GENERAL DATA PROTECTION REGULATION 2018

PREPARING YOUR BUSINESS FOR GDPR

From one of Ireland's leading independent funding specialists

WE BELIEVE IN **YOUR** BUSINESS

INVOICE FINANCE • EXPORT FINANCE • BAD DEBT PROTECTION • FX

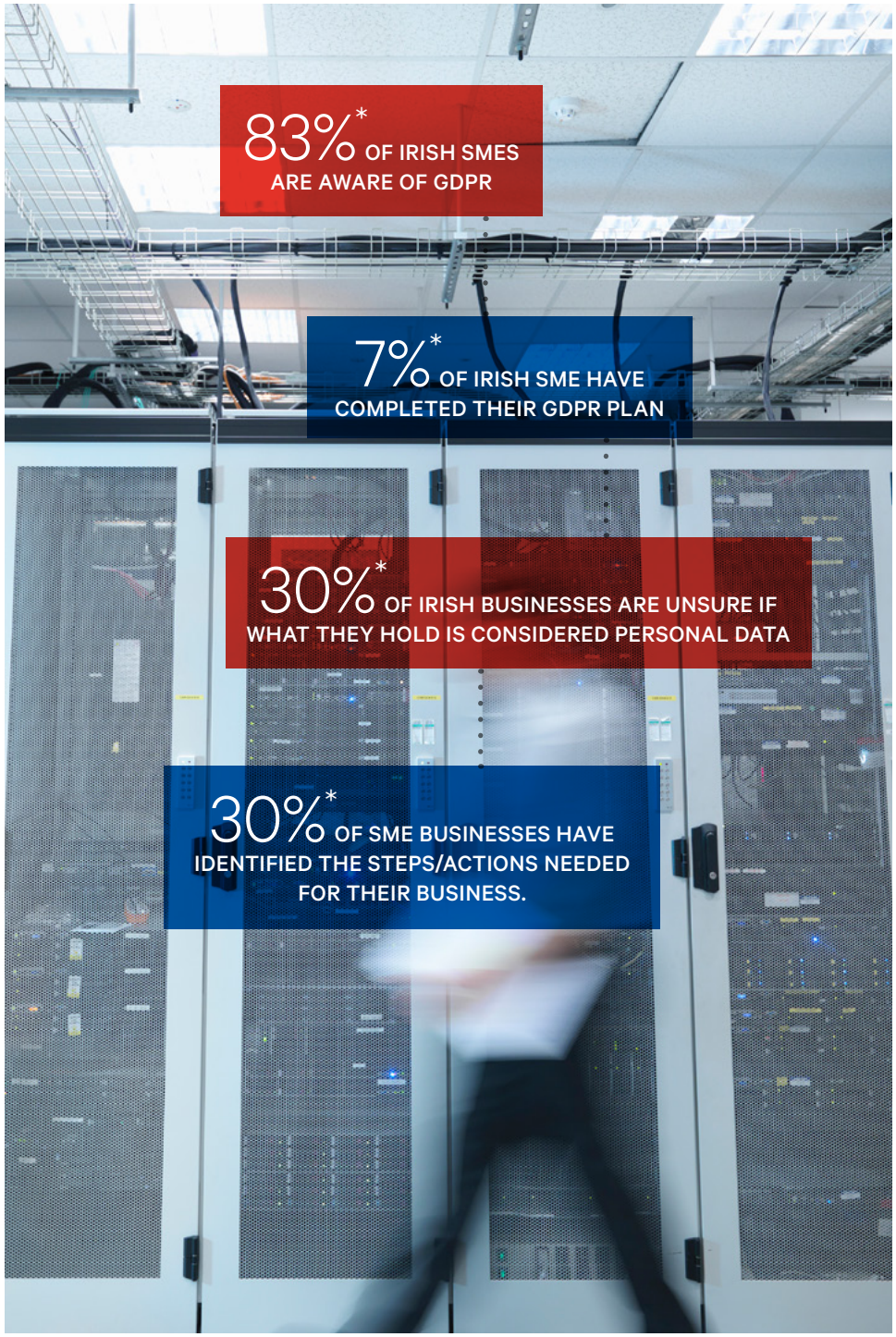
BIBBY FINANCIAL SERVICES

GENERAL DATA PROTECTION REGULATION 2018

In April 2016, the European Union adopted the General Data Protection Regulation (GDPR), which will replace the Data Protection Acts 1998 and 2003 and apply to all businesses that process, handle and store any personal data of EU residents – regardless of size or industry. GDPR also increases the powers that regulatory authorities have to act against companies who don't comply with it.

The new regulations that form the GDPR will come into effect on 25th May 2018, requiring Irish businesses to be more accountable for protecting people's identity, as well as minimising the risks of a data breach. Contrary to popular belief, personal data is not just consumer information. Whether you have employee data, customer data or supplier data – if the data relates to an individual, your business will be subject to the GDPR requirements.

With less than a year to go before the GDPR becomes effective many businesses are yet to prepare. Our guide provides the proactive steps your business can take to understand and prepare for the GDPR and protect it from the potential costly outcomes of non-compliance.



*GDRP survey by ISME January 2018

1 WHAT DOES THE GDPR MEAN FOR YOUR BUSINESS?

At the core of GDPR is the aim is to simplify, unify and update the protection of personal data. Changes under GDPR are aimed at moving away from tick-box compliance regarding the security and privacy of personal information, and towards a company-wide approach to managing the lifecycle of personal data.

