BCLP. Client Intelligent

Insights

DATA ISSUES WHEN ACQUIRING ASSETS FROM AN INSOLVENT VENDOR

12 November 2020

Recent M&A deals the teams have worked on involving insolvent corporates have highlighted the challenges which exist around the transfer of customer lists and databases, which are often a significant asset for the buyer.

Transactions involving insolvent corporates are typically structured as business and asset sales, rather than share transfers; as such there will always be a change to the "controller" of any personal data contained in customer lists; this in turn engages the requirements of the General Data Protection Regulation ("GDPR") and, specifically in relation to direct marketing by email or SMS, the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR").

It is also customary in sales arranged by insolvency practitioners that the seller will not provide any representations or warranties in relation to its compliance with data protection legislation including any previous security breaches (and W&I coverage for these types of risk is unlikely to be available). It is therefore incumbent on the buyer to be satisfied with its own due diligence and assessment of the risks and any potential liability, before proceeding with the acquisition. As well as assistance in spotting the red flags, the BCLP Data Privacy & Cyber Security and Restructuring & Insolvency teams are able to help clients assess the associated risks and how best to protect against them.

We have summarised below some of the key issues and points to be aware of in this context.

Is the seller's transfer of data compliant with the GDPR?

- The seller will usually be a "controller" of the personal data (including customer data) for the purposes of the GDPR and the Data Protection Act 2018. Increased obligations exist if the data being transferred implicitly and/or explicitly includes "special category" personal data under the GDPR (which includes data concerning a person's health, racial or ethnic origin, political opinions and genetic and biometric data). The sale of the customer database represents a transfer of personal data by the seller to the buyer – that of itself is a processing activity.
- The GDPR requires controllers of personal data to act "fairly, lawfully and in a transparent manner" in relation to individuals (Article 5(1)(a)). Articles 13 and 14 of the GDPR require

controllers to provide certain information to individuals whose data they process; this is commonly achieved through the publication of a privacy policy/notice. Article 6 requires a controller to be able to identify a lawful basis for any processing of personal data that it undertakes, including a transfer by a buyer to a seller of a customer database.

- Consideration of the seller's privacy policy will be relevant - it may (helpfully) contemplate certain types of corporate reorganisation involving the seller; however, this is only one factor. A proposed transfer of data from the seller (as controller) to a buyer can fall foul of the GDPR unless certain requirements are met.

In our experience, a risk-based approach to GDPR compliance will be necessary, particularly in relation to a corporate transaction involving an insolvent seller. The approach varies from transaction to transaction. Recent deals have included situations where the seller has experienced data security breaches, has received high volumes of data subject access requests and/or is facing complaints about its data handling. As well as the levying of substantial fines by the Information Commissioner's Officer ("ICO"), a seller may be facing data class action claims being brought in the UK on behalf of large numbers of affected individuals.

Can the buyer use the data for direct marketing?

- Direct marketing will often be a key part of revenue generation for the business (particularly if the business is consumer facing). The buyer's ability to carry out direct marketing to consumers lawfully following completion using the acquired database should therefore be investigated at the outset of the transaction. Direct marketing communications are regulated under the GDPR and, in the case of electronic mail (i.e. email and SMS) sent to "individual subscribers" (which broadly means individuals in their personal capacity), the PECR also apply.

- The PECR provide that unsolicited communications by means of electronic mail may only be carried out where (a) the individual has consented to this or (b) a form of implied consent (the so-called "soft opt-in") applies.

- In order for consent to be validly obtained, the ICO has stated that "any third party controllers who will be relying on the consent must be named". This puts the buyer in a challenging position: it cannot simply rely on consents previously obtained by the seller for the purposes of the seller's own electronic marketing. This is also the case for the "soft opt-in", as the ICO has made clear in their guidance that the soft opt-in "can only be relied upon by the organisation that collected the contact details", i.e. the seller.

- There are workarounds that can be adopted as part of the acquisition, but these will rely on the cooperation of the proposed insolvency practitioners and, if solutions can be agreed, the buyer should expect to fully indemnify the seller and the insolvency practitioners for any liability they may incur as a result. There are also approaches to mitigate risk which can be taken by the

buyer following the acquisition of the data (but before it is used for any direct marketing purposes), which can be implemented after closing.

The BCLP Data Privacy & Cyber Security and Restructuring & Insolvency teams would be happy to discuss any questions you may have regarding the matters described in this note.

RELATED PRACTICE AREAS

- Restructuring & Insolvency/Special Situations
- Special Situations Team
- M&A & Corporate Finance
- