An independent publication from canongate.org | Distributed with The Times Scotland | 17 May 2018 | THE TIMES SCOTLAND

GDPR

INSIDE

2 Brodies
3 Wright, Johnston & MacKenzie
4 Anderson Strathern

As society moves increasingly online, data protection law needs to have comprehensive reach, says the UK's regulator

ICO outlines new tech strategy

Providing a focus on cyber security, artificial intelligence, and device tracking

BY ELIZABETH DENHAM

Under the General Data Protection Regulation (GDPR), I will have the power to audit all those who hold, use and share personal data. In other words, soon I will be able to 'look behind the curtain' and see what those who hold our data and personal information are doing with it.

However, in the context of our investigation into the Cambridge Analytica-Facebook allegations, the GDPR's audit power is already being outpaced by technological advances in data analytics. I want to see this addressed. I am in consultation with government, to ensure that, as part of the Data Protection Bill, the ICO has the ability to move more quickly to obtain the information we need to carry out our investigations in the public interest.

We need to respect the rights of companies but, we also need streamlined warrant processes with a lower threshold than we currently have in law. We need the regime to reflect the reality that data crimes are real crimes. As society moves increasingly online, data protection law needs to have the comprehensive reach people would expect of laws in the physical world.

25 May will merely mark the end of the beginning of a very long journey for the data protection community. As the regulator of the GDPR in the UK, we support, educate, consult, audit and enforce. I am strengthening my team in both number and expertise, and we'll be ready to deliver our new responsibilities and obligations to organisations and, most importantly the public.

WE ARE recruiting all levels of staff, including ten newly created director roles, across the UK to give us the capacity, capability and resilience to tackle our developing regulatory brief. We have a current headcount of 520; we expect numbers to increase to 700 by 2020. We have around 200 case officers working on issues raised by the public, a 60-strong enforcement department taking forward our investigations and a similar number charged with developing our information rights policies and guidance.

There's nothing like taking advantage of a comprehensive change to the law to develop, to grow and to re-invent ourselves. Over the past eighteen months the ICO has undergone a phenomenal internal change programme. We know we need to be a tech savvy, relevant regulator which is why I have recently published the ICO's first technology strategy.

> "Across the world people are beginning to wake up to the importance of personal data"
>
> Elizabeth Denham

WE HAVE identified three areas of focus: cyber security, artificial intelligence, and device tracking. These three areas will inform our guidance, our proactive work, our investigations, audits and advisory services.

Taking proactivity further, we recognise that innovation is essential. We are working to establish a 'regulatory sandbox', to beta test new initiatives, supporting innovative digital products and services, whilst ensuring the right safeguards are in place. We intend to focus on AI applications and will launch the programme in 2019, after this year's consultation.

This technology strategy is based on the strong belief that privacy and innovation go hand-in-hand. It also allows us to develop our own skills; recruiting and retaining technology expertise and establishing partnerships on tech issues with outside experts, other regulators and international networks.

I have no intention of changing our proportionate and pragmatic approach after 25 May. My aim is to prevent harm, and to place support and compliance at the heart of our regulatory action. Voluntary compliance is the preferred route. But we will back this up by tough action where necessary; hefty fines can and will be levied on those organisations that persistently, deliberately or negligently flout the law.

It's all about people and increasing the public's trust and confidence in the way their data is handled. I think the recent revelations in the media have fired up the data protection debate. Across the world people are beginning to wake up to the importance of personal data, and it is up to us – as regulator and those striving to comply with the law – to keep that fire burning.

Elizabeth Denham is the UK's Information Commissioner.

Embrace GDPR to succeed

Failure to do so could mean consumers are less willing to engage with products and services

BY WILLIAM PEAKIN

As challenging GDPR may be for those working on compliance, the regulations should force a much-deeper appraisal of what values companies apply to their interactions with customers.

It should serve as a mechanism for brands to deepen relationships with their customers around consent. For those willing to think beyond pure compliance, GDPR presents a chance to build consumer trust at a time when trust is scarce.

"GDPR is all about trust and transparency," said Martin Sloan, a Partner at Brodies. "That means organisations must clearly articulate what they do with personal data and why, where that data is collected from, with whom it is shared, and for how long it is retained. Organisations also need to explain to individuals what their rights are."

"The Information Commissioner, Elizabeth Denham, has said that her office's immediate concern is 'invisible processing'. If an organisation fails to explain what it does with an individual's personal data, then that processing may be unlawful.

"If processing is being carried out on the basis of consent, then the individual needs to have a genuine choice and clearly understand to what he or she is being asked to consent."

The scramble by companies to comply has largely been about avoiding the risk of being fined. Rather, it should raise questions about corporate values. Customer data is both a source of competitive advantage to the company and the subject of rapidly-increasing suspicion to consumers.

IT IS FUNDAMENTAL to digital business models and the most precious thing a customer can share. In some ways it is more valuable than money. As consumer concern about privacy grows, how companies treat data will define the brand experience.

"Organisations should use GDPR as an opportunity to stop and think about how they use personal data," added Sloan.

"At a time when individuals are becoming more aware of their rights and questioning what organisations are doing with their data, there is an opportunity for organisations to embrace GDPR and the principle of transparency to help build trust.

"That in turn should help organisations that embrace GDPR to succeed, whereas those that do not may find individuals less willing to engage with their products and services."

As consumer concern about privacy grows, how companies treat data will define the brand experience

> **"There is an opportunity to embrace the principle of transparency"**
>
> Martin Sloan, Brodies

GDPR will re-set expectations for consumers, both in Europe and beyond. It will explicitly tip the balance of power their way, giving them real control over what data they share and how it is used.

Those companies that welcome the change, that treat their customers as partners in how they use their data, that truly put their customers first, will build new levels of loyalty and unlock even more opportunities to put data to work.

EXPOSING SOME MYTHS AROUND GDPR

- GDPR is a revolution in data protection: The principles that underpin GDPR are largely the same as those that apply under current data protection law.
- High fines will be commonplace: Fines are just one part of the ICO's toolkit for enforcing GDPR – alongside issuing warnings, reprimands and corrective orders.
- A product/service can provide GDPR compliance: While technology undoubtedly has its part to play in compliance, it is not a solution.
- Every personal data breach needs to be reported: Not if it is unlikely to result in risk to the rights and freedoms of individuals – but the organisation must retain a record of it.
- There is an exemption for small businesses: That exemption is qualified. In particular, it will not apply where the organisation processes special categories of personal data, such as medical information or trade union membership. As most organisations will hold special category personal data relating to their staff, the exemption is likely to be very limited.

The web's economics upturned

Email marketing and ad-tech face disruption

BY WILLIAM PEAKIN

Data is the "raw material of the 21st century", according to Germany's Chancellor Angela Merkel. Speaking at the World Economic Forum in Davos in January, she said that the answer to the question of who owns this data will ultimately decide whether "democracy, participation, sovereignty in the digital age, and economic success can go together".

Merkle added: "I believe that our European social market economy gives us a chance to foster a fair digital age in which the privatisation of all personal data is not simply accepted as the normal state of affairs, but it is accepted that, in order to make the best of this era for the public, data is the raw material of the 21st century".

The issue of data ownership is key to GDPR; after nearly two decades in which companies have been financially incentivised to trawl the web for user data, now consumers have the right to opt-in rather than carry the burden of opting-out. It presents a real chance to renegotiate the terms of engagement between people, their data, and companies. For the latter, particularly in the marketing and ad-tech sectors, the implications are significant.

"In terms of the marketing sector, any business which relies heavily on e-mail newsletters to generate business is likely to be most affected by GDPR consent," said Stephen Grant, solicitor and GDPR expert at Wright, Johnston & Mackenzie LLP. "The business which stands out to me is the Groupon-type which emails consumers on a daily basis, if not multiple times a day.

"Over the past few weeks, consumers have been asked to re-opt-in; my assumption is that many will see this as a way of stopping the daily onslaught of semi-spam. This will hit the effectiveness of e-mail newsletters drastically; many of these businesses rely on sheer quantity of subscribers to generate any return.

The issue of data ownership is key to GDPR

> "The email newsletter will become a thing of the past as companies think of new ways to advertise their products and services"
>
> Stephen Grant, Wright, Johnston & MacKenzie LLP

"I think the email newsletter will become a thing of the past as companies think of new ways to advertise their products and services."

