GDPR has forced us to upgrade our data infrastructure and review data storage/retention procedures."

"GDPR will contribute significantly to the reduction in ad fraud and removal of low quality digital advertising. We see GDPR as an opportunity to improve the supply chain in media and advertising. In the longer term, properly targeted and permissioned direct advertising will be more effective due to a reduction in poor quality direct marketing."

"We tend to look at security and privacy as a competitive advantage rather than a burden."

"Definition of a common set of regulations for Europe and need to implement best practices."

"Additional weight to data security/ cybersecurity issues gives company boards more insight into cybersecurity risks."

"Those customers that remain will view us in a more positive light as we have made the effort to comply with GDPR In addition the data from the opt in customers likely to be more accurate and current."

"The data which can be brought will be prequalified. Users would have consented to advertising and as an advertiser we can create more personalized ads to users. Also deleting unwanted and outdated data is a great way to clean databases and servers and save on space and time from data analysts mining inaccurate and outdated data."

"It gives consumers the ability to better control their data sharing with the company and will allow us to be more focused on what consumers want."

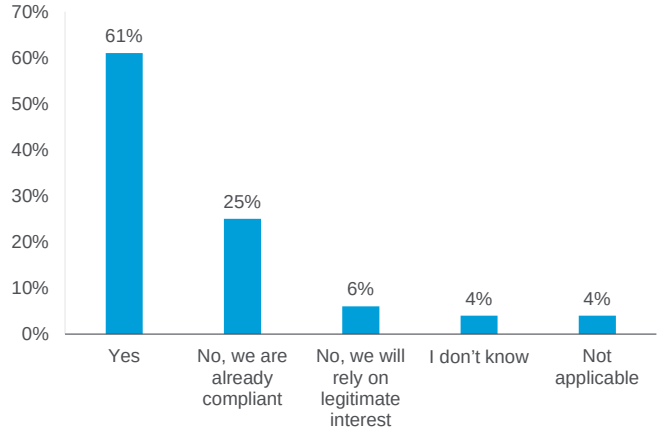
"It's helpful to fully understand all of the business processes that are involved or interact with personal data collection, transmission, storage or usage. This was not mapped E2E in the past."

Approach to Consent

The tightening of consent requirements has been a hotly debated area and one which is identified as a challenge, so we dug into it further in the survey. The majority of companies (61%) expect to change the way they obtain consent from consumers for using personal data. Only 25% think they don't need to as they are already compliant — this rises to 42% amongst technology companies. Only 6% plan to rely on legitimate interest.

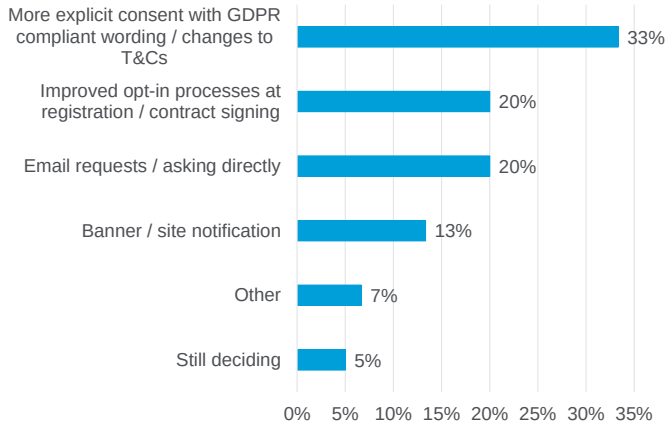
For those who will need to change how they obtain consent, a third are planning to obtain explicit consent and change terms and conditions (T&Cs), 20% of companies are emailing customers directly to request consent, and 20% plan to improve the registration process or amend contracts.

Figure 44. Need to Change How Consent is Obtained from Consumers



Source: Citi Research

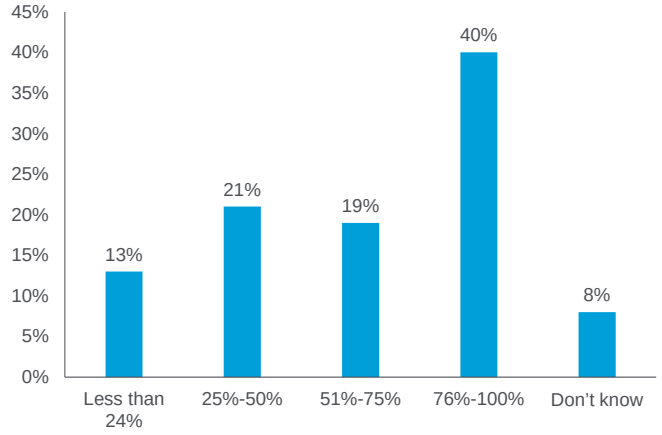
Figure 45. Ways in Which Consent Will be Obtained



Source: Citi Research

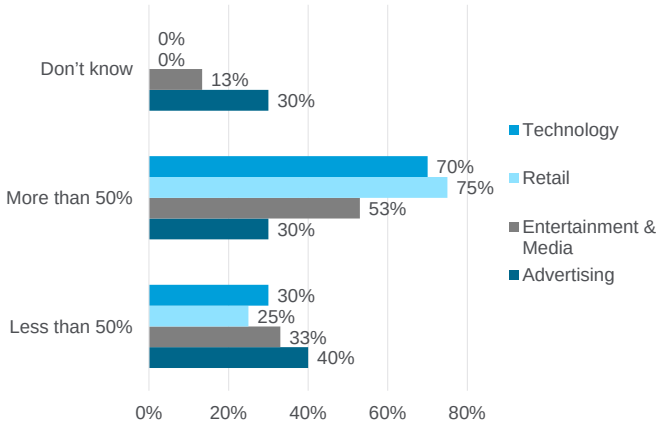
There is general optimism amongst companies about their ability to obtain the consent to some degree but only 40% expect >75% of consumers to provide the necessary consent. There are variances by sector. The retail and technology industries are much more optimistic about obtaining consent from >50% of consumers than the advertising and media industries.

Figure 46. Percentage of Consumers Expected to Provide Consent Required



Source: Citi Research

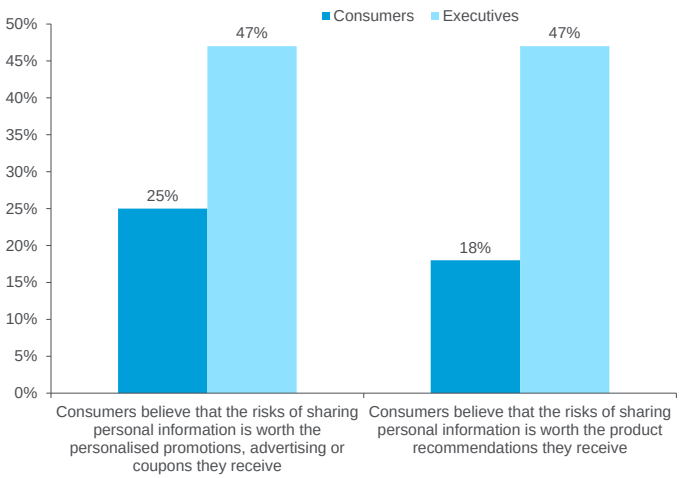
Figure 47. Percentage of Consumers Expected to Provide Consent Required by Sector



Source: Citi Research

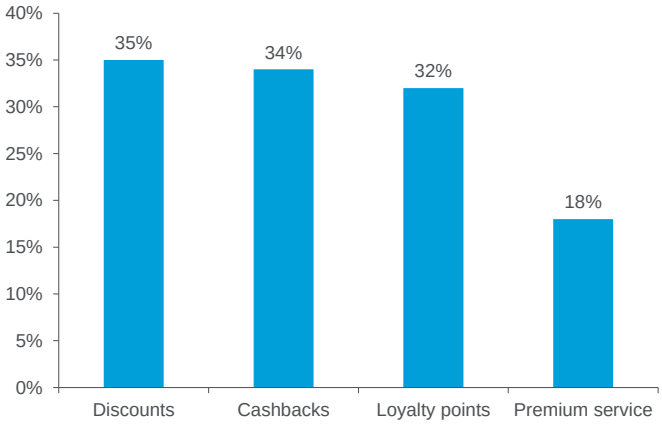
The risk is that companies are still overestimating consumers' inclination to consent to sharing personal data, especially for more personalized ads or areas where the benefit is not perceived to be attractive enough by the consumer (as the previous chapter suggested). According to a Deloitte survey, only 25% of consumers believe the risk of sharing personal data is worth personalized promotions, advertising, and coupons while 47% of executives believe consumers would be willing to share for this purpose. There is scope under the GDPR to incentivize consumers to consent to providing access to personal data, e.g., offering loyalty points, coupons, etc. Even when there is a tangible benefit on offer, consumers' propensity to offer up their data appears to be reasonably low — only a third of consumers claim they would exchange data for discounts, cashback, or loyalty points.

Figure 48. Consumers vs. Executives – View on Sharing Personal Data in Exchange for Personalized Offers



Source: Consumer product consumer and executive survey on data privacy and security. Deloitte LLP. August 2014

Figure 49. Preferred Consumer Compensation for Data Sharing



Source: Syzygy and Attest (April 2018)

Implications

It has been two years since the regulatory changes were set in stone, but while companies are now accepting of the regulation (and have been preparing for the past year), sentiment towards it remains broadly negative. The use of data has been broadly free of onerous regulation, until now. Companies that have been able to utilize and monetize data at scale have, in some cases, been huge successes (if market capitalizations are the measure of success) and the regulator wants to level the playing field. The blanket approach to regulation brings with it a risk that in trying to get the genie back in the bottle it leads to other unintended consequences. Larger companies may get stronger while smaller companies flounder under the red tape. As one respondent put it:

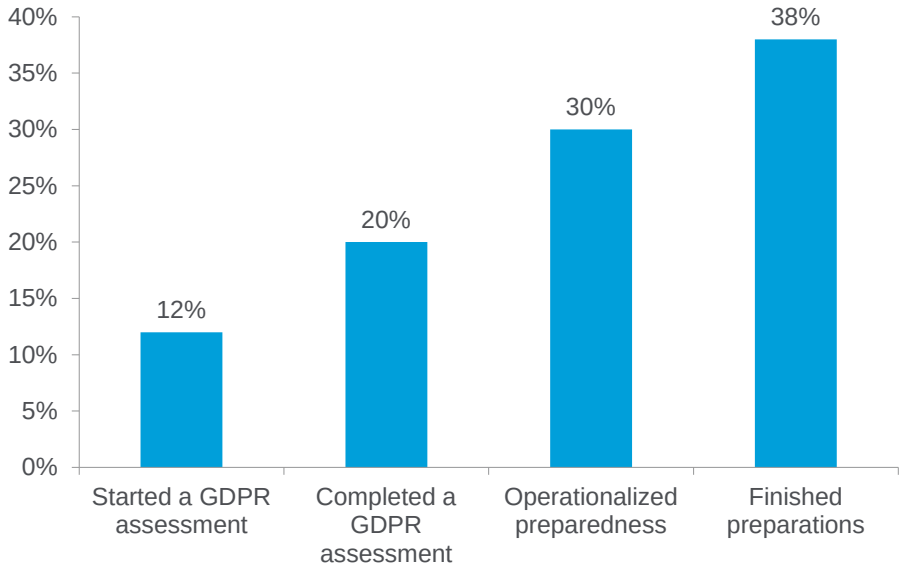
"*The range of plausible outcomes includes a total destruction of the online ad ecosystem in Europe all the way to a minor blip. It's extremely hard to plan with that type of uncertainty*. *Further, there is an irony that the regulation could actually help the largest players, Google and Facebook, relative to independents*."

Some businesses may exit Europe and/or reduce investment or capital allocation to the region as the risks associated with innovation and operating in Europe are too high. The expectation that there will be a reduction in the volume of data, and limitations around the use of data, also brings into question whether this regulation could impact areas such as machine learning, artificial intelligence, and the Internet of Things, all of which are reliant on being able to access a copious amount of data.

The EC believes that the new regulation could reduce inefficiencies and data related costs. Less data may mean there is scope for reduction in some costs e.g. storage but corporates do not share the same view. The majority expect cost of compliance to increase which may mean some level of pressure on margins. For start-ups and smaller entities in the early stages that tend to be loss making, this adds not only another layer of complexity but also additional unwelcome expense.

We expect to see a shakeout of some industries and definite winners and losers — we have already seen evidence of this in AdTech as Drawbridge (a cross-device identity platform) announced it will exit the media business in Europe in response to the GDPR. The flipside of this is that it could present an opportunity for others to take share or act as consolidator. It is likely to favor scale operators that have the resource to manage the regulatory requirements. Those most progressed in preparation for the GDPR are more likely to have involved investor relations (IR) in the implementation process, which helps distribute the message that early preparation could be a competitive advantage.

Figure 50. Companies Involving Investor Relations in GDPR Implementation



Source: PwC GDPR Pulse Survey

That shake out is most likely to come from third parties. The closer a company is to the consumer, and stronger the relationship, the higher the chance the company has of obtaining the consent needed to continue to use personal data. Third parties will be reliant on publishers to obtain consent and publishers will use this as the chance to clean up their sites— clearing out third parties that are not vital for the operation and revenue generation of the site. Doug McPherson, OpenX's VP and General Counsel, believes that many name-brand publishers will reduce supply chain vendors from an average of three or more to just one or two.[11]

We may see a move to an environment where there are more paywalls and requests to log, which could lead to consumers concentrating their usage online across fewer sites. One of the main tenets of the GDPR is data minimization and while it doesn't necessarily set different rules for first-party data versus third-party data, it certainly makes organizations more paranoid about data leakage as it could have significant financial and reputational implications. This could lead to 'data protectionism', both at a country and a company level. For some companies, the GDPR could be used as an excuse to limit access to others, which may lead to less transparency. The unintended consequence being that the walls of the large tech operator's walled gardens are likely to become even more impenetrable, while at the same time their own access to large pools of data may barely change.

In turn, the regulation could accelerate the shift to a 'direct-to-consumer' approach as access to first-party data becomes even more important. To achieve this they need to build a relationship with consumers directly. For example, consumer goods companies often relied on retailers for data in the past, and there is a risk that data becomes harder to share, or certainly the granularity of the data being shared could alter.

[11] Adexchanger.com (26 March 2018)

Companies feel well prepared for GDPR, but there is a risk that they have been overly optimistic in their assessment of the ability to obtain consent needed from consumers, especially for marketing purposes. We have already started to see collaboration between companies, e.g., third-party AdTech operators around central consent and telecoms on data portability:

- In Germany RTL, ProSiebenSat.1, and United Internet have created a log-in alliance with WEB.DE and GMX to create a platform where users can use a single log-in to access services across sectors (Zalando was the first partner to sign up to the solution) and centrally control passwords, profile data, and consents.

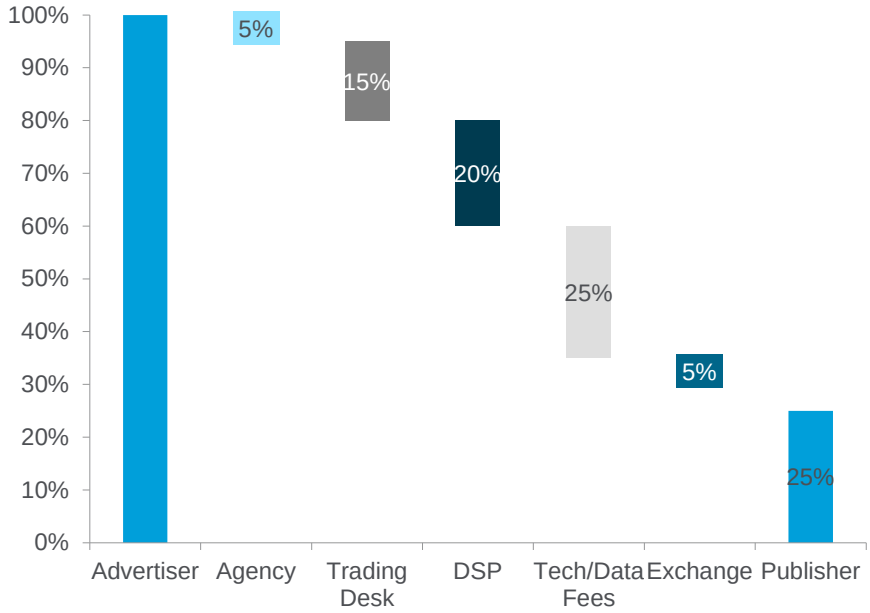
- IAB Europe in conjunction with a number of AdTech companies (AppNexus, MediaMath, Quantcast) has developed a Framework which it hopes publishers will adopt so there is a standardized means to signal consent and only vetted vendors will be allowed on the Global Vendor List. The Framework is also geared towards encouraging global consent so that consumers can provide consent for trackers across sites, rather than specific to a site.

- IBM and Mastercard have joined up to form Truata which has been developed to help organizations conduct data analytics through anonymizing data.

An increase in data anonymization (and the use of hashing to remove the personally identifiable data points) is an obvious route to go down. In the online ad space we could even see a move back towards contextual advertising – this may lead to a reduction in advertising effectiveness, which in turn has implications for pricing (see section on ePrivacy regulation). It may not be as damaging for publishers as it first seems; a cleaner and more simplified AdTech chain (with less third parties sat between the advertiser and publisher) could see publishers taking a higher share of the ad spend than the 25%-50% they currently retain.

We could also see a rise of new solutions to increase transparency and trust, such as the use of blockchain — an area that IBM and the advertising agencies have been exploring.

Figure 51. Digital Advertising – Illustration of the Programmatic Supply Chain



Source: ANA, Firm Decisions, Citi Research

We are starting to see inventive ways to encourage consumers to share data. For example, People.io gathers data on individuals for market research and targeted advertising in return for points that can be converted into money for Netflix, Amazon, and Apple; Ctrlio provides anonymized data to price comparison companies and offers loyalty points to users for switching.

The data mapping process may be a painful one but could prove very useful if it drives companies to centralize and link systems. While the size of databases are likely to fall, companies may make better use of the data they have in areas such as product development, customer service, etc. It could certainly help to focus the mind.

There appears to be a consensus view that the regulation could unintentionally favor larger companies. At the same time, regulators are likely to be watching these companies extremely closely. The next question we tackle is how the regulation will be enforced.

Actions of the Regulators

The question we are often asked is how regulators are going to enforce such far reaching regulation, and what the risk of the highest level of fine (4% global annual turnover) being issued is.

The regulation will be enforced by the Data Protection Authorities (also known as supervisory authorities, or DPAs) and they will have more power than they currently do, not least due to the higher level of fines.

There is evidence of increasing budgets for data protection authorities ahead of the GDPR, but it is still relatively small scale in comparison to the size of the potential task ahead. For example, the Data Protection Commissioner's Office in Ireland announced that its budget has been increased by €4 million for 2018 to €11.7 million (a 55% increase) and it will add 40 staff (taking the total to around 130). It will also use the additional funds to raise awareness amongst businesses and individuals. Ireland is the European headquarters for many technology companies and it will have a key role in enforcing the regulation.[12] This still leaves it under resourced in comparison to the U.K. Information Commission Office (ICO) which is planning to recruit 200 staff to take its headcount to over 700 over the next three years.[13]

While the regulation is set in stone, it is such a broad piece of regulation in terms of stakeholders and interested parties and it has avoided being too narrow, which means many have found it confusing and ambiguous. Guidance has been published by the Article 29 Working Party on 14 key areas; although some of the guidance has come very late in the day and is still being consulted on (guidelines on Consent and Transparency were only finalized in April).

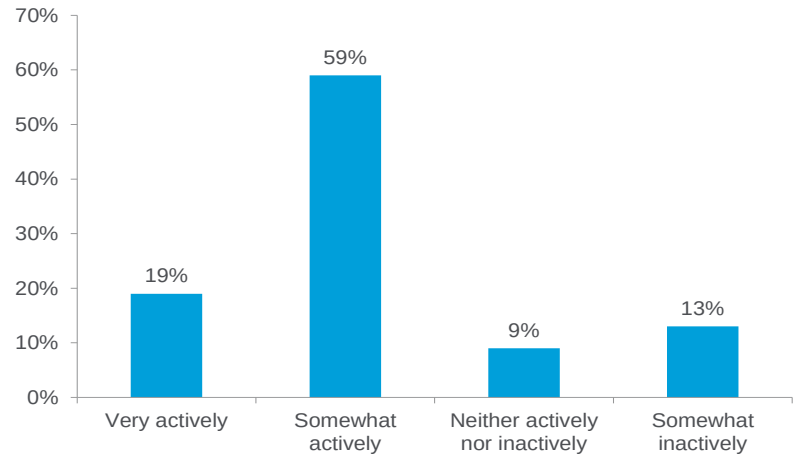
The European Commission has also laid out the actions it plans to take to support member states and businesses including providing an online practical guidance tool, funding for awareness raising (of up to €2 million), closely monitoring the application of the Regulation in member state law (and taking action where it does not appear to be consistent with the Regulation) and a review of the implementation of the regulation in 2019, reporting on it in 2020.

Individual DPA's have also offered more specific guidance. We could see a range of approaches across the various DPAs in Europe. The ICO in the U.K. and the Norwegian Data Protection authorities tend to be perceived as pragmatic compared to the authorities in Germany, Spain, and France. Given resource constraints there is likely to be an element of enforcement that is reactive when there are data breaches etc. The lead regulatory authority will typically be from the 'main establishment' in which the accused is based but regulatory authorities from other member states can challenge decisions if not satisfied.

Our survey found that 19% of respondents believe the authorities will enforce the GDPR very actively and 59% believe they will enforce it somewhat actively. There were no respondents that think the authorities will not enforce the GDPR at all.

[12] https://www.dataprotection.ie/docs/EN/11-10-2017-Data-Protection-Commissioner-welcomes-significant-%E2%82%AC4-million-Budget-2018-funding-increase/b/1670.htm.
[13] https://www.decisionmarketing.co.uk/news/major-ico-recruitment-drive-to-prevent-gdpr-meltdown.

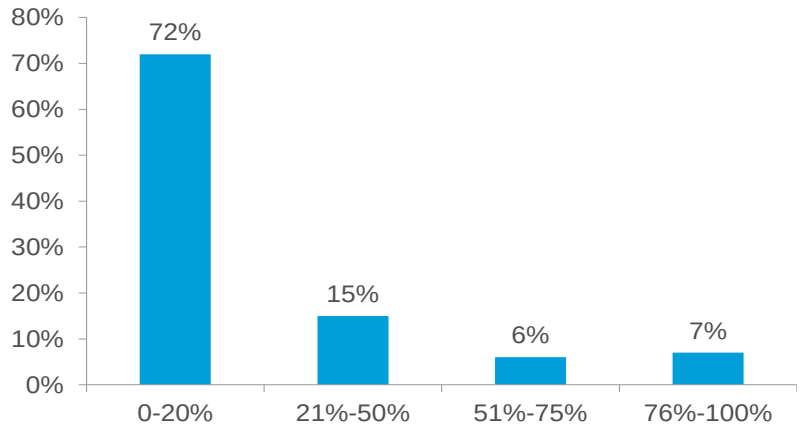
Figure 52. How Actively Will the Authorities Enforce the GDPR?



Source: Citi Research

The respondents see the chance of a maximum fine, i.e. 4% of global annual turnover, as unlikely within the first year. Seventy-two percent (72%) put the chances at 0-20% while only 7% see >75% chance of a maximum fine being issued in year one.

Figure 53. Likelihood of a Maximum Fine Within 12 Months



Source: Citi Research

There is certainly a view that the authorities will look to make an example of a high-profile company through the enforcement of the GDPR:

> We think because they [regulators] don't have more staff to deal fairly [with each case], they will [target] symbolic cases, and some of that enforcement may be arbitrary and unfair
>
> – TOWNSEND FEEHAN, CEO OF IAB EUROPE[14]

[14] Digiday.com, 3 October 2017 (comment made at Dmexco).

The Growing Importance of Data Protection May Inspire Other Regions to Follow Suit

Following several high level data breaches and an increase in newsflow around data being garnered by companies, we think the bigger question now is whether we see other regions starting to adopt the more stringent approach that Europe has taken in order to increase transparency and give consumers more control. The use of data is clearly to going to have a key role in to play the future of the global economy, and building consumer trust will be vital. Interestingly, one of the responses from our survey commented on the potential for other regions to implement a similar regulation:

> "I think that long term it really flips the script on what potentially will be a long-term, broad-reaching phenomenon in other regions, which will have industry-wide impact. For example, in North America the potential ramifications this will have on creating a sense of urgency for our government to institute similar regulation."
>
> – CITI RESEARCH SURVEY

As we highlighted in the original Citi GPS there are a range of approaches to data protection globally. The GDPR is at the stricter end of data protection regulations while the U.S. has typically taken a more laissez-faire approach, opting for regulation at a state and/ or sector level. This leaves a patchwork of regulatory requirements across the U.S. rather than overarching federal legislation. Under President Barack Obama's watch it looked there may be an attempt to introduce national online privacy regulation (Consumer Privacy Bill of Rights), which would bring legislation closer to the GDPR, but there had been limited news on this under the Trump administration, until recently. The Facebook/ Cambridge Analytica news has prompted rumblings that nationwide privacy legislation could come back onto the agenda as Sen. John Kennedy and Sen. Amy Klobuchar have introduced a bipartisan bill aimed at protecting consumer privacy online.[15]

There are challenges with attempting to tackle a global issue with a regional/local approach, as is currently the case, not least the issues this can cause for the flow of data across borders, which may be why some companies are choosing to apply the regulation universally. The European Commission only recognizes 12 countries as providing adequate protection of data (adequacy status) — Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay. and the U.S. (limited to the Privacy Shield). These are regions where data can be transferred from the EU. Adequacy talks are ongoing with Japan and South Korea (South Korea has amongst the tightest regulatory requirements in Asia Pacific in relation to data protection).

[15] USAtoday.com, 12 April 2018.

There are signs that other regions are looking to amend and tighten their data protection regulation. Over the past couple of years individual countries have been reviewing and tightening rules in Asia.[16]

- Hong Kong's Privacy Commissioner for Personal Data announced a review of reform, with a view to the possible implementation of reforms similar to the GDPR.
- The Philippines appointed a National Privacy Commissioner in March 2016 and brought in new data measures (under Implementing Rules and Regulation), some of which are similar to the GDPR, e.g., a 72-hour breach notice period and right to data portability.
- China adopted the Cyber Security Law in November 2016 which was part of the China's three 'pillar' approach to security. While the laws are broader than just data protection, there is a focus on data localization.
- Singapore introduced its Personal Data Protection Act in 2014 and finalized its cybersecurity act in February 2018.
- The Act on the Protection of Personal Information in Japan dates back to 2003, making it one of the oldest in Asia. It was updated and extended in September 2015.

In our conversation with Telefónica later in the report, the team noted that Latin American countries are likely to follow EU-style regulation sooner rather than later. The Ibero-American Data Protection Network (RIPD) is focused on encouraging interest and regulation around protection of personal data. There is evidence that data protection laws are coming to the fore across the region[17]:

- Argentina has had data protection laws in place since 1994 and is seen as the pioneer in the region (hence the adequacy status from the EC). A draft bill was tabled last year which includes consent requirements, breach notifications, and the tightening of individual rights.
- Brazil does not have a general data protection law but there is sectoral-based regulation. There are two data protection bills currently being discussed in Congress to enact a national law across sectors and the Bill on the Protection of Personal Data may come into effect this year. Many of the proposed rules are along the same lines as the GDPR.
- In Mexico, the General Law on the Protection of Personal Data Held by Mandated Subjects was published in January 2017. This lays out general principles for protection of personal data.
- Uruguay has adequacy status from the EC and the data protection authority (URCDP) is planning to issue a report on the impact of the GDPR on Uruguayan data protection regulations. The URCDP is also currently the president of RIPD from 2017-19.

[16] Asia Pacific Data Protection and Cyber Security Guide 2017, Hogan Lovells.
[17] Tracking Privacy trends in Latin America in the age of the GDPR (Feb 2017), EBV.

One of the major areas of contention for privacy groups is that of data surveillance by governments. The Snowden revelations were a major factor behind GDPR getting through the approval process in Europe as well as the cause of the downfall of the Safe Harbor agreement between the U.S. and EU, since replaced with the Privacy Shield. The challenge to Facebook's use of Standard Contractual Contracts (SCCs), which is an EU-U.S. data transfer mechanism, has been referred to the European High Court to determine if EU consumers are adequately protected by data transfer mechanisms such as the Privacy Shield and SCCs (given U.S. government mass surveillance). An unfavorable ruling could ultimately risk the collapse of these mechanisms which could stop dead the transference of data between the EU and U.S. by many companies[18].

Consumers expect to be kept safe and access to data is a crucial tool in providing the intelligence services with a means to do so. The GDPR broadly leaves interpretation open to the individual member states in relation to data being processed for the purpose of prevention, investigation, detection, or prosecution of criminal offences and preventing threats to public security. As recently as November 2016 the controversial Investigatory Powers law was passed in the U.K. (enabling certain state surveillance). The Cyber Security Law in China has raised concerns around whether it could lead to increased surveillance as it requires network operators to store Internet logs for at least six months, block the dissemination of illegal content, and provide 'technical support and assistance' to the authorities in national security and criminal investigations.

Implications

How vigorously the data protection authorities enforce the regulation is likely to be constrained by resource levels. The large scale fines that the regulators will be able to issue substantially increases the risk for all companies managing personal data. Even if the general view is that the maximum fine is unlikely to be issued in year one, the threat of this should be enough to prompt companies to take the regulation seriously.

A resource constrained regulator means enforcement could be unpredictable. The regulators are likely to react to news about breaches. Where there is evidence that organizations have not done everything in their power to comply with the regulation and protect personal data, the risk of a large fine will rise.

The regulators are also likely to want to make an example of a high profile company. The regulation itself potentially reinforces the strong position of some of the existing large Internet platforms, ecommerce operators, etc., but these are also the companies that will have to be completely watertight on their approach to GDPR as they will face the greatest scrutiny. A lot of the debate around privacy and data protection is political and this is likely to influence the approach to enforcement.

It has become increasingly clear to regulators globally that self-regulation does not work; in some cases, profits have been prioritized over privacy. One of the biggest risks facing organizations is that data protection regulation not only becomes a more common feature worldwide, but that rules similar to those laid out by the GDPR become the norm. Given it is based on the principle of data minimization and increased consumer control it could have far reaching implications if rolled out globally. The more data related scandals that occur, the greater the risk that personal data becomes an area that has to be regulated more tightly.

[18] https://techcrunch.com/2018/04/13/privacy-shield-now-facing-questions-via-legal-challenge-to-facebook-data-flows/ .

Organizations could go from untrammeled access to data to a world where there is much greater scrutiny over how personal data is used. It could have implications for areas such as artificial intelligence (which requires vast troves of data) and the speed at which it develops.

As technology develops at such a rapid pace it may not be long before we are asking if this regulation is fit for use as we move to a world of voice assistants and commerce. People want personalization, but they also want to control how that personalization occurs.

In the next two chapters we delve into the complex area of consent —as one of the most contentious parts of the GDPR it warrants more explanation and the potential for the regulation to tighten even further in Europe with the ePrivacy Regulation coming down the pipe.

Understanding Consent and Legitimate Interest

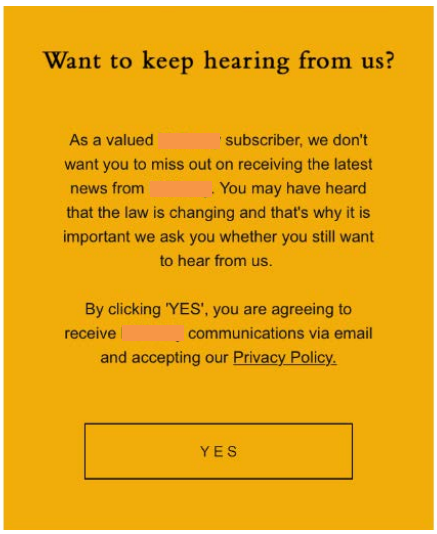
Six Bases for Legal Justification for Processing Personal Data:

1) Consent;
2) Compliance with a contract to which the data subject is party;
3) Compliance with legal obligation to which the controller is subject;
4) Necessary to protect the vital interests of another subject;
5) Necessary for the fulfilment of a task conducted in the public interest;
6) Processing is necessary for the legitimate interests pursued by the controller. Expectations of data subject to be taken into account.

The area of consent is one worth digging into in more detail. It is one of the six legal bases that companies can use to justify collection and processing of personal data. It is one that has caused a lot of confusion and ambiguity and it will also become an even greater focus for electronic communications if the ePrivacy Regulation comes into effect as currently proposed. One of the other justifications for data collection is 'legitimate interest', and this has led to various interpretations (the ePrivacy regulation is proposing to remove this as a basis for electronic communication).

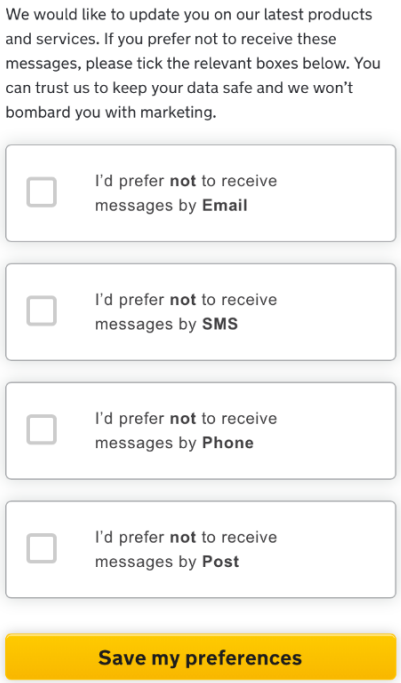
Over the past month the emails from companies notifying (EU-based) customers about the change to the data protection law have been coming thick and fast. We have seen several different approaches in the lead up to the GDPR, ranging from emails stating that email communications will no longer be sent unless consent is given (requiring explicit opt in) and email requests for customers to provide communication preferences, e.g., post, email etc. through the use of tick boxes, to emails linking to long privacy notices stating that profiling using various sources of data will occur due to the legitimate interest they have in marketing activities to offer products/services that may be of interest (with an email address to contact to opt out). We have included some of the examples below (removing the company names) from across a range of industries.

Figure 54. Email Requesting Explicit Consent (retail brand)



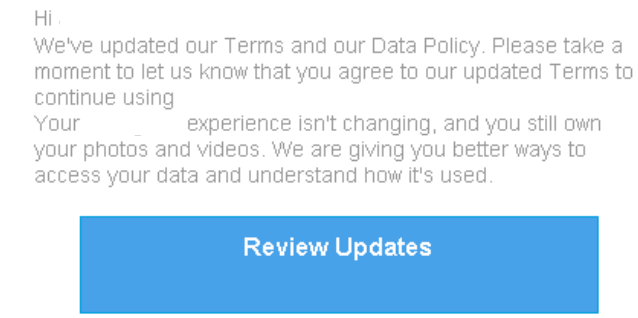
Source: Company

Figure 55. Email Requesting Communications Preferences (insurance brand)



Source: Company

Figure 56. Email Requesting Agreement to Change of Terms to Continue Use (Social Media Platform)


Hi

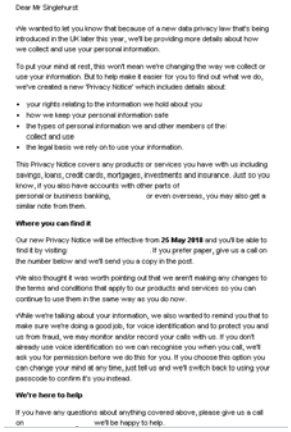
We've updated our Terms and our Data Policy. Please take a moment to let us know that you agree to our updated Terms to continue using

Your experience isn't changing, and you still own your photos and videos. We are giving you better ways to access your data and understand how it's used.

Review Updates

Source: Company

Figure 57. Email Providing Link to Privacy Policy (Financial Brand)


Dear Mr Singlehurst

We wanted to let you know that because of a new data privacy law that's being introduced in the UK later this year, we'll be providing more details about how we collect and use your personal information.

To put your mind at rest, this won't mean we're changing the way we collect or use your information. But to help make it easier for you to find out what we do, we've created a new 'Privacy Notice' which includes details about:

- your rights relating to the information we hold about you
- how we keep your personal information safe
- the types of personal information we and other members of the collect and use
- the legal basis we rely on to use your information.

This Privacy Notice covers any products or services you have with us including savings, loans, credit cards, mortgages, investments and insurance. Just so you know, if you also have accounts with other parts of personal or business banking, or even overseas, you may also get a similar note from them.

Where you can find it

Our new Privacy Notice will be effective from **25 May 2018** and you'll be able to find it by visiting . If you prefer paper, give us a call on the number below and we'll send you a copy in the post.

We also thought it was worth pointing out that we aren't making any changes to the terms and conditions that apply to our products and services so you can continue to use them in the same way as you do now.

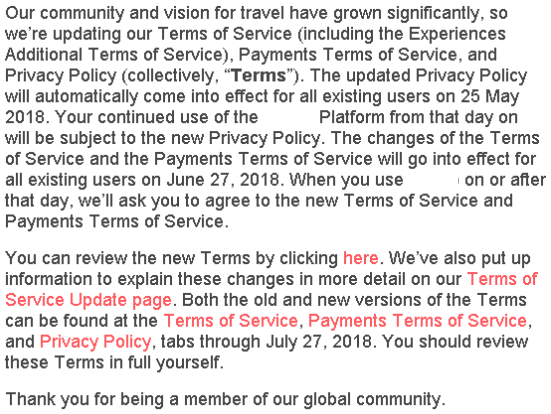
While we're talking about your information, we also wanted to remind you that to make sure we're doing a good job, for voice identification and to protect you and us from fraud, we may monitor and/or record your calls with us. If you don't already use voice identification so we can recognise you when you call, we'll ask you for permission before we do this for you. If you choose this option you can change your mind at any time, just tell us and we'll switch back to using your passcode to confirm it's you instead.

We're here to help

If you have any questions about anything covered above, please give us a call on we'll be happy to help.

Source: Company

Figure 58. Email Requesting Agreement to Change of Terms to (Travel Platform)

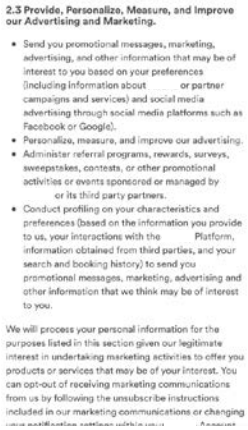

Our community and vision for travel have grown significantly, so we're updating our Terms of Service (including the Experiences Additional Terms of Service), Payments Terms of Service, and Privacy Policy (collectively, "**Terms**"). The updated Privacy Policy will automatically come into effect for all existing users on 25 May 2018. Your continued use of the Platform from that day on will be subject to the new Privacy Policy. The changes of the Terms of Service and the Payments Terms of Service will go into effect for all existing users on June 27, 2018. When you use on or after that day, we'll ask you to agree to the new Terms of Service and Payments Terms of Service.

You can review the new Terms by clicking here. We've also put up information to explain these changes in more detail on our Terms of Service Update page. Both the old and new versions of the Terms can be found at the Terms of Service, Payments Terms of Service, and Privacy Policy, tabs through July 27, 2018. You should review these Terms in full yourself.

Thank you for being a member of our global community.

Source: Company

Figure 59. Snapshot of Privacy Policy Highlighting Use of Data for Marketing on the Basis of Legitimate Interest (Travel Platform)


2.3 Provide, Personalize, Measure, and Improve our Advertising and Marketing.

- Send you promotional messages, marketing, advertising, and other information that may be of interest to you based on your preferences (including information about or partner campaigns and services) and social media advertising through social media platforms such as Facebook or Google).
- Personalize, measure, and improve our advertising.
- Administer referral programs, rewards, surveys, sweepstakes, contests, or other promotional activities or events sponsored or managed by or its third party partners.
- Conduct profiling on your characteristics and preferences (based on the information you provide to us, your interactions with the Platform, information obtained from third parties, and your search and booking history) to send you promotional messages, marketing, advertising and other information that we think may be of interest to you.

We will process your personal information for the purposes listed in this section given our legitimate interest in undertaking marketing activities to offer you products or services that may be of your interest. You can opt-out of receiving marketing communications from us by following the unsubscribe instructions included in our marketing communications or changing

Source: Company

Consent According to GDPR

The GDPR characterizes consent as the following:

Article 4(11) "… *freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."*

The GDPR attempts to further specify the conditions necessary for consent in order to increase consumer control over what, and how, personal data is used. To be clear, the consent we are focusing here on relates to personal data, not sensitive personal data or children's personal data both of which entail an even more rigorous approach to consent. The GDPR makes two main changes:

1. Standards for consent bolstered under the GDPR

Consent was one of the most contentious elements of the regulation negotiations, with agreement only being reached in the final rounds. Under the Directive regime, standards of consent varied across Europe. The Data Protection Directive specified that consent had to be 'unambiguous'

Subsequently, the 2009 ePrivacy Directive (09/136/EC), which governs electronic communications, introduced the requirement that clear and comprehensive information be provided to the data subject before consent can be acquired. Most consumers in Europe have become used to the appearance of Cookie banners popping up when landing on a webpage and specifying that, on the basis of continued use of the website, consent for dropping cookies will be assumed.

The GDPR tightens consent requirements. It must be freely given, specific, informed and unambiguous by a statement or clear action. Pre-ticked boxes do not qualify.

The GDPR stops short of uniform 'explicit consent' for all personal data, but does tighten up consent requirements. Under article 6, it requires proactive expression of consent and consent must be unambiguous and demonstrable. Recital 32, states that "*… the use of default options which the data subject is required to modify to object to the processing, such as pre-ticked boxes, does not express free consent…but consent can be given through "another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data."*

The controller needs to be able to demonstrate consent has been obtained.

It is also no longer good enough to be satisfied that consent has been obtained, the controller also needs to be able demonstrate this is the case: Article 7 "*Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*"

2. The GDPR will increase regulation on the framing and context of the consent decision for consumers

Consent must be obtained for each form of tracking. Consent for processing cannot be bundled into a single consent option or T&Cs if it is not necessary for the performance of the contract or delivery of the service. Equivalent services should be reasonably obtained without consenting to tracking.

Consent will also have to be given to each form of tracking independently. Currently, many permissions are 'bundled' within a single consent option, sometimes with scope even beyond data processing. The GDPR changes this, rendering such consent decisions illegitimate. Article 7(2) of the GDPR specifies that *"consent shall be presented in a manner which is clearly distinguishable from the other matters."* In the recitals, the meaning of this is further specified, *"…Consent is presumed not to be freely given if it does not allow separate consent to be given to different data processing operations…."* As a result, consent tools will increasingly have to allow consumers to determine individual tracking operations. Collecting data for the sake of it will no longer be easy as the controller has to be transparent about the purposes the data is being used for, and notify the consumer if that changes.

Article 13: "*Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information.*"

The regulation appears to render access to services conditional on consent to data collection illegal in many contexts. The regulation itself, under Article 7(4) says:

"When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, ***the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."***

This is further fleshed out in the recitals. Here, when considering whether consent is legitimate, the EDPS say that "*Consent is presumed not to be freely given… if the performance of a contract is made dependent on consent… and the data subject cannot reasonably obtain equivalent services without consent.*"[19] The implication, then, is not a blanket ban on the practice. Crucially, the GDPR emphasizes whether equivalent services can be reasonably obtained without consenting to tracking.

The overall aim here is to ensure consumers are not held at ransom and consent is not 'forced' by requirements that are irrelevant to the actual purpose of the data processing. The guidance allows for a little flexibility here, as we will see.

Finally, the GDPR will also require consent can be withdrawn at any time with equivalent ease as giving consent.

Controller vs. Processor

Controllers and processors must comply with the GDPR but the responsibility for obtaining consent lies with the controller. Both will need to ensure suppliers are compliant with the GDPR and contracts reflect increased obligations.

Both controllers and processors will have to comply with the GDPR but the delineation of responsibility for obtaining consent from consumers will depend on whether you are controller or processor, with the duty falling to the former. Most companies operating within the online advertising space will be making the distinction between when they are operating as controller and when they are operating as processor. Both processors and controllers will need to ensure that suppliers are trustworthy and compliant with GDPR and, subsequently, that contracts with those suppliers are watertight.

Google and Facebook have both laid out their positions with respect to this, for example Google has stated it will operate as controller for some of its key ad products such as AdMob, AdWords, and DoubleClick Exchange, but it will be processor for Google Analytics and DoubleClick Bid Manager, for example. When it operates as controller it will take responsibility for obtaining consent from first party users across its sites but publishers and advertisers will have to get consent from their own users to use Google products, such as Analytics, on their site. Facebook will also be controller for any data generated by users on Facebook and it will take responsibility for consent. For brands that use Custom Audiences or Facebook's measurement and analytics tools, it has defined itself as processer which means that Facebook will now request that advertisers guarantee they have the right consent for any data they upload to Custom Audiences (which matches email lists with Facebook's database).

Companies such as Adobe and Salesforce, with AdTech assets, and the advertising agencies are making it clear that their role is generally as a processor. Alisa Bergman, Chief Privacy Officer of Adobe, said "It's very important to be careful that we don't take on the role of controller — it's their data and we process it on their instruction."[20]

[19] Recital 34 EDPS.
[20] Adexchanger.com (13 March 2018)

Legitimate Interest According to GDPR

Legitimate interest justification depends on proposed action being proportionate to need. The rights of individuals must not be undermined.

Beyond consent, the other basis on which processing can be undertaken is for so called 'Legitimate Interest' purposes. Legitimate interests are commonly understood to include things such as ensuring the integrity of IT networks. Another example, used by the ICO, where legitimate interests could be applicable is:

"*A finance company is unable to locate a customer who has stopped making payments under a hire purchase agreement. The customer has moved house without notifying the finance company of his new address. The finance company engages a debt collection agency to find the customer and seek repayment of the debt. It discloses the customer's personal data to the agency for this purpose. Although the customer has not consented to this disclosure, it is made for the purposes of the finance company's legitimate interests – i.e., to recover the debt.*"'[21]

A legitimate interest justification for processing depends on the proposed action being proportionate to need. It must also not undermine the rights and interests of the individual whose data is being processed to an 'unwarranted' degree.

The GDPR inserts 'reasonable expectation' condition which may make legitimate interest a harder basis to justify. It also states direct marketing may be regarded as a legitimate interest which some may use as a loophole to continue existing marketing practices.

'Legitimate interest' was a basis for processing in the 1995 Directive. While the GDPR is broadly similar in this regard, the regulation does insert a 'reasonable expectation' condition in the considerations of whether legitimate interests justify processing:

"The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration ***the reasonable expectations*** *of data subjects based on their relationship with the controller……The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest"*

This small wording change could have far reaching implications as it may make the use of the legitimate interest basis, overall, more difficult to justify. What has caused a lot of debate, however, is the final line which states that direct marketing may be regarded as a legitimate interest (as long as the data subject is made aware of the right to object to the processing). Some could effectively see this as a loophole by which to continue with existing marketing practices.

How to Interpret the Requirements

Both the consent and legitimate interest requirements prompt a number of questions:

- What constitutes unambiguous consent?
- What is a proactive expression of interest e.g., a tick box, scrolling down the page etc.?
- Do I need to re-obtain consent for existing databases?
- Can access to a site be conditional upon obtaining consent?
- What is a 'reasonable expectation' under legitimate consent?

[21] https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/

– What types of direct marketing falls under the legitimate consent basis?

Only one basis can be used to process personal data and consent is the higher hurdle (for marketing purposes the ePrivacy Directive is applicable alongside the GDPR). If a consumer does not provide consent then the controller cannot use legitimate interest as an alternative.

The controller has to choose which basis is being applied to justify data collection. If consent is not given when requested, the controller cannot continue with processing personal data on the grounds of legitimate interest.

Guidance has been provided by the Article 29 Working Party and DPAs (including the ICO in the UK).

The Article 29 Working Party has provided guidance on both areas as has the ICO. Consumers will generally have stronger rights when using consent as the basis — such as right to erasure and right to data portability. For the purposes of marketing the ePrivacy Directive is also applicable alongside the GDPR (until it is replaced by the ePrivacy Regulation).

Taking the topic of consent first, the Article 29 Working Party issued its final guidance on consent on the 16th of April 2018. There are several areas that it provides clarity on:

Freely given: For data that is not essential to the delivery of the service/product, consent should not be bundled into T&Cs or made a condition of the contract. An equivalent service must be available to those not consenting. Companies have some scope to incentivize consumers through loyalty schemes and possible paid access.

The online advertising industry may use Recital 25 of the ePrivacy Directive as a justification for making access condition on acceptance of cookies.

- **Freely given:** Consent should be not be bundled up as a non-negotiable part of the T&Cs. The example it provides makes that very clear:

  "A bank asks customers for consent to use their payment details for marketing purposes. This processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services. If the customer's refusal to consent to this processing purpose would lead to the denial of banking services, closure of the bank account, or an increase of the fee, consent cannot be freely given or revoked."

  The A29 WP suggests that if companies offer services that include consenting for use of personal data for purposes other than those necessary to fulfil the service and an equivalent service is available to those who choose not to consent, then this could be deemed to be a genuine choice. It is made clear that both services need to be equivalent. The ICO also states that companies can incentivize consumers to consent as long as there is no penalization of those who do not provide consent. We could see organizations become more creative about how they offer loyalty schemes, early access to product/services and even possibly a paid access tier.

  Whether a service can be withheld without consent for processing remains an area where interpretation varies. The IAB Europe, for example, has interpreted it in a fairly loose way in its Consent Working Paper (28 November 2017) stating that the GDPR doesn't necessarily prohibit making access to a service conditional on consent, and quotes the ePrivacy directive (Recital 25): "*Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose*." The IAB Europe makes an assumption that advertising is a legitimate purpose as it relates to the consumer experience, and many will probably use this 'loophole'.

Specific: Consent must be obtained for the specific purpose the data is being used for. Consent must be obtained if data is going to be used for a new purpose that has not been specified in the past.

- **Specific:** The controller has to be specific about the purpose it is processing the data for. For example, if a company wants to send marketing by email to a customer and share their details with other companies within the group, the controller would have to obtain consent separately for the two purposes. If the controller wants to use data for a new purpose that it has not obtained consent for in the past, then it would have to seek new consent (and it cannot rely on legitimate interest for new purposes). The example given by A29WP is:

"A cable TV network collects subscribers' personal data, based on their consent, to present them with personal suggestions for new movies they might be interested in based on their viewing habits. After a while, the TV network decides it would like to enable third parties to send (or display) targeted advertising on the basis of the subscriber's viewing habits. Given this new purpose, new consent is needed."

In the Article 29 Working Party's guidelines on Transparency it states that a layered privacy notice can be used online to help guide the user to a certain section of the privacy notice (which should not require them to scroll through lots of text to find). The first layer of the notice should include the purpose of processing, the identity of the controller and a description of the data subject's rights.

Expression of consent: Consent must be via an affirmative action and given before data is processed. The controller must record how consent was obtained. Scrolling down a webpage is not sufficient but swiping a request bar or tilting a phone could be.

- **Expression of consent:** Obtaining consent should not be disruptive to the user and A29WP clarifies that using physical motion (e.g., swiping a screen bar, turning a smartphone clockwise), could all be considered an indication of consent to a specific request as long as the information has been clear (e.g., instruction to swipe left to agree to the use of information X). Scrolling down or swiping through a website will not be sufficient. The controller must record how consent was obtained and consent has to be given before the controller starts to process the data (which the A29WP believes is implied by the GDPR).

The Internet Advertising Bureau has built its consent framework on the assumption that consent given to a controller is relevant across all sites that third party operates across.

The IAB's Framework for consent is based on the premise that consent can be obtained on a "global basis" i.e. consent given to a controller is relevant across their sites and across other sites that the relevant third party may operate. This stems from A29 WP's opinion on online behavioral advertising in 2011[22] which stated that "*if a third party ad network on a website receives consent for an OBA cookie, this consent will not only be valid on other pages of the same website, but also for other websites that share the same OBA network. Consequently, for an average user, the number of consent requests will decrease as he/she navigates and expresses his/her choices.*"

This guidance was provided prior to the GDPR so it may not necessarily be sticking to the spirit of the law which requires greater transparency.

Withdrawal of consent: It should be as easy to withdraw consent as it was to provide consent. It should not have a detrimental impact on the service.

- **Withdrawal of consent:** Withdrawal of consent should be as easy as the process to provide consent. For example, if an individual purchases tickets online and provides consent for marketing purposes at the same time, then the means to withdraw consent should not be over the phone. It should be online in the same way the consent was requested. Consumers should be able to refuse or withdraw consent without a detrimental impact on the service the user can access. An example from A29WP:

Historical data can be used if the means to obtain consent was compliant with the GDPR.

"A data subject subscribes to a fashion retailer's newsletter with general discounts. The retailer asks the data subject for consent to collect more data on shopping preferences to tailor the offers to his or her preferences based on shopping history or a questionnaire that is voluntary to fill out. When the data subject later revokes consent, he or she will receive non-personalized fashion discounts again. This does not amount to detriment as only the permissible incentive was lost."

[22] Article 29 working party Opinion 16/2011, WP188

Historical data can be used if the means to obtain consent was in line with the GDPR. A29WP states that as a one off during the initial transition to the GDPR, if the data does not meet the requirements of the GDPR consent then the controller can determine whether there is scope for processing using a different lawful basis.

Legitimate Interest

Three part test to determine if legitimate interest is a reasonable basis: consider the purpose for the processing (has to be a clear benefit to the company); consider if processing is necessary; consider if individual rights are not being overridden and if the purpose would be reasonably expected by the individual.

According to the ICO an organization should apply a three part test to ascertain whether legitimate interest is a reasonable basis: consider what the purpose is for the processing, which has to be a clear benefit to the company e.g., marketing goods to existing customers to increase sales — data cannot be gathered on a 'just in case' basis; consider whether the processing is necessary; consider whether rights are being fairly balanced and individual rights are not being overridden (this includes whether people would expect details to be used in such a way).

The Article 29 Working Party published an opinion on legitimate interest in April 2014 (06/2014). It acknowledged that legitimate interest could be used to personalize offers to existing customers but it also places a great deal of emphasis on the balancing test, arguing that combining data across sources, collected for different purposes, to create a 'complex profile' of customers would not be acceptable without consent as it is '*likely to present a significant intrusion into the privacy of the customer, and when this is so, the controller's interest would be overridden by the interests and rights of the data subject.*'

Article 29 Working Party's opinion on legitimate interest specifies that personalized offer to existing customers is allowed under this basis as long as customers are informed how to opt out. Creating complex profiles of customers (through the combination of various data sources) would not be allowed without consent.

The Article 29 Working Party also includes examples of scenarios where legitimate interest could be used. The case below highlights that the data used was kept to a minimum, actions are not seen as intrusive (limited data used), the user may reasonably expect it and the customer was informed about how to opt out:

> *"Claudia orders a pizza via a mobile app on her smartphone, but does not opt-out of marketing on the website. Her address and credit card details are stored for the delivery. A few days later Claudia receives discount coupons for similar products from the pizza chain in her letterbox at home."*

The scenario below is **not** deemed acceptable under legitimate interest due to the scale of data collection and the techniques used to influence the consumer. There was also no clear "opt out" provided, and the balancing test is clearly tilted in favor of the company. Consent would be required in this type of scenario.

> *"Claudia's address and credit card details as but also her recent order history (for the past three years) are stored by the pizza chain. In addition, the purchase history is combined with data from the supermarket where Claudia does her shopping online, which is operated by the same company as the one running the pizza chain. Claudia is provided by the pizza chain with special offers and targeted advertisement based on her order history for the two different services. She receives the adverts and special offers both online and off-line, by regular mail, email, and placement on the website of the company as well as on the website of a number of selected partners (when she accesses these sites on her computer or via her mobile telephone). Her browsing history (click-stream) is tracked as well. Her location data is also tracked via her mobile phone. An analytics software is run through the data and predicts her preferences and the times and locations when she will be most likely to make a larger purchase, willing to pay a higher price, susceptible to being influenced by a particular rate of discount, or when she craves most strongly for her favorite desserts or ready-meals.*

She was unable to find user-friendly information or a simple way to switch off these advertisements although the company claims there is an industry-wide opt-out scheme in place.'"

Direct marketing via electronic means faces a higher bar than postal direct mail. Electronic marketing can only be used if it is to an existing customer who has bought a similar product or service from the company (soft opt-in) or if consent has been received.

In practical terms, direct marketing by electronic means may not be quite as easy to justify as postal direct mail. The reason being that the ePrivacy directive provides more specific rules (on top of the GDPR) in relation to electronic communications. The directive requires that individuals need to provide consent for some forms of electronic marketing. Electronic mail marketing (which includes emails, texts, social media messages) should not be sent to individuals unless they have specifically provided consent to receive it or they are an existing customer who has bought a similar product or service from the company in the past, and an opt out was provided at the time (known as 'soft opt-in').

Those with an existing relationship can only market their own similar products or services, and the boundaries depend on what would be reasonably expected. For example, the ICO believes that someone who has shopped at a supermarket may reasonably expect messages about a wider range of goods than someone who has shopped at a specialist store for a specific product, although they may not expect messages from the supermarket about financial products i.e. products not bought in a similar context. The ICO's table below provides more clarity on when legitimate interest can be used as justification for direct marketing.

Figure 60. ICO's Guidance on Use of Legitimate Interest for Direct Marketing

Marketing Method	Is legitimate interest likely to be appropriate?
Post	✓
'Live' phone calls to TPS/CTPS registered members	×
'Live' phone calls to those who have objected to your calls	×
'Live' phone calls where there is no TPS/CTPS registration or objection	✓
Automated phone calls	×
Emails/text messages to individuals — obtained using 'soft opt-in'	✓
Emails/text messages to individuals — without 'soft opt-in'	×
Emails/text messages to business contacts	✓

Source: Information Commissioners Office

Implications

Consent and legitimate interest as bases to justify data processing favors those with existing (strong) customer relationships. Many will prefer the legitimate interest route as there is no need for a clear consent notice (although opt out has to be made clear), which brings with it the risk of low consent levels, and user's rights are stronger under the use of consent. Legitimate interest, in particular, is likely to reinforce the strength of well-established operators (especially in the retail space), raising barriers to growth for those that are smaller or starting up. For targeting prospective customers it will be very hard to use databases of acquired email addresses to do so. One consequence of this is we could see the resurgence of direct mail. This is good news for the postal services.

While the guidance on the use of legitimate interest makes the point that there is a fine line between acceptable use of data for direct marketing purposes and an intrusive use of data, it still means there is some scope for variations in interpretation of what is acceptable versus what is intrusive, and each company's assessment will vary depending on its customer base. The IAB Europe pointed out a 'loophole' that some will use to justify the collection of data for online advertising and recommendations as a legitimate purpose.

Consent is a complex area. The distinction between controller and processer has to be clearly established. Access to a service cannot technically be withheld if consent is not provided for the use of personal data (that is not necessary to fulfil the service) and access to non-essential data cannot be bundled in the T&Cs but the guidelines provides scope to incentivize users to share some level of data (as long as the purpose is made clear) that offers a benefit in exchange for the data, as long as an alternative equivalent service is offered to those not providing consent. We are likely to see organizations become more creative with means to incentivize consumers to consent e.g. through points schemes, early access to products and we may even see some introduce a paid tier as an alternative (although it is questionable as to whether this would be perceived as detrimental to a user). As we noted earlier, we have started to see collaboration between companies to offer central log in platforms for consumers. Both an increase in incentivization schemes and central privacy control tools could lead consumers to limit the number of sites they interact with.

The guidelines on consent corroborate the points made earlier that those closest to the consumer and with the strongest relationships will be in the best position to continue as they were.

More Regulatory Change: ePrivacy Regulation

The ePrivacy Directive is set to become regulation with the same level of fines as the GDPR. It would override the GDPR in relation to electronic communications and could have damaging consequences for the digital industry.

The GDPR is certainly not the last of the new data protection rules we are likely to see. There is another piece of ePrivacy related regulation in Europe, more specifically focused on electronic communication, which is in the pipeline. The European Commission is in the process of converting the ePrivacy Directive into regulation (with the same level of fines as the GDPR). The proposed amendments to the directive could lead to damaging consequences for the digital industry, especially those reliant on an advertising funded model. As the ePrivacy Regulation is what is known as lex specialis, it would override the GDPR requirements (lex generalis) in its specific area of focus i.e., electronic communications.

Implications of ePrivacy Regulation Could Be Damaging for The Digital Ad Industry

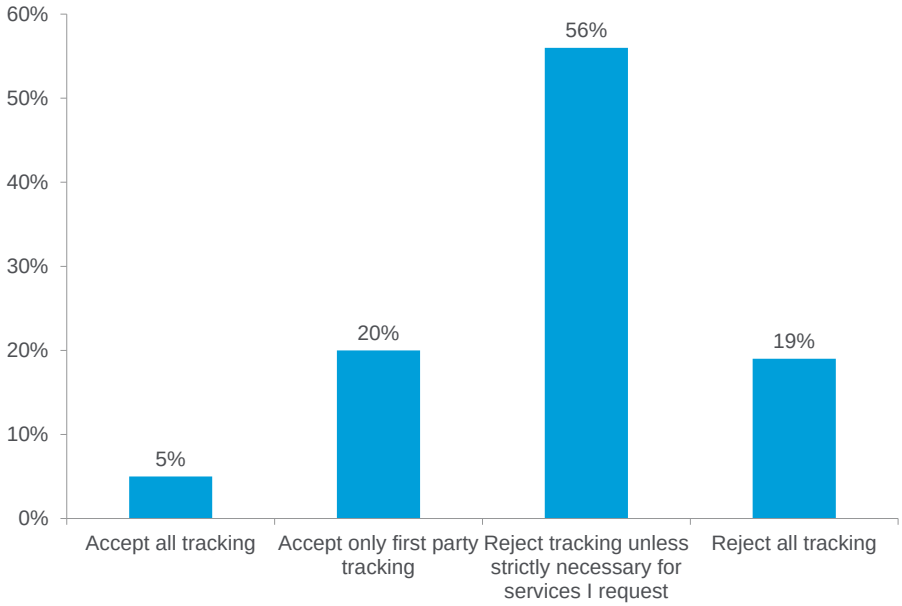
Before we provide the background, details and timing of the ePrivacy Regulation we will delve into what the economic impact could be if the proposed regulation comes into effect in its current form.

It is very clear that the online advertising industry is concerned about the implications of the ePrivacy regulation and the risk that limiting the use of personal data as a currency will hinder behavioral advertising. So, what could happen to advertising if this regulation comes in?

The proposed ePrivacy regulation requires unconditional consent for most forms of tracking and removes the legitimate interest concept. It proposes the browser becoming gatekeeper for privacy settings and tracking options. One survey indicates only 5% of would accept tracking.

While the GDPR allows six (6) bases to justify the processing of personal data, the ePrivacy Regulation essentially requires unconditional consent for most forms of tracking (although there is a suggestion that those with a relationship with a customer can send marketing information related to its own products and services), and completely removes the concept of legitimate interest. As we noted earlier, one of the biggest unknowns is what consumers will consent to, and the ePrivacy Regulation proposes using the browser as gatekeeper for privacy settings with several tracking relate options: Accept all tracking; Accept only first party; Reject tracking unless strictly necessary; Reject all tracking as the options provided. A Pagefair survey testing how U.K. consumers may respond to the browser settings approach proposed by the EC found that 75% claim they would opt to either reject tracking that is not strictly necessary or reject tracking altogether. Only 5% would accept all tracking.

Figure 61. What Would You Select if Shown the Following Message?



