**Data Protection: Corporate Transactions/Due Diligence**

This section considers the effect of the Data Protection Act 2018 and the retained version of the General Data Protection Regulation ((EU) 2016/679) on corporate transactions – and on due diligence in particular

**Introduction to data protection**

* **Information or data** is a key asset to any business or company.
* There are strict legislative provisions regulating the **use and transfer of data** by a UK entity.
* Compliance with **data protection legislation** is therefore of critical importance to the proper functioning of a business.
* Failure to comply could lead to **serious adverse consequences**.

**Data protection legislation**

The two key pieces of data protection legislation in the UK are:

* **UK GDPR** (see below); and
* **the Data Protection Act 2018 ('DPA'**)

The two pieces of legislation sit alongside each other: UK GDPR sets out the key principles and obligations and DPA supplements its application (e.g. by providing exemptions)

**UK GDPR:** since Brexit, an amended version of the  **General Data Protection Regulation (**EU) (2016/679) has been 'retained’ in the UK and applies to UK entities (and also to certain operations in the UK by non-UK entities).

The **Information Commissioner's Office ('ICO'**) is the statutory regulator responsible for monitoring compliance with UK GDPR and the DPA.  The ICO is a useful source of guidance on the application of the legislation.

The **Privacy and Electronic Communications Regulations (SI 2003/2426) (‘PECR’)** also supplement the data protection rules in areas such as electronic marketing, use of cookies and security/privacy of communications networks.

**Key Data Protection Definitions**

Set out below are some key definitions used in UK GDPR

‘**Personal data’** is any information relating to a data subject that identifies that person or makes them identifiable – for example, information such as birth dates and addresses could make a person identifiable.

A ‘**controller**’ is someone who decides the purposes and means of the processing of personal data.

‘**Processin**g’ is defined very widely and includes any operation or set of operations performed on personal data (including simply holding or deleting data).

A ‘**data subject’** is an identified or identifiable natural person to whom personal data relates.

A ‘**processor**’ is someone who processes personal data on behalf of a controller.

**Data Protection Principles**

All processing of personal data must comply with the six principles set out in **Art. 5 of UK GDPR:**

**Lawful and fair processing principle** -personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject**.**

**'Purpose limitation' principle** - data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

**'Data minimisation' principle** -  personal data must be limited to what is necessary in relation to the purposes for which the data is processed.

**'Accuracy' principle** -personal data must be accurate and, where necessary, kept up to date

**'Storage limitation' principle** - personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of the processing

**'Integrity and confidentiality' principle** - personal data must be processed in a manner that ensures appropriate security of the personal data

**Data protection – application to due diligence**

Vast amounts of information are made available to, and are transferred between, parties in a corporate transaction.

Where the transfer of information or data as part of a due diligence exercise is made by a UK entity, and where it includes personal data relating to a data subject, it will amount to **processing** by a **controller** and will be subject to the legislative framework which protects the rights of that data subject.

As a result, data protection and the relevant rights and obligations will need to be **considered by all parties throughout the course of a corporate transaction.**

Giving personal data to prospective buyers during due diligence will amount to ‘processing’ as 'controllers' by both:

1. the **seller** processing the information by providing it as due diligence; and
2. the **prospective buyer(s)** who receive such information and use it to carry out their due diligence investigation.

**Lawful and fair processing principle**

Both seller and each prospective buyer(s) involved in a share or business sale need to be aware of the **principles relating to processing of personal data (Art. 5 UK GDPR)**, as they will be directly responsible for their own compliance with these principles.

Principle 1 is that personal data must be **processed lawfully, fairly and in a transparent manner**.

In order to process data lawfully, it must satisfy one of the **legal processing grounds** in Art. 6 UK GDPR.

These grounds include: (i) where the data subject has **given consent to the processing (Art. 6(1)(a))**; and (ii) where the processing is **necessary for the purposes of the legitimate interests** pursued by the controller **(Art. 6(1)(f)).**

**Consequences of Breach** **Art. 83**

For breaches of other provisions, such as record keeping: The ICO can levy a fine of the higher of £8.7 million and 2% of the total worldwide annual turnover of the undertaking being fined.

For breaches of key provisions, such as the data provision principles or the data subject's rights: The ICO can levy a fine of the higher of £17.5 million and 4% of the total worldwide annual turnover of the undertaking being fined.

Data subjects also have a right to compensation for non-material damages, including distress (Art. 82(1))  
AND  
The reputational damage to a business can cause even greater issues.

**Legal processing grounds**

In considering which of these grounds they might rely on to share personal data during due diligence on a corporate transaction, the parties need to consider the following:

* The **legitimate interest condition** allows for disclosures which are in the legitimate interest of a controller or third party, providing that such interests are not overridden by the interests and fundamental rights and freedoms of the data subject which would require protection of that personal data.  This is the ground that is usually relied on in a corporate transaction – but the parties must actually **carry out and document** an assessment of (i) the purpose and necessity of the disclosure, and (ii) the balance of this against the individuals' interests (ICO Guidance) - so it cannot just be assumed.
* **Obtaining consent** from all employees/individual customers before completion of a confidential commercial transaction is impractical. The GDPR sets strict rules on what will constitute valid consent, including the need to show that consent has been freely given. This may also be difficult to show – particularly where there is an imbalance of power, e.g., in an employment relationship. It might be practicable in relation to senior employees/directors only.

