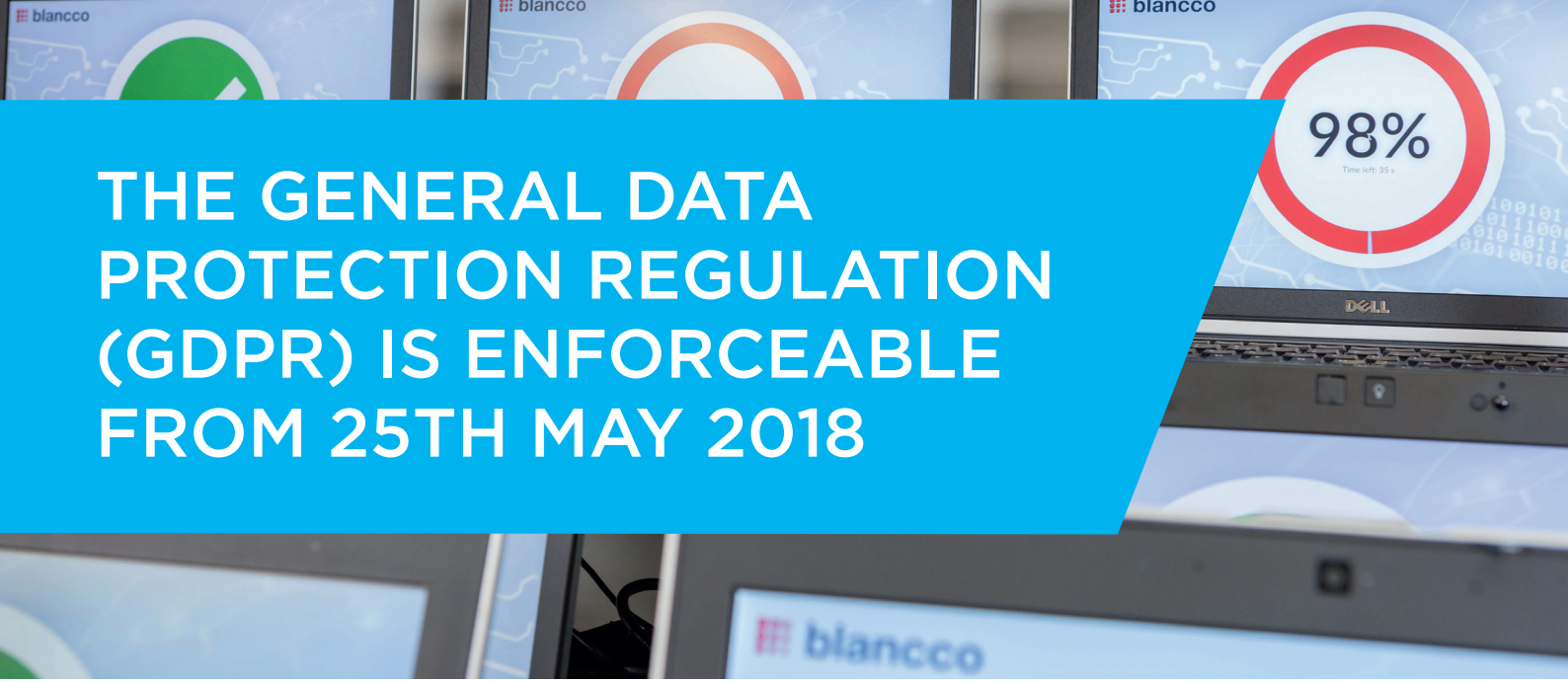
IMPLICATIONS OF THE GDPR FOR LEADERS IN BUSINESS

AN ICEX GUIDE

By Dr John Russell
(BSc, MSc, PhD, CEng, MIET, MIoD)
Chief Executive Officer

ICEX
TECHNOLOGY REPURPOSING



THE GENERAL DATA PROTECTION REGULATION (GDPR) IS ENFORCEABLE FROM 25TH MAY 2018

THE FACTS ARE THAT ON 14TH APRIL 2016, THE DATA PROTECTION ACT (1998) WAS REPLACED BY THE GENERAL DATA PROTECTION REGULATION (GDPR), FROM 25TH MAY 2018, THE REGULATION IS ENFORCEABLE. IN OTHER WORDS, A FAIRLY LOOSE SET OF GUIDELINES BECOMES A STRINGENT LAW WITH PUNITIVE PENALTIES FOR ANYONE CAUGHT BREACHING IT.