Grant anticipates that legislation will not stand still either: "The last enactment of data protection legislation in the UK was the Data Protection Act 1998 – 20 years ago. I envisage it will be a moving feast, with various updated guidance notes from the ICO and the Article 29 Working Party over the next couple of years as businesses try to squeeze their business models into the GDPR mould.

The businesses which adapt may survive - those who don't will be forever waiting and worrying about the knock on their door from the ICO.

"The companies that will fair best and profit most out of the GDPR are those who see it and use it as a customer advantage rather than a hindrance. These companies will use it to connect and engage with customers to build trust."

Why GDPR is not Y2K

Organisations and businesses should avoid post-25 May complacency

BY WILLIAM PEAKIN

Information Commissioner Elizabeth Denham has made it clear that while enforcement is part of her remit, she prefers that "education, engagement and empowerment" comes first, adding: "Prevention is better than cure".

It is a key point in how organisations and businesses should regard GDPR compliance, said Douglas McLachlan, a Partner at Anderson Strathern. "There is this focus on 25 May, but the reality is that many will overshoot this date. The public sector is probably the best prepared, along with regulated and larger businesses. But a significant proportion of businesses are not ready, or at least not completely ready. The Information Commissioner recognises this; that compliance is a process, not an event.

"Working with clients on compliance, we have been getting them to look at their procedures and processes and using this as an opportunity to understand what data they hold, what they are doing with it (and what's the legal basis for that), asking themselves are they collecting too much or keeping it too long? Making sure they have the right protocols, that they have strong defences, that staff are knowledgeable and trained, and that there is good governance."

However, McLachlan believes that the problem for organisations and businesses may come from complacency: "The reality is that the Information Commissioner is not going to be inspecting everyone from 25 May; her office simply does not have the resources. But the risk is that if there is not a sudden rush of news, people become complacent; looking at 25 May as a bit like Y2K, the millennium computer bug which did not cause the problems anticipated. As though it was a big fuss about nothing.

"And the danger is that 12 or 18 months down the line, an organisation or business may become the victim of computer hacking, or maybe an employee will just lose a paper file full of people's personal data – both of which could be a reportable personal data breach under GDPR. At this stage, the Information Commissioner may investigate the organisation further and the problems for them will stem from how little they have done to mitigate against a personal data breach occurring, or how little they have done in terms of GDPR compliance overall. If they have not considered and addressed their compliance risks and do not have good policies and procedures, and strong defences, in place then they risk a high-level fine."

'There is this focus on 25 May, but the reality is that many will overshoot this date' - Douglas McLachlan.

So, McLachlan has been advising clients to conduct their own audit of what data they hold and process, for what purpose, on what legal basis, and how the data are handled. That includes looking at how well protected is the data. As well as good IT security, organisations and companies need also to look at their physical structures; the external and internal security of their building, how visitors are managed, and document handling issues such as shredding.

"The human element of data security can't be overlooked either," said McLachlan," "by having the right vetting procedures, good training, creating a culture of confidentiality and compliance where employees should not fear reporting a data incident. And these IT and human elements combine in terms of things like password strength and vulnerability to social engineering.

"The Information Commissioner recognises that data incidents occur, but you are for more protected against the consequences if you follow best practice, invest in your IT and physical security, and invest in and train your staff."

ACCOUNTABILITY AND SECURITY

- Accountability is one of the data protection principles - it makes you responsible for complying with the GDPR and says that you must be able to demonstrate your compliance.
- You need to put in place appropriate technical and organisational security measures to meet the requirements of accountability and the principle of "integrity and confidentiality" (security).
- There are a number of measures that you can, and in some cases must, take including: adopting and implementing data protection policies; taking a 'data protection by design and default' approach; putting written contracts in place with organisations that process personal data on your behalf; maintaining documentation of your processing activities; implementing appropriate security measures; recording and, where necessary, reporting personal data breaches; carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests; appointing a data protection officer; and (in the future) adhering to relevant codes of conduct and signing up to certification schemes.
- Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.
- If you implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation.
- Being accountable can help you to build trust with individuals. It may also help you mitigate against any risks of enforcement action.