**Application of other principles to due diligence**

* The second principle of processing data is the **'purpose limitation' principle (Art 5(b) UK GDPR).**

This requires that data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.  The parties must therefore consider if the sharing of data during due diligence is incompatible with the purpose for which it was collected: if the seller uses a well drafted privacy notice for employees/customers, this should refer to processing in respect of a potential sale.

* The third principle of processing data is the **'data minimisation' principle (Art 5(c) UK GDPR).**

This requires that the **minimum of personal data** necessary for the purpose should be shared.  For example, during due diligence, it is generally not necessary to share employee data in such a way that individuals (other than senior individuals) can be identified.

* The sixth principle of processing data is the **'integrity and confidentiality' principle (Art 5(f) UK GDPR)**.

This requires that data must be processed in a manner that ensures appropriate **security** of the personal data.  So due diligence information should be shared in a secure manner, and the seller should place obligations on the buyer(s) as to its security and confidentiality.

**Anonymisation/ Pseudonymisation**

Given the principles that apply to the sharing of data, a seller will generally seek to remove identifying information from data shared in relation to data subjects during a due diligence process.  Depending on how successful this is, it may either **anonymise or pseudonymise** the data:

* **Anonymisation**  
  If data is amended so that all personal identifying details are removed and the **recipient cannot re-identify** the data subjects from what they are given (for example, this would include deleting office location and/or department if there are fewer than 5 employees who would fall into that category), then the ICO's current position is that this information is anonymous in the buyer's hands – so it would no longer be personal data and would fall outside the provisions of UK GDPR.
* **Pseudonymisation**  
  Instead of removing all identifying details, data could instead just be amended to remove the obvious details (such as names and job titles).  Although UK GDPR would still apply to the information, this would act as a security measure, helping the parties demonstrate that they are ensuring data minimisation and also appropriate security for the data.

**Information Notices**

To comply with UK GDPR, controllers must also provide the data subjects with certain prescribed **fair processing information**. The required information is often provided by way of a **privacy notice**.

In particular, the data subject will need to be informed:

1. of the fact that their data will be **processed**, and
2. of the **purpose** for which their data will be processed.

This obligation will apply to both the seller and the buyer(s), creates issues for maintaining the confidentiality of the transaction.

If the seller uses a well drafted privacy notice for use when collecting data from employees/customers, this should already refer to **processing in respect of a potential sale**: in which case the data subject would already have the information.

As the buyer(s) will have obtained the data indirectly, they have up to a month to give the notification – or they may postpone notification until the transaction becomes public, relying on Art 14(5) UK GDPR, which applies where a notification would **'render impossible or seriously impair'** the objectives of the data processing.

**Target's data protection compliance**

In addition to complying with data protection provisions on the transaction, the buyer will want to carry out enquiries and investigations in relation to the target's compliance with data protection legislation as part of its due diligence exercise. Key actions points include:

* Checking the records of the target's processing activities.
* Requesting details of any material breaches of UK data protection legislation by the target.
* Seeking details of the target's dedicated data protection officers.
* Seeking confirmation that all consents have been obtained in respect of personal data used by the target.
* Requesting details of how personal data is collected.
* Requesting details of all data protection policies, systems and processes.

Some of the issues which may cause the buyer serious concern are:

* if the target has no data protection policies;
* if the target has been the subject of data protection complaints; or
* if there is evidence of mass marketing without consent.

**Data protection at completion of a transaction**

* On a **share sale**, only the shares will transfer and so the identity of the data controller (the target company) will not change. Therefore, **no additional processing of personal data** will occur.
* Data protection is therefore unlikely to be a further issue at the completion stage on a share sale
* On an **asset sale**, however, the **Transfer of Undertakings (Protection of Employment) Regulations 2006 (‘TUPE’)**require personal data about the employees to be transferred from the seller to the buyer at completion. Both the provision and the receipt of this information will amount to **processing**, so **both parties** will be under a duty to inform the employees that a new controller is now holding their personal data.
* In practice, it is enough for one party to inform the data subjects. It is normally the **buyer** who will do this. The seller will, however, want some assurance that this will be done - so the acquisition agreement will often include **an undertaking** that the buyer will inform all relevant data subjects of the transfer.
* You will learn more about TUPE in later Topics.

**Summary**

* The transfer of personal data relating to an identifiable living individual from seller to prospective buyer in a corporate transaction will be considered to be ‘processing’ by both parties as ‘controllers’.
* Care must therefore be taken by both parties to ensure compliance with the ‘lawful and fair processing’ principle – which requires either consent from the data subjects or, in most commercial transactions, demonstration of a legitimate interest.
* The seller is likely to aim to 'anonymise' the data provided, which may mean that the data is no longer subject to the data protection rules – but will in any case ensure that data is minimised and kept as secure as possible (in line with the other data processing principles).
* In addition, the data subject must be informed: (1) that their data will be processed and (2) the purpose for which it will be processed.  This may be delayed until after the transaction ceases to be confidential if the disclosure would seriously impair the purpose of the processing.