Protection by design

Data protection is not a new concept, but the EU's decision to adopt legislation that applies equally across all 31 countries of the EU and EEA brings with it a whole new set of challenges. We explain the most important actions you need to take right now to begin your route to compliance.

An evolution in data protection, not a burdensome revolution, is how the UK Information Commissioner's Office (ICO) has described the EU General Data Protection Regulation (GDPR), which will come into effect from 25 May 2018. The new legislation aims to reinforce and enhance the rights of individual data subjects, increase the accountability of organisations that control and process personal data, and simplify the regulatory environment.

"Any regulation has some sort of impact on an organisation's resources," said ICO Deputy Commissioner for Policy, Steve Wood, in a recent blog. "But thinking about burden indicates the wrong mindset to preparing for GDPR compliance." This message is part of the ICO's wider efforts to debunk the myths around the regulation, the principles of which the government has confirmed will become enshrined in UK law, regardless of Brexit.

Wood further noted that organisations complying with the terms of the 1998 UK Data Protection Act (DPA), and with an effective data governance programme, are "already well on the way" to being ready for GDPR. "Many of the fundamentals remain the same," he said, "and have been known about for a long time. Fairness, transparency, accuracy, security, minimisation and respect for the rights of the individual whose data you want to process – these are all things you should already be doing with data and GDPR seeks only to build on those principles."

New provisions

Despite the ICO's reassuring words, however, there is no room for business complacency. Wood also stressed that the GDPR brings in important new provisions, and urged organisations to "start making preparations now, if they haven't done so already". Some of the key developments include:

- increased territorial scope (the GDPR extends to organisations processing data related to the offering of goods or services to data subjects in the EU or monitoring their behaviour, regardless of the organisation's location);
- strengthened consent standards – consent must be a freely given, specific, informed and unambiguous.
- There must be some form of clear affirmative action (a positive opt-in) – consent cannot be inferred from silence, pre-ticked boxes or inactivity;
- higher penalties for compliance failures;
- mandatory data breach notification to the local regulating authority within 72 hours of discovery if it is likely to "result in a risk for the rights and freedoms of individuals";
- data subjects' increased right to access (including for individuals to have their data provided to them in a structured, commonly used format); a right to data erasure (sometimes known as the "right to be forgotten") in certain circumstances, and a right to transfer personal data from one data controller to another;
- privacy by design as a legal requirement – designing data protection into the development of products, services and systems; and
- data protection officers – certain types of organisation must appoint a data protection officer, including all public bodies plus other organisations that – as a core activity – monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale.

"If you are not currently complying, it will be a very long journey in the next six months; you can't build an extension if the house is falling down."

The GDPR's data protection principles set out the main responsibilities for organisations (see box below). These mirror those in the current DPA, with added detail and an important new accountability requirement to show how the organisation is complying, for example by documenting decisions taken about a processing activity.

Headline penalties

Although there is a high level of public and press interest in the changes, the UK government's 2017 Cyber Governance Health Check Report, published in August, showed that awareness of GDPR is "variable" among FTSE 350 companies. While almost all respondents reported some level of awareness, this ranged from 37% claiming to be very aware to 15% saying they were slightly aware. Almost three-quarters (71%) said they were somewhat prepared to meet the new requirements, but just 6% reported being completely prepared.

BASIC PRINCIPLES

Under Article 5 of the GDPR, personal data must be:

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle")
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle")
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimisation principle")
- accurate and where necessary kept up to date (the "accuracy principle")
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle")
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle")
- Article 5(2) states that the controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle").

Source: Information Commissioner's Office

Security expert Mike Gillespie, a member of IIRSM Technical Advisory Network (TAN), is concerned that "too many organisations have been paying lip service to data protection generally for so long that they have almost talked themselves into believing everything is OK, when actually a large number are not complying. If you are not currently complying, it will be a very long journey in the next six months; you can't build an extension if the house is falling down."

Organisations breaching GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater). "The focus on 4% for serious breaches is obviously grabbing headlines," says David Emm, Principal Security Researcher at Kaspersky Lab and a fellow member of IIRSM's TAN. "It is much larger than that available at the moment." But he points out that this is the maximum fine for the most serious infringements and there is a tiered approach to penalties. "[The authorities] are not gunning for every slip up," he says. "But they will want to see that people have taken appropriate measures." For her part, the Information Commissioner, Elizabeth Denham, has made it clear that the legislation is not about fines, but about "putting the consumer and citizen first". She has described it as "scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm".

Business opportunity

Gillespie also deplores the misinformation and scaremongering surrounding the GDPR. "What we need is good quality compliance, not fear," he argues. "What people should be saying is that there are really good reasons for this. It's about protecting information and treating it with respect. Personal information is a subset of a business's wider information asset; you need to respect people, use it properly, and be transparent about what you are doing with it."

Andy Taylor
APMG

At its most fundamental, GDPR requires businesses to look at what data they have got and how they handle it. "This mirrors what businesses should be doing on general cyber security," stresses Emm, "looking at what data is held, where it is held, and what are we doing to secure it."

"The point is not to see [GDPR] in terms of a penalty or problem," advises TAN member Andy Taylor, lead cyber assessor at APMG, "but to see it as a way to revamp existing processes. If you follow guidance and good practice, you will ultimately have more streamlined management of data; rather than bolt it on, design it in. The idea is to look at what you do with information and design processes with GDPR in mind. Even small businesses with half a dozen employees need to think about all the aspects of how they use their employee database, for example."

David Emm
Kaspersky Lab

"This is a fundamentally a core management issue," adds Gillespie. "It's about good governance, not something farmed off to IT as another project. But we also need technology itself to step up and play its part; every piece of technology connected to the internet of things should be manufactured and designed to be secure."

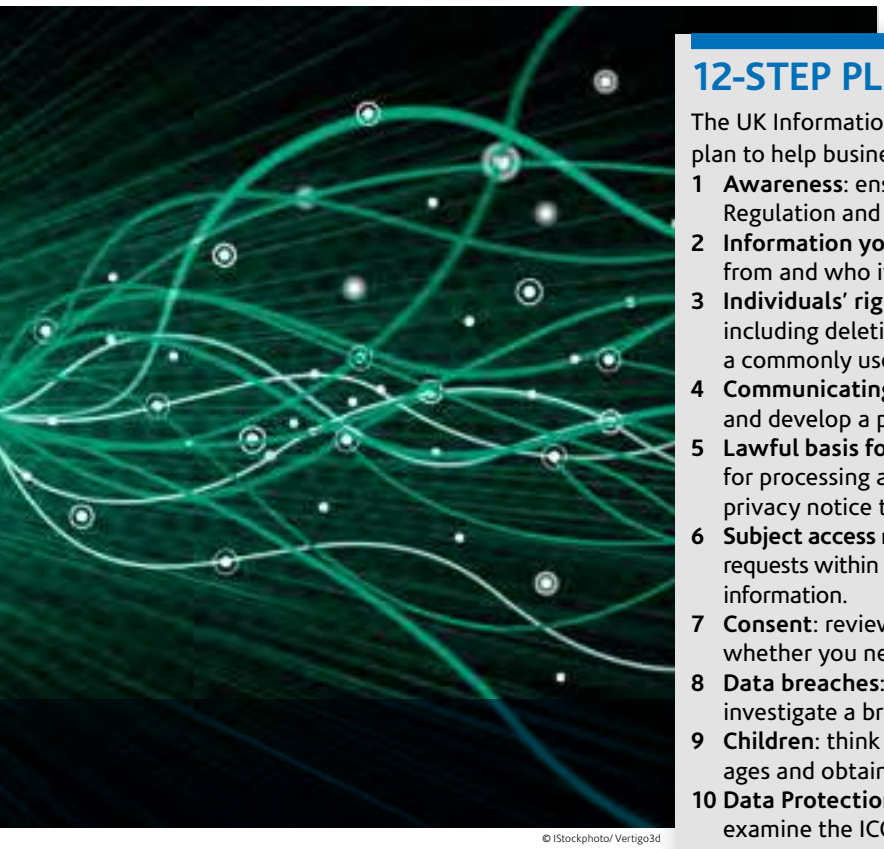
Despite the widely held view that GDPR is giving data protection a much needed leg up the corporate agenda, in practice, UK boards are only occasionally considering the legislation

Consent and erasure

Two aspects of GDPR that have generated most debate are the strengthened consent requirements and the so-called "right to be forgotten". "There could be a big impact for some organisations regarding what constitutes consent," says Emm. It will have to be explicit, as opposed to implicit and it must also be separate from other terms and conditions, and simple for data subjects to withdraw.

