Data Protection Due Diligence in Transactions FAQs

Date : August 23, 2021

Introduction

Data protection/privacy rules play a prominent role in merger and acquisitions transactions. The degree of data protection compliance in a transaction could have an effect on the final price or even make or break a deal, or lead to unwelcome surprises later on.

The ICO's enforcement case against Marriott International Inc. where in 2020 it imposed a fine of £18.4 million for a 2014 data breach affecting Starwood Hotels and Resorts Worldwide Inc. which Marriott had acquired in 2016 is a case in point, which we've written about here https://www.corderycompliance.com/ico-fines-marriott-for-data-breach/. Although the ICO specifically stated about that case that it was not making any infringement finding about the acquisition and even said that "there may be circumstances in which in-depth due diligence of a competitor is not possible during a takeover" an inescapable takeaway about this case is that there is no option but to take data protection due diligence seriously in a transaction.

These FAQs set out some of the data protection issues that should be considered in a transaction – they are by no means exhaustive.

What is meant by data protection compliance aspects in a transaction?

Generally-speaking there are two broad aspects to data protection compliance in transactions:

- What data protection compliance policies, procedures and processes the target business has in place; and,
- Ensuring data protection compliance as part of the actual transaction process itself.

Is this an ongoing process during the transaction?

Yes – it is a moving target. There will inevitably be a mass of personal data involved in every stage of a transaction, including customer and employee data – the further the general due diligence goes the more personal data will likely be handled. This can't be ignored or downgraded in the due diligence process and important decisions will have to be made from the start and along the way, especially about what can be shared and if shared what compliance protection measures to put in place.

What should I do first?

The initial things the seller should consider determining include the following:

- What personal data it has and where it lives;
- That its privacy policies etc. provide adequate notice that personal data can be disclosed in a transaction;
- The lawful basis on which personal data can be disclosed in a transaction, both as regards "regular" personal data and sensitive (special category) personal data;
- If the transaction is likely to result in a high risk to the rights and freedoms of data subjects, the seller will also need to carry out a Data Protection Impact Assessment before providing the personal data; and,
- What it can put in place to protect personal data (e.g. redaction, anonymisation & pseudonymisation etc.) that may be shared as part of the transaction, which should also be set out in the relevant transaction agreement.

The initial things the potential buyer should consider determining include the following:

- What investigation it needs to do of the target group business' data protection compliance;
- When thinking ahead about the negotiations about the relevant agreement, what warranties and

indemnities to possibly put in place; and,
- Thinking ahead about planning post-completion migration and integration of the personal data acquired with its own IT systems and data protection arrangements.

Are there any considerations for the data room?

Putting material with personal data in it into a data room will need to be done with the following data protection considerations in mind:

- Probably the top priority is to ensure that personal data is held as securely as possible – a data room is a hacker's dream. The seller will need to ensure that it has a Data Processing Agreement with the organisation that is hosting the data room, i.e. to ensure the security of the personal data during the due diligence process, and also to ensure the return or destruction of the personal data after the due diligence process is complete;
- Only share with those with whom the personal data needs to be shared, i.e. put in place access controls. Persons accessing the data room should be bound by non-disclosure confidentiality obligations;
- Only share what personal data is necessary for the purpose of doing the transaction (purpose limitation);
- Only share the amount of personal data that needs to be shared (data minimisation);
- Pay special attention in all instances to sensitive/special category data as a higher standard applies in this area; and,
- Where possible, either pseudonymise, redact or (more difficult) anonymise personal data.

What questions should the proposed buyer be asking?

The proposed questions the potential buyer should consider asking include the following questions (and also request copies of documents where appropriate):

- Are there any data protection registrations with, and/or payment of any data protection fee to, any data protection regulators?
- What categories of data subjects are there whose personal data is processed by or on behalf of the business (e.g. employees, customers, suppliers, job applicants etc.)?
- What categories of personal data and sensitive personal data are processed by or on behalf of the business (e.g. health data etc.)?
- Does the business process criminal offences data?
- What data protection or privacy notices, processes and procedures are used by the business for data subject rights and requests (e.g. Subject Access Request procedure etc.)?
- What processes does the business have to deal with data breaches (Data Breach policy etc.)?
- Has the business had any data breaches?
- What policies, processes or procedures does the business have governing the Technical and Organisational Measures implemented for the security of personal data processed by the business (e.g. concerning physical access controls, anonymisation, pseudonymisation and encryption etc.)?
- Has the business had any compensation claims from individuals concerning data protection infringements (e.g. data security breaches)?
- Has the business been subject to any investigations and/or enforcement action from a data protection regulator?
- What data retention materials does the business have (e.g. Retention Schedules etc.)?
- What data protection consents does the business have (e.g. for sending marketing materials etc.)?
- Does the business have any IT systems used for automated decision-making purposes which involve decisions which significantly affect individuals?
- Has the business carried out any Data Protection Impact Assessments?
- Has the business carried out or been subject to any data protection or cyber security audits?
- What third parties process personal data on behalf of the business and what data processing agreements does the business have in place in such cases?
- What international data transfer processes and arrangements does the business have in place (e.g. Standard Contractual Clauses etc.)?

