rackspace®

Xcina Consulting White Paper
**xcinaconsulting.com**

# Just when you thought it was safe to go back into the water!!!

June 2018

xcina Consulting


# The UK Data Protection Act 2018

The terror from the deep – aka the General Data Protection Regulation (GDPR) – is now in force.

For those of you who deployed your shark nets in order to ensure you were GDPR ready: BEWARE! There still may be a significant hole; namely the new UK Data Protection Act 2018 (DPA) that requires your attention.

The Secretary of State for Digital, Culture, Media and Sport, Matt Hancock said:

*"The Data Protection Act gives people more control over their data, supports businesses in their use of data, and prepares Britain for Brexit.*

*"In the digital world strong cyber security and data protection go hand in hand. The 2018 Act is a key component of our work to secure personal information online."*


# What's the difference between GDPR and the Data Protection Act 2018?

The GDPR has direct effect across all EU member states and has already been passed into law.

Organisations still have to look to the GDPR to fulfil most legal obligations. However, the GDPR gives member states limited opportunities to make provisions for how it applies in their country.

The DPA is a complete data protection system so, as well as governing general data covered by the GDPR, it covers all other general data, law enforcement data and national security data.

Furthermore, the DPA exercises a number of agreed modifications to the GDPR to make it work for the benefit of the UK in areas such as academic research, financial services and child protection.

# Does the DPA require organisations to improve cyber security?

Effective data protection relies on organisations adequately protecting their IT systems from malicious interference.

In implementing the GDPR standards, the DPA requires organisations that handle personal data to evaluate the risks of processing such data, and to implement appropriate measures to mitigate those risks.

For many organisations, such measures will need to include effective cyber security controls (i.e. people, process, systems and external events).


# You're gonna need a bigger boat!!

The Data Protection Act 2018 received Royal Assent on the 23rd May 2018.

It implements the government's manifesto commitment to update the UK's data protection laws.

Part of the Act includes applying the EU's GDPR standards and preparing Britain for Brexit.

By having strong data protection laws and appropriate safeguards, businesses will be able to operate across international borders. The DPA will ensure that modern, innovative uses of data can continue whilst, at the same time, strengthening the control and protection individuals have over their data.

# The main components of the DPA

### General data processing

- Implement GDPR standards across all general data processing.
- Provide clarity on the definitions used in the GDPR in the UK context.
- Ensure that sensitive health, social care and education data can continue to be processed to ensure continued confidentiality in health, and safeguarding situations can be maintained.
- Provide appropriate measures around rights of access, including the right of erasure, the right to object and the right to restrict processing.
- Set the age of child consent to 13 in the UK.

### Law enforcement processing

- Provide a bespoke regime for the processing of personal data by the police, prosecutors and other criminal justice agencies for law enforcement purposes.
- Allow the unhindered flow of data internationally whilst providing safeguards to protect personal data.

### National Security processing

- Ensure that the laws governing the processing of personal data by the intelligence services remain up-to-date and in-line with modernised international standards, including appropriate safeguards with which the intelligence community can continue to tackle existing, new and emerging national security threats.

### Regulation and enforcement

- Enact additional powers for the Information Commissioner who will continue to regulate and enforce data protection laws.
- Allow the Commissioner to levy higher administrative fines on data controllers and processors for the most serious data breaches, up to £17m (€20m) or 4% of global turnover for the most serious breaches.
- Empower the Commissioner to bring criminal proceedings against offences where a data controller or processor alters records with intent to prevent disclosure following a subject access request.

Factsheets giving an overview of the DPA have been published - https://www.gov.uk/government/publications/data-protection-act-2018-overview


# I'm not going to waste my time arguing with a man who's lining up to be a hot lunch!!

The Information Commissioner has responsibility in the UK for promoting and enforcing the Data Protection Act 2018, the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003, as amended.

