GDPR Briefing Note

TISA, Dakota House, 25 Falcon Court, Preston Farm, Stockton, TS18 3TX
Tel: 01642 666999
web: www.tisa.uk.com
email: engagement@tisa.uk.com

19th October 2018

GDPR: What's Just Happened?

So soon, already?

It seems like only five minutes but nearly a full five months have passed since the implementation of the EU's General Data Protection Regime on 25 May, underpinned in the UK by the implementation of the new Data Protection Act 2018 which replaced the old Data Protection Act 1998. The spate of *"can we pleeeeease have your consent…?"* emails seem at last to have dried up to a trickle, although the nuisance emails and calls from people you can't recall giving your details to still seem to come. We've also become used to those irritating Consent pop-ups drawing attention to the firm's online Privacy policies. Firms seem to have quietly got on with meeting the various technical challenges raised by the GDPR, such as the processing of Data Subject Access Requests (which existed pre-GDPR in any case) and 'Right to be Forgotten' requests.[1] It is apparent however that some firms seem to have struggled with the concepts of 'consent, freely-given[2]' and 'legitimate interest'[3]. Perhaps rather cynically it seems to me that some firms have seemed willing to deliberately misinterpret these concepts, but my guess is that over time their customers, and (in the context of the regulated world) an Ombudsman and if necessary a regulator, will point out their error. There is undoubtedly, as reported by data protection regulators across Europe, a much greater awareness of the rights of individuals to call data controllers to account, and that awareness is being felt forcefully.

So was that it – a big fuss about nothing?

The calm before the storm? Giovanni Buttarelli, the man in charge of the EU's new European Data Protection Board, has not minced his words in warning us of much more to come, very soon. In a recent interview with Reuters he said; *"I expect first GDPR fines for some cases by the end of the year. Not necessarily fines but also decisions to admonish the controllers, to impose a preliminary ban, a temporary ban or to give them an ultimatum…"*[4]. He tells us he is *"expecting, before the end of the year, concrete results".*

The UK's own regulator - the Information Commissioner's Office – has obviously needed no encouragement from Signore Buttarelli. The ICO's website contains a list of recent enforcement actions[5], a list that just seems to grow and grow; 21 actions alone since the GDPR implementation date. All but one of these actions[6] have been brought under the pre-GDPR regime and relate to breaches of the old Data Protection Act 1998. The old Act limited the ICO's fines to a maximum of

[1] We would be happy to offer support to any firm which is still struggling with challenges in these areas.
[2] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/
[3] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/
[4] https://uk.reuters.com/article/us-eu-gdpr-exclusive/exclusive-eu-privacy-chief-expects-first-round-of-fines-under-new-law-by-year-end-idUKKCN1MJ2AY
[5] https://ico.org.uk/action-weve-taken/enforcement/
[6] Relating to AggregateIQ Ltd. Although as I discuss it isn't in fact shown on the ICO's Enforcement Actions page.

£500,000. Only one firm has so far had that amount levied; Equifax, although the ICO has also warned Facebook that it is also facing a full £500K fine, as I discuss later[7].

So, what have been the main themes behind the ICO's disgruntlement? What are firms getting wrong?

So far as the regulated financial services industry is concerned, Andrew Bailey, the FCA's CEO, answered this question quite pointedly in a speech he gave at the FCA's recent Annual Public Meeting on 11 September: *"My assessment based on events over the last year or so is that data issues have been the fastest-rising risk on our landscape. They take two forms: The first involves the loss of personal data belonging to customers, whether caused by harmful actions such as cyber attacks or due to mismanagement of data and negligence by firms. The second involves how firms use personal data, and whether this is consistent with our rules and principles."*[8]

Let's take Mr Bailey's first issue first:

Cybercrime and negligent data loss:

Well, there is no doubt that the ICO has being seeing plenty of that kind of thing. The list of the ICO's recent enforcement actions is an eye-opening read. To take a few recent examples:

- *Heathrow Airport Ltd, 8 Oct*
  £120K fine. In October 2017 a member of the public noticed a USB flash drive lying in the street in the London suburb of Kilburn. After plugging the drive into a computer at their local public library he discovered it contained information relating to the airport's security arrangements and procedures, including a great deal of personal data. Needless to say none of the data was encrypted or password-protected. The member of the public told the Sunday Mirror newspaper about the find which days later published a story[9] claiming the loss could have compromised airport security, including putting politicians and VIPs and even HMQ at risk. The ICO was deeply unimpressed with the airport's security arrangements, pointing out that only 2% of its employees had received data security awareness training - which did not even include its security trainers.
- *Equifax UK Ltd, 20 Sept*
  Following a joint investigation with the FCA the ICO fined Equifax £500K (the maximum permitted, pre-GDPR) for allowing cybercriminals to access records relating to 15m Britons via security weaknesses that had been recognised by Equifax' management at a senior level for some time.[10] 20,000 of those records included people's names, dates of birth, telephone numbers and driving licence numbers. 637,000 records included names, dates of birth, and telephone numbers. 27,000 records included the customer's email address, and 15,000 of the stolen records included names, addresses, dates of birth, account usernames and plaintext passwords, account recovery secret question and answer, obscured credit card numbers, and spending amounts.

[7] https://www.bbc.co.uk/news/technology-44785151
[8] https://www.fca.org.uk/news/speeches/andrew-bailey-speech-annual-public-meeting-2018
[9] https://www.mirror.co.uk/news/uk-news/terror-threat-heathrow-airport-security-11428132
[10] https://ico.org.uk/media/2259808/equifax-ltd-mpn-20180919.pdf

- *BUPA Insurance Services Ltd, 28 Sept*

  Fined £175K. A Bupa employee extracted the personal information of 547,000 Bupa Global customers and offer it for sale on the dark web. The employee accessed the information via Bupa's customer relationship management system and sent bulk data reports to his personal email account. The compromised information included names, dates of birth, email addresses and nationality. The ICO found that BUPA had inadequate arrangements for determining who had access to the CRM system, and inadequate arrangements for monitoring activity including bulk transfers of data.[11] The ICO pointed out that "*the threat of a rogue employee is widely recognised in industry".*

It isn't just the ICO which has been busy in this regard. The FCA has also been forced to investigate serious data loss incidents, such as:

- *Tesco Bank plc, 1 Oct*

  Fined £16,400,000 for allowing cyber attackers to exploit well-recognised deficiencies in the design of its debit card. Those deficiencies left Tesco Bank's personal current account holders vulnerable to a largely avoidable incident that occurred over 48 hours and which netted the cyber attackers a cool £2.26m. Not too shabby for a couple of days' work. As the FCA describes it the Bank's response to the attack was woeful; the FCA cites *"a series of errors, which included Tesco Bank's Financial Crime Operations Team emailing the fraud strategy inbox instead of telephoning the on-call fraud analyst (as Tesco Bank's procedures required), it took Tesco Bank's Financial Crime Operations Team 21 hours from the outset of the attack to make contact with Tesco Bank's Fraud Strategy Team, a specialist group in the Financial Crime Operations Team. In the meantime, nothing had been done to stop the attack, the fraudulent transactions multiplied, calls from customers mounted and the attack continued."* [12]

So, what about Mr Bailey's second concern?

The way in which some firms are using personal data.

Regrettably Mr Bailey did not go on to elucidate this rather cryptic statement by explaining what his concerns are in this regard. However, I'm going to take a guess by referring to two recent ICO actions, one relating to the pre-GDPR regime, and the second relating to the post-GDPR regime:

- *Emma's Diary, 9 Aug*

  Emma's Diary is a website owned and operated by a firm called Lifecycle Marketing (Mother and Baby) Ltd[13]. In its own words: *"Our mission is to make sure that every mum-to-be and new mum has the information she wants to support her through her amazing experience of pregnancy, birth and early motherhood."* Mums and mums-to-be are invited to register with the website, inputting their name, address, email address, and the names and dates of birth of children under

[11] https://ico.org.uk/media/action-weve-taken/mpns/2259871/bupa-mpn-20180928.pdf
[12] https://www.fca.org.uk/publication/final-notices/tesco-personal-finance-plc-2018.pdf
[13] https://www.emmasdiary.co.uk/

five years of age. If they had been asked, I doubt very much whether any of those mums would have given LMMB Ltd permission to use that personal information thus: As the ICO reports: "*LMMB Ltd sold the information to Experian Marketing Services, a branch of the credit reference agency, specifically for use by the Labour Party. Experian then created a database which the party used to profile the new mums in the run up to the 2017 General Election. The Labour Party was then able to send targeted direct mail to mums living in areas with marginal seats about its intention to protect Sure Start Children's centres."*[14]

Records relating to over one million mothers and young children changed hands in this way. LMMB Ltd was fined £140K.

The campaigning technique described above is often referred to as 'profiling' or 'micro-campaigning' or 'micro-influencing'; using personal information about a person to target that person with emails, phone calls or online pop-up advertisements with a view to influencing their voting or buying behaviour. Understandably the ICO is deeply concerned about firms' and political parties' willingness to use this technique without considering whether the data subjects might expect their data to be used in this way, or whether they might object if they did know. Let's look at the second, post-GDPR, example of this:

- *AggregateIQ Data Services Ltd, 6 July*

  All of the ICO's actions described above related to events that took place before 25 May and which were therefore investigated by the ICO as breaches of the old, pre-GDPR, Data Protection Act 1998. The ICO's action against a Canadian firm called AggregateIQ Data Services Ltd relates to events after that date and has been conducted under the new 2018 Act.

  One would think that the first successful action undertaken by the ICO under the new GDPR would be the subject of some fanfare. But strangely the ICO has not even listed the action on its enforcement page (which is described as including "*the latest…enforcement notices*"). The AggregateIQ notice[15] can be found, with some difficulty, attached as an annex to the ICO's report into its '*Investigation into the use of data analytics in political campaigns*'[16] - a report which explains very fully the ICO's deep concerns regarding so-called micro-campaigning, and which is linked to another report entitled '*Democracy Disrupted*'[17]. Both of these reports are aimed at the relevant Parliamentary Committees which have asked the ICO to keep it informed of developments in this area. The AggregateIQ enforcement notice shows it as "redacted" with a big black cross across its title page, although the only redacted part is the signature of Ms Denham, the Information Commissioner[18].

[14] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/08/emma-s-diary-fined-140-000-for-selling-personal-information-for-political-campaigning/
[15] https://ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf
[16] https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf
[17] https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf
[18] The ICO routinely redacts the signatures of its personnel. It is the ICO, after all.

The actual notice is surprisingly thin; only three and a half pages of content to cover what is obviously an important matter. The notice leaves a great deal to the imagination but in summary we learn that AggregateIQ was obtaining personal data which it then sold to the campaign managers of Vote Leave, BeLeave, Veterans for Britain and the DUP Vote to Leave. This, the ICO reports, involved "*processing personal data in a way that the data subjects were not aware of, for a purpose they would not have expected, and without a lawful basis for processing".*

AggregateIQ has been linked to a firm called Cambridge Analytica (although it is now denying those links). Cambridge Analytica is under criminal investigation by the ICO, the Police and the Electoral Commission for obtaining and misusing personal information obtained from Facebook[19]. The ICO has also warned, in its '*Investigation into the use of data analytics in political campaigns'* report, that Facebook should expect a £500K fine in relation to these events[20].

AggregateIQ has reported its intention to appeal the ICO's action and fine, although Facebook, for its part, seems so far to be contrite: Its Chief Privacy Officer Erin Egan has stated that *"we should have done more to investigate claims about Cambridge Analytica and take action in 2015. We have been working closely with the ICO in their investigation of Cambridge Analytica, just as we have with authorities in the US and other countries. We're reviewing the report and will respond to the ICO soon."*[21] Nevertheless the ICO reports that Facebook is challenging the ICO's jurisdiction.

These are deep, dark waters indeed. There are many legal, moral, political and (for Facebook at least) commercial issues that will no doubt be thoroughly explored in relation to Aggregate IQ, Cambridge Analytica, Facebook and the political clients who bought and used the personal data. I am sure Mr Bailey and his colleagues are keeping a close eye on events.

The EU/US Position

I do not need to explain the importance of US/EU trade and the crucial part data security and privacy plays in that, even putting aside any implications arising from the perplexing Brexit debate. Silicon Valley plays a preponderant role in online commerce and data sharing but trade across the Atlantic is obviously far more than just social networking; it is almost impossible to conduct a commercial transaction of any kind without exchanging personal data.[22]

For its part Facebook has always claimed to be fully GDPR compliant.[23] Signore Buttarelli is obviously unconvinced, pointing out (without mentioning any names) that the global data controllers based in the US tend to rely on assumed, tacit consent to collect and use data, arguing that customers can simply revoke their account if they disagree with this. Signore Buttarelli points out that the GDPR obliges firms to obtain explicit consent that is freely given and which can be freely

[19] See https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far for example - there are lots of other reports.
[20] This fine suggests that Facebook's actions occurred pre-May 2018. The AggregateIQ notice does not properly explain in what way AggregateIQ's actions took place after May, although reference is made to the "processing" of data after that date – and 'processing' can include simply storage.
[21] https://www.bbc.co.uk/news/technology-44785151
[22] Cyptocurrency transactions aside, of course – which is why they are so attractive to the criminal fraternity.
[23] See for example https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr

revoked without requiring termination of the contract between the service provider and the customer. The tendency of some US firms (and there are some notable exceptions, such as Apple Inc) to rely on tacit consent are the subject of high-profile European-led class-action claims for damages, targeting Facebook, Instagram (owned by Facebook) WhatsApp (owned by Facebook) and Google's Android, amongst others.[24]

The US authorities also argue that the EU/US 'Privacy Shield' agreement provides European business and individuals comfort that the US operates a regime that offers GDPR-equivalence. The Privacy Shield was implemented to replace the previous 'Safe Harbour' agreement which the European Court of Justice ruled as inadequate in a ruling in October 2015: "*In the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency ('the NSA')), the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country.*"[25]

