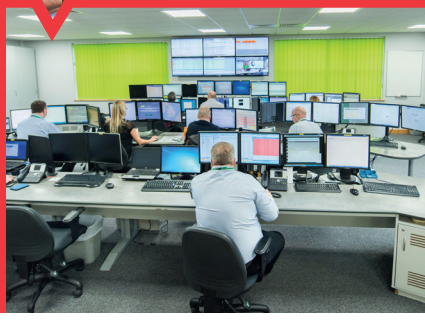
Summary of General Data Regulation & Actions



DYER & BUTLER
A part of MGroupServices

1. Introduction

The new General Data Protection Regulation (GDPR) replaces the 1998 Data Protection Act (DPA) and comes into effect on 25 May 2018. It is a European Directive which will survive Brexit and is applied to all nations worldwide who do business with the EU.

GDPR provides more comprehensive and far- reaching criteria for businesses to adhere to with regard to personal data that we hold on our systems. The main reason for introducing these regulations is to bring them in line with the digital age in which we now live and recognise the rights of the individual with regards to the use of their personal information.

The key risk areas for Dyer & Butler are two fold; managing our own staff data securely, and just as importantly managing personal information that we process on behalf of our clients. To put this in context, as part of M Group Services, we hold records for approx. 8,000 staff, 3,000 suppliers, 2,000 sub-contractors and millions of customers, largely due to our meter reading activities.

We need to move forward now to ensure we can evidence compliance by May 2018.

A governance team comprising representatives across the business will be in place to guide the changeover to the new legislation

1.1 Differences between DPA & GDPR

The major differences between the new regulations and the DPA are:

	DPA	**GDPR**
Reach	Only applied to the UK.	Applies to the whole of the EU and, crucially, also to any global company which holds data on EU citizens.
Enforcement	Enforced by the Information Commissioner's Office (ICO).	Compliance will be monitored by a Supervisory Authority in the UK (ICO) with each European country having its own SA. The impact of this is that organisations will be required to provide evidence of compliance when required by that authority.
Penalties	Non-compliance can result in fines of up to £500,000 or 1% of annual turnover.	The potential penalties for non-compliance are much more severe with fines of up to €20 million or 4% of the businesses annual global turnover.

Data Protection Officers (DPO)	Under the current legislation there is no need for any business to have a dedicated Data Protection Officer DPO.	A DPO is recommended for any business or organisation with more than 250 employees. The DPO will be responsible for: • Overseeing data protection strategy and its implementation to ensure compliance with GDPR requirements. • Educating the company and employees on important compliance requirements. • Training staff involved in data processing. • Conducting audits to ensure compliance and address potential issues proactively. • Serving as the point of contact between the company and GDPR Supervisory Authorities.
Data breaches	Businesses are under no obligation to report data breaches though they are encouraged to do so.	Any data breach of personal data must be reported to the Supervisory Authority within 72 hours of the incident. If this does not take place, the company will face fines.
Data removal	There is no requirement for an organisation to remove all data they hold on an individual.	An individual will have the 'Right to erasure' – which includes all data including web records with all information being permanently deleted. On the basis that as a business we hold personal data on several Million people, we will need to plan for this.
Privacy by design Privacy impact assessments (PIAs) are a tool that you can use to help identify and reduce the privacy risks of your projects. A PIA can reduce the risks of harm to individuals through the misuse of their personal information.	Protection Impact Assessments are not a legal requirement under DPA but has always being 'championed' by the ICO.	PIAs will be mandatory and must be carried out when there is a high risk to the freedoms of the individual. A PIA helps an organisation to ensure they meet an individual's expectation of privacy.
Opting in **Opting in by individuals to allow use of their personal data.**	Data collection does not necessarily require an opt-in under the current Data Protection Act.	The need for consent underpins GDPR. Individuals must opt-in whenever data is collected and there must be clear privacy notices. Those notices must be concise and transparent and consent must be able to be withdrawn at any time.

2. Dyer & Butler - 12 Steps to compliance

Dyer & Butler will co-ordinate GDPR compliance activities through HR and Information Security. Activities already underway include an in-depth review of all policies and procedures associated with data security, implementing Privacy by Design and undertaking a series of audits and assessments.

Initial preparation has been made easier for businesses by introduction of a 12 step checklist by the Information Commissioner's Office (the ICO), and Dyer & Butler have based our implementation plan on these 12 steps.