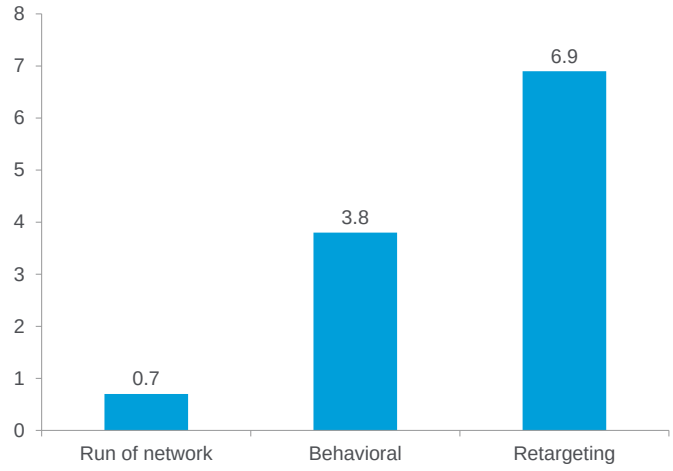
Source: Pagefair

Quantifying the Impact

There are two studies that have attempted to quantify the impact of the ePrivacy regulation on online advertising. One is from IAB Europe/IHS Markit and the other was conducted by WIK-Consult on behalf of the German Federal Ministry for Economic Affairs (November 2017). Neither paints a particularly pretty picture.

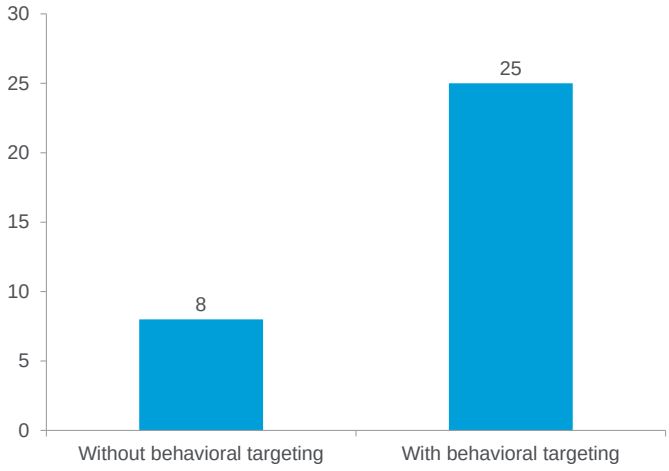
The IAB Europe/IHS Markit study estimates that two thirds of digital targeted advertising revenue is generated from online behavioral advertising (which includes data from online and offline browsing, purchase behavior and signals of intent – data that enables advertisers to identify particular groups e.g. those looking to buy a car). It also predicts that by 2020 out of the €23.5 billion ($28.4bn) European online targeted display advertising market, €21.4 billion ($25.9bn) will be generated by behavioral targeting. Conversion rate and pricing is higher when behavioral targeting is applied.

Figure 62. Average Conversion Rates Display Banner Advertising in Europe



Source: IAB & IHS Markit (The Economic Value of Behavioral Targeting in Digital Advertising, 2017)

Figure 63. Cost Per Thousand Uplift for Behavioral Advertising in Europe (Max, €)



Source: IAB & IHS Markit (The Economic Value of Behavioral Targeting in Digital Advertising, 2017)

IAB Europe and IHS Markit predict that if end users no longer allow third party cookies there could be a 50-70% reduction in display advertising in Europe with the long tail of publishers likely to feel the most pain.

If end users no longer allow third party cookies (due to a combination of the GDPR and ePrivacy regulation), the study estimates that there will be a 50-70% reduction in display advertising revenue based on its 2020 view of the digital ad market. The pain will be felt by the long tail of publishers (not in the top 50% of market size contributors) — revenue contractions are estimated to be 2-5x more pronounced than for larger counterparts.

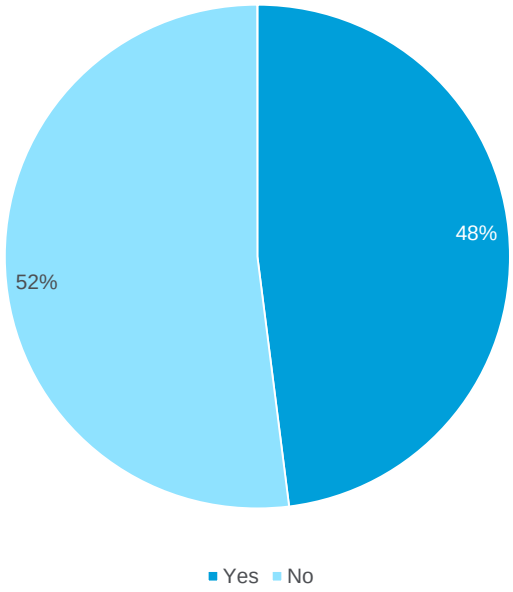
The WIK report concludes that in Germany digital advertising budgets could be cut by a third and programmatic advertising would not be feasible.

The WIK report is based on the EC's claim that 11% of users will accept cookies. It concludes that in Germany this would lead to:

- Consumers blocking cookies without realizing consequences, negatively impacting consumer experience. Limited alternative models as consumers expect content to be free.
- Digital advertising budgets being cut by a third with the greatest impact on display and affiliate advertising and limited impact on search and social meta advertising. Elimination of online behavioral advertising (to contextual based) will lead to price declines and an increase in the number of online ads.
- Programmatic advertising would not be feasible as it requires storage and retrieval of data from end user terminal (which the regulation would limit).
- Medium to long term there will be a move to closed log in systems and payment barrier solutions which could lead to more extensive data collection within these ecosystems as well as less choice for consumers (as usage becomes more concentrated). Publishers and content providers funded by display advertising lacking a strong brand will suffer most, and these are typically national and small and medium sized businesses.
- It will stifle innovation in the European market and lead to further de-coupling from U.S. growth.

Given the potentially catastrophic impact that is being predicted for the revenues that underpin the functioning of the Internet, it is surprising that our survey suggests that awareness of the draft ePrivacy Regulation is not higher than 48%. By industry, awareness is higher amongst technology companies (at almost 60%) but it is below 50% for advertising companies.

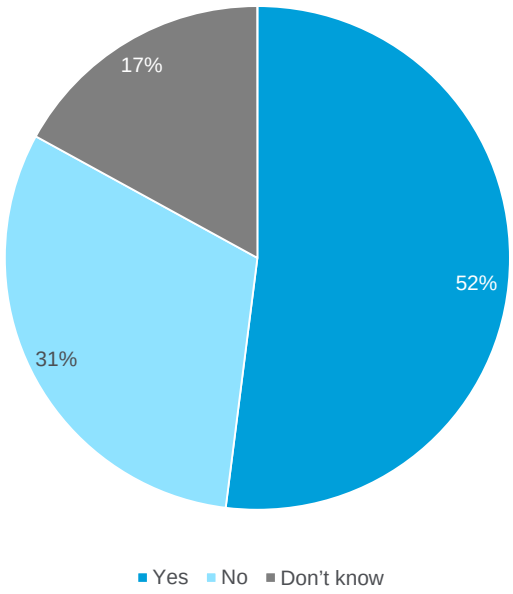
Figure 64. Awareness of Proposed ePrivacy Regulation



Source: Citi Research

Of those who claim to be aware of the regulation, 52% believe that it could present challenges for their business and industry. The technology companies were almost unanimous in this view as 86% believe it will be a challenge.

Figure 65. Could the ePrivacy Regulation Present Challenges if Approved in its Current Form?



Source: Citi Research

Awareness of the draft ePrivacy Regulation is 48%, according to our survey, and 52% expect it to present challenges such as increasing costs, limiting growth and impacting marketing

When asked what the challenges could be, most believe it creates additional and restrictive layers of compliance that could increase the cost, limit growth and further impact marketing capabilities. There were also comments that suggested that the lack of certainty on the outcome of the regulation creates challenges in itself.

Quotes about Challenges Related to Proposed ePrivacy Regulation

"No clarity on where the regulations will land makes current investments challenging."

"Ratcheting regulations will make doing business in the EU increasingly difficult."

"Reduce direct marketing activities such as to promote services rendered/offered/needed by our machines to help customers which might be lazy. Remember functions might be faulty and also communication between customers and producers might be affected as IoT cannot be implemented."

"This will greatly impact our ability to target advertising on our website, against our email database and through our mobile app."

"Inconsistent and disharmonious regulations."

"It will add new levels of compliance that takes away focus from growing our business."

"Getting consent from consumers who do not use cookie based technologies is going to be hard to initiate."

"Limits on growth of e-commerce."

"This is additional compliance focused on electronic communications, devices, browsers etc... Additional restrictions and controls would cost us additional money. We have for example some products (own developed products - similar like Skype) which will be impacted by this ePrivacy Regulation."

With the implications in mind, we outline the key points of the ePrivacy Regulations and the possible timing below.

The Contentious ePrivacy Regulation

The ePrivacy Directive was first introduced in 2002 (replacing the 1997 Directive) to protect consumer privacy and data protection in the provision of electronic communication, setting out rules for the telecoms and Internet service providers in particular (regarding confidentiality, data breaches and security). In 2009 the Directive was updated to include more specific rules on obtaining consent for the use of cookies. This led to the pop-up banners we frequently see when landing on a website in Europe which notifies us that continued use of the website implies consent for the usage of cookies.

Intensive Lobbying Efforts

With the introduction of the GDPR the European Commission conducted a review of ePrivacy Directive under its REFIT program. There was some hope from industry that the introduction of the GDPR would lead to the ePrivacy Directive being rendered redundant during the review process. In July 2016 a joint statement was issued by 12 associations across the tech and telecoms industries calling for the repeal of the Directive arguing that "simplifying and streamlining regulation will benefit consumers by ensuring they are provided with a simple, consistent and meaningful set of rules designed to protect their personal data" and "sector-specific rules on privacy are no longer able to address the challenges of the digital age." Industry bodies representing the publishing industry (including the IAB Europe, EMMA and News Media Europe) sent a letter to the VP of the European Commission (Andrus Ansip) and the Commissioner for the Digital Economy & Society (Gunther Oettinger) in November 2016 highlighting the 'critical role' that interest based advertising plays in financing online media, requesting that the regulation does not dictate business models.

Several industry bodies have been lobbying against the draft regulation. The advertising industry has been most vocal as it is 'risks significantly disrupting the current advertising model.'

According to one industry publication there were at least 41 lobby meetings held with the relevant Commissioners, their cabinet members and Director General, and 36 of these were meetings with corporates. The lobbying continued as it became clear, in December 2016 when draft of the regulation was leaked, that not only would the ePrivacy Directive not be repealed, but it would become broader in nature (moving beyond a focus on cookies to any form of tracking), raise the bar around consent requirements and would become regulation (i.e., will automatically be converted into law across the member states), with the same fining power as the GDPR.

In December 2016 Digital Europe (an association representing the digital technology industry in Europe) released a statement to express its concerns about the leaked draft claiming that it "*would risk significantly disrupting the current advertising funded model of the digital ecosystem, on which the vast majority of content and services in Europe and beyond rely. The draft provisions would also impede – if not make impossible — the funding of digital media and applications in Europe*."

Over the past three years several industry bodies have spent significant sums of money on lobbying.

Figure 66. Industry Lobby Efforts (as of October 2017)

Lobby Organization	Members include	Annual lobby spend (self-declared)	Number of lobbyists (FTE equivalents)	Number of Commission meetings since December 2014 - October 2017
Computer and Communications Industry Association (CCIA)	Amazon, Facebook, Google, Intel, Uber, Mozilla	€300,000-399,999 (2015)	2.75	39
DigitalEurope	Apple, Google, HP, INM, Microsoft	€1,900,000 (2016)	9.75	107
European Association of Communications Agencies (EACA)	PUBP, WPPP, IPG agencies	Less than €9,999 (2015)	1.75	4
European Digital Media Association (EDiMA)	Apple. Ebay, Facebook, Google, LinkedIn, Twitter	€100,000-199,999 (2015-16)	3	20
The European Interactive Digital Advertising Alliance (EDAA)	EACA, EMMA, ENPA, IAB Europe	Less than €9,999 (2015)	0.25	3
European Magazine Media Association (EMMA)	National Associations, Axel Springer, Roularta	€400,000-499,999 (2016)	5.25	46
European Newspaper Publishers' Association (ENPA)	N/A	€340,000 (2016)	4	35
European Telecommunications Network Operators' Association (ETNO)	BT, DT, Orange, Telefonica	€1,000,000-1,249,999 (2016)	3	51
Federation of European Direct and Interactive Marketing (FEDMA)	National associations, Havas, Merkle	€50,000-59,999 (2016)	1.5	9
GSMA Europe	DT, Orange, TI, Vodafone	€1,000,000-1,249,999 (2016-17)	6.75	33
Interactive Advertising Bureau (IAB) Europe	IAB National Associations, Google, Microsoft	€300,000-399,999 (2016)	2.75	9

Source: corporateeurope.org, LobbyFacts

The Draft Proposals

What was detailed in the draft proposed ePrivacy Regulation when the Commission published it in January 2017 was not quite as stringent as the leaked draft, but it was not far off. It is worth remembering that data protection is a fundamental right in the EU and the European Commission also pointed out that whilst the GDPR covers a wide range of data protection related issues it does not cover the right to confidentiality of communication and the right to freedom of expression.

Widening Scope of Companies Which Have to Comply

The draft ePrivacy Regulation was first published by the European Commission in January 2017. It proposes that that consent is required for all forms of tracking (apart from essential first party cookies), including certain metadata. Browser settings would be the tool for consent.

The definition of an electronic communication service according to the 2009 ePrivacy Directive does not currently include over-the-top (OTT) services e.g., WhatsApp, iMessage etc. so the EC has extended the regulation to apply to any company processing data in connection with electronic communication services, regardless of where the processing takes place, which means that OTT providers will be included. Even where communications is not the core business, but there is an element of electronic communication, then the regulation may be applied e.g. review sites, ecommerce sites, web based email services. It will also apply to machine to machine communications, which the EC believes is needed to promote a secure Internet of Things.

Consent: Clamping Down on Tracking

The previous 2009 ePrivacy directive introduced the focus on consent for cookie use, which led to the pop up banners requesting approval for cookie use. The Commission appears to acknowledge that the cookie consent rule has led to "consent fatigue" and has not met its objectives as it lacks transparency on how to withdraw or manage consent, does not distinguish between the cookie types i.e. included those essential to a site operating as intended, does not encompass a wide range of tracking techniques e.g., device fingerprinting, and consumers did not necessarily understand the meaning of accepting tracking cookies:

"The consent rule is over-inclusive, as it also covers non-privacy intrusive practices and under-inclusive, as it does not clearly cover some tracking techniques (e.g. device fingerprinting) which may not entail access/storage in the device."[23]

The proposal makes a distinction between tracking cookies and some essential first party cookies. Consent will not be needed for cookies used to improve the Internet experience e.g. shopping cart history or for a site to measure web traffic.

Consent requirements for tracking users online with cookies or other tracking tools face more stringent consent requirements. Browser settings may become the key tool for consent, which will eliminate the need for cookie banners and notices, and reflects the findings from the Eurobarometer survey conducted in 2016 in which 89% of respondents supported privacy by default in the browser setting.[24] Web browsers are seen as potential 'gatekeepers' to help information being unknowingly accessed/stored.

The proposal notes that the default setting for web browsers is currently 'accept all cookies'. The draft Regulation proposes that the software is reconfigured to offer a range of privacy setting options: 'never accept cookies', 'always accept cookies', 'reject third party cookies, or 'only accept first party cookies'. In the case of third party tracking cookies the web browser should "*require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies.*" This means that at the point of software installation consumers should be informed about the privacy settings choices, and asked to make a choice. The information should not be biased in a way that dissuades users from selecting the higher privacy settings, and users should also be provided with information on the risks of allowing third party cookies. Users should be able to easily change privacy settings at any time, and should be able to whitelist certain sites or specify which websites' third party cookies are always or never allowed.

The proposal has specified certain metadata e.g. time of call and location, from electronic communications are deemed to have a high privacy component and will need to be anonymized or deleted if users have not provided consent, unless required for billing. If consent is provided then telecoms operators have greater scope to use the data to provide additional services or use the data to help public authorities e.g. heat maps of individuals' presence.

Following the first draft by the Commission, the Committee on Civil Liberties, Justice and Home Affairs (LIBE) which is responsible for the ePrivacy Regulation in Parliament, reviewed the proposal. The rapporteur and author of LIBE's amended draft was Estonian Marju Lauristin MEP, a Social Democrat. Over 800 amendments were offered by various stakeholders. As it looked like the proposal would be tightened, rather than loosened, the online advertising industry continued to highlight the potential damaging impact of the legislation.

[23] ePrivacy proposed regulation – COM (2017) 10 final, 2017/0003 (COD).
[24] 2016 Eurobarometer survey (EB) 443 on ePrivacy (SMART 2016/079).

Article 29 Working Party & EDPS Supportive of a Tough Regulation

Article 29 Working Party and the European Data Protection Supervisor's reviews of the draft regulation offered even tighter requirements such as the default setting in terminal equipment being privacy protective, explicit prohibition of tracking walls, which means a service should not be withheld if tracking is not accepted, and clarification that legitimate interest is removed as a basis for processing.

At the same time, the European Data Protection Supervisor (EDPS) and Article 29 Working Party published their views of the proposed draft regulation. Both proposed even tighter requirements around the processing of personal data than had offered in the EC's first draft.

The Article 29 Working Party issued its opinion in April 2017, highlighting 4 areas by which it proposed regulation should be more explicit:

1. Tracking of location of terminal equipment should only be with consent or if data is anonymized.

2. Analysis of content and metadata should be prohibited without consent if it is not related to billing or anything requested by the user e.g., virtual assistants.

3. The default settings of terminal equipment should be privacy protective (this is based on 69% of respondents to a barometer survey stating that default settings of browsers should be used). It should include apps, Internet of Things connected devices etc. Users should have clear means to change settings and the privacy preferences should not be limited to third parties and cookies. Do Not Track should be mandatory but users should be able to provide separate consent to a site or app (although implicit consent should not override do not track).

4. There should be explicit prohibition of tracking walls i.e., a service should not be withheld if tracking is not accepted. This relates to fundamental right of freedom of expression which includes the right to access information.

Article 29 Working Party also believes that the definition of direct marketing should be broad, including all advertising sent, directed, or presented to users.

The EDPS published recommendations on ePrivacy on 5 October 2017, which were similar to that of the Article 29 Working Party. The EDPS stated:

"*We strongly oppose any amendments that would introduce the ground of legitimate interests as a basis for processing under the ePrivacy Regulation.* ***Any possibility for further processing must not create a back-door to the high level of protection of confidentiality of communications.***

*In particular, we support the proposed amendments to Article 6, which clarify that consent to the processing must not be '****a condition to access or use a service****'. This should apply to processing of both content and metadata. Similar proposed amendments to Article 8, clarifying that consent must not be a '****condition to access or use a service or use a terminal equipment****' are also welcome."*

Tightened Regulation Passes Two Voting Milestones

The Committee on Civil Liberties, Justice and Home Affairs (LIBE), responsible for the ePrivacy regulation in European Parliament, reflected the recommendations of the Article 29 Working Party in its amended text in October 2017. Both the LIBE Committee and the European Parliament voted in favor of the amended draft.

The recommendations of Article 29 Working Party were broadly reflected in the amended draft regulation that was proposed by the LIBE. On October 19, 2017 the LIBE Committee voted in favor of the amended text (31 for, 24 against, 1 abstained). What was more surprising for industry was the European Parliament voted in favor of the LIBE Committee draft on 26th October, with limited changes. It was close, polarizing the parliament, with 318 MEPs voting for, 280 against and 20 abstaining. This is not the end of the process but it does mean that if the regulation came in as it stands:

- The definition of direct marketing will be broad (any form of advertising via electronic means) (Article 4).
- Processing of metadata can only occur if strictly necessary for the service or the user has given consent (Article 6).
- Collection of information from end users terminal equipment is prohibited unless strictly necessary for providing the service or the user has provided specific consent (Article 8).
- Access to a service cannot be denied on the grounds of not obtaining consent for the use of personal data (Article 8).
- Settings, such as on the browser, will be set to privacy protective by default and the user will be prompted to select privacy settings (Article 10).

The approval of this draft prompted further statements from across various communications and online related industries, which illustrates how concerned industries are about the risk of reinforcing the dominance of the existing global operators and the effect of removing a publisher's ability to refuse access to their site:

ENPA: "*By preventing the use of cookies on press websites at the browser's installation, the EU legislators will consolidate the dominance of only few technological players which will have a total control of the whole EU data market. This will de facto exclude European smaller and medium digital players, therefore affecting EU competition.*"

Raoul Grünthal, CEO of Schibsted's Sverige newspaper: "*Only 20 percent of our revenue is generated from user payment, the rest is from ads. Today a major part of advertising revenue goes to the global players. Their strong position is linked to their access to data. Publishers, unlike the big players, must work with third parties. The global players can do everything in house. What will happen in practice is that this proposal will favor the big global players.*"

Ecommerce Europe – "*Ecommerce Europe expressed its concerns over the disbalanced outcome of the agreement. In fact, the Regulation may negatively impact the business models of online merchants, jeopardizing the online shopping experience of consumers. Moreover, Ecommerce Europe is also concerned that technological innovations might be hampered by the proposed provisions. Policymakers should take sufficiently into account the crucial role that electronic communications and data-driven marketing play in modern e-commerce in the next steps of the legislative process.*"

Federation of European Direct and Interactive Marketing (FEDMA): "*Unfortunately, the LIBE report is focused solely on consent and omits any mention of legitimate interest, instead opting for a very strict legal framework for the direct marketing and data driven advertising sectors…..The report's current stance will no longer allow European digital and media companies to provide free access to information and services through advertising revenues, which will hurt both businesses and citizens*'."

Next Steps

The European Council is yet to publish its review of the draft regulation. Once this is published then the regulation will enter trilogue phase with the Commission, Parliament and Council working together to attempt to reach an agreement on the final draft.

The next steps are that the European Council (which is where EU member states interact on policy and the agenda) has to publish its final review of the draft. The dossier is being handled by the Telecommunications and Information Society for the European Council which could mean will be more pro industry than the view of the European Parliament.

As of now, the Council is yet to provide details of its final 'general approach'.[25] Given it requires the input of all of the member states there will clearly be different agendas and different opinions on whether the Commission's proposal is too tough or not tough enough

The original timeframe was for the ePrivacy Regulation to come in 25 May with the GDPR. As it stands, it is unlikely to come into effect before 2019, or even 2020.

Once the European Council has published its version of the regulation then it will enter trilogue phase, which is when the Commission, Parliament, and Council will come together to attempt to reach an agreement on the final draft during the first reading. If that fails after a third reading then conciliation occurs — which happens with 10% of EU legislation. This is when the Commission tries to reconcile the differences between the Parliament and Council, aiming to approve joint text within eight weeks.

The original ambition was that ePrivacy Regulation would come in the same time as the GDPR in May 2018. Given the contentious nature of the proposal this is definitely not going to happen. Most of the expert commentators believe that the ePrivacy Regulation is unlikely to be agreed before the end of 2018 and is therefore unlikely to come into force before 2019, or even 2020. There is no set timeframe for the trilogue phase so it could drag on (as we saw with the GDPR).

Implications

We are far from the end of the process as the regulation could be altered significantly yet. However, as we noted in our previous GPS, the more privacy related scandals that come out of the woodwork over the next 12 months or so, the greater the risk that the ePrivacy regulation is pushed through in a form that is close to the current draft.

In short, this could be devastating for the online industry in particular and future innovation. Consent is the be all and end all of the regulation (extending beyond personal data), as legitimate interest is not an option, and it is very clear that access to services cannot be made conditional upon consent to access data. The use of browser settings may limit the level of consent fatigue but it forces consumers to take a blanket approach to privacy (little room for distinction between services and sites) and, ironically some may argue, the browsers tend to be controlled by the large tech companies that regulators are attempting to rein in. Ultimately, European consumers could lose out if it undermines the ad funded model which has been a key plank of support for the development of the Internet. Companies may think twice about investment and innovation in Europe.

25 https://www.parlament.gv.at/PAKT/EU/XXVI/EU/01/38/EU_13835/imfname_10792028.pdf.

Expert Views

A Conversation with John Bowman

Senior Principal, Promontory Financial Group, an IBM Company

John Bowman advises clients on all aspects of compliance with data-protection laws and regulations. He is a specialist on the European Union's General Data Protection Regulation.

Prior to joining Promontory, John worked at the U.K. Ministry of Justice, where he was the head of EU and international data-protection policy and lead negotiator on the GDPR at the EU Council's DAPIX working group in Brussels. John also represented the U.K. at the European Commission's Article 31 Committee, which is responsible for determining the adequacy of non-EU data-protection regimes.

How prepared are companies for GDPR?

It varies considerably, not only in terms of size of organization but across sectors as well. The companies who started in 2015/2016 are seeing the benefit of that now because they've had more time to plan for it. What we are seeing coming into the market now is firms who are waking up to the fact the GDPR is not so far away and they need to do something about it. It might have been on their radar but they've had other priorities. In financial services, MIFID 2 was definitely one of the things that took time for lawyers and compliance and change program managers. GDPR was the next one to come afterwards.

Those that started early don't regret it because the amount of effort required to deliver a GDPR change program shouldn't be underestimated. Those who are coming on board now are unlikely to be fully ready by the May deadline so they may have to focus on priority areas like the records of processing activities or ensuring that their legal bases for processing, including consent, are properly in place.

In terms of companies you have been working with, what have been the main areas of focus?

I think the records of processing activities are a key deliverable. Article 30 requires effectively undertaking a data mapping process. It's important because it makes companies understand what their data flows are, what types of things they are doing. Not only is it a regulatory requirement, but it enables them to spot risks and gaps — have they got the right safeguards to transfer data in and out of the EU? Do they have contracts in place to transfer data? Is the data properly secured? Do they know the purpose of the data processing, and are they limiting it to those purposes under the purpose limitation and data minimization principles?

The controller/processor relationship is a priority for some. Some organizations are going through all of their contracts, and some might have thousands, and are thinking about whether the contracts are in line with GDPR requirements. The GDPR provides a lot more detail about what needs to be in agreements with processors around meeting data subject rights, managing data, and deleting it and handing it back.

Is there a logical roadmap that you talk about? Do you have to do data mapping before you can think about obtaining consent?

It's fair to say no two projects are the same. It depends on the nature of the client and type of data they are dealing with and what their own priorities are. You will find that there is a risk-based approach which is allowed for in the GDPR. Some small organizations decide they don't need a data protection officer because they don't meet all the triggers required to have one. At the same time, others may decide they do need a Data Protection Officer (DPO) and have a person in one place and another DPO in another place in Europe depending on how they're structured.

Any U.K.-headquartered organization is at least thinking about whether post-Brexit they need to designate a main establishment location outside of the U.K., in the EU. The main reason they may consider this is if they want to maintain access to the one-stop shop. This allows them to establish a single regulatory relationship for data protection matters.

If they didn't have an establishment in the EU, then they would have to appoint a representative, which means they can't take advantage of the one-stop shop. That representative would have to travel around to every regulator and deal with cases as they come up, which would be more onerous. What we have seen is some analysis about the options available outside of the U.K. — do they think about going to Dublin, Madrid, Luxembourg, Paris, or Frankfurt for example? This may depend on the offices and staff they already have in locations such as these.

Are there any areas where you think more work needs to be done?

The transparency element is key — guidance only recently came out, and it's being consulted on by the Article 29 Working Party at the moment. I think where organizations rely on technology, such as phone apps, how do you provide notice to individuals that you are processing their data and get appropriate consent? Linked into that is things like how do you know an individual has provided unambiguous and informed consent to a particular data processing activity. That's where ePrivacy comes in as well. The draft ePrivacy Regulation as it stands looks at a number of things, in particular — one is around how do you accept cookies where they're effectively using browser settings instead of a consent box. The other is whether organizations can send electronic direct marketing. The GDPR allows direct marketing under legitimate interest; ePrivacy limits it to opt-in consent. There is concern that one rule says one thing and one rule says another. EPrivacy being the specialist law would override the GDPR on this area. We probably won't see a conclusion on ePrivacy by the end of this year. EU negotiators are being lobbied quite hard and ask why they can't have legitimate interest or other GDPR options for electronic direct marketing.

On the proposed ePrivacy regulation can you tell us what stage it's at and likely timing?

The European Parliament delivered a report towards the end of last year and set out their amendments. The Council, that is the member states, are debating the fine detail. They still have an open question on the point around consent on direct marketing. The Council has been a bit slower, which was the case with the GDPR, as you have to reconcile 28 member states, and it's a long and detailed process.

The feeling is it will be towards the end of the year before the Council gets a general approach, so before they enter the trilogue phase where the council and parliament get together to determine compromise text. The trilogue phase can take a while. The GDPR took 6 months, although it seemed like many things were agreed in the last two weeks, including the controversial issue around consent for processing children's data. The negotiators initially agreed an age of up to 16 for parental consent, but they afterwards came up with a compromise, which was that member states can legislate and lower it to 13 if they want. Some countries are going for 13, some 16, and some for ages in between. For certain businesses marketing to over 13s, they will have to adapt to the member state law which means they lose the benefit of a harmonized regulation.

We're starting to find the member state implementation of the GDPR in some aspects moves away from a harmonized framework. For example, Germany has retained this idea that you should have a DPO if you have more than 10 employees. It could be a small shop down the road. This starts to make some elements of the GDPR feel more like a directive which is applied in member state law rather than a regulation which is directly applicable across the EU.

Going back to 2012, the view of the U.K. and some other member states was that the GDPR should have been a directive because generally a regulation regulates measurable things. This was the first time the EC had tried to legislate for a fundamental right that is actually open to interpretation. What the GDPR does is attempt to find a balance between protection of personal data against maintaining the free flow of data and other rights such as freedom of expression. It was always going to be a grey area as to which side a particular processing activity goes. Some countries historically had more risk tolerant positions than others. It's interesting because the EC has to track all member state applications of the law, which must be a nightmare. For example, the U.K. Data Protection Act is a significant piece of drafting and has a complicated structure. As the guardians of the EU treaties, the EC has to decide if the laws have applied the regulation properly. Member states are not supposed to gold plate a Regulation unless there is specific latitude in the text to add more specific rules. So if they consider that the Regulation has been gold plated then potentially the EC could bring an infringement proceeding against those member states if non-compliant with EU legislation.

Direct marketing is clearly an area of contention with ePrivacy. Are there any other areas of contention with ePrivacy? Could it get watered down?

I think the European Parliament looks at things like spam emails and nuisance calling and thinks you need consent. They see it as a protection of the fundamental right to privacy. As with GDPR, there will be some tension as the member states and parliament may look at things from a different point of view.

ePrivacy also has GDPR level fines, so 4% of global annual turnover. In terms of enforcement, it will be the same DPA

ePrivacy is a kind of hybrid. It started as a telecoms directive, designed to protect the integrity of communications networks and confidentiality of that data. What the proposed Regulation has brought into scope is OTT telephony providers. Those companies may argue they aren't running a network and they're just running a platform and providing the ability for voice transmission, so there's some contention about that. Ultimately, those companies will probably have to fall into line with these rules.

In 2014, the EU Data Retention Directive was repealed by the ECJ. The idea behind the Data Retention Directive was to maintain telecoms metadata for terrorist prevention and prevention of serious crime. Because the European directive went, the member state laws fell away. In the U.K., we had RIPA and then DRIPA, which was stop-gap legislation to allow surveillance of telco data. That went, and we have the Investigatory Powers Act now. The government is trying to make some concessions so it fits with European law but the legislation remains controversial in terms of the retention of data.

We get asked about consent in relation to the GDPR. What's your view on the Article 29 Working Party guidance?

It's interesting as the guidance was published for consultation, and as soon as it passed the consultation date, it disappeared from the website. Apparently, it won't be agreed by the Article 29 Working Party until their April plenary meeting. All of the guidance is long and detailed. What they've tried to do in that draft was address the situation where companies got implied consent and can't prove they've got unambiguous consent. GDPR says you can't grandfather in those types of consent if not compliant with the GDPR.

The Article 29 working party suggested that as a one-off exercise, data controllers could assign another legal basis for that data processing as a transitional period. There's nothing in the GDPR to suggest they can do it. Presumably they're saying they won't enforce on any non-compliant consent that was gathered before the regulation as long as there's an alternative legal basis to rely upon so possibly you can rely upon legitimate interest or contractual basis if available.

What's your view on use of legitimate interest? What scenarios could companies apply this?

You may have signed up years ago for promotional activity, but they may not have a record of it. They could say that as long as it's going in the post, then they will rely on legitimate interest as you can rely on it for postal marketing. But data controllers still need to be transparent about legitimate interest and an explanation of that interest needs to be included in the privacy notice.

Another example may be that you get a value-added service from a bank and you didn't consent to the processing, but they may consider it a legitimate interest that you're offered a discount or free phone insurance or something like that.

Have companies tried to go back to reobtain consent?

Some feel satisfied they have appropriate consent in the first place. Others may not have a record of consent but, as an example, in the case of a bank where an account was set up years ago, they may assume it's a contractual arrangement or legitimate interest as they can't prove consent was given.

Some companies may use it as an opportunity to cleanse their marketing database. The argument being there's less cost overhead with less names on it, and you may get better quality responses from marketing communications. Lawyers like that idea but marketers may not as numbers are important, and they may want to preserve the sales database as much as possible.

There was an ICO case where the company sent out emails asking for marketing preferences. Someone complained saying they didn't recall giving consent and asking how their details were obtained and if the company didn't have consent then they shouldn't have got in touch with them in the first place.

How can anyone really be sure they've got consent?

It's keeping a record of having ticked a box, signed a form, or given verbal consent. You need a record of obtaining the agreement.

These situations are usually complaint driven, and when you look at the list of ICO adjudications, there's quite a lot around direct marketing. They tend to reserve their serious fines for contravention of Privacy & Electronic Communications Regulations (PECR), which is based on the current ePrivacy. Nuisance calling is a topic that has received a lot of attention from the regulators.

Another interesting element is data subject rights. Will there be mystery shoppers? The FT did a mystery shop and investigated whether a number of companies could respond to subject access requests. Some companies are anxious about savings expert's sites and whether they will flag to consumers that they can take their data in a portable file and move it elsewhere. One of the uncertainties is how many people will exercise data subject rights. No one knows. Once the £10 fee goes, then it's a low-level deterrent that's been removed. Once you get free access requests there could be some acceleration from individuals or there could be a campaign or claims management companies looking out for compensation opportunities.

Do you think that the GDPR will become a global standard?

Yes. Any international company operating in Europe will have to apply those rules generally. On our global projects we are seeing some applying a global standard based on the GDPR. Some think it's a good thing, as it is about maintaining a reputation and being a good corporate citizen. People are looking at what's happening on breaches, and it's not great for reputation. The public is becoming savvier about data protection rights. I'm sure there'll be a lot of publicity around the 25 May which may be enough to keep people's interest.

Any clarity on how it will be policed?

Every DPA has put in a case for more staff. ICO has come to a funding settlement. The Irish DPA expanded quite significantly. It moved into the center of Dublin. Ireland will be a focal point because a lot of big tech companies have their European HQs there so it will be their lead authority.

One reason why the one-stop shop evolved as it did is because the original proposal put a lot of power on that lead authority. The compromise on the one-stop shop was that other authorities could intervene if the complaint involved data subjects located on their territory. If there's a disagreement, it goes into the consistency mechanism at the new European Data Protection Board. From there onwards, it's based on majority voting. It's one member, one vote as well.

What has been the response of the tech giants?

The platforms have evolved a lot over five years. They want to be seen to be sensitive to privacy concerns. They're having to address questions that have been raised in Europe.

Any other issues to flag?

Data retention is an issue. It's quite a difficult one because companies have taken various approaches to records management. GDPR doesn't specify you must keep records for a certain amount of time. There are storage limitation and data minimization principles in the GDPR. Good practice is only using data for as long as required. You can't hold on to it on a 'just in case' basis. It's part of risk management. The more you hold the more exposed you are to a breach. There's also cost of storage even though that's getting cheaper.

If you've got lots of legacy systems or lots of paper files, then how do you deal with it? It can be a time consuming and expensive process to work out where your information is, what you do with it, and how you dispose of it

Do you think most companies are adopting GDPR without it being too disruptive?

They want to minimize the disruption. I think what is difficult if you're a large international organization is that GDPR applies horizontally. Anywhere there's personal data — product services, HR, vendor management, etc. What companies can find challenging is managing those stakeholders and figuring out who is important and transmitting a message that GDPR is important and needs to be applied. The scope of the programs can be huge but there'll be different views internally about how important it is.

Is GDPR good or bad from a client's perspective?

The majority would say it's a good thing. The sample may be self-selecting as someone has decided to address GDPR and therefore we have been engaged. There are some using it as market differentiator and like to publicize they have a comprehensive GDPR program in place.

People are coming around to the idea that data protection is important. GDPR forces organizations to address some important questions like where is your data, what do you do with it, and is there fair and lawful processing.

The other thing to explain is it was heavily lobbied during the negotiations. These went on for four years. It was prescriptive text and could add costs and impact on business models. However, the lobbying came to a natural end, and from early 2016, many organizations started looking at the practical application of the GDPR. What we're seeing now are late comers. They've done some work but not in a systematic way so they need support getting their GDPR-readiness across the line. It can be hard if GDPR is just a proportion of someone's job role. We think, for many organizations, you need dedicated project management resource to drive GDPR readiness activities. Some big organizations have however set up specific project teams as well as wider stakeholder networks.

Now companies generally aren't keen on U.K. divergence from GDPR because it would mean another separate set of rules to apply. The U.K. government has stated that it doesn't want divergence as it wants the U.K. to maintain unhindered data flows with the EU. The government also wants the regulator to be involved in the European consistency mechanism, but it remains to be seen what's in the U.K. Withdrawal Agreement. In theory, the U.K. should be adequate as it has applied the GDPR and has an independent regulator and strong enforcement, but it often comes down to politics. It would be difficult for many companies if the Brexit settlement resulted in restricted data flows because you can't transfer data between here and Europe freely without contracts or some other safeguard or basis for transfer like consent in place.

Do you think the regulator will test out high level fines in the first year?

Article 29 issued guidelines on how to make fines consistent across Europe. Regulators will want to be proportionate and considered in their approach, but they may want to reflect a prevailing public mood. One advantage of the new systems, though, is you won't get fined by more than one DPA under the consistency mechanism for the same infringement. There is also a route of appeal in certain situations with the ECJ as the court of last resort.

Disclaimer: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

A Conversation with Telefónica's Data Team

How is big data impacting your business?

Telefónica is a leader in big data transformation regarding data exploitation. We operate in 17 countries, meaning that each operation has different systems and we are focused on digitizing these in a unified way. We are migrating the operational systems and legacy systems in all countries in the group to new systems. We want to provide access to data across countries in order to have scale in product development and data exploitation. This data-driven transformation and the migration to new systems will reduce/improve considerably the time to market for new products and services.

Regarding data exploitation, we are implementing a normalized access to operations data and batch data. Normalization means access to the same information in the same way everywhere. One of the key advantages is the replicability of new services in all the countries. For example, products like AURA are developed once and can be deployed 17 times, implemented quickly in every country, following a prescribed process. We are creating a normalization framework for any new development so it can be easily exported to other countries.

What do you think the implications of the GDPR are at an industry level?

The GDPR is a tool to provide trust to customers. Data security is key. We believe the GDPR offers an opportunity to increase customers' confidence and their trust in us, to build better customer experience and, also, to improve the services that the industry offers.

How have you gone about preparing for the GDPR? What is the greatest challenge from an implementation perspective?

We have adopted a phased implementation, depending on the availability of technical capabilities and channels to interact with our customers. The whole company is focused on it. The legal team is looking at it and safeguarding security.

Personal data portability is a very big challenge for the telecoms industry, but it provides great value for customers, too. That is why we are leading an initiative with other telco operators — Orange, DT, KPN — called 'Data Portability Cooperation' (announced during the most recent Mobile World Congress).

The initiative is analyzing the implementation of portability of data in a way that adds value to customers while protecting their privacy. We want to add new telco operators in the near future to this collaboration as we are convinced that telco companies are in a lead position to enable customers to exercise this right while providing reassurance to customers.

The Data Portability Cooperation is a working group in the GSMA with room for other telcos, with the purpose of defining an interoperable data portability framework that must meet the implementation deadline of the GDPR while being representative for the whole Industry.

What is the challenge around data portability?

Data portability presents some key issues in terms of implementation. These include the processing effort of the big amount of data that we have from customers, the datasets that will be affected by the portability right, the format in which the information will be delivered to the recipient third party, the communication protocol, etc.

As a consequence, the main challenge around data portability will be the agreement of the implementation aspects across a potentially large set of companies. This is something that has not been performed, at this scale, so far.

What does the telecoms partnership involve?

We are working together with the GSMA and several telco operators in the interoperability framework for data portability that implements the points described before in an organized way. The bigger challenge is to normalize data portability within Telcos and other companies. We need to know what data we will receive so that we are able to process it. We need to understand how we will connect between operators and third parties which means we need to create a framework for interoperability. If we do this right, our customers will be able to enrich their digital lives significantly.

How does AURA work?

Aura is a very new way of engagement and communication with customers. We are trying to change how we communicate with customers. We think it will provide us with a level of engagement in a new and different way. One of our industry problems is that we are facing disintermediation by OTT and retailers (i.e., customers go to the retailers to buy devices). We want to keep and develop the relationship with the customers in a direct and friendly way. AURA is a high-technology tool that will support the generation of engagement and that will prevent being disintermediated.

We are in our customer´s home with our services and now we want to go a step forward offering them a new way of interacting with us in their own home. AURA offers a more friendly way to interact with the operator and to manage the telco services. Our plan is to go further in the services and the capabilities we provide to manage what we offer to the customer.

When the industry was growing we were focused on customer acquisition, but this has shifted to customer retention and upselling. The industry has always found it hard to monetize the engagement of customers and loyalty has always been difficult. In the medium-term we think Aura will drive more engagement which will drive more efficiency in customer retention spend. It is being launched, with a first set of capabilities and channels, in 6 countries (Spain, Brazil, the U.K., Germany, Argentina, and Chile) and we will be delivering the same experience to the rest of our footprint once the normalized capabilities are ready.

What is your view on the consent requirements under GDPR?

We absolutely respect consumers' will when it comes to our services. We will only deliver a certain service or capability if we have the required permission. 4th Platform will provide GDPR-compliant methods to ensure that privacy of our customers is preserved.

