Information Age

27 May 2019

Michael Baxter

GDPR anniversary: has the regulation backfired? What next?

GDPR anniversary: privacy is a human right, but does this mean that regimes, where spying on citizens is considered acceptable, have the advantage in the AI race?

Another year older, sung John Lennon, but then for GDPR that makes it just one-year old. As GDPR passes its anniversary, we ask, has it been a success? Has it been another Y2K? What about those pesky pop-ups? Has GDPR backfired, as some seem to think? And what's next? We have been speaking to experts on GDPR, privacy, the question of who owns data and the value of data? Or put it another way; imagine there's no GDPR, you are not the only one? Imagine there's no privacy, imagine all the people, living life being spied upon.

"How do we measure the success of ground-breaking legislation that demands real transformation and cultural change? asks Abigail Dubiniecki, a speaker and educator, and privacy specialist at My Inhouse Lawyer

"Many organisations" says Ardi Kolah Executive Fellow, Henley Business School and Privacy Consultant, and Data Protection Officer (Europe) at Hitachi Consulting, "are still at the 'work in progress' stage and many are still playing 'catch up.'"

Truth is, those who compared GDPR with the Y2K or millennium bug, missed the point. Y2K was only ever going to be a one-off problem associated with computers not being programmed to be able to deal with the date shift from 1999 to 2000, as computers tended to only look at the second two digits in the date, so the switch from 99 to 00 was meant to cause computers to crash around the world, as each time zone entered the new millennium.

The General Data Protection Regulation was never going to be like that; it was an attempt by regulators to get ahead of what is set to be one of the most crucial battles of this century, our innate human right to privacy, without curtailing the extraordinary benefits that should arise from the fourth industrial revolution, a revolution that has data at its heart.

Dubiniecki says that GDPR has "re-shaped the conversation, prompting individuals who were uncomfortable with how their information was being handled to demand better."

It has re-shaped the conversation in more ways than one. The Cambridge Analytica saga helped: thanks to this, the conversation was promoted from the business pages of newspapers to the front pages. All of a sudden, privacy and protecting democracy became inextricably linked — and for many, the perception of GDPR was moved from a mental box entitled 'irritating regulation' to something that sits on the front line in a battle of enormous importance.

The GDPR has produced other benefits. For one thing, it has set a bar for the rest of the world to reach.

"The biggest impact of GDPR has been not in European capitals, but in Washington, Palo Alto, Sydney and beyond," says Kevin Bocek, VP security strategy and threat intelligence, Venafi. He added: "Privacy is now a popular topic with both politicians and technology CEOs, this is a credit to the rise of GDPR."

Dubiniecki echoes those sentiments: "On a macro level, GDPR has had a seismic impact with knock-on effects outside the EU, not just because of its extra-territorial reach but because it's emboldened other countries to adopt similar legislation and measures."

Maybe there has been another benefit. A key component of GDPR is privacy by design and default, a concept introduced to the world by Ann Cavoukian, who had been Information and Privacy Commissioner for Ontario for 17-years. Privacy by design and default means that privacy is built into a product at the inception, not later on when a product is at an advanced stage and compliance finally 'gets their sticky paws in'. But the concept of privacy by design has got wings; now you hear experts in other fields talking about ethics by design, or security by design. Maybe a new concept is slowly emerging, one that corporate boards are embracing, partly because of a sense of urgency created by GDPR, partly because GDPR has helped enlighten them, and that concept is building 'trust by design'.

Increasingly, companies are understanding that building trust with customers is vital to long-term success, something that in time, even the markets may factor in when valuing a company: how much have they integrated trust by design?

Fines up to GDPR's first anniversary

Yet the fines imposed on companies since GDPR was introduced have been modest. This is where some draw an analogy with Y2K. Just as the millennium bug failed to bring down computers, GDPR fines didn't impose a massive hit on corporate profits.

As Peter Hughes, Technical Director, Skybox Security pointed out: "While there have been some fines dished out by the Information Commissioner's Office (ICO) to companies such as Uber, none have topped the £500,000 penalty that was the previous limit under the Data Protection Act 1998."

Related: GDPR one year on: what fines have been issued so far?

Colin Truran, Principal Technology Strategist, Quest said that "the total fines to date are around €56 million – which you would initially think is a lot, but actually, almost all of it comes from French data watchdog CNIL's €50m fine for Google."

