Gateley Plc

General Data Protection Regulation (GDPR)

A Guide for Corporate Transactions

gateleyplc.com

Contents

Is your business prepared for GDPR?

The General Data Protection Regulation (GDPR) is due to come into force in May 2018 and all businesses need to be aware of changes that are likely to affect them.

From 25 May 2018 all businesses in the UK will be subject to the new GDPR legislation.

This legislation replaces the old Data Protection Act and will heighten the responsibilities of data controllers and processors as well as the rights of individuals. The GDPR will apply to all businesses controlling and processing the personal data of individuals residing in the EU, even if the business is based outside the EU. The UK government has stated that it will create something very similar to the GDPR for UK businesses following Brexit, meaning that organisations should act as soon as possible to ensure compliance.

The GDPR introduces a far-reaching framework that will impact many corporate transactions. It will now be necessary to carry out enhanced due diligence and take extra precautions throughout all stages of the M&A process. It will be important to confirm that a target company has implemented effective, GDPR compliant systems to ensure that the buyer is not 'stung' by the new regulations. Despite the challenges it will bring, the GDPR represents a major opportunity to transform your approach to privacy and ensure your organisation is fit for the digital economy.

Is your business compliant and can you prove it?

Under a new principle of accountability, businesses will need to review and change their consent processes, processing notices, policies and procedures to reflect the law under the GDPR. It will no longer be enough to be compliant with data protection legislation, you will have to be able to demonstrate compliance with the GDPR principles.

The 6 other principles of GDPR

1. Lawfulness, transparency and fairness

The lawful basis on which the data is processed must be demonstrated fairly and transparently to the data subject.

2. Purpose limitation

Data should only be captured for specific and legitimate purposes.

3. Data minimisation

Personal data should be adequate and relevant.

4. Accuracy

Personal data should be kept up-to-date.

5. Storage limitation

Data should be kept no longer than necessary.

6. Integrity and confidentiality

Appropriate measures should be in place to ensure security of the data, including the prevention of unauthorised and unlawful processing to protect against accidental loss, destruction or damage.

What steps should companies take?

Having adequate procedures in place will reduce the risk of a company being caught out. Start by considering the following:

1. **Understand where your data is and how it is accessed** - who has access to it? Is it easy to delete? Is data well managed and well organised?
2. **Ensure data given to third parties is adequately protected** - you are likely to share data with clients, suppliers or partners regularly and therefore you should be aware of the risks. Any breach of the GDPR stemming from the sharing of data with third parties will be the company's responsibility.
3. **Use the GDPR to stand out from the crowd** - take clear steps to show customers and employees that you are taking the new regulations, and their data protection, seriously. Being transparent builds trust with your customer base and workforce.
4. **Improve data management and governance processes** - currently, how easily could you locate a piece of data on your systems? Under the GDPR you should be able to locate an individual's personal data instantly; not being able to do so could be a breach.
5. **Reduce data storage** - do you need all the data you currently hold? Consider removing old data or data that is no longer required. Removing irrelevant data will help to reduce the risk of data leakage.
6. **Manage consent** - individuals will be entitled to know exactly how their data is being used. Individuals can withdraw their consent at any time and systems must be in place to allow this to be actioned immediately.
7. **Cyber security** - ensure a strong cyber security system is in place to prevent any breaches of the GDPR.
8. **Appoint a Data Protection Officer (DPO)** - most organisations will need to appoint a DPO to act as a go between with the regulators. The DPO will also be required to maintain levels of privacy awareness within the company and monitor compliance.

The impact on corporate transactions

The importance of being diligent

Due diligence is a fundamental part of any corporate deal, in particular M&A transactions.

The due diligence process should place greater emphasis on a target company's internal data protection systems and processes, including compliance with the new GDPR.

The more onerous requirement relating to third parties should lead a buyer to check any contracts with suppliers and sub-contractors, which must also comply with the new regime.

Using the early stages of the M&A process to adequately examine and understand how a target company collects, stores, uses or transfers personal data will help to make an assessment of the risk involved in the transaction. There may also be existing data protection liabilities which will be inherited by the buyer following completion, including fines resulting from historic non-compliance. It may be necessary to consider a wider range of remedies than previously in order to protect the buyer, such as warranties and indemnities or a condition precedent seeking to address non-compliance at an early stage.

The buyer will also need to assess whether the target needs to appoint a DPO under the new regime.

Buyers' considerations

Post completion, buyers should be wary of the process of integration.

Integrating assets and data into an existing company can raise privacy and compliance issues. It is important to ensure that the data included in the business transfer can be used in the way intended by the buyer. This will likely require consideration of a substantial number of consents. The consent given, by clients and/or customers, to the target company may now need re-establishing if the way in which the data is to be used is changing. Under the GDPR, consent must be given positively, so a buyer must ensure effective processes are in place for this to be determined.

Following a successful deal, it is not unusual for a company to restructure its workforce or see a higher than average turnover of staff. The new GDPR will enable departing employees to demand that their personal data is removed from systems immediately. Appropriate processes must be in place to enable this to happen.

Corporate transactions in some sectors will require higher levels of data protection compliance. For example, those in the healthcare sector, big data businesses and businesses targeting children will need extra precautions to ensure the highly sensitive data held is not compromised.

Buyers will also need to understand what steps are necessary in order to ensure the target's everyday activities are compliant. Some companies will need to appoint a DPO. This is not currently a requirement under data protection law but the appointment of a DPO will become mandatory when the core activities of a business involve the 'large scale processing of sensitive data' or the 'regular and systematic monitoring of data subjects on a large scale' (such as online behaviour tracking or profiling, or the monitoring of employees by an employer). The DPO is responsible for ensuring the company's activities comply with the GDPR.

Companies also need to be aware of the broader rights introduced for individuals. It will be easier and more accessible to lodge a complaint against a company and receive compensation. Businesses need to be ready to deal with a likely increase in subject access requests.

The impact on corporate transactions

Sellers' considerations

The stricter controls on data processing mean sellers should try to limit the amount of sensitive data and personal information disclosed as part of a due diligence review.

Entering into non-disclosure agreements will also help to control access to personal data. If a due diligence investigation reveals that a target company does not adequately protect the personal data it holds then this could make the company appear less desirable to a potential investor, affecting the price and/or success of a deal.

Historically it has been common for companies involved in an M&A transaction to take limited risks with data protection requirements in order to get the deal done. Parties often agree to waive any potential problems due to the negative impact dealing with them can have on the sale process. For instance, a buyer's need to understand the target's workforce and customers may be seen to outweigh the risks of the unauthorised processing of that data that would be involved in the seller making it available to the buyer for review. However, the GDPR may force parties to reconsider their evaluation of the pros and cons of taking (or not taking) these risks for the sake of completing a deal.

Cybersecurity

Cybersecurity considerations are becoming more prevalent in all businesses following a spate of recent high profile cyber-attacks and the GDPR further enhances the importance of cybersecurity.

Cyber-attacks can compromise all of the data held by a company, whether it is personal or confidential. They can also reveal corporate secrets and release intellectual property. The costs of recovering from a cybersecurity attack can be substantial and there are also negative implications on a company's reputation and business operations.

Under the time constraints of a deal, many buyers can overlook cybersecurity considerations. A lack of adequate capabilities to prevent an attack can reduce the value of a target company as well as affect the viability of any transaction.

Also, newly acquired companies are often targeted as a route to their larger parent companies and any vulnerability in an acquired company can threaten the assets of the parent. The risks involved in a cybersecurity attack throughout a company could lead to a breach of data protection regulations, but it could go much further than that.

Preparing for GDPR may be at the bottom of the current to-do list for many companies, with matters such as Brexit or other sector specific regulations taking priority. However, despite the GDPR still being months away, it is crucial to plan for it now. Doing so will ensure a company can prepare and implement any new procedures and consider the impact on budgets, IT systems and employees.

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
- Ensure that GDPR is part of your business strategy.

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

Karen Anderson
Solicitor, Commercial

dt: +44 (0) 121 234 0293
karen.anderson@gateleyplc.com

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

Gateley Plc