We also provide other important set services to other companies under the brand LUCA, such as Smart Steps or Smart Digits. For example, LUCA Audience (a service from the Smart Steps family) helps in the decision-making about where retailers place stores. In this service, all the data is anonymized and aggregated and there is no personal data is used at all.

Other services, for example LUCA Smart Digits, works always with the consent of the customer as a starting point and will help third parties, for example, a bank to use the telco data to check on fraud, e.g., someone accessing cashpoints in another country.

How differentiated is your approach versus the industry?

Each operator has their own point of view on GDPR. We believe that the differentiation is the engagement, in how we go about it: we firmly believe that GDPR needs to bring value to our customers. The implementation will be a standard approach across operators. The difference will be in how each operator will provide access to data to customers.

Regarding our customers, we want to provide them with mechanisms to access their personal data. Our view is that we want to give personal information of our customers – this is more than the GDPR implementation — we want to give them relevant information e.g., what you consume etc. We see it as an advantage as we could have more engagement with our customers.

We are very open and want to provide the relevant information for our customers and we think we can give them value. We see it as an opportunity to provide a better service and improve the customer experience and increase the trusted relationship with the customers. However, one problem of GDPR is the potential role of data brokers. We, as highly regulated telco companies, have an important role as consumers are not aware of the value of their data. We are worried about brokers using the customers' information without customers knowing the amount of data they are getting access to. It is hard for consumers to maintain control of data across data controllers, and how data is being used. This is a real risk for consumers.

Small countries need to gain scale in the new era of big data exploitation. Big countries have some advantages. In some of our smaller markets like Ecuador, Uruguay, etc., there is no local operator that can adapt in the same way. We think we will gain competitive advantage as we will have synergies and efficiencies at a Group level, leveraging the big countries where we are present. So, we will gain competitive advantage by: (1) synergy efficiencies (P&S for optimizing the network, algorithms regarding the value of the customers); (2) changing the way of working internally; and (3) spreading the efficiencies of our use cases seamlessly throughout our footprint.

What is your view on the draft ePrivacy regulation and the implications of that if it stays in its current form?

The regulation implementation is still some way off. It would require more efforts around consent to customers. We believe it is a bit unnecessary. Telcos have always been strictly regulated around customer privacy. For us, this is an over-regulation in our industry that unnecessarily complicates our treatment of data and really applies more to OTTs as telcos have always been more concerned with privacy.

How does EU's approach to privacy and data protection to compare to other markets that you operate in?

We are very focused on GDPR and will take a GDPR like approach across all countries. We believe LatAm will follow the EU regulation sooner rather than later. The U.S. has a more open regulation but is always looking at the EU regulation, while more focused on commercial issues related with the use of personal data.

A Conversation with Ingvild Næss

Group Privacy Officer, Schibsted

Ingvild Næss is Group Privacy Officer in Schibsted Media Group. Schibsted is an international group with 7,300 employees in 22 countries divided in two main divisions; Marketplaces and Media. Ingvild has the global, overall responsibility for privacy and data protection in Schibsted and has held this position since January 2016. Before she joined Schibsted Ingvild headed the practice group for technology, telecoms and data protection in the Norwegian law firm Thommessen and was ranked in Legal 500, Chambers and Who´s Who Legal.

We are fast approaching the implementation date, how prepared do you feel you are for the GDPR?

The clock is ticking towards the 25th of May. We can very clearly see that the 25th of May will not be a magic date. All product development going forward will require privacy to be an integral part and requires a lot of work. This is a continuous process. We will have to invest in the future with dedicated privacy work. The GDPR requirements will be an integrated part of what we do. We have some systems that pre-date GDPR so there is a lot of work required on those. The GDPR requirements have changed the way we handle data and build products.

Can you give some examples of how you have gone about preparing for the GDPR?

We welcome GDPR and have done extensive preparations across all the organization.

One part is transitional compliance and legal work around the impact assessment. GDPR has helped us to get a better overview of what data we have and how we use it. We have had to have a clean-up – do we need this data? Do we need it for this period? What kind of third party contracts do we have? GDPR has some positive effects as causes us to have a better overview and clearer value proposition as to why we collect data.

The two really important aspects are the product and tech dimension.

For the product dimension we have put a spec in place to indicate what we must do to fulfill the rights of the e user in our products. This relates to transparency — the kind of information to provide and how it's presented. It also covers what kind of control options the user should have and the rights of the users, such as data portability, right to access the data. Everything is user-facing.

Then we have the implications for the tech stack. Privacy by design principle really pushes us to look at the whole tech stack and what we do is in line with the principles.

We also have to think about user expectations. We need to adjust how we control data based on the user choice. It must be possible to do as data runs across the systems.

For it to work, privacy isn't just done by lawyers. We have privacy engineers and specialized product people to make sure the privacy expectations are an integral part of the day to day jobs. That's been a huge shift over the past couple of years.

Will your relationships with suppliers and third parties alter?

Yes. The transparency requirement really makes us do a more thorough assessment of what kind of third parties we want to have a relationship with. We have a clear advantage in the fact that we have direct relationships with the end users. What we see now is the dynamic in the market is changing. Those that have a lot of data but no relationship with the end user, they are trying to find a way to be able to meet the requirements around transparency and user empowerment.

There are companies approaching us that want us to get consent on their behalf.

Will it change the amount of data you have access to?

Transparency requirements force us to have a clear proposition as we have to tell users what we are collecting and how we are using it, so this is one of our top priorities. We need to have a good story to tell our users. No more mindless collection of data. It pushes us to towards 'good quality' data as users will have more control over the data and get value in return. As we see it this push will also help us provide better products and services to our users.

At an industry level do you think there could be any implications for the online advertising landscape - from both a growth perspective and that of the operators within the industry?

It is a clear advantage to be end user facing. The companies not end-user facing are in the middle position where they are reliant on others to continue as they were. The companies that don't live up to the new standard will struggle going forward from a regulatory perspective as well as a business partner perspective.

Could Schibsted have a competitive advantage?

We can utilize the fact that we have direct, strong relationship with our users. Focus on clear value in return to users for data. Building upon end user trust and strengthening it. We have extensive dialogue with regulators to understand where they are going and also to try to influence and explain our business - why we do what we do. That goes for the proposed ePrivacy regulation as well.

We are really trying to be one of the players that is impacting the development of this area going forward.

It feels like the area of consent is a big focus for online publishers but also an area that is open to interpretation - how are you approaching it at Schibsted? Will it vary by market across Europe? Have you done any research on the proportion of users you think will provide the consent needed?

We need to have in place the same approach across Europe. It will take a lot of time before we are there. We take into account the views of the local DPA but we also have to take into account the expectation of the end users. The expectations of privacy of end users vary by market. We are dependent on end user trust.

We have engaged in the debate around the ePrivacy draft regulation. We have a big focus on the area of transparency and user empowerment, and it is a high priority. We need to move away from 10 page long privacy policies. We need to use storytelling that people can understand. We will have a layered approach when it comes to more detailed information. We are implementing extensive control options and toggles for users to turn on and turn off how their data used. We continuously assess the best way to present the information and provide the control options. We are also doing user research to understand user expectations when they use our services. We will continue to develop the kind of toggles are given to users. We want users to understand it so we will give users consent options within the product flow when it makes sense.

How do end users differ across markets?

We see that on many areas. One example: In Norway it is common that when you post an item you want to sell then you would include the address. In Spain people are more reluctant to include the address detail.

What are the different approaches you are seeing around consent? Are you seeing any reliance on legitimate interest?

So far it seems to be some kind of hybrid solution. There are still a lot of click options to accept a privacy policy but it's not quite in line with the consent requirements per the A29WP. There is a focus on good transparency.

You could argue that it's not one or the other. The purpose of the GDPR is to make sure the user understands and can take control of their data.

The focus of the industry, us included, is to figure out how to encourage users and help them to understand. We don't want a bad user experience with lots of tick boxes. Our focus is on how we best can be transparent and let the end users control their own data.

Consumer rights will be enhanced - how does a publisher prepare for this?

We strive to design for trust and develop good privacy solutions to give users the best products and services; to empower users while protecting their data. As a user I will be much more willing to share with my vendors valuable data about myself if I am engaged and compelled to extend my trust, so this is important both from end user, business and GDPR perspective.

Do you have any more clarity on how it will be policed?

We are prepared that this will likely vary a bit between different jurisdictions. I hope that most regulators will try to push and guide companies to come up with good solutions and try to help companies. GDPR establish extensive and complicated requirements so it will take quite a lot of resource to guide companies. In Norway we have had good experience with the regulator here. They have generally communicated that they really want to guide companies to comply; that what is important is that companies do what they can to handle data in the best interest of the users.

Schibsted has been involved in discussions in Brussels about the draft ePrivacy regulation - what is it about the regulation that causes concern?

The principles regarding transparency and user control in the GDPR is important and there is a lot of effort focused on that. Our view is that we should give the GDPR time to work and see if this solves the challenges in this area. It's bad that before the GDPR it has been concluded that the ePrivacy regulation has been drafted.

A particular with the ePrivacy regulation as it is proposed, is that consent is the only available legal basis — with some narrow exceptions. It removes other legal bases and thereby also the flexibility and thereby also not see privacy innovation around how we best can inform users and let them control their data. We are concerned that users might be overwhelmed and that we will see consent fatigue. That we will have the same problem as with the cookie banners.

Also, we see risks with the role the browsers are given. They may end up being a gatekeeper to the Internet. They will be the starting point to obtain consent and we see a risk that the browsers may use this. From a technical perspective it's unclear how the signals will be distributed. If you obtain consent how is the signal sent back to the browser. It is crucial to understand the implications of this before such extensive change.

What is the likely timing of implementation?

It seems it will still take some time — at least 2019 before will have a regulation on ePrivacy.

How does it really differ from the GDPR? What impact do you think it could have on the online landscape?

The most important difference is of course the rigid consent requirements. As I have mentioned already, we see challenges - not least for our users - if these requirements are implemented. At the same time we are of course preparing for the potential new consent requirements by doing user research and taking part in industry standard initiatives related to potential new consent requirements.

Which areas, if any, do you think could be watered down/amended?

We need clarity related to the browser role and the scope of the exceptions from the consent requirement.

A Conversation with Jan Wittrodt

Senior Legal Data and IT Law, Zalando

Jan Wittrodt joined Zalando in September 2015 as Senior Legal Counsel to manage the Data and IT law practice in the legal department. Since April 2017 he has been leading the Data and IT law practice as Senior Lead. The scope of his work comprises all matters of IT law, including Data Privacy, data monetarisation, data marketing, AI & ML as well as the digitisation efforts of the legal department.

What sensitive data do you collect? How does Zalando use this data and how does it impact your business?

Through our business we gather two different kinds of data about our customers: (1) process data (content and transactional data like name, address, payment details etc.); and (2) click-stream and tracking data to follow the customer's journey on the World Wide Web — on and outside of Zalando premises. All data is pseudonymized and aggregated to ensure the customers privacy.

Process data is used to perform the contract when a customer submits an order. Click-stream data is used for three business cases: (1) personalization; (2) AI and machine learning; and (3) marketing.

Personalization is a very important topic for us as we consider ourselves a personalized online shopping platform where every customer sees its own personalized shop. AI and machine learning is an important lever to achieve personalization at scale as it allows to build in more automation to improve the customer experience. We have data engineers who work with big data pools to build, smart recommendations, sizing tools, look-alike models, etc. to understand, based on customer data, what they are interested in so we can provide better personalization.

We also use data for marketing purposes — we use Facebook's custom audience tool, to name one, to address and reach new customers.

How does the GDPR impact the way you use this data? What processes have you changed as a result of GDPR?

We see GDPR is an update to the existing data protection we have in Germany. I always look at if I am permitted to do something and how. The 'if' under the GDPR stays essentially the same. The basic principle is consent, a contract in place or justified interest. What is truly new is the increase in the 'how' around compliance efforts. We need to increase documentation, add the legal justification and conduct privacy impact assessments, to name a few examples.

We make sure we have strict access control and we use pseudonymization. Teams working on big data need access to all kinds of data and need to connect it to build models but we must ensure they don't get access to data directly — they have digital identities rather seeing the actual customer or customer profile behind it. We have centralized access control between the technology security and the legal teams to make sure we are satisfied that we are meeting the GDPR requirements.

How prepared do you feel for the GDPR? How have you gone about preparing? What has been the greatest challenge?

At Zalando we have deviated from what other companies have done to prepare for the GDPR. There are usually two separate GDPR projects — one is focused on the legal side, drafting policies, and the other is usually a team looking at technical controls. We have a joint project and steering committee so both legal and technical teams are working together. German data protection compliance is level 1 and GDPR is level 2. We have done a gap analysis to understand the difference, on the compliance side, between the German data protection requirements and the GDPR and then we have defined relevant work streams.

For example, looking at the documentation of processes, we defined the departments processing personal data on a data privacy risk and impact basis, and then drafted a plan and scheduled workshops with each department. We used this as the basis for other relevant workstreams, i.e. to draft the privacy policy using simple language in a way customers will be able to understand.

The tech teams around the company have done surveys to understand the technical controls for each application, where there are deficiencies and what is needed to step up. Other work streams focused on data access and data deletion, for example.

We calculated back from the 25th of May and structured workstream timings and implementation accordingly. I feel comfortable with the level of compliance we have achieved. No one can achieve 100% compliance as no one knows, and no authority is telling you, what 100% compliance actually looks like. Defining what GDPR compliance really means for Zalando was a challenge in itself. Once we had established that then we had a better idea of what we needed to do. The challenge is not only the effort it requires to undertake that — you need to have the resources and track the log through the company to adhere to the requirement – but also the actual definition of what compliance under GDPR means.

How will relationships with third parties and suppliers change as a result of the GDPR?

This is all about supplier management. It's part of our GDPR work stream package. In Germany there have always been strict requirements to have a data processing agreement in place with processors and to apply and review the technical and organizational measures applied by service providers. We prepared a new template which went live in September 2017 so new suppliers come on to that and we are upgrading existing suppliers. Accordingly, we have no need to change relationships with third parties as the GDPR requirements do not fundamentally differ from the existing German data privacy requirements. It may differ for other data controllers located in other markets in Europe.

Do you see implications for how you approach marketing as a result of the GDPR?

With the current GDPR wording, and what we think it requires, then we can continue direct marketing under the legitimate interest basis. We believe justified interest is still a justification for online tracking and retargeting. What remains to be seen is whether the authorities share this view or whether they will have additional requirements for control. We have aligned our approach with other companies and that is the baseline for best practice currently.

What do you think the implications of the GDPR are for your industry? Will it change the amount of data the industry has access to?

I don't think we will see a change in the data we can collect as it stands right now. The legal justifications don't change. What remains to be seen is how the data protection authorities deal with online clickstream and tracking data. The authorities may make a preliminary push to what the ePrivacy regulation is setting out, which would change what data we could have access to in the future. We need to understand from authorities what they actually mean when it comes to the consent requirements. There is more than just tracking for marketing — tracking for personalization services, which is all handled internally — authorities have shown they have not understood the different business cases.

What are your views on the implications and timing of the ePrivacy Regulation?

The proposed ePrivacy regulation is not only a change on the level of 'how' but also on the level of 'if'. The current draft requires that you need consent, there is no justified interest. If it comes in then that would change the mechanism of how this works. The bigger challenge is that we would need to understand how we can work with data to build the business because ePrivacy regulation is confusing. We have been talking to a lot of policy makers to make them aware that it's about more than online tracking, profile building and Google and Facebook. It's hard to make ourselves heard. We have done business analysis to understand what could happen if there are strict consent requirements. We have joined forces with one of the major consent networks in Germany. We are also making sure our infrastructure could switch to those consent requirements sooner rather than later. We think our service is a personalization, and we see personalization as part of the performance of the contract so that could be permissible under ePrivacy. We have put mitigation measures in place and we have an action plan at the lobbying and business case level.

Regarding timing: It was initially meant to be enacted with the GDPR but that is not happening. We believe that when the trilogue phase is over at end of this year we will see what ePrivacy will look like. It may be enacted in 1Q19 with a 12 month transition period, so it could potentially apply from 1Q 2020.

Are you planning to rely on legitimate interest?

With the existing customers, use of data will be based on a contract or legitimate interest. The key question is whether legitimate interest will work for online tracking for marketing purposes. If we can't rely on that basis under the ePrivacy regulation, then we will need consent and we need to see how we rely on that in practice, i.e. how consent collection can be achieved in practical terms in accordance with ePrivacy.

Where, in the view of the authorities, consent might be required under GDPR is tracking and profiling as it is unclear who is behind the data and where the data is going. For artificial intelligence and machine learning the data stays internally at Zalando and we have full control of the data. We are also building a tracking opt-out for customers to make it easier for customers to click on a link to opt-out and then tracking is turned off. We can use this to show authorities that we are able to control that process and thus that the reasons indicated by authorities for consent requirements do not apply to Zalando in that context.

Could you talk about the log in alliance that has been formed in Germany which you are a partner of – how does it work and how do you think consumers will respond?

We have joined an alliance with some publishers in Germany which have set up a trusted consent network. The idea is that customers would consent to data processing by the partners of the trustworthy network so customers have a level of control within the network. Customers' data can be exchanged within the network for targeting etc. A single sign on solution makes customers' lives easier to manage their identity for different services. This is one of the mitigation measures for the ePrivacy regulation — what you can do is convince customers that it is in their interest to share data. Being transparent about the fact the data will not be transferred to other markets is a competitive advantage.

It has been launched but the difficulty from a technical point of view is what ePrivacy will eventually look like. There has not been a big push. It makes sense to set it up and bring it to life in a stable manner once we know what ePrivacy will require.

How will the industry ensure it's prepared for the enhanced consumer rights?

In Germany we already have a process in place to inform customers about how data is being used and to deal with customer requests. We are preparing for a possible increase in the number of customers who are asking to remove their data. It is a matter of upgrading the processes that are already there.

We will do a revamp of the privacy policy and will expand the information in the privacy policy to give customers more insight into the data we use. We will also improve the language so it is simpler. We believe others in the industry are doing the same. You will see revised and extended privacy policies being published. It depends on how well you're prepared under the existing regime — for some it's more effort and for some it's less effort.

Do you think Zalando has a competitive advantage?

We are proud to be not just a German Company, but also a European company. We are proud to be part of one of the strictest data protection regimes in Europe. We have generated a lot of trust with customers and the GDPR was important to continue to build on the trust. We are trying to think ahead and figure out what is coming, to think about the business models, full technical solutions and to build tools we need to be compliant and continue serving customers in the best possible way. We believe we have some competitive advantage there.

Data deletion is a challenge for every player due to legacy systems. I have been discussing approaches with other operators across industries and some are defining retention and deletion policies but they have not necessarily got a technical control in place to implement it. We have technical controls to make sure we can delete data, or at least block it until they can. We have defined a roadmap. These things give me comfort we are covering GDPR from beginning to end.

Does the regulation benefit large companies and make it harder for start-ups?

A start-up needs to pitch to VCs and provide an assessment of the risk of the model, funding requirements and identify data processing. They will need to have a privacy compliant regime and that will cost more now and require more resources. This will have an impact on the business case they present, so the question is whether the VCs are ready to spend more money to build privacy by design into a start-up. This is a bigger risk for start-ups and it makes it more difficult for start-ups in Europe. Maybe they focus on growth outside of Europe first, in the US, to generate sufficient revenue before working out how to comply with European regulation.

Having built a level of trust with an established customer base is an advantage. It will be more difficult for a start-up to get build a customer base.

How do you think the regulation will be enforced?

The regulators would like to be active but it seems they are not well resourced. They are facing a lot of challenges around what compliance actually means and they are struggling to find a common ground with the "Article 29 Working Party". Authorities in the past have understood that it is not always best to apply such strict views.

In the beginning I believe they will be careful to understand what companies are doing. They want to see companies have a GDPR program running, understand the key challenges and are implementing the requirements to adhere to the regulation. They will learn from their process step by step and build on that so that they have more specific compliance requirements later on. If they have an issue they will probably enquire, ask questions and have a dialogue with companies. It is a legal regulation and not easy to understand at a technical level so they need to understand how the companies work. It will vary by company and what they are doing with data. Where you need to be careful is if you don't have any actual GDPR implementation in place, for example if you do not have processes for data access and you're not informing the customer about how to access to data as that is a clear breach.

We expect authorities will be more flexible if it is clear you have understood and put processes in place and if you can show the challenges you are facing and how you plan to deal with them.

Do you think there will be a change in the approach to data protection globally?

My view keeps changing. The European framework is challenging although it adds improvement and awareness and helps within Europe as companies are now more aware. For example, at Zalando we see a lot of teams are reaching out with questions so it is a chance to educate them. It has a knock-on effect to global companies operating both inside and outside of Europe and this impacts their overall system set up.

I don't think GDPR will be a role model for U.S. legislation because I still have a feeling that the GDPR is 20 years old. It is an upgrade of the former directive but it has kept a lot of the old principles and has focused on increased compliance requirements. Is this the right answer for digital services in a changing society? I'm not sure GDPR is really prepared for new products and a single digital market as such.

The U.S. might take a different approach that is more balanced which will look more at a technical framework. The U.S. has said they will not rush with a revamped framework. There is sometimes an over estimation from Europe. It has an influence and affects discussion overseas, but we don't see an overall willingness to really implement something like we have in Europe. We don't think companies will proactively implement it in the U.S. as it would be a huge investment and would consume a lot of resources.