> "The principles of the regulation will become enshrined in UK law, regardless of Brexit"

Rather than a problem, businesses could see this as opportunity to sharpen up data handling. "If they take people's data and consent for granted, organisations may be less inclined to quantify what they are doing," suggests Emm. "This should make them appraise or review how they obtain and use information, forcing them to nail down what they've got, where they're storing it and on what basis they are allowed to use it." While individuals



© IStockphoto/ Vertigo3d

have a right to have personal data erased and to prevent processing in specific circumstances, GDPR does not provide an absolute "right to be forgotten". Examples of specific circumstances include where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed, where an individual withdraws consent, or where the individual objects to the processing and there is no legitimate interest for continuing it.

Another key change is the new requirement to notify the appropriate data protection authority of a data breach within 72 hours of discovering it. "72 hours is not long," stresses Taylor. "You've got to know what data is affected and who is affected, which means you need a good record of what you have and where, as well as good technology systems. With some companies now storing most of their information in the cloud, there are also obviously important questions around how you check and react if storage is breached there."

Board attention

Despite the widely held view that GDPR is giving data protection a much needed leg up the corporate agenda, the government's latest cyber security report shows that, in practice, UK boards are only occasionally considering the legislation. Just 13% of respondents from FTSE 350 companies said GDPR was regularly considered by their board, while 42% said it was discussed once or twice at board level, but was not regular.

"It [data protection and security] should be an integral part of managing risk," says Gillespie. "The trend to make it a separate discipline with separate consultants drives a wedge between the business and information risk. It should be an integral part of board risks."

Last year, Denham suggested to a UK House of Commons Public Bill Committee that directors be held personally accountable for breaches of data protection law by their companies, indicating that this may be something the ICO might press for in future. Gillespie believes such a move "makes perfect sense", noting how directors can already be held responsible for poor financial conduct and health and safety violations.

"It's right that businesses be responsible; the GDPR should discipline thoughts and force organisations into examining their procedures and processes," adds Ellie Hurst, marcomms and media manager for Advent IM. "What does it say about a business's culture if it doesn't value personal information, one of its biggest resources?"

Mike Gillespie
Advent IM

12-STEP PLAN

The UK Information Commissioner's Office (ICO) has produced a 12-step plan to help businesses prepare for GDPR:

1 **Awareness**: ensure decision makers and key people are aware of the Regulation and understand its impact.
2 **Information you hold**: document personal data held, where it came from and who it is shared with.
3 **Individuals' rights**: check procedures cover all the rights of individuals, including deleting personal data or providing data electronically and in a commonly used format.
4 **Communicating privacy information**: review current privacy notices and develop a plan for making any necessary changes.
5 **Lawful basis for processing personal data**: identify the lawful basis for processing activity in the GDPR, document it and update the privacy notice to explain it.
6 **Subject access requests**: update procedures and plan how to handle requests within the new timescales and provide any additional information.
7 **Consent**: review how you seek, record and manage consent and whether you need to make any changes.
8 **Data breaches**: make sure you have procedures to detect, report and investigate a breach.
9 **Children**: think about whether you need systems to verify individuals' ages and obtain parental or guardian consent.
10 **Data Protection by Design and Data Protection Impact Assessments**: examine the ICO's code of practice on Privacy Impact Assessments and latest guidance from the EU's Article 29 Working Party.
11 **Data Protection Officers**: designate someone to take responsibility for data protection compliance – consider whether you are required to formally designate a Data Protection Officer.
12 **International**: if the organisation operates in more than one EU member state, determine your lead supervisory authority.

The ICO has also produced a video for board directors outlining the commercial benefits of good data protection (https://ico.org.uk/for-organisations/data-protection-reform/gdpr-messages-for-the-boardroom) and a "Getting ready for GDPR" interactive tool (https://ico.org.uk/for-organisations/data-protection-reform/getting-ready-for-the-gdpr).

Source: Information Commissioner's Office