GDPR is still not ready for prime time, here's why

02 JULY 2019

Yancho Yanchev
DATA PROTECTION SPECIALIST | UK

BACKGROUND
It has now been a little more than a year after the General Data Protection Regulation (GDPR) claimed celebrity status and came into effect. Around its effective date on 25 May 2018, GDPR was probably the single most-discussed piece of legislation in the media. The Information Commissioner’s Office (ICO), the UK’s competent authority tasked with enforcing the regulation, proudly reported more than one million visits of its webpage over a single month.

INITIAL REACTION
When the GDPR first came into effect there were varying voices on what it would mean to individuals on one hand and to companies on the other. The Regulation caused a flurry of frenzied activity that built up to a boiling point on 24 May 2018 when our inboxes overflowed with SPAM seeking our approval to receive even more SPAM. Yet that activity almost completely disappeared the day after. Up to that point the GDPR was considered to be sort of ‘end of the world’ scenario, especially for people in sales and marketing. Simultaneously, some individuals thought the new law would instantaneously give them total control over (and perhaps even monetisation of) their own information. None of that really happened though, did it? Despite a substantial rise in data breach reports to the ICO and with one notable exception, the massive multi-million euro fines never materialised. With a few exceptions, class actions for breach of data protection law never picked up the momentum they were expected to generate. Those heavily data-driven players who did not fully comply with the previous data protection regime hardly made any genuine attempt to change their personal data management practices. And that, in essence, delivered the first €50 million GDPR fine imposed by the French authorities. Nevertheless, it remains highly questionable whether the law achieved its intended effect or not.

WHO SHOULD TAKE THE BLAME?
Should we blame the citizens? After all, not everyone cares about privacy and people often receive a free service in exchange for their data being sold to advertisers. Many consumers are unwilling to pay for such a service with money but are at the same time happy to pay with data.

Should we blame the regulators? After all, the ICO endorsed a book on the GDPR they never read which later on turned out to be plagiarised and taken off the shelves. The ICO did raid the offices of Cambridge Analytica (after the arguably biggest data scandal in recent times) with men in blue jackets but not before giving the company a whole week’s notice. More recently, the ICO admitted that even its own website is not compliant with the GDPR.

With this background, how can we blame businesses? It is difficult to blame organisations which are finding it increasingly irrelevant to continue investing in data protection compliance before an adverse event such as personal data breach or another type of infringement occurs. However, a sober look at the legal developments in the preceding 12 months quickly reveals that there has already been a major rise in the importance attributed to data protection matters that cannot be ignored.

WHAT DOES THAT MEAN FOR ME?
First and foremost, we should appreciate the position of the regulators and second, we need to consider the current implications of the law with respect to specific business contexts. According to the French competent authority, the preceding 12 months should be considered a transition year which national data protection authorities used to finalise their rules and regulations implementing the GDPR. Therefore, given that the ‘unofficial’ transition period is over, we can expect data protection authorities to start utilising the stick rather than the carrot. On the other hand, when considering compliance, businesses need to put the various GDPR obligations in the right context as that context may determine some
compliance priorities that are more urgent than others. Let’s take a look at a few different perspectives.

**The employee:** Disgruntled employees not only continue filing their data subject access requests against their (usually) former employers but now threaten them with small claims litigation as soon as they hear their information has been compromised.

Do you have processes in place to ensure that you respond to a subject access request without undue delay and within one month of receipt? This is one of the first things the ICO will be looking for.

**The consumer:** People are more aware of their rights under data protection law and they now exercise their rights more than ever before. Yet the privacy policies which are supposed to inform individuals of their rights remain impenetrable in terms of language and daunting in terms of length. The New York Times reported that people need a degree to be able to understand the average privacy policy, whilst the European Commission reported that 66% of citizens do not read these policies at all, citing length as the most common reason.

Do you yourself understand your organisation’s privacy policy? Make sure you have an answer to that question before the regulator asks it.

**The (business) customer:** In order to comply with their own obligations, companies (i.e. controllers) now need to conduct a risk assessment of their vendors (i.e. processors) before delivery of almost any service takes place. This is now a standard and established procurement process. Moreover, customers often seek to enforce their own data processing terms on their vendors that are, in standard form, usually in the interest of the customer and not the vendor.

Are you in a position to warrant to your customers that your organisation is fully compliant with the law? Do you have a process in place to request such a warranty from your vendors? Do you really know what you signed up for when you agreed to that data processing addendum?

**The supply-chain:** One of the terms in standard data processing agreements would always require the same undertakings provided by the vendor to the (business) customer to be enforceable throughout the vendor’s supply-chain. Any breaches by a vendor supplier are attributable to the vendor and the customer is usually entitled to claim directly from the vendor.

Can you guarantee that all your suppliers comply with the GDPR, to such a degree that you would accept liability if your suppliers are in breach?

**The investor:** There is hardly an acquisition or investment round happening at the moment without the target company being asked to provide warranties in respect of its compliance with the GDPR. So even start-ups that have been busy with developing a product as opposed to dealing with compliance may be required to retrospectively implement the GDPR.

You didn’t consider that the GDPR will haunt you even after you decide to exit your own business, did you?

**The regulator:** Over the last year, the ICO has, among other things, recruited over 200 new employees, issued and updated guidance, launched public consultations, and invited businesses to proactively engage with it. The authority is actually keen to assist business with their obligations under the law. Simultaneously, however, the ICO continues to issue fines against infringers on an almost weekly basis.

Have you kept up to date with guidance? Have you taken part in the consultations that directly influence your business? For example, the ICO’s codes of conduct, which complement the GDPR, will soon be open for consultation. Do not miss your chance to join these consultations, especially if your organisation is dealing with data sharing, direct marketing, journalism or children’s information.

**The privacy activist:** It is not only the regulators that are trying to force companies into compliance. It is also the citizens. At present, there are several live proceedings/complaints against the biggest tech companies in the world. Such and such and such complaints have already been changing the law and will continue to do so. It is not over! These complaints are likely to drive a substantial change in online business models. They are against dominant players in AdTech, social media, search, etc. who often serve as intermediaries and when they are affected everyone is.

For example, a court hearing in July 2019 may potentially lead to the invalidation of the standard contractual clauses and the privacy shield, that are the mechanisms relied upon by the vast majority of businesses exporting personal information outside the EEA. Does your business rely on these mechanisms?

**The online advertising underpinning the ‘free’ web:** Personal data flows are becoming increasingly complex. This on its own makes complying with data protection law even harder whilst industries such as AdTech are high on the regulator’s radar. The ICO announced, on 20 June 2019, that it has general, systemic concerns around the level of compliance of real-time bidding in AdTech. In essence, the ICO declared that a big part of the advertising industry today operates unlawfully.

The ICO invited businesses in the AdTech space to reevaluate their approach to privacy notices, use of personal data, and the lawful bases they apply within the real-time bidding ecosystem. If you are in AdTech, would you not act upon this invitation?

Is it time to double check that your thinking is correct?

We regularly deal with cross-border data protection issues and we have reviewed privacy compliance for leading internet brands and conducted data privacy audits for international manufacturers. Whatever the scale or industry of your business, Withers tech can advise you on how to store, process and manage data to ensure compliance with the ever-expanding body of regulations, guidance and cases.
Authors

Yancho Yanchev
DATA PROTECTION SPECIALIST | LONDON

Intellectual Property and Technology

📞 +44 20 7597 6673
✉️ yancho.yanchev@withersworldwide.com