A Conversation with Alexander Hanff

Founder and CEO, Think Privacy

Alexander Hanff, Founder and CEO of Think Privacy. Think Privacy AB is a consultancy and solutions provider for organizations seeking to embrace privacy and data protection. Mr. Hanff has been involved with GDPR since the process started in 2011, and for the last 18 months has been engaged directly in Brussels, including participating in drafting parts of the regulation.

Maybe if you could just start us off with an intro?

I've studied computer science for my first degree and worked in the tech industry for 15 plus years. Then in 2005, I became concerned with the impact of technology on society, so I returned to the university to study that as a sociologist. And upon graduating the second degree, I moved into privacy as an advocate working for an NGO called Privacy International in London for three years. During that time, I was responsible for sweeping changes across Europe with regards to, I mean, ePrivacy directive as it was then, 2025 ADC, and what many people refer to as the Cookie Law.

I ran a campaign in 2008/ 2009 regarding behavioral clouds and profiling which led to the changes being implemented by the European Commission in 2009 and then becoming into effect in 2012. Obviously, I was very heavily involved in GDPR from the first leak drafted in 2001 right the way through, including all the consultations and roundtables, et cetera, which take part from the European Commission and the European Parliament. And for the last 18 months, I've been very heavily involved in the ePrivacy Regulation which is apparently making its way through the legislative process as a Special Advisor to European Parliament and working on the drafting team on specific issues related to privacy communications, privacy by design, and by default, tracking of profiles of people through their terminal equipment, etc.

So, it's a subject that's very close to my heart, one that I do, I will hope to do, for the rest of my life, because of my belief in using technology to empower people rather than to control and commoditize them. I am the Co-Founding CEO of the company here in Sweden called "Think Privacy". It's a company name I've used for the last ten years in the various places I've lived. We're a consultancy; we work with organizations across a whole range of issues including GDPR program management, legal services, advisory work, privacy-by-design, software development, educational resources, and training. Literally everything that's a very holistic approach to privacy and base protection because it's one thing being advocate and campaigning for stronger privacy laws, but we also have a responsibility to try and help organizations meet those obligations and understand those obligations. So, that's what we do to consult to the side of things.

They call me the "Cookie Monster" in Brussels, but I'm really not that terrifying. I do try and be quite pragmatic. So, with regards to GDPR, it's, as we all know, will be coming into effect on the 25th of May this year. The ePrivacy Regulation is now going to be delayed somewhat. The European, the Council of the European Union, will not have the report ready until June, it's believed, at the earliest. Which means we're looking at trial law towards the end of this year and implementation probably around Spring, maybe as late as Fall, after the Summer recess 2019. Which means it's probably going into effect at the earliest, we would expect it to be Spring 2020, potentially a little later. And that could slip accordingly, obviously, if things get delayed to trial law. So, at the moment, that's the timeline we're looking at for the ePrivacy Regulation and GDPR as we all know will be in effect in May of 2018.

Can you maybe describe a little bit of the backdrop, the history, of EU protection and legislation? What is the importance of GDPR and ePrivacy, what brought this about, and what's changing?

1949 was really the beginning of the privacy landscape here in Europe and globally, with the assignation, or the Universal Declaration of People's Rights, which granted the right to privacy in the home and private life in communications, et cetera. That was followed though, through the European Convention in I believe 1951, which really echoed the Universal Declaration but was a binding agreement within the European Union.

Then in 1980, we had the OECD Guidelines, which were developed in the U.S. and they became really the foundation of modern day protection of privacy. And again, in Europe, we followed on from that in 1981 with Convention 108, which is a Council of Europe Convention, which is an International Convention that anybody can, or any country can, sign up to. And it's binding, so, you know, the legal responsibilities or the responsibilities if you sign up will become a signatory of that convention.

Then in 1995, we had the Data Protection Directive that came into effect which was known as 9546EC — the official title — which is what everybody has been working with up until this point, or up until May of 2018. In 2002, we had the ePrivacy Directive (20025AEC) which looked at providing the same level of protection for communications as we have for personal data. And that's the important thing to remember, that data protection with regards to GDPR and the Data Protection Directive, are focused primarily on personal data and protecting personal data, setting rule of governance and how personal data can be processed, the level of the control that the data subjects have, the access rights, and so on and so forth.

ePrivacy covers a separate side, which is the privacy of communications data — this is not related to personal data. Although it may involve personal data, it's more explicitly to do with any information regarding communications data. The reason for this, certainly now, since the European Fundamental Rights Charter, or Charter for the Rights of the European Union, which became into effect I believe in 2007, I could be wrong. But since then, the EU Charter, we have now two different Articles within Constitutional law within Europe with regards to privacy and data protection. And privacy falls under one Article and data protection falls under another Article. So, they're two distinctly different entities in law, which is why we have two distinctly different pieces of legislation (in this case, regulations or directives, in order to deal with them).

So, when GDPR came into course in 2016, obviously it doesn't come into force of May of this year. And within GDPR itself, there is a section which requires a review and kind of refreshment of the ePrivacy Directive. And that makes sense because the Data Protection Directive and the ePrivacy Directive work well together as secondary legislation. But the GDPR is primary legislation because it's a legislation, which means that it has be the same in every single member state. And it wouldn't make sense to couple the regulation with a directive. I mean, the ePrivacy Directive wouldn't work as well with the GDPR as it stands. So, we need to refresh the ePrivacy Directive and turn that into a regulation as well, to give a similar level of protection, and to also make it fit and work really well with GDPR.

So, that's where we are now; the reason why the changes took effect and through no small part in my own work. As I said back in 2008, I was very heavily involved in campaigning on privacy, particularly with regards to ePrivacy and digital profiling and that really was the beginning of these changes.

We had the changes that affected the ePrivacy Directive known as the Cookie Law, Article 53, in 2009, which came into effect in 2012. And as result of the discussion around privacy at that time, the European Commission then set about creating the new proposal for the GDPR, which was first leaked in November or December 2011. And then, was officially announced in January 2012 in Brussels on the 25th of January, I believe it was.

And then, as we can see that's moved forward. We've seen legislative changes elsewhere as well, such as in the United States with the Privacy Act. There's been State legislation in the U.S. as well, California and various other states, have introduced specific privacy laws. We have the Central and South America working very hard on data protection and privacy laws. We have the Asia-Pacific region also, particularly places like South Korea and Japan, which are working very hard on privacy and data protection laws.

So, this isn't something which is just limited to Europe. Over the last 10 years, we've seen a very significant shift globally with regards to concerns over digital privacy and data processing of personal data, whereas Europe has kind of spearheaded with very strong regulation and very strong laws and rules on the governing to processing of personal data and private communications. It's not something that we can stand and say, "We're the only ones doing it". It's happening globally and will continue to happen. In fact, there are multiple countries within the African subcontinent who have recently all become signatories to Convention 108, which is the one we discussed from 1981.

So, even now, we're seeing a Convention from nearly 30 years ago or over 30 years ago, gaining new strength and finding new signatories. And that is partially because if you sign up to Convention 108, you'll probably 70% of the way towards GDPR compliance. And with Europe being the second largest economy on the planet, obviously companies want to be able to trade with Europe. And in order to do that, they need to come and comply with our laws. So, they need to make institutional changes within their own borders to ensure that they can meet the level of adequacy that's required in order to be able to do business here in Europe. So, it's a really fundamental shift globally towards privacy and data protection.

You touched a little bit on this, but can you highlight some of the major requirements of GDPR that differ from what's currently required?

The important thing about GDPR is that there are actually not very many differences between the GDPR and the previous Data Protection Directive. There are some differences which I'll try to go over, but much of the work that was covered by the Data Protection Directive is also covered by GDPR. The problem we see generally, certainly from a consulting perspective, is we had a very significant lack of enforcement of the previous Directive in various member sectors. And that was particularly because of the fact that it was secondary legislation. So, we had 28 different interpretations of the Directive in each member state, which made it very difficult to have any form of cohesive enforcement.

With the GDPR, that enforcement becomes much easier. This is particularly because of the change of the enforcement regime and this is one of the most significant changes that comes with GDPR. Previously under the Data Protection Directive, we had lots of working parties which are made up a regulator from each member state, along with European Commission and European Data Protection Supervisor.

There is an advisory body that had no legal weight as such, but their opinions and their advice were taken onboard by the Commission and also, by the Court of Justice of the European Union, which made it to the courts. So, as they weren't officially legally binding, they were taken very seriously and should be regarded is having significant power.

But again, because of this regulative issue we had, through what we call "forum shopping", where companies would set up their established headquarters in a country with a particularly weak data protection authority or supervisory authority in their courts. With the GDPR and the one-stop shop, this becomes a much different regulated regime, because we have instead of now the Article 29 working party, we have the European Data Protection Board. Who essentially do the same job, they provide advice and issue opinions, an annual report, et cetera, et cetera. But they also have oversight powers over the rest of the supervisory authorities in each of the member states and have the final say in any cases of dispute where an agreement on enforcement cannot be obtained. So, that in itself, adds an extra tier to the enforcement regime which didn't previously exist.

On top of that, obviously we have, and I try and not to talk about this very much because I really don't like using big fines as a way of threatening people to take responsible action. But we do have more significant penalties now as a result of GDPR. Under the previous Directive, there were many regulators who had no powers to issue fines or issue monetary penalties. They could issue notices, enforcement notices etc. but they didn't have any real effect on companies who could see no effect on their loss of line. Under GDPR obviously, the one of the big things which is discussed is the new penalties of 2% or 10 million euros, whichever's higher, and the 4% and 20 million euros, whichever is higher.

And obviously, that's something that companies need to be aware of, but it shouldn't be the driving focus when we come into GDPR compliance. The whole point of having these rules and regulations in place is to make the world a better place and to empower society in ways in which to enable us to control our privacy, but still conduct business. And we have to bear to mind that both the Directive previously and the current legislation GDPR, that primary focus is to allow the free trade of information throughout Europe. And they do that by setting up these safeguards and these rules on how that data can be processed. So, the purpose isn't to obstruct, the purpose is to enable. It's a very positive and proactive regulation for businesses and should be seen that way and should be acted on that way.

So, the regulation regime has changed significantly as I said. There are a couple of new rights as such with regards to data subjects. So, the right to data portability, which allows data subjects to demand any data that they've submitted to me on the contract to be returned to them in a standardized or standardized as possible, machine-readable format or transferred to another third party at their request. So, they can effectively take their data from your service and move it to a competitor service. Or, simply take it from your service and bring it back to them, to their own environment, if they so wish. That didn't previously exist, it's quite controversial, and has been difficult to format with regards to how we're going to see this happening in principle. Because trying to standardize something which is based on companies who have multiple proprietary methods is a very difficult thing to do.

So, there hasn't been as much corporations from industry, although this is not what we would like to see, but it's going to come into effect in May. So, it's something that companies need to prepare for. We've seen some of the big players such as Google, Facebook, LinkedIn, Microsoft, now have facilities in place, I believe. Twitter does as well, which allow people to download and file copies or certainly some amounts of data they've submitted. But still generally across the entire industry, there are a lot of companies who are not prepared for data accountability issues.

The right to be forgotten, you probably all heard about this one. It's often misunderstood as being a right to delete or right to erase, it's not the same thing. Right to be forgotten is the right to be de-indexed. So, if you consider a library, for example, where you used to have the index cards. You would go in and pull the card and it would tell you where the book was. If you tear that card up, the book is still there, it's just much more difficult to find. And that's essentially the same as what we see in the right for the forgotten.

So, it's a situation where an individual or data subject who has a fabrication indexed against their name in a search engine or some other service. Which has as significant impact on their private life or their right to conduct business or various other things, but is not in the public interest and they have a legal right now to have that index removed. That doesn't mean as I said that the data is removed, it could still be found through other means. But certainly, it would not be indexed against their name anymore and therefore, it would not be seen to be having such a significant impact on their day to day lives.

But again, the important part here is the public interest balance. It's not an absolute right, it's something that they, the controller, has the right to refuse if they feel that there's a public interest in that data remaining linked to that person's name. And this is case, this was actually tested recently in Japan, of all places, I Bellevue it was earlier on last summer. A case where somebody who had been convicted of a violent criminal offense has attempted to have their name de-indexed from the information in news reports and search engines. It went to the courts, the courts applied the same balance test that was applied by the Court of Justice of the European Union, and came to the conclusion that is was in the public interest that that information remained linked to his name and the right was refused. So, it's not an absolute right and it's important to do this balancing test and ensure that if it is I the public interest, then you could refuse to de-link that information.

Are there any meaningful changes related to the consent rules?

Consent is a mixed bag. The definition of consent remains the same as it has been since 1981, going back to Convention 108. So, consent must be freely given, you cannot refuse services if somebody does not consent. Consent must be as a direct result of positive action or an affirmative action, not non-action. So, you can't have free check boxes, for example. But none of these things are new; these things have been active for some time. What is new with consent is we now must record consent. You must be able to provide that consent has been obtained.

And this important, this is one of the other things, it's not just consent which causes this recordkeeping under GDPR. It's far more significant a requirement then it was under the previous Directive. But accountability which is one of the biggest sections in GDPR includes significant record keeping. And the only exception to recordkeeping is companies who have less than 250 employees. And even then, the recordkeeping, they're only exempt from recordkeeping if the process that they're doing is occasional.

So, if they're doing the same processing over and over again of personal data, then even if they're a small company with less 250 employees, they're still required to keep records of that process and activity.

Recordkeeping, if the, dealing with what we used to call "sensitive data" is now called "special category data" removes that exemption as well. So, anybody dealing with criminal data as well are not exempt. So, recordkeeping is one of the more onerous parts of GDPR and I know some of my clients who have been, over the last 18 months, 24 moths working on GDPR compliance and 75% of their time has gone on setting up recordkeeping.

I thought I had read that these rules might require companies doing personalized advertising to receive consent more frequently than they do today- is there any truth to that?

Well, I mean, consent doesn't need to be done more frequently. But one of the principles of data protection law with both the previous Directive and GDPR, is storage limitation. So, ensuring that you only store data for a reasonable period of time or for period of time where it's actually necessary. And there's an expectation from the data subject that that data's going to be processed. What, with regards to consent, consent must be specific, so you cannot have blanket consent, the base subject must be aware of what they're actually consenting to. It must be specific, and this must be included in the privacy notice and they must be informed of any third parties that that data is going to be shared with.

So, again, this comes down to accountability and the reporting information to the data subject, so they can make a conscious and informed decision with regards to consent. So, it's important to know that consent is not the only legal basis for processing under GDPR. So, there are six (6) legal bases for processing data under GDPR, consent is one of them, legitimate interest is one of them, performance of the contracts, protection of legal claim, and public interest. So, if you can find another legal basis for processing data, then I recommend that you use consent as infrequently as possible. There are certain circumstances where consent will be necessary, but if you can find a different legal basis, then I would suggest you go with it.

The reasons why consent and this is the thing, the same is true of logical interest by the way. The reason why consent is problematic is because it can be withdrawn at any time. You know, the data subjects can withdraw their consent and in most cases, they have the right to withdraw their consent. And if they do that and if you're using consent as a legal basis, then you have to cease processing and that's where the exception applies.

Do you think that every time there is a targeted ad that there has to be some sort of consent process?

The first one is advertising, particularly because this is based largely online. There's more focus of the ePrivacy Regulation. The ePrivacy Regulation is still in draft, so it's impossible at this time to say exactly how it works with regards to retention periods. It certainly doesn't fall under GDPR, GDPR is more focused on data protection with regards to things which are related to communications data. So, any behavioral advertising or profile on Facebook or on another form of those Websites will fall firmly under the ePrivacy Regulation.

And there is an expectation in the ePrivacy Regulation that, first of all, software which people use to access online services will have privacy enabled by default. So, you will need to try and find a way to incentivize or to persuade data subjects to turn those protections off or to agree or consent to receive your marketing materials or allow you to do behavioral advertising. The difficulty there is, you must also give them the means to control the types of advertising that they're seeing. So, there's a very strong requirement t in the ePrivacy Regulation that those controls be granular which would give the data subject more control over the types of advertisements they're seeing. And of course, they have the right not to receive those advertisements and not to be profiled. And they have those rights by default in the ePrivacy Regulation.

So, it's going to be much more difficult for companies like Facebook to be able to pull people into their advertising ecosystem where just a notice in their privacy notice. There's going to need to be some form of affirmative action which goes beyond just something in a privacy notice. Unless that privacy notice is incredibly specific, which will enable those end-users to turn off their detection. And with regards to the ePrivacy Regulation as well, if an end user has their browser set or whatever app they're actually using to actually serve a set with the privacy settings on, then that is seen as an action by the end user against consent. So, that would be seen effectively as they're not consenting. So, you cannot assume if they have these things turned on that they consent to these. You need to then obtain relevant consent and have a record of that consent.

On the ePrivacy Regulation, where you're talking about privacy set by default, using browsers and things like that, I have seen some articles suggesting that gives quite a lot of power to the browsers. What are your thoughts on that and is that a sensible route to go down?

I personally fought for this and wrote the paragraph within Article 10, along with the documentation, which ensured this right. So, I have quite strong feelings on this. I support this, and this isn't just browsers. The Article 10 as it currently stands states that any software, which is used in conveyance of communication, that includes service-side software and client-side software. So, emails services, Web services, applications, operating systems, Web browsers, etc., are all covered under Article 10 of the EPrivacy Regulation. There's even something just restricted to browsers, your Android operating system on your android phone or your iOS operating system on your Apple phone will need to have these sections built in by default as well

I think it's a very positive thing. I agree that it may be difficult when you see some of the companies who are most reasonable for, how should we put this politely? For using personal data for targeting adverts are also some of the biggest browser manufacturers such as Google as a prime example or Microsoft with the Edge browsers. But they need to separate the development shop from the advertising and marketing shops. It's a rule stated that the browsers have to have these turned on by default and then just because they happen to run a multi-billion-dollar advertising arm, that doesn't mean they can ignore the rules with regards to how these browsers are configured.

You mentioned legitimate interest. We've had a lot of conversations with people in the industry about how they're thinking about GDPR and implementing it. Quite a few seem to be thinking about using legitimate interest as a means to get around having to ask for more explicit consent then they get now. Is that something that fits with the GDPR? Within the personalized ad space what would be regarded as acceptable?

Currently, there is no legitimate interest in ePrivacy, for starts. The only means for processing communications data currently, with very limited exceptions to the National U.S. Convention of Crime, etc., is consent. So, there is no legitimate interest in the ePrivacy Regulation and actually just last month in Brussels, I asked the new repertoire whether or not the European Parliament would stand strong on screening the legitimate interests from being added to the EPR during the trilogue. She made it very clear that there is no intention from the European Parliament to allow legitimate interest into ePrivacy Regulation.

And the reason being that, communications data is considered sensitive data and there is no legitimate interest in GDPR for sensitive data. It's unlikely we will see legitimate interest in the ePrivacy Regulation. Legitimate interest by direct marketing within GDPR, falls under Recital 47 in GDPR which states at the very end of Recital 47, direct marketing may be considered as a legitimate interest.

Now, the important thing there is, this is often being misinterpreted, particularly by the advertising industries in believing that they now have a right to just serve advertising under legitimate interest. And that is not the case. This has been made clear several times already by various regulators. The important key word in that last sentience in Recital 47 is the word "may". Now, in order for any processing of personal data under GDPR to be able take place legally, it must be lawful, it must be necessary. There are a whole bunch of principles which may be met in order for that to actually occur and the key one here is the lawfulness. And what we mean by lawfulness, is that the processing of data, you cannot be in breach of any of the laws, yes?

So, in the case of direct marketing under Recital 47, there may be occasions where direct marketing can be considered as legitimate interest, but only if that isn't in breach of any other laws. And with regards to digital marketing, that means you have to take into account the ePrivacy Regulation laws that currently stands as the EPrivacy Directive. So, if what you are planning to do with your direct marketing is not compliant for example or the ePrivacy Regulation or the ePrivacy Directive, then it's not lawful under GDPR.

If there's no concept of legitimate interest or consent in the ePrivacy rules. What are some of the challenges?

You raise an interesting question because what it actually does is just confirms what I've just said on lawfulness. Under the ePrivacy Directive and what will be the ePrivacy Regulation, processing information, marketing to individuals with who you already have an existing relationship is lawful. And therefore, would be lawful as a legitimate interest under GDPR. But that relationship must be in the content of silo of goods and services. So, if somebody has purchased something from you previously that under the ePrivacy Regulation, you have a right to market to them. They have an absolute right to object and withdraw from that marketing via an opt out basis. But initially, if they're an existing customer, you have a right to market to them.

There are certain circumstances you must or certain obligations you must adhere to, so they must be given information on how they can opt out of that direct marketing with each marketing piece that you send to them. And the right to object and withdraw from that marketing is an absolute right as well. So, you cannot refuse for them to object their marketing and you must cease direct marketing to them if they object to it. But these are lawful — this is where the ePrivacy Regulation falls into lawfulness. So, in that situation you described, it would be lawful under the ePrivacy Regulation which is why it becomes a legitimate interest under the Recital 47 under the GDPR.

If you're a retailer, you aren't necessarily going to have to go back and re-consent everyone? Where does this boundary lie?

If they're an existing customer, you are entitled to market to them, other products and services of your own. You can't start promoting products and services from other companies, on the provision that the consent that you originally obtained was lawful. So, if you brought in a huge amount of data from a third-party company and you're not sure that that data is obtained in a lawful fashion, then you may have a problem to face with regards to obtaining or reobtaining consent.