It is independent of government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The Commissioner does this by providing guidance to individuals and organisations, solving problems where it can, and taking appropriate action where the law is broken.

xcina Consulting

rackspace

*"The introduction of the UK Data Protection [Act] ... will put in place one of the final pieces of much needed data protection reform. Effective, modern data protection laws with robust safeguards are central to securing the public's trust and confidence in the use of personal information within the digital economy, the delivery of public services and the fight against crime."*

Elizabeth Denham - Information Commissioner

# The danger that lurks beneath the surface

The latest figures, when taken as a proportion of all businesses operating within the EU, could translate into tens of billions in fines.

The Information Commissioner's Office stressed it would not embark on a "witch hunt" on the 25th May.

Despite concerns over compliance, it appears that some businesses are still demonstrating a lack of awareness about the implications of failing to comply with GDPR, and ultimately the DPA.

44% of all businesses said they were "concerned" about their ability to be GDPR compliant after 25th May.

30% of businesses said they believed financial penalties would have no impact on their business.

Given these figures, it is hardly surprising that with the additional requirements posed by the DPA to UK businesses, many organisations are standing there with only a lifebuoy, somewhat ill-equipped to face the actual danger that lurks beneath the surface.

# It's all psychological. You yell barracuda, everybody says, "Huh? What?" You yell shark, we've got a panic on our hands!!

We eluded to the fact earlier that the DPA incorporates the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003, as amended.

It is essential that organisations give appropriate consideration to these regulations and note the requirements which are above and beyond those stated in the GDPR.

We have chosen to focus on the Privacy and Electronic Communications Regulations 2003, as amended (PECR) because, in our opinion, this is where we see the greatest potential for non-compliance.

The Information Commissioner's Office has already publicly stated that they will take enforcement action against organisations that persistently ignore their obligations, starting with those that generate the most complaints.

PECR stands for Privacy and Electronic Communications (EC Directive) Regulations 2003 and are derived from European law. They implement European Directive 2002/58/EC, also known as 'the e-Privacy Directive', which is due to be replaced in the future by the new 'e-Privacy Regulation'.

The e-Privacy Directive complements the existing data protection regime and sets out more-specific privacy rights on electronic communications. It recognises that widespread public access to digital mobile networks and the internet opens up new possibilities for businesses and users, but also new risks to their privacy.

PECR have been amended four times so far. The more recent changes were made (in 2015) to allow emergency text alerts and to make it easier to take action for breaches of the marketing rules; and (in 2016) to require anyone making a marketing call to display their number.

**PECR covers specific rules on:**

- Marketing calls, emails, texts and faxes.
- Cookies (and similar technologies).
- Keeping communications services secure.
- Customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