GDPR follows similar rules to existing data protection legislation. So, if you're already complying with the current Data Protection Acts (DPA), then most of your approach to compliance will remain valid under the GDPR and this can be the starting point to build from.

The key points of the GDPR to be aware of are:

- GDPR has a wider geographic scope. You do not have to be based in Europe for it to apply. If your business transacts with EU residents, you will be subject to GDPR.
- Data Protection Authorities (DPAs) will have the power to enforce much more severe penalties for breaches of personal data; this means fines of up to €20 million or 4% of turnover.
- The definition of 'personal data' has widened and now explicitly includes IP addresses and mobile device identity. It also enforces a far more robust process around the management of contact data from events. No longer can your event attendee lists just be included in marketing campaigns, without being able to show evidence of 'opt-in' to communications.
- Technical and organisational measures regarding the protection of personal data are to become mandatory to test the effectiveness of security measures.
- Data processing registries will become mandatory and require that you keep a written (electronic) record of personal data processing activities.
- Data protection impact assessments will be required for technology or processes that are likely to be high risk to individuals.
- The reporting of personal data breaches will become mandatory and you will need to report breaches of personal data to the Data Protection Commissioner (DPC) within 72 hours.
- If your business processes data relating to Government services, data is at the core of your business, or you manage highly sensitive data, you will be required to have a Data Protection Officer (DPO).

2 STEPS TOWARDS GDPR PREPARATION

The critical first step to prepare for GDPR is to determine where all the personal data held by your business is located. You need to understand where information is being stored (even if it's on a mobile device or in the cloud), who has access to it, how long it is being retained, and where it is being moved to. This is key to understanding how your business can prepare for GDPR.

The DPC suggests 12 steps you should take now:

Staff

1. Make sure that decision-makers and key people in your business are aware that the law is changing and the impact this is likely to have. Training will be essential to ensure staff understand what's expected of them, how to respond and how to handle data.
2. Designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within the structure of your business and governance arrangements.

Processes

3. Document what personal data your business holds, where it came from and who it's shared with. This may mean organising an information audit.
4. Check procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
5. Update procedures and plan how you will handle subject access requests within the new timescales.
6. Look at the various types of data processing you conduct, identify your legal basis for carrying it out and document it.
7. Review how you are seeking, obtaining and recording consent and whether you need to make any changes.
8. Start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity of children, if this applies to your business.

Systems

9. Review your current privacy notices and put a plan in place to make any necessary changes in time for GDPR implementation.
10. Make sure you have the right procedures in place to detect, report and investigate a personal data breach.
11. Familiarise yourself with the guidance the DPC has produced on Privacy Impact Assessments and work out how and when to implement them.
12. If you operate internationally, you should determine which data protection supervisory authority you come under.

3 COMPLYING WITH THE NEW GDPR RULES

While getting to full compliance can be complex, once achieved you will realise significant benefits – especially if you are looking to enter new markets. Since data protection regulations will be the same throughout Europe, businesses will no longer need to consult local lawyers to ensure local compliance, which will result in direct cost savings and legal certainty.

The key new requirements include:

Direct liability – For the first time, if you process personal data in the course of providing a service, you will have direct liability for breaches of the GDPR, including the risk of being fined.

Mandatory breach notification – It will be compulsory for data controllers to notify, within 72 hours, the relevant Data Protection Authority about data breaches that may result in a risk to the rights and freedoms of individuals whose data is compromised.

Individuals rights on the use of information and the right to be forgotten – The GDPR gives individuals a new 'right to be forgotten' (have their personal data removed), a new right to data portability (have their personal data copied and transmitted to another business for further use, including competitors) and enhanced data subject access rights.

How to process data fairly – There will be new limitations on data profiling, including a requirement that you obtain prior consent.

Compulsory 'data mapping' and documentation requirements – Controllers and processors of personal data will have to prepare and maintain comprehensive records of processing activities.

Privacy notice requirements and right to access – The GDPR sets out specific information to be included in privacy notices and requires that people are given clear information as to what is done with their data in an easily accessible way.

Data protection impact assessments – These will be compulsory before undertaking 'high risk' data processing, including profiling or heavy use of sensitive personal data.

Responding to complaints – The GDPR also establishes a right to compensation for anyone affected by a data breach and will enable them to lodge complaints, and receive compensation.

Double opt-in – You will need explicit double 'opt-in' consent regarding the processing of data and marketing communications. This means clear confirmation from a prospect or customer saying they want to receive your communications. Gone are the days of a pre ticked box. To ensure double opt-in get people to fill out a form, then send an email asking them to confirm they are interested in receiving communications.

Third Parties – Name your organisation and any third parties who will be relying on consent – even precisely defined categories of third-party organisations will not be acceptable under the GDPR.

SUMMARY

Although the standards will be far more stringent and require businesses to implement many new data protection measures, this requirement could make doing business simpler and improve the way personal information is managed. To check how prepared your business is, you can complete a data protection self-assessment. You may also require advice and support from experts to assist you who can make sure you're meeting the new requirements. To get prepared for the GDPR you can access the Data Commissioner's comprehensive guide to the new regulations.

ABOUT US

Bibby Financial Services has been supporting businesses of all sizes since 1982. We are a trusted financial services partner to over 10,400 businesses worldwide and have built a reputation for consistently delivering high levels of client service. We don't just fund your business,

OUR PRODUCTS AND SERVICES

We We help businesses unlock working capital for a range of scenarios,including cashflow funding, growth and expansion.

Our range of financing options includes:

- Invoice Discounting
- Bad Debt Protection
- Export Finance
- Foreign Exchange

Published May 2018.