- Does the business have a Data Protection Officer?
- Does the business have any Data Protection Representatives and if so does the business have any agreements in place with them?
- Does the business undertake any monitoring (including intercepting, blocking, recording or otherwise accessing) of data subjects' personal data through the business' systems (computer networks, CCTV/surveillance, email, phones etc.)? And,
- Does the business have any cyber insurance policies?

What about international data transfers?

Where personal data is going to be transferred internationally, such as where the server holding the data room information, or the buyer, is located outside the EEA or outside the UK the appropriate safeguards and mechanisms will need to be in place such as Standard Contractual Clauses, unless an Adequacy Decision applies.

What about security?

The buyer will need to ensure that its systems (and any legacy infrastructure) are adequately secure to protect any personal data it receives under the sale – this is of crucial importance. The potential buyer should therefore consider doing due diligence and a risk assessment on the seller's systems and the incorporation of the seller's personal data into the potential buyer's systems and closely look at the potential seller's legacy systems (if there are any) and look for any historic issues that could pose risks.

What about hard copy data?

Personal data in hard copy is still personal data and so data protection rules still apply. So don't overlook reviewing hard copy documents such as those in a disclosure bundle and applying appropriate measures such as redaction.

What about warranties and indemnities?

Where possible, the buyer will likely want to consider ensuring, that an agreement (share or asset purchase) has suitable warranties and indemnities, for example, including:

- A warranty that employee personal data, sensitive data and criminal offence data has been processed in accordance with the seller's policies and privacy notices;
- A warranty that there have been no employee grievances or complaints relating to data protection issues;
- An indemnity in respect of any data protection liability with regard to a pre-completion breach; and,
- Specific warranties and indemnities to cover any gaps or deficiencies that come up in the due diligence process.

What about completion?

The target or asset may need to be integrated into the buyer's business *between* exchange and completion. In this case consideration will need to be given as to how to best deal with personal data, e.g. through anonymisation or redaction.

Where the sale is of an asset the identity of the data controller will change, so the potential buyer will need to consider informing affected individuals accordingly through a privacy notice. The seller may need to consider agreeing a pre-completion undertaking with the potential buyer to ensure that the potential buyer will undertake implementing such a policy.

What about post-completion?

Both the seller and the potential buyer will need to consider whether there will be a change in the purpose or use of personal data as a result of the transaction. If there is, both will need to consider changing their privacy policies to

reflect any new purposes.

The potential buyer should consider checking to ensure that after the sale any international transfers of personal data are protected through appropriate safeguards such as Standard Contractual Clauses. The potential buyer should consider determining how long it should be retaining personal data that it has received under the sale. The potential buyer should ensure that it documents everything that it does with the personal data.

The seller should close the data room as soon as possible following completion.

What if the deal doesn't happen?

If the deal doesn't go ahead, the unsuccessful buyer will need to return to the unsuccessful seller, or destroy, personal data received as part of the due diligence process and, where destroyed, the unsuccessful seller should confirm or provide evidence of such destruction. This should be agreed at the start of the due diligence process.

Do I need to show compliance?

Yes. You'll need to demonstrate that during the transaction you have complied with data protection compliance (accountability) – note this e.g. in a log.

Are there any other particular situations to consider?

Yes – TUPE transfers. When a business changes owner, its employees may be protected under the so-called "Transfer of Undertakings Protection of Employment Regulations", or TUPE. Whilst much of what has been said above may apply to a TUPE transfer there are also additional TUPE-specific issues to address too so consider drawing up a specific TUPE data protection action plan.

Is there any regulatory guidance?

The ICO has issued guidance on TUPE transfers entitled "Disclosure of employee information under TUPE" (https://ico.org.uk/media/for-organisations/documents/1063/disclosure-of-employee-information-under-tupe.pdf) although it hasn't been updated in line with the UK Data Protection Act 2018 and UK GDPR. The ICO's "Employment Practices Code" also has some brief guidance about disclosing information about workers in a merger, acquisition or business re-organisation (https://icosearch.ico.org.uk/s/search.html?query=employment+practices+code&collection=ico-meta&profile=_default) although this too hasn't been updated in line with the UK Data Protection Act 2018 and UK GDPR. Further, the ICO has also set out due diligence considerations for when sharing data following mergers and acquisitions in its "Data Sharing Code of Practice" (https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/data-sharing-a-code-of-practice/due-diligence/).

Always bear in mind though that guidance is only guidance – the courts have the last word!

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the security aspects of GDPR in paper and on film;
- A template data breach log;
- A template data breach plan; and,
- A template data breach reporting form.

For information about our Breach Navigator tool please see here: https://www.corderycompliance.com/solutions/breach-navigator/

We report about data protection issues here: https://www.corderycompliance.com/category/data-protection-privacy/.

For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/ and our Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary.

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com