Step 1 – Awareness
GDPR change: The GDPR will significantly amend current data protection law.

Action to be taken: We will make the GDPR reforms known to key people in the business, and make them aware of the effects of such reforms. Management are being briefed, staff will be trained and a page on our Intranet will be available.

Step 2 – Information you hold
GDPR change: If a business has shared inaccurate personal data with another organisation, the GDPR requires that the business notify that other organisation of the inaccuracy. As part of the new accountability principle, businesses will also have to be able to show how they comply with the data protection principles.

Action to be taken: We are undertaking an information audit which documents the personal data held by the business, the source of such data and details of with whom data is shared.

Step 3 – Communicating privacy information
GDPR change: Additional information must be given to individuals when their personal data is obtained.

Action to be taken: We will be reviewing current privacy notices/policies and identify those areas which will require updating to ensure compliance with the GDPR.

Step 4 – Individuals' rights
GDPR change: Individuals will have enhanced rights to:-
Access their information.
Have inaccuracies corrected.
Have information erased.
Prevent direct marketing.
Prevent automated decision making and profiling.
Data portability.

Action to be taken: We will be reviewing privacy/data protection procedures and policies to ensure that they provide for each enhanced right under the GDPR and making this information much more accessible.

Step 5 – Subject access requests
GDPR change: Current rules for subject access requests, when an individual asks for all information the organisation holds on them to be made available in a readable format, are changing – timescales for compliance will be reduced, fees will generally no longer be chargeable and additional information will require to be provided to individuals e.g. about data retention periods and the right to have inaccuracies corrected.

Action to be taken: Review and update current procedures for handling subject access requests.

Step 6 – Legal basis for processing personal data
GDPR change: The legal basis for processing will need to be explained in privacy notices and when responding to subject access requests. The rights afforded to individuals will vary depending on the legal basis for data processing.

Action to be taken: We will review the data processing done by Dyer & Butler and then identify and document the legal basis for processing.

Step 7 – Consent
GDPR change: Consent must be freely given, specific, informed, and unambiguous. The recording of consent is important as data controllers must be able to demonstrate that consent was given.

Action to be taken: We will be undertaking a comprehensive review of methods for seeking, obtaining and recording consent to ensure compliance.

Step 8 – Children
GDPR change: Parental or guardian consent must be obtained to process personal information of children (i.e. those under 13 in the UK). Consent must be verifiable and written in child friendly language.

Action to be taken: This is an area Dyer & Butler have little or no involvement in.

Step 9 – Data breaches
GDPR change: The GDPR widens the number of businesses obliged to notify the ICO and private individuals of data breaches. Failure to comply with this obligation may lead to significant fines by the ICO.

Action to be taken: Ensure that there are procedures in place to detect, investigate and report on personal data breaches. The ICO suggests assessing the types of data held and documenting which ones would trigger notification in the event of a breach. Dyer & Butler will follow this guideline.

Step 10 – Data protection by design and data protection impact assessments
GDPR change: Organisations must adopt ‘privacy by design’ (i.e. an approach that promotes privacy and data protection compliance from the outset). Organisations should also carry out a Data Protection Impact Assessment (DPIA) in high-risk situations. If processing is high risk, the ICO should be consulted on whether processing complies with the GDPR.

Action to be taken: We are undertaking a DPIA review and are organising who should be involved and the process to be adopted.

Step 11 – Data protection officers
GDPR change: Public authorities and large businesses that move large quantities of personal data will be required to appoint a Data Protection Officer to oversee compliance.

Action to be taken: Dyer & Butler will appoint a Data Protection Officer.

Step 12 – International
GDPR change: The GDPR creates a system for determining which data protection supervisory authority takes the lead when investigating a complaint which is international in nature.

Action to be taken: This does not directly affect Dyer & Butler.

3. Fines

A two-tiered sanctions regime will apply. Breaches of some provisions by businesses, which law makers have deemed to be most important for data protection, could lead to fines of up to 20 million or 4% of global annual turnover for the preceding financial year, whichever is the greater, being levied by data watchdogs.

For other breaches, the authorities could impose fines on companies of up to 10m or 2% of global annual turnover, whichever is greater.

The Information Commissioner's Office has indicated that the highest level of fines will only be applied for the worst cases that are brought to their attention.