LEWIS SILKIN

Introductory guide to data sharing

LEWIS SILKIN

Executive Summary

Most organisations carry out some form of data sharing, whether it be data sharing between organisations within the group or with external third parties. However, if the data being shared by an organisation is "personal data", additional steps need to be taken to ensure the sharing of such personal data is lawful.

This guide covers some of the relevant issues to consider before entering into any data sharing arrangement to help ensure your arrangement is compliant with the data protection legislation in the UK.

For the purpose of this guide, any references to data sharing shall be references to the sharing of personal data.

Prior to any data sharing, it is important to establish:

a) the identity of and relationship between the parties (including whether the personal data is being shared between two or more data controllers , or between a data controller and a data processor , or between a data processor and a sub-processor);

b) the type of personal data being shared;

c) the legal grounds for sharing such personal data; and

d) where the relevant parties are based.

This is because different rules apply depending on whether the parties are data controllers or data processors, where the parties are located and sectors in which the parties operate.

Legal backdrop

The principal piece of data protection legislation in the UK covering the sharing of personal data is the Data Protection Act 1998 (DPA).

Under the DPA, all legal responsibility for compliance with the DPA, including compliance with the rules relating to data sharing, rests with the data controller and not with the data processor. However, the DPA is being repealed and replaced with the General Data Protection Regulation (GDPR), a piece of European legislation, with effect from May 25, 2018 (despite the Brexit decision in the UK referendum). The GDPR will impose new obligations directly on data processors (which are set out in more detail below).

The Information Commissioner's Office (ICO) has published a code of practice that covers data sharing across and between organisations "ICO – Data Sharing Code of Practice" (Code). Whilst the Code is not legally binding, it is intended as best practice guidance for compliance with the DPA, and it is worth noting that this is a statutory code and the ICO, courts and tribunals can take account of compliance with the Code. We recommend that the Code should be consulted before structuring any data sharing arrangement.

Types of data sharing arrangements

There are three main types of data sharing arrangements:

a) sharing data between a data controller and data processor;

b) sharing data between a data controller and data processor; and

c) sharing data between a data processor and a sub-processor.

Depending on the type of data sharing, certain formalities need to be met.

Sharing data between a data controller and data processor

The DPA requires data controllers to have a written data processing agreement in place with any data processor. Such data processing agreement must provide, at a minimum that the data processor shall:

a) comply with the instructions of the data controller; and

b) have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction, or accidental loss, alteration, unauthorised disclosure or access, and provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

This can either be a stand-alone data processor agreement or be in the form of data processing clauses that form part of a wider agreement between the parties.

In addition to the "bare minimum", a data controller should seek to include additional data provisions within the data processing agreement, over and above those which are required by the DPA.

Such provisions may include obligations to ensure data protection obligations are passed down the chain to any subcontractors of the data processor (i.e. sub-processors), obligations to assist the controller with any data breaches and with any requests by data subjects to access their personal data. Data controllers should also look to include an obligation on the data processor not to do anything that might put the data controller in breach of its obligation under the DPA (although most data processors would look to resist such an obligation).

The GDPR sets out more prescriptive requirements of what should be in a data processing agreement between data controllers and data processors. Data controllers may want to review their current and future data sharing agreements with processors to ensure that all these prescriptive requirements are covered. For example data processors are now required to:

a) maintain written records of all processing activities carried out on behalf of a data controller;

b) obtain the data controller's consent to the appointment of a sub-processor; and

c) co-operate with the data controller in the performance of its obligations under the GDPR (including notifying the data controller of a personal data security breach without undue delay).

Further as data processors will have direct liability under the GDPR, it is in the data processors' interest to ensure that it is also protected in any contract with a data controller against any liability it may incur as a result of an act omission of a data controller.

Data sharing between data controllers

There is no obligation under the DPA for there to be a written agreement between data controllers in respect of data sharing. However, it is highly advisable for one to be put in place (even if the data is being shared by intra-group organisations) so that liability for failing to comply with their obligations under the DPA is apportioned appropriately. Further, setting out in writing the data sharing arrangement between data controllers helps ensure that the respective roles of each of the parties is appropriately articulated to avoid a situation whereby one party is seen as a controller and the other is seen as a data processor. These written agreements are often referred to as data sharing agreements or data sharing protocols.

A data sharing agreement between controllers should contain similar provisions to that of a data processing agreement (although it should be very clear in any data sharing agreement between controllers that each party will be determining the manner and processing of any personal data either jointly together or as controllers in common). For example, it makes sense for one of the parties to be nominated to deal with individuals requiring access to their personal data. The parties should also include cross-indemnities, whereby the party in breach of the legal or contractual data protection provisions reimburses the other party for any losses it may suffer as a result of the breach. Breaches could include, for example, misuse of data, failures in security, loss of data and poor procedure.

The Code also sets out the points that should be covered by a data sharing agreement between controllers including:

a) setting out the purpose of the sharing;

b) the data to be shared;

c) the basis of the sharing;

d) limitations on recipients of the shared data;

e) data quality, security and retention; and

f) practical governance.

Data sharing between processors and sub-processors

Similar to data sharing arrangements between data controllers, there are currently no statutory requirements to have a written agreement in place between a data processor and a sub-processor (although this will change under the GDPR). However, a data processor should always insist on having a written agreement in place with a sub-processor to back up the assurances it gives to the data controller under the data processing agreement and indeed the data processor may find it has agreed a contractual obligation to have a written agreement in place with any sub-processors.

Prior to entering into any data sharing agreement with a sub-processor, a data processor should always check whether the relevant data controller's consent needs to be obtained before sharing such data and whether there are any other contractual requirements imposed on it by the data controller in respect of the sharing of personal data between the processor and the sub-processor. Equally, a sub-processor should seek appropriate comfort from the data processor that all necessary consents have been obtained.

Lawful basis for data sharing

Both parties involved must take into account whether the data sharing meets the requirements of the eight data protection principles under the DPA.

In particular, any data sharing must be fair and lawful. This means that the data subject must be aware of the data sharing (this is usually achieved by way of a fair processing notice), unless an exemption applies and the parties sharing the data must have a clear legal basis for sharing data in the first place (e.g. legitimate interest of the data controller or with the consent of the data subject). Without a legal basis, the data sharing will not be lawful. Where considering whether a lawful basis for the data sharing exists, the parties will need to think about the type of personal data is being shared. For example if sensitive personal data is being shared, the scope of legal basis for data sharing is more narrowly con.

Irrespective of the types of personal data being shared, the parties should always think carefully prior to any sharing of personal data about the risks of such data sharing p and consideration should be given as to whether the parties' objectives can be achieved without sharing personal data (i.e. by redacting or anonymising the data).

Any data sharing arrangements should be reviewed regularly to verify that there is still a lawful basis for data sharing.

There may be other laws and regulations that should be considered before entering into a data sharing agreement such as the law of confidence and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended). Further there may also be sector specific laws regarding the sharing of personal data. By way of example, the banking sector has strict requirements on data sharing. The public sector can also only share personal data if it is within its statutory power to do so. Other relevant laws include compliance with human rights legislation and with the Freedom of Information Act 2000. (The latter is also relevant for businesses that share personal data with a public body).

Location

In any data sharing arrangement consideration should be given to the location of the data, the relevant data subject and those sharing the data. In particular, if personal data is being shared by UK data controller to another controller or process located outside of the EEA in a country that is not consider to have adequate levels of protection for the rights of data subjects by the EU Commission, additional measures may need to be put in place to ensure the transfer of data is lawful.

Further, if you are receiving personal data from a data controller located in another European jurisdiction, additional local law restrictions may apply to the data sharing arrangement (e.g. Works Council restrictions may apply to sharing of European employee personal data).

LEWIS SILKIN

Getting it Wrong

Unlawful data sharing can have huge consequences. At the time of writing, the ICO can impose a fine of up to £500,000 for a serious breach of the DPA. However, once the GDPR comes into force, a data controller or processor may be fined up to €20,000,000 or 4% of its global annual turnover for the previous year, whichever is the highest.

Further unlawful data sharing can lead to bad publicity and its adverse impact on brand value, consumer confidence and business profit, all of which should not be underestimated. Cases surrounding data investigations and breaches have become headline news stories in recent years – just ask Talk Talk!

Jargon Buster

Data controller:	the person determining the manner and the purpose in which personal data is processed
Data processor:	the person (other than an employee of the data controller) processing personal data on behalf of the data controller
Sub-processor:	the person (other than an employee) appointed by a data processor to carry out data processing activities on behalf of the data processor
Sensitive personal data:	personal data consisting of information as to: a) racial and ethic origin of the data subject; b) political opinions; c) religious beliefs; d) trade union membership; e) physical or mental health; f) sexual life; g) commission or alleged commission of offence; or h) court proceedings

For further information, contact:

Olivia Savage
Managing Asscoiate

+44 (0) 20 7074 8231
olivia.savage@lewissilkin.com

Bryony
Senior Asscoiate

+44 (0) 20 7074 8435
bryony.long@lewissilkin.com

LEWIS SILKIN

5 Chancery Lane – Clifford's Inn
London EC4A 1BL
DX 182 Chancery Lane
T +44 (0)20 7074 8000 | **F** +44 (0)20 7864 1200
www.lewissilkin.com