Does this mean that the well publicised potential fines GDPR introduced are more threat than reality, are regulators barking without biting?

Hughes said that "while some may claim this to be a great victory, the absence of a huge fine may just increase cyber security complacency among UK firms."

Truran said that "it is still early days where most of the breaches occurred before the GDPR was ratified into law. Therefore, this year will be the decider to determine if GDPR is an effective solution as it was intended or just another piece of bureaucracy that fails to have the desired effect."

Others see another issue. GDPR is complex, complying with it was never going to be easy. Indeed, when you speak to experts on GDPR they often say that no organisation will ever be 100% compliant and nor would the regulator expect them to be.

Instead, it is suggested that companies need to build a defensible position. If a breach occurs, the regulator will not smite them in fury, it's wrath seemingly without limits, if an organisation imposed reasonable safeguards. It's about managing risk. As so many experts say, 'it's a matter of time before a breach occurs, not if.' But if a breach occurred because of poor practice, because an organisation paid scant regard for its responsibility as a custodian of its customer's data, then the regulator may indeed impose the maximum level of fines. What it does not expect, is for GDPR compliance to take-over. "They are not expected to reinvest all their profits into compliance," said Kolah at the recent Data Leaders Summit.

On this theme, Kon Leong, CEO of ZL Technologies says that "the lack of significant fines under GDPR can be attributed to the fact regulators have come face to face with the complexity of implementing data privacy in large enterprises, and the reality that we are still years away from being there."

He argued that companies have insufficient technology to meet GDPR, while "regulators do not yet understand the digital ecosystem enough to properly address fines."

Or to put it another way, and sticking with the comment from Leong: “Regulators have barely begun to scratch the surface of the problem.”

Beyond the GDPR anniversary: just the beginning

And that is one of the key points. It’s early days. GDPR is a year old, it’s still at the kindergarten stage.

As Dubiniecki told Information Age “with something that’s as fundamental a shift as GDPR, which requires real cultural change and takes time, perhaps it’s unrealistic to expect dramatic change within one year. At the same time, maybe it’s fair to be impatient, to demand more ‘sweeps’ like the German cookie sweep and proactive public Data Protection Impact Assessments, as we saw with Microsoft.”

Ann Bevitt, partner at legal firm Cooley says that the “impact of the GDPR varies hugely across different organisations.”

She continues: “In some companies, there has been a wholesale change in their culture around privacy and data protection, with businesses wholeheartedly embracing GDPR compliance, almost like a USP (especially in sectors/industries where compliance has, historically, been fairly patchy). In other companies it’s definitely been more of a box-ticking exercise, with little to no embedded change in practice.”

“On a company level,” says Dubiniecki “GDPR calls for cultural change that goes into the deep tissue of an organisation. Some companies get that and were already poised to meet the challenge because trust, respect and customer-centricity are in their DNA. GDPR just formalises that when it comes to data protection. It still means a lot of work.”

But not all are getting it.

“Other companies,” continues Dubiniecki “see this as just a compliance exercise to do the bare minimum, tick some boxes with privacy notices and consent requests and call it a day. And they’re likely getting it wrong.”

The critics

GDPR has its critics, and on more than one level.

Jason Hart, Cyber security Evangelist, Thales: argues that “GDPR hasn’t improved data protection to the extent many in the industry had hoped.”

His evidence for this criticism: “With the number of breaches being reported dramatically increasing,” he explained “it’s clear the threat of fines and a potential hit to their

reputation is only having a small impact on how seriously businesses take their cyber security.

“Worse, just a tiny percentage of the attacks can be considered ‘secure breaches’, where the stolen data is encrypted, rendering it useless to cybercriminals. Unless businesses are made to adhere to GDPR recommendations such as encrypting data directly, it will continue to have minimal impact in the UK.”

The pesky pop-ups

Sometimes, though, in these post GDPR times, it feels like we can’t breath for pop-ups. As we try to battle fake news, for example, users might want to quickly double check a fact. Pop-ups, tick boxes, privacy this, privacy that, request for consent for this, that and the other, are the enemy of doing anything quickly. The odd pop-up is annoying, and hey, we publishers have to make money you know, but it feels like overkill.