But if you're sure that that information was obtained lawfully, so for example, if somebody's filling out a form in their supermarket and they check the box and they received a loyalty card through the post as a result of checking that box, then the chances are that the consent has been obtained in a lawful fashion and you will not need to do any more in order to do new marketing to them. But if you have any doubts over the lawfulness of the consent you have in the first place, that's where you need to think about how you deal with the consent.

How enforceable is all of this? Is there extra resource as going into the Data Protection Authorities?

One of the requirements of GDPR is the supervisory authorities must be appropriately resourced. And In fact, just in the news this week, the Information Commissioner's Office has been confirmed that they've been given a stronger budget to pay their staff more money to retain their staff and bring in more expert knowledge. The Irish State of Protection Commissioner has received a significant boost in funding over the past 18 months, to the point where they now have a new office and they've grown their staff by a massive amount. So, yes, I mean, there is certainly more resources going into data protection from a regulatory perspective.

On the enforcement side of things, pretty much every supervisor I've spoken to over the past two years are very keen on ensuring that the environment of GDPR actually happens. And as I said the European Data Protection Board has ultimate oversight; the regime is much stronger than it ever was before. In situations where somebody in Germany is making a complaint against a company who is headquartered in Dublin, then both Supervisory Authorities would be involved in that complaint. And they must agree on the enforceable action. And if the enforcement action isn't agreed upon, then that's where the European Data Protection Board would come into effect.

So, there has to be cooperation and collaboration between Supervisory Authorities now as it opposed to it must being a single Supervisory Authority who has the ultimate say as it was under the previous situation or previous regime. So, enforcement powers are stronger, the enforcement regime itself, the institutionalization of the enforcement, is much stronger. And obviously, the penalties are much higher.

What I will say is it's unlikely we will see really large penalties. You know, the regulators are not of the mind that they want to go to start beating people with a stick. They will work as much as they can in an advisory role and try to help companies become compliant.

But in situations where companies are ignoring their advice, or where particularly, sensitive breaches take place such as the processing of child data or other specialty data. Or where a company has repeatedly shown negligence or have made no effort to prepare or comply with GDPR, then we will start to see those penalties increase. I never preach penalties to my clients. You know they're there, there's a stick, and they will be used, but they won't be used in a way that's excessive.

You think it's unlikely that after these rules go into effect that one of the local enforcement agencies tries to test the compliance, or pressure some of the larger companies?

Yes.

Do you think it's more likely that this is more of a process where they're trying to come to an agreement on what needs to be done and do that behind the scenes?

There will inevitably be some regulators who try and test the waters. The Hamburg Regulator, for example, repeatedly, even under the previous Directive, repeatedly took action against large companies like Facebook and Google, etc. So, there will be some who go out there and do that, that's inevitable. Generally speaking, we will see a measured approach by Supervisory Authorities where it's necessary. In situations as we said where companies are, are really not making any effort, or deliberately negligent or are trying to use loop holes. That's where you will start to see stiffer enforcement.

If companies are making a genuine effort to comply and setting programs up and putting programs in place, documenting their activities appropriately, recordkeeping, installing data protection offices where they're required, doing things like taking an impact assessment and ensuring that their processor agreements are up to scratch with their processes, that their data breach response programs are appropriately in place. So, they're using adequate security, et cetera. If they're meeting the requirements of the principles and they're making a genuine effort to comply, then it's unlikely we will see significant enforcement action against these entities. Unless it's protective action as a result of not following the advice, or something that's particularly sensitive that's going to have a particularly dangerous impact on data subjects, such as, as I said, processing child data or highly sensitive medical data or financial data.

Are the larger, higher profile companies making legitimate efforts to meet the requirements in your opinion?

There are some efforts, yes. We just saw, I think, again this week, a ruling in Germany against Facebook with regards to their notice, the information that they give to end users, in their privacy policy not being adequate. I think there were four different points that were raised in the Court and they found to be inadequate on all four cases. And Facebook is one that is trying really hard and the reality is the easy way to overcome this program is to simply not have those boxes checked. So, it's a really simple issue for them to overcome from a legal perspective. They just have a desire not to do so because it might impact their marketing activities. So, you know, in situations like that, then, we may see a slap from the enforcers, for lack of a better phrase, from the regulators.

But Facebook has a reputation for pushing back, and pushing back, and pushing back. So, it's not kind of, it isn't, like we wouldn't expect a regulator to take that time back against that space. But whether repeatedly go in against the request of the regulators and in many cases or certainly in some cases, actually refusing to work with regulators to come up with a solution. So, Facebook is perhaps not the best example of information where we're talking about GDPR enforcement. It's likely that we will see some enforcement actually against Facebook, if they continue to push regulators the wrong way. But generally speaking, the market as a whole, if they're making a genuine effort they should be fine.

In many cases, we will see companies who've set up GDPR programs, set up the documentation, and all that security and there will be other requirements. Who suffer a breach and then don't suffer any financial penalties because they're able to show that they've been going through the process and doing their due diligence and really making an effort on the first offense. If they then repeatedly make the same mistake, then it should be expected that those penalties would increase.

Under your example of the Germany Supervisory Authority how active have they been? Is it correct under GDPR complaints would be looked at by the European Protection Board?

The Board really gets engaged if there was no agreement between agencies. If the German Supervisory Authority had to engage in a discussion with, say the Irish Supervising Authority, and no agreement could come into play for enforcement, that is when the European Data Protection Board would come into effect. But if an agreement on enforcement is met between the two Supervising Authorities, there would be no need for the European Data Protection Board to intervene.

Are there any particular either business or category of businesses within those kind of high profile, online companies that you think are more at risk or more susceptible or just have more work to do to come into compliance?

Google's privacy policy of 2012, they made it clear that all of their services, any data collected across any of their services, would be included in their marketing and advertising business. So, from that perspective, it makes it very difficult for Google to avoid enforcement or certainly their obligations under GDPR and ePrivacy. Simply on the basis that they use all the data they collect, including Google analytics, et cetera, for their advertising and marketing platform.

With regards to other companies in this space, I mean, if in any way their core businesses is touching on the process and personal data or communications data, then they will fall under the jurisdiction of GDPR and EPrivacy. We've seen there is substantial case law on this already. The Google Spain case on the right to be forgotten, one of the most important aspects of the case, was the establishment or the definition of establishment. The Court of Justice European Union came to the decision that because Google has an advertising office within Spain selling advertising and the core purpose of their search is to be able to provide advertising then it was determined that they were established within Spain as well because they were conducting activities within Spain which was core to their advertising business, and therefore, fell under the jurisdiction of the Spanish Regulator.

So, the whole definition of establishment was turned on its head almost as a result of the Google Spain case. And not just the Google Spain case, but there are number of other cases as well which have touched on establishment. Some in Germany, some in the Netherlands,

So, the definition of establishment is now clear cut in case law as being any country where a company's conducting significant activities focused on any aspects of processing personal data, with regards to GDPR and EPrivacy Regulation.

So, as I said previously, if your company, in respect to what your core business units are, if you're processing personal data or communications data as a core business activity within that region, within that member state then the chances are you would definitely have to comply with GDPR and ePrivacy.

If you already have an established commercial relationship then you have an easier time to serve your products to the data subject that is consented, assuming that it's lawful. Do you think that Article issued actually boosts dominate positions in a way?

Does it boost lock in? If you have an existing relationship, then under the previous ePrivacy Directive, you have a legitimate reason to send direct marketing to them.

Does this have any consequences for large companies? One could say possibly, "Yes", but at the same time if they built up a loyalty base, based on strong customer services and delivering what customers want then, surely that's a positive byproduct to the way that they've behaved in the past. Does it make more difficult for other companies? No, not really, I don't think so. I mean, if you don't have an existing relationship with somebody, then why would you assume that they would like to receive direct marketing from you? If somebody has expressed an interest in your goods and services, then that would be a reasonable point to assume that they might want to receive further information. But until that point, it literally, I mean, not meaning to sound harsh, it becomes spam and spam is hugely problematic, it costs society billions of dollars of year in processing and dealing with spam.

Now, one of the interesting things with the ePrivacy Regulation that currently being drafted is what was previously permitted under the ePrivacy Directive was business to business marketing without previous relationship. But there's been so many complaints by companies over the past 10 years with the amount of money it's costing them in man hours to deal with spam form other companies that do direct marketing they now been given the same protection as B2C direct marketing has under the new regulations.

That may change under the trilogue situation but at the moment, currently business to business marketing gets the same protection as business to customer marketing. With regards to, you must have that existing relationships in the context of the sale of goods and services. So, the reason why we have these rules in place is because of the damaging impact that spam had had on the society over the past 15 to 20 years and there's a way to mitigate that.

So, if you signed up to buy shoes on Amazon, does that translate into an umbrella agreement that they can also serve ads later on that are completely unrelated to things that you can buy on the marketplace, if you see what I mean?

It comes down again to interpretation. I mean, Amazon is kind of a multi-dimensional marketplace. So, they have products which they sell on their own behalf and then they have third party just so using their platform. With regards to product marketing for products they sell themselves, they would probably have quite a lot of horizontally in that respect. With regards to third parties that are just using the Amazon platform, then that would probably be a different situation entirely because that's not marketing from Amazon, that's marketing from somebody else using Amazon's platform which the customer may not have an existing relationship with.

On that point if you were Amazon or any other sort of retailer that a customer uses, and you then leave their website to another website, does that mean because you have a relationship, they are entitled to retarget you on other websites with their ads? How far does it go from a retargeting perspective?

Again, that comes down to the ePrivacy Regulation when the final version of it comes through in late probably in 2019. Existing relationships with regards to digital advertising and direct marketing, and you have an existing relationship with somebody and you're advertising directly to the one of your Websites. That's a different situation to advertising to them through Google on somebody else's Website because you're not directly advertising as Google is in control of the data that's being processed. You're not a controller in that context, Google is the controller, you may be considered a joint controller that case were currently to go to, the Court of Justice of the European Union, on this issue actually with regards to joint controllership. The chances are, if you're using a third-party advertising platform as a brand, there's no way that Google should know that that customer already has an existing relationship with you. Unless you have received or have a legal basis for this, you'd probably need consent with regards to EPrivacy for passing that information on to Google in the first place.

So, you may have already consented to Google for example. You know, going through the granular controls. But you are responsible as publishers if you have a Website for your e-commerce or retail site. Then you are responsible for the third-party scripts that you install on your Website as well and this is one of things that already exist under ePrivacy Directive is not really been enforced but will be much stronger word in the ePrivacy Regulations.

And as I've said, there's case law on this already. So, for example, there's a case involving Facet ID and Facebook like scripts. And it's already begun that Facet ID become a joint controller in that situation, even though they're not responsible for or have no control over how Facebook is processing that data. Because they initiate the processing of that data of having the scripts stored on their Website, they become a joint controller, and therefore, attract the same liability as Facebook with regards to the processing that they take.

It's going to be very difficult for companies to try and side step the law with regarding to direct marketing. Direct marketing is one of the things which has been taken seriously with both GDPR and the ePrivacy Regulation. And my advice to any organization would be do it as honestly and transparently has possible because it's going to be very difficult to side step the regulations at this point.

It sounds like as long as they are getting your consent to use the data that they have about you, they have a relationship with you, you bought something from them, you visit their site or whatever, as long as you've gotten that consent, they can target ads through Google onto other sites?

It depends because one the things that you do under GDPR, is you must make the data subject aware if you're going to share it. It must go through the notices, it must be specific. So, you cannot just say, you may share data with third parties. If you're going to share the subscription data with Google for the purpose of brand advertising, then you need to make it very clear in your privacy policy that you will share that data, that specific type of data, with that third party for that specific purpose.

So, this is one of the things that comes with GDPR, is the information noted that you must give to data subject, must be much more specific. You must provide what you're sharing, what the purpose of the sharing is, and who you're sharing with.

Citi Global Perspectives & Solutions (Citi GPS) is designed to help our clients navigate the global economy's most demanding challenges, identify future themes and trends, and help our clients profit in a fast-changing and interconnected world. Citi GPS accesses the best elements of our global conversation and harvests the thought leadership of a wide range of senior professionals across the firm.

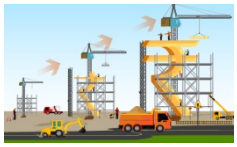
All Citi GPS reports are available on our website www.citi.com/citigps

Sustainable Cities
Beacons of Light Against the Shadow of Unplanned Urbanization
April 2018 2018

The Public Wealth of Cities
How to Turn Around Cities Fortunes by Unlocking Public Assets
March 2018

The Bank of the Future
The ABC's of Digital Disruption in Finance
March 2018

Investment Themes in 2018
How Much Longer Can the Cycle Run?
January 2018



Securing India's Growth Over the Next Decade
Twin Pillars of Investment & Productivity
February 2018

China Entering a New Political Economy Cycle
The World According to Xi Jinping Thought
December 2017

2018 Corporate Finance Priorities
January 2018

Disruptive Innovations V
Ten More Things to Stop and Think About
November 2017

Women in the Economy II
How Implementing a Women's Economic Empowerment Agenda Can Shape the Global Economy
November 2017

Technology at Work v3.0
Automating e-Commerce from Click to Pick to Door
August 2017

Inequality and Prosperity in the Industrialized World
Addressing a Growing Challenge
September 2017

Solutions for The Global Water Crisis
The End of 'Free and Cheap' Water
April 2017

Education: Back to Basics
Is Education Fit for the Future
July 2017

Digital Disruption - Revisited
What FinTech VC Investments Tells Us About a Changing Industry
January 2017

ePrivacy & Data Protection
Who Watches the Watchers? – How Regulation Could Alter the Path of Innovation
March 2017

2017 Corporate Finance Priorities
January 2017

2017 Investment Themes
A Wind of Change
January 2017

Infrastructure for Growth
The dawn of a new multi-trillion dollar asset class
October 2016

Car of the Future v3.0
Mobility 2030
November 2016

Re-Birth of Telecoms into a New Digital Industry
Time to Dump the Dumb Pipe
October 2016

Virtual & Augmented Reality
Are you sure it isn't real?
October 2016

Digital Disruption
How FinTech is Forcing Banking to a Tipping Point
March 2016

Disruptive Innovations IV
Ten More Things to Stop and Think About
July 2016

Technology at Work v2.0
The Future is Not What It Used To be
January 2016

The Coming Pensions Crisis
Recommendations for Keeping the Global Pensions System Afloat
March 2016

Investment Themes in 2016
New Normal or No Normal
January 2016

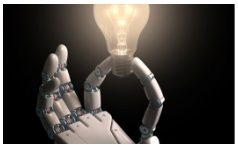
Global Political Risk
The New Convergence between Geopolitical and Vox Populi Risks
January 2016

Energy 2030
Financing A Greener Future
November 2015

2016 Corporate Finance Priorities
January 2016

The Curtain Falls
How Silicon Valley is Challenging Hollywood
October 2015

The Global Art Market
Perspectives on Current Drivers & Future trends
November 2015



Disruptive Innovations III
Ten More Things to Stop and Think About
July 2015

Energy Darwinism II
Why a Low Carbon Future Doesn't Have to Cost the Earth
August 2015

Beyond China
The Future of the Global Natural Resources Economy
March 2015

IMPORTANT DISCLOSURES

This communication has been prepared by Citigroup Global Markets Inc. and is distributed by or through its locally authorised affiliates (collectively, the "Firm") [E6GYB6412478]. This communication is not intended to constitute "research" as that term is defined by applicable regulations. Unless otherwise indicated, any reference to a research report or research recommendation is not intended to represent the whole report and is not in itself considered a recommendation or research report. The views expressed by each author herein are his/ her personal views and do not necessarily reflect the views of his/ her employer or any affiliated entity or the other authors, may differ from the views of other personnel at such entities, and may change without notice.

You should assume the following: The Firm may be the issuer of, or may trade as principal in, the financial instruments referred to in this communication or other related financial instruments. The author of this communication may have discussed the information contained herein with others within the Firm and the author and such other Firm personnel may have already acted on the basis of this information (including by trading for the Firm's proprietary accounts or communicating the information contained herein to other customers of the Firm). The Firm performs or seeks to perform investment banking and other services for the issuer of any such financial instruments. The Firm, the Firm's personnel (including those with whom the author may have consulted in the preparation of this communication), and other customers of the Firm may be long or short the financial instruments referred to herein, may have acquired such positions at prices and market conditions that are no longer available, and may have interests different or adverse to your interests.

This communication is provided for information and discussion purposes only. It does not constitute an offer or solicitation to purchase or sell any financial instruments. The information contained in this communication is based on generally available information and, although obtained from sources believed by the Firm to be reliable, its accuracy and completeness is not guaranteed. Certain personnel or business areas of the Firm may have access to or have acquired material non-public information that may have an impact (positive or negative) on the information contained herein, but that is not available to or known by the author of this communication.

The Firm shall have no liability to the user or to third parties, for the quality, accuracy, timeliness, continued availability or completeness of the data nor for any special, direct, indirect, incidental or consequential loss or damage which may be sustained because of the use of the information in this communication or otherwise arising in connection with this communication, provided that this exclusion of liability shall not exclude or limit any liability under any law or regulation applicable to the Firm that may not be excluded or restricted.

The provision of information is not based on your individual circumstances and should not be relied upon as an assessment of suitability for you of a particular product or transaction. Even if we possess information as to your objectives in relation to any transaction, series of transactions or trading strategy, this will not be deemed sufficient for any assessment of suitability for you of any transaction, series of transactions or trading strategy.

The Firm is not acting as your advisor, fiduciary or agent and is not managing your account. The information herein does not constitute investment advice and the Firm makes no recommendation as to the suitability of any of the products or transactions mentioned. Any trading or investment decisions you take are in reliance on your own analysis and judgment and/or that of your advisors and not in reliance on us. Therefore, prior to entering into any transaction, you should determine, without reliance on the Firm, the economic risks or merits, as well as the legal, tax and accounting characteristics and consequences of the transaction and that you are able to assume these risks.

Financial instruments denominated in a foreign currency are subject to exchange rate fluctuations, which may have an adverse effect on the price or value of an investment in such products. Investments in financial instruments carry significant risk, including the possible loss of the principal amount invested. Investors should obtain advice from their own tax, financial, legal and other advisors, and only make investment decisions on the basis of the investor's own objectives, experience and resources.

This communication is not intended to forecast or predict future events. Past performance is not a guarantee or indication of future results. Any prices provided herein (other than those that are identified as being historical) are indicative only and do not represent firm quotes as to either price or size. You should contact your local representative directly if you are interested in buying or selling any financial instrument, or pursuing any trading strategy, mentioned herein. No liability is accepted by the Firm for any loss (whether direct, indirect or consequential) that may arise from any use of the information contained herein or derived herefrom.

Although the Firm is affiliated with Citibank, N.A. (together with its subsidiaries and branches worldwide, "Citibank"), you should be aware that none of the other financial instruments mentioned in this communication (unless expressly stated otherwise) are (i) insured by the Federal Deposit Insurance Corporation or any other governmental authority, or (ii) deposits or other obligations of, or guaranteed by, Citibank or any other insured depository institution. This communication contains data compilations, writings and information that are proprietary to the Firm and protected under copyright and other intellectual property laws, and may not be redistributed or otherwise transmitted by you to any other person for any purpose.

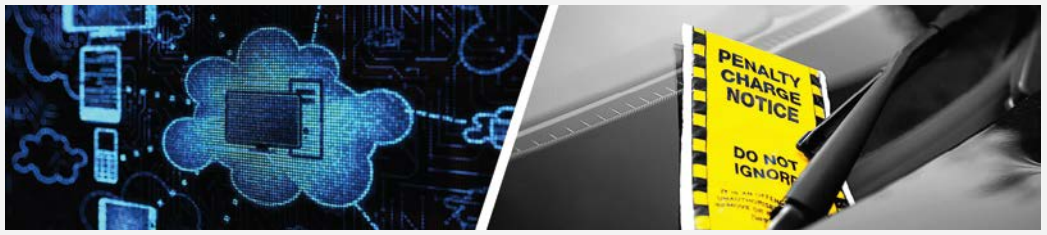
IRS Circular 230 Disclosure: Citi and its employees are not in the business of providing, and do not provide, tax or legal advice to any taxpayer outside of Citi. Any statements in this Communication to tax matters were not intended or written to be used, and cannot be used or relied upon, by any taxpayer for the purpose of avoiding tax penalties. Any such taxpayer should seek advice based on the taxpayer's particular circumstances from an independent tax advisor.

NOW / NEXT

Key Insights regarding the future of ePrivacy

REGULATION

The opportunity from data is clear but in the rush to exploit the data opportunity, not all companies have paid enough attention to, or fully factored in, the necessary safeguards for either cybersecurity or privacy. / The implementation of the GDPR in May 2018 represents a game changer in terms of not only its scope and ambition, but also the significant penalties for non-compliance with fines up to 4% of global annual turnover.



SHIFTING WEALTH

Consumers across the world profess to be concerned about privacy issues but also appear not to significantly moderate their behavior when faced with a data breach. / The aim of the evolving data protection regulation in Europe is to shift power back to the consumers and ultimately increase transparency and trust in how companies use data.

TECHNOLOGY

Although there appears to be a global consensus that privacy and data protection are important issues that need to be addressed by regulation, the asymmetric approach across regions is likely to make compliance a challenge. / These differences could lead to a similar level of asymmetry in terms of access to investment and 21st century consumer services – artificial intelligence, machine learning, and the Internet of Things.