I think it is fair to say that that the EU is sceptical of the Privacy Shield's effectiveness and equivalence. The European Justice Commissioner Vera Jourova is currently meeting U.S. Commerce Secretary Wilbur Ross in Brussels to discuss the arrangements. Mr Ross, whose politics are closely aligned with those of Mr Trump and who makes no effort to hide his impatience with the EU, got his retaliation in early, in an FT article on Wednesday 17 Oct in which he stated boldly that he "*can take pride in one overriding fact: Privacy Shield works*". Entertainingly in the same article he also addressed one of the EU's over-arching concerns; that the US has not to date appointed a Privacy Ombudsman to handle complaints. He said that *"In 2016, the state department established a Privacy Shield ombudsperson to address requests by EU individuals about US intelligence access to their personal data. Contrary to some accounts, that position has never been vacant. Even though the ombudsperson has remained ready for more than two years to address EU requests, not a single inquiry has been received."*[26] Perhaps one of the reasons the ombudsperson hasn't received "*a single inquiry*" is that the US didn't get round to revealing who it was until 28 September 2018, when we learned that the job had gone to Ms Manisha Singh, Acting Under Secretary for Economic Growth, Energy and the Environment and Privacy Shield Ombudsman. The synergies between these roles are obvious, of course. The US Dept of State's website explains that Ms Singh *"is responsible for advancing American prosperity, entrepreneurship and innovation worldwide. This includes levelling the playing field and providing opportunities for US companies and their workers to compete and succeed."* So we can be sure that Ms Singh's Privacy Ombudsman duties will be at the forefront of her mind.

Nevertheless the discussions between the EU and the US are going as well as might be expected; so long as one does not read anything between the lines of a joint communique issued today (19 Oct).[27] And we also have the assurance of Mr Gordon Sondland, US Ambassador to the EU, who said

[24] See for example https://noyb.eu/ One can follow the progress of this action on its Facebook page.
[25] https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf This judgment followed a complaint to the Irish regulator relating to Facebook, led by Austrian lawyer Maximillian Schrems. Mr Schrems lodged a complaint with the Irish Data Protection Commissioner arguing that in the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency) the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country. The Irish Commissioner rejected the complaint but was effectively overruled on appeal to the ECJ. Mr Shrems is a key player in the ongoing class action lawsuits facing Facebook and others.
[26] https://www.ft.com/content/0f76f05e-d165-11e8-9a3c-5d5eac8f1ab4
[27] http://europa.eu/rapid/press-release_STATEMENT-18-6157_en.htm

recently: *"There is no non-compliance. We are fully compliant. As we've told the Europeans we really don't want to discuss this any further."*[28] I think we can take a great deal of comfort from that.

Despite these assurances from US politicians it seems that Facebook's management team is feeling at least some pressure from the EU. It was announced very recently that Facebook has hired Nick Clegg, former MEP, former MP and former UK Deputy Prime Minister, into a new role of 'Head of Global Affairs and Communication'. Once can either read into this an increasing determination by Facebook to keep GDPR-type obligations regarding consent at arm's length, or a declaration that Facebook is becoming more willing to see things the European way. We shall no doubt see in due course.

It is important to note that not all US behemoth data controllers reject the EU's point of view. Particularly notable for instance is the position of Tim Cook, CEO of Apple. On a conference platform in Brussels shared on 24 October with Signore Buttarelli, and in praise of the latter, he said this: "*We should celebrate the transformative work of the European institutions tasked with the successful implementation of the GDPR. This year, you've shown the world that good policy and political will can come together to protect the rights of everyone. It is time for the rest of the world, including my home country, to follow your lead. We at Apple are in full support of a comprehensive federal privacy law in the United States."*[29]

How is TISA helping its members?

1. We will continue to keep track of developments. As can be seen from the above GDPR has become a highly-charged issue driven by global political tensions. The landscape is changing almost daily. We will continue to report those developments, as plainly as we can, highlighting anything which we see as of material interest to our members;
2. We have established a CyberCrime Technical Policy Committee comprising of a group of experts in the field. The Committee has as its objective the production of Best Practice Guidelines for the management of CyberCrime risks, with a first draft scheduled for the end of the year. The Guidelines will be kept updated to reflect changes in the criminal environment and new tools and techniques in CyberCrime risk management;
3. We are on hand to advise and support any member who has become victim of a CyberCrime event;
4. We are happy to advise any member who has any other issue relating to GDPR and data privacy generally. Please email me on andy.gordon@tisa.uk.com if you have a matter you would like to discuss.

Andy Gordon

Regulation Executive

07384 79560

[28] https://www.euractiv.com/section/digital/news/us-fully-compliant-with-eu-privacy-shield-ambassador-reveals/ At least Mr Sondland has gone beyond Mr Kissinger's famous complaint about talking to Europe.
[29] https://www.bbc.co.uk/news/technology-45963935