Gateley Plc

General Data Protection Regulation (GDPR)

A guide for your board

gateleyplc.com/gdpr

Introduction

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018. It requires greater transparency from those who process personal data and provides individuals (also known as data subjects) with enhanced rights when it comes to the handling of their information.

The regulation applies to:

- **data controllers** - the person or body that determines how data is processed and for what purpose (eg an organisation which processes personal data about its staff, customers etc.); and
- **data processors** - those that process personal data on behalf of data controllers (eg a third party who has received the personal data from a data controller to process that data upon the instructions of the data controller).

Company directors are the decision makers at the highest level of an organisation and so it is up to them to decide on the appropriate steps the company should be taking in relation to GDPR. However the board will need clear and reliable updates from those more directly involved in the management of data throughout the company, this includes legal, HR, IT and other departments such as marketing, sales and after care, all of which are likely to process the data of individuals, including information relating to employees.

What steps should your board be taking?

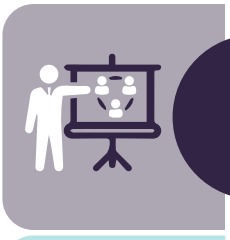
Every company will hold some personal data, irrespective of the sector in which the business operates. In preparation for the GDPR, directors should consider taking these seven preliminary steps.

1. Establish a team

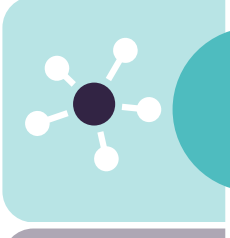
2. Complete data-mapping exercise

3. Consider processing notices

4. Update consents



5. Assess internal processes



6. Embed Data Protection Impact Assessment

7. Governance: raise internal awareness

1. Establish a team

Put together a specialist team tasked with ensuring GDPR compliance.

This team should include the individual who is predominantly responsible for data protection within the organisation, as well as other representatives from the legal, HR, IT, sales and risk and compliance teams, if applicable.

Perhaps most importantly, the board should determine whether or not a Data Protection Officer (DPO) is required. The appointment of a DPO is a mandatory requirement for some organisations. Every business is likely to benefit from appointing someone to oversee data protection compliance to ensure the highest levels of compliance. This individual is responsible for advising on GDPR principles and monitoring compliance. They act as a main point of contact for data subjects and supervisory bodies (in the UK this will be the Information Commissioner's Office).

The board must evaluate whether the individual currently designated as being responsible for data protection is an appropriate appointment for any DPO. Current arrangements may not fulfil requirements of autonomy, expertise and internal reporting. There should be no conflict between the role of a DPO and his/her other duties for the organisation.

The DPO must be free to act independently and be given adequate resources to carry out the required functions of the role. The board must not penalise the DPO for any opinions or advice given to the directors and the DPO cannot be dismissed merely on the basis of any disagreements with the board.

2. Undertake a data-mapping exercise

To ensure GDPR compliance an organisation will need to consider:

- what personal data the organisation collects, about whom and for what purpose;
- how that data is processed;
- how long the data is held for;
- the legal basis for processing the personal data and, if relying on consent, whether the correct consents have been obtained; and
- where the data comes from and whether the data is sent on to any third parties (if so, whether that party should be identified as a data processor for GDPR purposes).

The board should ensure that a robust 'data-mapping' exercise is carried out to answer these questions and allow informed decision making for any future plans involving the processing of personal data.

3. Processing notices

As part of the data mapping exercise, businesses should consider the legal basis for processing personal data.

Whether an organisation is relying on consent, legitimate business purposes, performance of a contract or compliance with a legal obligation (the most common lawful bases for processing personal data), this should be documented in the processing notice which is provided to individuals whose personal data is being processed. The GDPR sets out a long list of other information which also needs to be provided to individuals. Despite the amount of information which needs to be provided, a processing notice under the GDPR must also be concise, transparent, intelligible, easily accessible and it must be written in clear and plain language.

As a result of these new requirements, current notices must be reviewed and amended to ensure compliance with the GDPR.

4. Update consents (if needed)

Where consent is required, the data subject must have freely given specific, informed, unambiguous consent for the personal data to be processed in a specific way.

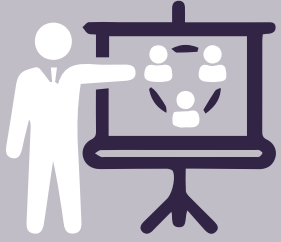
The onus is on the data controller to demonstrate that consent was given so organisations need to be able to record that individuals have provided such consent.

