INLINE

Can data sharing survive the new data protection regime?

ASSESSING THE FALLOUT AND TRENDS, MARCH 2019

Over the past year, the extent to which tech companies hold and process user information has become increasingly politically charged. Parliamentarians across Europe are more and more **apprehensive about the practice of data sharing** and are still surmising whether the new data protection regime has gone far enough to protect users against the misuse of their data.

Nine months after the **EU General Data Protection Regulation** (GDPR) came into force, the rules and regulations for processing and sharing personal data are not completely set in stone. Market practices have changed in light of a higher threshold on personal data sharing, but certain practices remain disputed. In parallel, data sharing is taking its tentative first steps into new advancements in technology legitimised by new regulatory structures.

This note explores the recent trends on data sharing influenced by a profound **shift in the data protection policy environment**. It highlights the innovations that free up a greater share of valuable data, and outlines where difficulties for tech companies remain while policymakers and regulators battle to get to grips with a rapidly advancing data sector.

CONSUMER-FACING ADJUSTMENTS, SUCH AS DETAILED COOKIE BANNERS AND UPDATED T&CS, ARE NOW COMMONPLACE

Since the introduction of GDPR and its implementing Act in the UK, **the Data Protection Act 2018**, many companies have adjusted their data handling processes, consent forms, and privacy policies to comply with the requirements. Some of these changes are clearly evident to the public, while some have required internal review of practices.

Most noticeably, many businesses have revamped the text of their 'terms and conditions' or privacy policies with users. These new privacy notices follow legal advice and largely stick to the checklist of information needed to gain the user's full consent. For example, direct marketing industry must now disclose information on which third parties might use the data and for which purpose. However, there has been some migration away from the use of third-party tools (like social media sharing tools) to functions on a first-party basis.

This has caused companies that process data to revisit their supply chain, both data obtained to inform customer engagement and also data used to enrich datasets. A knock-on effect of this is the marked proliferation of elaborate checkbox-based cookie banners. Researchers from Germany and the US assessed over 6,500 websites one month after the implementation of GDPR and found a **16 per cent rise in cookie banners**. While, websites that were unwillingly to risk falling foul of the new rules, restricted cookie trackers on their websites, with a separate survey of news sites in seven EU countries revealing a **22 per cent drop in third-party cookies** per page, between April and July 2018.

So, at least initially, it appears that online platforms have taken steps to remove the inclusion of third-party tools deemed unnecessary for their service. Whether or not Big Tech is thus gaining from this reaction, solidifying its monopoly of personal data and information, remains widely contested.

FURTHER INFORMATION

When the Reuters Institute for the Study of Journalism and University of Oxford researched the effects of GDPR in the paper Changes in Third-Party Content on European News Websites after GDPR, August 2018, it found that "the introduction of GDPR has been followed by significant reductions in the volume of third-party cookies set without consent on many European news sites". This is in parallel to the raise in cookie banners post-GDPR, found by academics in German and the US.

FUTURE EU RULES WILL AFFECT THE LEGAL BASIS FOR PROCESSING DATA, AGAIN

In January 2019, Google was fined €50 million by the French data regulator CNIL for offering users inadequate information, spreading it across multiple pages, and failing to gain valid consent for ads personalisation. It demonstrated the importance of businesses, big or small, correctly identifying and applying the particular lawful basis for processing data. In this case CNIL claimed users were unable to understand that Google is relying on consent as the legal basis for processing, rather than the legitimate interest of the company.

For some organisations the decision between seeking explicit opt-in consent and pursuing a legitimate interest basis for processing data was not obvious. Once you have opted for one basis you cannot change your position once the data has been gathered – procedures must be followed along each step of the process. And for those who rely on legitimate interest, a possible predicament lies in wait in the form of a new ePrivacy Regulation.

The proposals in the ePrivacy Regulation aim to adapt the existing rules concerning the traditional telecoms services to the new forms of electronic communication services. The foundational principle is that communication data should always remain confidential, and any interference with the communication of that data, either directly by a human or through automated processes, without the consent of the user, is prohibited. In a bid to keep regulation in line with rapid adoption of new digital services its remit greatly expands to cover so-called "over the top" (OTT) service providers, machine-to-machine communications and online marketing.

While GDPR outlines six separate legal grounds for processing personal data, the only legal ground referred to in the current draft ePrivacy Regulation is consent. The European Data Protection Board backed this position, stating that it supports "the approach of the proposed Regulation, based on broad prohibitions, narrow exceptions, and the use of consent.

Accordingly, there should be no possibility under the ePrivacy Regulation to process electronic communications content and metadata based on open-ended grounds, such as 'legitimate interests', that go beyond what is necessary for the provision of an electronic communications service".

FURTHER INFORMATION

The French data regulator CNIL's fine of Google was interesting for a number of reasons, not least because it singled out ad personalisation as the key battle ground for future disputes into the lawful basis for processing of data.

The details of the ePrivacy Regulation remain disputed among Members States and EU Institutions, and there are serious questions over whether it will be adopted before a new European Parliament and Commission is in place later this year. In the meantime, the European Data Protection Board has flagged the incompatibilities between GDPR and the new legislation.

GOVERNMENT IS IN SEARCH OF A ROLE TO FACILITATE NEW DATA REPOSITORIES

Against the background of adjustments in the industry, there are also new data sharing opportunities presenting themselves to the private and public sector due to government intervention. In a keynote speech to tech companies at the beginning of the year, the **Secretary of State for Digital, Culture, Media and Sport Jeremy Wright** called for "breaking down barriers" to allow for "the flow of data [that] sits behind all of our online interactions", recognising the "untapped opportunities here".

Accordingly, the UK Government has sought to develop frameworks, known as **'data trusts'**, that allow for the sharing of data in a security and accessible environment. First proposed in an **AI Review** lead by Dame Wendy Hall and Jérôme Pesenti, data trusts operate by allowing multiple individuals or organisations to give some control over data to a new institution – the trust – so that it can be used to deliver benefits, for themselves or other people.

The UK Government is currently testing such an arrangement through a partnership with the **WILDLABS Tech Hub** and conservation charities. The project is investigating the launch of data trust that can help make wildlife data from across the globe more accessible, to help tackle the illegal wildlife trade through sharing image data, and algorithmic decision-making.

Similarly, as technology advances, location information and geospatial data are becoming more valuable in how organisations deliver services too. With the regulatory foundations of a new data protection regime, a Government-backed **Geospatial Commission** will build an information management tool by using geospatial and earth observation data. This

will inform decision-making and build a well of data to assist wider public and private innovations.

These are just two examples. The new norms and standards that will guide the public sector data sharing enable a range of different data initiatives, including in regard to 'Data-Driven Health and Care Technology', ensuring government departments are making non-sensitive data available and data portability of customers' information in regulated markets.

FURTHER INFORMATION

Secretary of State Jeremy Wright's speech at Doteveryone's Responsible Tech conference in January gives a good overview of the Government's plans to increase data sharing among certain sectors. The Government's new Centre for Data Ethics and Innovation (CDEI) plays a key role in facilitating these initiatives. A concept first explored in the AI Review, the Open Data Institute (ODI) explores the meaning of a 'data trust' here and further updates and information on the new Geospatial Commission can be found here.

COMPANIES MUST PAY GREATER ATTENTION TO DATA CATEGORIES AND THE UNIQUE RULES OF EACH

For tech companies to continue sharing data in a secure and complaint manner, extra care must now also be given the category in which the personal data falls under. A widely reported example of this trend towards categorisation of data was seen in the Information Commissioners Office's (ICO) recent Democracy Disrupted report into the use of data analytics in political campaigning.

The UK information watchdog says that its investigation into the nexus between data analytics, social media and political campaigning is now "the largest of its type by any data protection authority", and its initial findings were revealing. Aside from the fines and investigation into certain misdemeanours, the underlining message from the ICO is that data used for political purposes is very different to other forms of data usage. For the ICO, there is greater importance, now more than ever, on whether data has been processed lawfully and the data subjects know their personal details were going to be used for political purposes.

In February 2018, the House of Commons Digital, Culture, Media and Sport Select Committee published its final report into "Disinformation and 'fake news'", backing regulatory intervention in the use of data for political campaigns. The Committee aligns itself with ICO's call for the Government to legislate at the earliest opportunity to introduce a statutory code of practice for the use of personal information in political campaigns. The ICO said it will work closely with Government to determine the scope of the code.

Where the line is drawn between sensitive data and fully anonymised data remains contentious too. A recent Privacy International complaint claims "inferred data is flourishing" in the platform, adtech and data broker ecosystem. The companies argue they anonymise data and obtain individuals' consent for using their information, but Privacy International maintain that by amalgamating large amounts of anonymous or "pseudonymous" information, companies are able to infer sensitive facts such as political affiliation, religious beliefs and ethnicity. Is it fair to call this sensitive data, when it is non-specific guesswork or a rationale conclusion to fully consented non-sensitive data? Privacy International's complaint remains outstanding in three European data regulators, UK, Ireland and France as of February 2019.

FURTHER INFORMATION

The ICO's "Investigation into the use of data analytics in political campaigns" provides insight into the extent to which different data categories are viewed. It forms the rationale for introducing a statutory code of practice for the use of personal data in political campaigns, and could lead the way for more codes in different categories. The House of Commons Digital, Culture, Media and Sport Select Committee report into Disinformation and 'fake news' fully supported this move and added pressure on the Government to work with the ICO.

With the implementation of GDPR, there have been multiple complaints from privacy groups attacking the procedures tech firms have in place. Privacy International has filed complaints against seven data brokers, ad-tech companies and credit referencing agencies with data protection authorities in France, Ireland, and the UK. 'None Of Your Business' has filed "a wave of 10 strategic complaints" against eight online streaming services under the principle of Right to Access in GDPR.

REGULATORS AND THE DATA SECTOR HAVE DIFFERENT VIEWS ON WHAT USERS CAN REASONABLY EXPECT

Arguably the new data protection regime is not yet fully formed - in the eyes of the regulators and policy makers at least. In February 2019, the UK Information Commissioner Elizabeth Denham summarised the progress made since the implementation of the new data protection regime, stating that companies "had got themselves over the line" and done the minimum that needs to be done. According to Denham, the next step in the implementation process is accountability requirements - greater emphasis on privacy by design, data protection impact assessment, the audits that are required to be made available at board-level.

What the Information Commissioner is pushing for is less legalistic adjustments and more organisational, or even cultural,

changes to follow the spirit of the new data regime. One such example is data minimisation. The ICO believes companies must consider data minimisation separately for each individual, or for each group of individuals sharing relevant characteristics. Clearly the regulators are sceptical of the amounts and the means by which data is currently being gathered, particularly by large tech companies.

The Irish Data Protection Commissioner Helen Dixon revealed that she has instigated 16 investigations into large US tech companies headquartered in Ireland. While many of the investigations cover 'self-referred' data breaches, others examine, for example: whether transparency obligations were met when processing information between WhatsApp and other Facebook companies; and whether obligations on the lawful basis for processing personal data for behavioural analysis and targeted advertising were adhered to by both Apple and LinkedIn.

Germany's competition watchdog, the Federal Cartel Office (FCO), has also also provisionally announced it will prohibit Facebook from collecting and linking user data from its own suite of services. The decision is being appealed. The outcome of these investigations will not only have repercussions in individual Member States but across Europe.

Under the legitimate interest basis for processing data there must be a 'reasonable expectation' from the user regarding how the data is used. This is clearly subjective. The criteria considered by the FCO for assessing how data is processed includes taking into account the "data type and the way in which it is processed, and reasonable expectations of users". It points to a misalignment in the how the spirit of this new data protection regime is being understood by European data regulators as opposed to the tech sector – one which is not easily reconciled.

FURTHER INFORMATION

The ICO is still apprehensive about the extent to which data-driven firms have taken on the spirit of the new data protection regime. This is evident in the ICO's statements on adtech, 'tech giants' and Elizabeth Denham's recent speech at an Institute for Government event.

I single out the German FCO provisional pronouncement on Facebook and combining personal data from different sources because it challenges the concept of what users' expectation of how its data is compiled. Equally interesting, Facebook responded in kind arguing that this form of data sharing is required "so that people and businesses in Germany can continue to benefit from all of our services".

We hope you find this note helpful. If you would like more information about the issues affecting you, or to discuss the political and regulatory challenges your business faces, then please get in touch.

CONOR BRENNAN
ACCOUNT MANAGER
conor.brennan@inlinepolicy.com
@conor_fbrennan

OLAF CRAMME
MANAGING PARTNER
olaf.cramme@inlinepolicy.com
@olafcramme

The specialists in politics and regulation for the tech sector

www.inlinepolicy.com

Inline Policy Ltd, 310 Vox Studios, 1 Durham Street, London SE11 5JH
Inline Policy Sprl, Avenue Marnix 17, 1000 Brussels