Some argue that companies have been given bad advice — throwing requests at us for consent when in fact consent is us just one of six legal bases under GDPR by which an organisation can process data. They don’t need your consent to process your data when they are required to do so by law, for example, dashing the excitement of smart Alec’s who think that a superficial contradiction between different regulations betrays a fatal flaw in GDPR.

Then there is legitimate interests. You don’t need consent when there are legitimate interests in processing data. Whether an interest is legitimate or not is ambiguous, which is one of the reasons why GDPR requires a degree of risk management.

Kon Leong feels that this issue becomes even more vexing when applied at international level. “Since the release of GDPR, the US has followed suit with an array of new privacy regulations in states such as California, Delaware, New York, and Washington. While they all have similarities, it’s their differences that make them difficult to navigate. The United States will soon resemble a checkerboard of digital privacy regulations as each state creates their own. The technology to manage a single privacy regulation is hardly there, let alone an array of them. A federal privacy law may be forthcoming, but that will come with its own consequences.”

Maybe companies can solve their customer a good deal of hassle by applying legitimate interest. On this theme, Information Age spoke to Guy Cohen from ‘privacy engineering company,’ Privitar.

“Under GDPR,” he explained “there is legitimate interest, we see a lot of consent fatigue: the fundamental theory is that everyone should have control, and that means consent, but

this assumes the person who gives consent had the ability to understand the risks and benefits to them. That is rarely true.

“I work in this field and I still don’t understand the risks and benefits. Legitimate interests says that it is on the organisation to carry out the balancing test, to weigh up their legitimate interests against the risk to any individual, and if they think it is reasonable, can process the data without consent, but it is on them. They are accountable, but you can still object, so you have control.”

Does this mean some companies are over cautious, we asked Cohen. “They are terrified,” he said, so they throw consent pop-ups at us when legitimate interest makes it unnecessary.”

Maybe this point may provide a clue as to why fines have been so low to date. Regulators don’t want to paralyse organisations with compliance requirements. For an organisation applying legitimate interest there is a balance of risk, a fear of being fined into near insolvency, maybe some organisations apply the balance act too cautiously, and by only imposing relatively modest fines, perhaps the regulator, the ICO, is trying to be a little more encouraging to organisations, applying the more subjective legitimate interests test.

Another reason why GDPR may be backfiring

A year on, as GDPR celebrates its first anniversary, Sarah Whipp, CMO and Head of Go to Market Strategy, Callsign, reckons she has spotted a fatal flaw. “GDPR and other ‘privacy by design’ laws, built to empower individuals to have greater control over their data and protect their identities, have actually opened loopholes that cybercriminals can easily take advantage of to gain access to valuable (and personal) data without people ever knowing about it.”

“If we breakdown what GDPR really means, the term ‘data protection’ may be a bit of a misnomer. The reason being that the legislation doesn’t ‘protect’ data, it just creates a more transparent system. Perhaps a more appropriate acronym would be ‘GDTR — general data transparency regulation. Under the guidelines, organisations are encouraged to hand over data quickly without charging the data subject. But the real issue is proving the person requesting the info is really who they say they are.

“From our experience this could manifest itself as follows: The organisation holding your data being targeted — like a healthcare company or a financial institution — gets a request from an individual, they assume is you, for their data. But before they turn over the data, they must verify the individual is actually you. Unfortunately, cybercriminals have caught onto this and proved its quite easy to mimic a person by easily answering common security questions (in our oversharing age, much of this data is out there on social networks). They have even been successful using more advanced techniques that

easily crack 2FA (two factor identification) that can be bypassed or be duped using SIM-swap or call-divert fraud. By exploiting this loophole and some digital trickery, the fraudster convinces the organisation that they are actually you and the organisation releases the data. From their perspective, they have acted as described and recommended in the law and are none-the-wiser, yet they just handed over a customer's financial data or health history or other information that can be easily sold on the black market.

"The loophole remains because while the regulation does advise to check identity, it doesn't mandate how, leading for interpretation and therefore vulnerability."

The solution, she suggests, lies with applying "behavioural biometrics and AI to detect anomalies to ensure people are who they say they are, so that organisations don't inadvertently reveal information that could land them in hot water." These are topics Information Age often considers in some depth.

We will leave you with just one question. As GDPR becomes a toddler will citizens become custodians of their own data? Read on for an answer to that: Post GDPR and the ownership of data. Will citizens become custodians of their own data and will companies have to ask them for permission to use it?