If it is discovered that the required consents are not recorded and cannot be established then fresh consent must be obtained. If this cannot be done the data must not be processed based on consent. Organisations, therefore, also need to consider the historic data they hold and have processed prior to 25 May 2018 and whether demonstrable consent must be obtained in order to continue to process such data.

5. Assess internal processes

The internal processes of the business should be reviewed to ascertain whether or not they are reliable and provide the required level of security governance and functionality under the GDPR.

Any requests made by a data subject must be actioned and dealt with within much stricter time frames under the new regulations. In particular, the board should also look to implement a process to deal with any Subject Access Requests (SARs). Ensuring that these are dealt with efficiently and effectively is an important aspect of the GDPR. The GDPR requires SARs to be dealt with within one month of receipt (under the Data Protection Act the period was 40 days). These onerous requirements mean organisations will need to isolate data more quickly and employees will likely need training to ensure SARs are dealt with in line with the GDPR. Similar issues arise in relation to the right to be forgotten, objecting to direct marketing and withdrawal of consent.

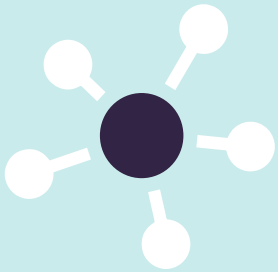


Data breaches/loss may need to be notified to the ICO within 72 hours of the breach/loss being discovered and so the board will need to review or implement a breach notification plan. The ICO, and (depending on the severity of the breach) the individual, may need to be notified and made aware of the nature and scale of the breach and the potential impact on the data subject. Having a pre-determined and tested process in place will ensure that a business is better prepared as and when a data breach occurs.

6. Embed data protection by design and default

Any new business practices or processes that are to be adopted by the board must have data protection considerations integrated from the outset.

Maintaining privacy and data security must be a key focus for the board before implementing any new systems and simply adding these in as an afterthought will not be considered to be fully GDPR compliant. The board must also ensure that any new technology, practice or process, which could result in a high risk to the rights and freedoms of individuals, is accompanied by a Data Protection Impact Assessment (DIPA) which assesses the impact the envisaged processing will have on the protection of personal data. Organisations may also need to consult with the ICO in respect of these risks.



An effective DPIA will allow organisations to identify and fix, or mitigate, problems relating to the protection of data at an early stage, reducing the costs of putting things right at a later date and reducing any risk of damage to reputation. The ICO has promoted the use of DPIAs as an integral part of taking a data protection by design approach.

7. Governance

Robust internal governance is required to ensure that data protection is integral to the way an organisation operates and that breaches are dealt with appropriately and efficiently.

Raising awareness throughout the organisation will ensure all employees are clear on their responsibilities.

A data protection policy should be adopted by the board which outlines practical considerations for employees. A policy and the provision of training will help people within an organisation to understand when they can override an individual's wishes to exercise certain rights of their personal data, on what grounds this can be done and who within the organisation can make that decision. As part of the internal policies and procedures, template documents should be prepared for written communications relating to a data subject's rights to ensure the required content is included.

If personal data is being disclosed to third parties, particularly where a party is acting as a data processor for the other, a GDPR compliant data processing agreement needs to be in place. Existing agreements, therefore, need to be reviewed and updated and where no terms are in place in respect of data protection, formal written agreements should be drafted.

Data usage runs throughout an organisation and so the board, as the most senior level of management, will be responsible for ensuring an ongoing and integrated approach to compliance is maintained.

The importance of data protection means that GDPR should be treated as an organisational risk and the board should include it in its existing risk management processes.

Useful resources

GDPR Webinar

For practical guidance on how to prepare your business for GDPR, watch our free on demand webinar at **http://info.gateleyplc.com/helping-you-prepare-gdpr-webinar**

GDPR Toolkit

Our expert team can help you demonstrate compliance with a specialised GDPR Toolkit that will:

- Assess if your business is already compliant with GDPR.
- Identify key risk areas in your business and how to address them.
- Ensure that GDPR is part of your business strategy and project manage your business towards compliance, including the new principle of accountability..

Register for our GDPR Toolkit at **http://info.gateleyplc.com/gdpr-toolkit** to ensure that your business is prepared for 25 May 2018.

Key contacts

Andrew Evans
Partner, Commercial

dt: +44 (0) 207 653 1658
andrew.evans@gateleyplc.com

Peter Budd
Partner, Commercial

dt: +44 (0) 161 836 7928
peter.budd@gateleyplc.com

Katie Hall
Solicitor, Commercial

dt: +44 (0) 207 653 1618
katie.hall@gateleyplc.com

info@gateleyplc.com
@GateleyPlc
/company/gateley-plc
gateleyplc.com/gdpr

Gateley Plc