The biggest headline surrounding GDPR is the potential fines we all face if compliance is not met. A hefty 4% of global annual turnover can be levied by the ICO, or €20m, whichever is the higher.

The new rules focus on the protection of personal data. It will reduce the number of nuisance calls and emails. It will help to reduce cyber-crime, and it will help to unlock prosperity from the digital economy. Conversely, as business leaders, we will have to make some significant changes within our organisations to facilitate these improvements in society.

Information protection and cyber-security are inextricably linked, and therefore the GDPR extends far beyond IT system security, and will impact all industries and areas of business, but it is worth pointing out that the key benefit to society will be to restore confidence in the digital economy. It is also worth pointing out, that although it is European legislation, it will not be impacted by BREXIT, and has the full support of the Information Commissioner Office (ICO) and the UK government.

The ICO has published some useful information on the GDPR, and we would recommend reviewing what they have to say after you've read this paper. We have laid out 5 easy steps below to help you get started.

The biggest headline surrounding GDPR is the potential fines we all face if compliance is not met.

A hefty 4% of global annual turnover can be levied by the ICO, or €20k, whichever is the higher.

STEP 1
MANAGEMENT BUY-IN AND AWARENESS

A high proportion of business leaders have disregarded the GDPR, taking the view that it doesn't affect them. If they are fully compliant with the DPA then the changes to be made will be minimal, however we have found that many businesses within the UK have used the DPA as a loose set of guidelines and aren't necessarily compliant, therefore more drastic action must be taken in terms of policies and practices. Implementing the GDPR could have significant resource implications for those that have not adhered to the DPA fully.

To achieve compliance, we strongly recommend sitting down with senior members of your organisation and discussing any actions you need to take, ensure decision makers and key people are aware of the law change. Following this, relevant information should be fed down to your staff ensuring they have the resources in preparation of any changes needed in their specific role, many companies are achieving this through periodic emails, meetings and notice board posts, as well as word of mouth.

As a business leader, you will need someone senior to take control, but you may also need a champion, who can dedicate some time to getting things done.

Now the appropriate personnel are in place and taking the GDPR seriously, let's concentrate on the next important early tasks, which will be the information audit, risk assessment, and gap analysis. Here you will be ensuring that you know where all of the information is stored, you can justify why you have the information, and you can identify any risks it may face.

Be clear about what personal data you hold, where it's come from, and if shared with third parties, that the correct consents are in place. This also involves a complete audit trail which needs to be documented in case evidence of compliance is required.

The GDPR enforcement deadline needs to be taken seriously. It will have impacts on your cyber-security as well as information handling. We would recommend

As a business leader, you will need someone senior to take control, but you may also need a champion, who can dedicate some time to getting things done.

starting with something tangible that everyone can focus on, and obtaining the government backed Cyber Essentials standard is a good place to start. This will allow you to manage and realise your level of security, and any extra steps you might need to take to be breach proof. Whilst you will never be 100% secure, there are steps that can be taken to reduce the risks, and the level of risk appropriate to you is likely to be specific to your industry.

STEP 2
MARKETING AND SANITISATION

This is an opportunity as well as a threat. A business that shows they are fully compliant will likely see an increase in business prospects, furthermore the GDPR presents a great opportunity to review and map your data flows – and restructure them not only for compliance, but also for business efficiency. For those organisations willing to think outside the box, relatively new concepts such as privacy by design, profiling and data portability present the opportunity not only to innovate, but also to build customer trust and confidence and therefore ultimately drive sales. We have found that those companies who embrace openness are benefiting from real competitive advantage.

GDPR is directly concerned with the collection, storage, and use of personal data.

- Do you know where the data came from?
- Are the correct permissions to use the data in place?
- Have you made contact with the data subject in the last 12 months? You need to make sure that the personal data is compliant, or remove it.
- Do you need to be holding the data, and what are you using it for?