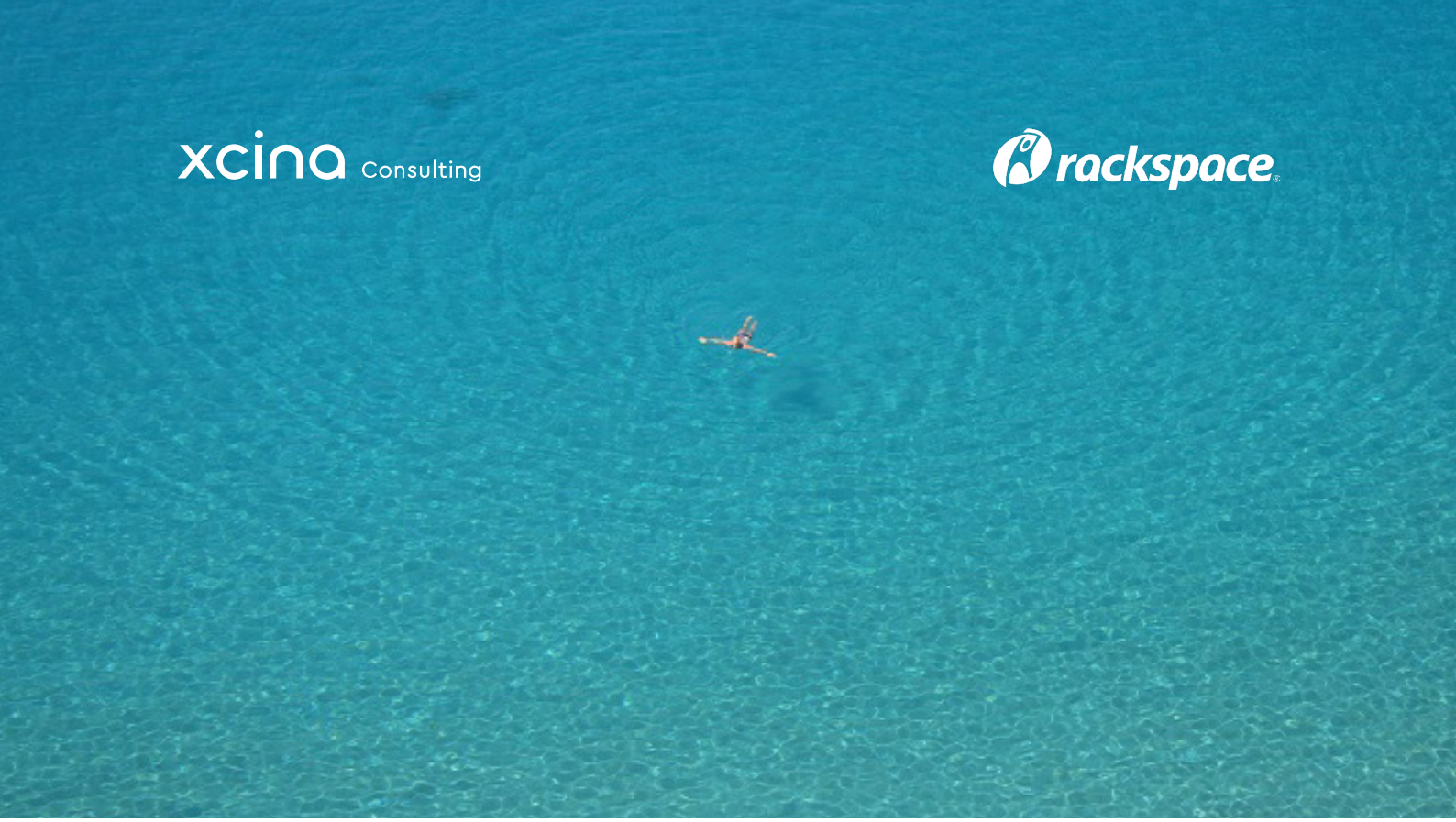
**PECR also gives focus to the following:**

- Solicited and unsolicited marketing.
- Marketing to individuals, businesses and internationally.
- Consent, recording of consent, valid consent, implied consent and consent over time.
- Opt-in, including 'soft opt-in' and opt-out.
- Buying and selling marketing lists and creating suppression lists.
- Other regulatory considerations and future state.

Organisations must continue to comply with both PECR requirements and those of GDPR. The DPA makes provision for a Direct Marketing Code of Practice, which contains practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of data protection legislation and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

*"What we are dealing with here is a perfect engine, an eating machine. It's really a miracle of evolution. All this machine does is swim and eat and make little sharks, and that's all."*

In summary, Hooper's comment to Mayor Vaughn in Jaws is perhaps a reflection of what organisations are facing today.



If you consider the key rationale behind the requirements to overhaul data protection legislation, it is primarily driven by digital transformation; what businesses have done is create that "perfect engine" to capture, analyse and transmit data in ways that weren't considered possible 20 years ago.

No doubt technology will continue to evolve as will the requirements governing it. But this new legislation will go a long way to ensuring Data Subjects can safely swim in today's digital economy.

xcina Consulting

For further information please get in touch with our team.

Email: consulting@xcina.co.uk
Phone: +44 (0)20 3985 8467

Xcina Consulting
1 King William Street
London
EC4N 7AF

**xcinaconsulting.com**

rackspace®

For further information please get in touch with our team.

Email: ManagedSecurityUK@rackspace.com
Phone: 020 8734 8107
Intl: +44 20 8734 2600

Rackspace Ltd
5 Millington Road
Hyde Park Hayes
Middlesex UB3 4AZ

**rackspace.com/en-gb/solutions/protect-my-data**