The grounds for processing personal data are consent or legitimate interest. The GDPR states that consent must be: "...freely given, specific, informed and unambiguous, and given by means of a statement of clear affirmative action."

Silence or pre-ticked boxes will not be acceptable forms of consent under the regulation. A controller cannot make a provision of a service conditional on consent; consent must be specific to each data processing activity; consent can be withdrawn at any time and must be easy to do.

> Businesses must be able to confirm that people have given their permission to receive text messages or emails, and they must have the evidence to prove it.

> ***Silence or pre-ticked boxes will not be acceptable forms of consent under the regulation***

Data controllers are those companies who collect, hold and determine the purpose of personal data, and data processors are those who process the data on behalf of the controller.

Do you process personal data? Consider if your business is involved in any of the following

- Do you use a CRM system?
- Do you collect information on your customers?
- Do you market your products or services using electronic and/or direct marketing?
- Do you buy B2B data for marketing?

If yes, then you must have a clear audit trail, which documents where the data came from, what permissions you have to use the data, and any third parties it has been shared with.

You will need to ensure that any data added to your systems is compliant with the GDPR, and that you can prove this and provide appropriate documentation if needed, retain audit trails of where data was sourced, and any information that confirms that consent was given.

It is likely that a significant amount of data will need to be removed from some marketing databases to make them GDPR compliant.

STEP 3
WHAT'S A DATA SUBJECT?

The new legislation lists 7 rights of the individual (or data subject), and these are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

The GDPR also says that individuals have the right not to be subject to automated decision-making including profiling, where The GDPR defines profiling as processing intended to predict an individual's:

- Performance at work
- Economic situation
- Health
- Personal preferences
- Reliability
- Behaviour

Companies must ensure that processing is fair and transparent by providing meaningful information about why the processing has taken place.

It is highly likely that you will need to update your 'privacy statement', to ensure that it is transparent. Meaning that it has to be written in an easy to understand way that provides clear information to individuals about what their personal information will be used for.

Individuals can ask for their personal data to be provided in a useable format so that it can be transferred to another data controller.

An individual can request access to their data, and this must be done within one month and with no fee charged. This is known as a subject access request (SAR). This is an example of somewhere you will possibly need a new policy to show how you will

> ***It's no longer acceptable to just achieve the deadlines, you will need to be able to prove that you have systems in place, should you be audited.***

achieve this. It's no longer acceptable to just achieve the deadlines, you will need to be able to prove that you have systems in place, should you be audited. If the data controller processes a large quantity of data about the individual, it is reasonable to ask for the request to be narrowed down.

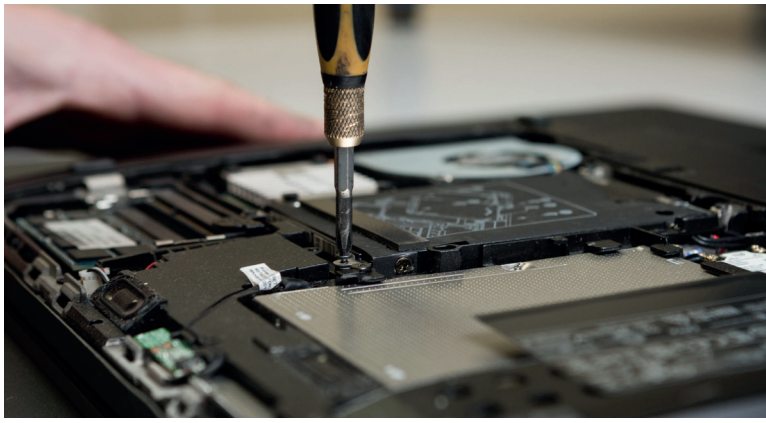
The right to be forgotten allows for an individual to request that their data is deleted, providing that there are no legitimate grounds for keeping it. Data controllers must take reasonable steps to inform other data procesors with whom the data has been shared. You will also need to make sure that backup recovery can't restore a subject that you are supposed to have forgotten.

STEP 4
DO I NEED A DPO?

A data protection officer is a specifically defined role with legally defined responsibilities.

One is required in organisations whose core activities consist of processing operations that require regular monitoring of individuals on a large scale, and those dealing with sensitive data.

Most small businesses will not require a DPO. However, a designated individual to perform many of the required duties would be a useful additional function to one of your staff's normal activities.



STEP 5
WHAT IF IT GOES WRONG?

Reporting data breaches is mandatory, and organisations must notify the ICO of data breaches within 72 hours of them occurring. They must also communicate to the data subject any high-risk breaches so that appropriate measures can be taken. Those 3 days are your last chance to make sure that your processes are in order, and to seek professional advice if required.

The GDPR has introduced the phrase 'by design', to ensure that data protection and privacy will be at the forefront of any project from the start. It is also concerned with the amount of data collected, the purpose, and length of time that the data is kept. Where necessary, a 'Privacy Impact Assessment' may need to be conducted to identify and reduce any privacy risk from the earliest stages of development. PIAs are mandatory for companies dealing with processes that present a high risk to their data subjects.

The bottom line is, if you've designed the processes and activities correctly in the first place, then there is much less chance of a breach, and you will have the proof to show you've done everything you can.

Reporting data breaches is mandatory, and organisations must notify the ICO of data breaches within 72 hours of them occurring.

The last point to consider here is whether you need a contract with your clients, and other data subjects? Should there be a breach, then there needs to be clear evidence of who owns the data, and who is responsible for it. This provides additional protection for all parties.

SUMMARY

Every business that holds or processes personal data must have reviewed their processes, and put in place whatever changes are required to ensure that they are GDPR ready.

Furthermore, they will have to have reviewed all of the personal data that they hold, and sanitise it for GDPR compliance.

At ICEX we take the GDPR very seriously, and will help our clients to comply in whatever way we can.

We will work with you on areas such as contractual compliance and mitigation of liability. Our Service Level Agreement (SLA) contains a specific clause to take away your liability once we collect your redundant IT equipment.

Furthermore, our expert advisors will help you choose the appropriate data destruction method to best suit your risk profile and budget.

IF YOU ARE STILL UNSURE ABOUT WHAT YOU NEED TO DO, THEN GET IN TOUCH FOR AN INFORMAL CHAT

CALL NOW ON

01376 503 900

(LINES ARE OPEN UNTIL 5PM)

ABOUT ICEX

ICEX has been providing its clients with contracted secure data destruction, IT disposal, IT repurposing and remarketing solutions for over 15 years.

We provide tailored IT asset disposal programmes that meet all of our client's IT disposal needs while optimising the retired asset value in a secure and environmentally- friendly manner.

Our experienced professionals utilise their unrivalled knowledge and expertise to meet and exceed existing laws, legislation and government requirements offering clients full confidentiality and security.

Conscientious and motivated, the ICEX team supports a large range of organisations - from local charities to large corporates, as well as the public sector, including schools, emergency services, councils and the NHS.

Our philosophy is to make it simple for our clients - we offer a straightforward and transparent service that ensures our customers return to us time after time.

CONTACT US FOR A FREE CONSULTATION ON:

- **IT ASSET DISPOSAL**
- **DATA DESTRUCTION**
- **ONSITE SERVICES**
- **GDPR COMPLIANCE**
- **IT ASSET REMARKETING**
- **DOCUMENT SHREDDING**

ICEX
TECHNOLOGY REPURPOSING

ADISA ACCREDITED MERIT ICEX

bsi. ISO/IEC 27001 Information Security Management IS 559242

bsi. ISO 14001 Environmental Management EMS 81051

bsi. ISO 9001 Quality Management FM 594023

2017 Computing Security Awards ★ FINALIST ★

blancco Gold ITAD Partner

HEAD OFFICE
ICEX Limited, Europa Park,
Croft Way, Witham, Essex CM8 2FN
T: 01376 503 900

LONDON OFFICE
ICEX Limited, Kemp House,
152 City Road EC1V 2NX
T: 0207 412 8943

E: info@icex.co.uk
www.icex.co.uk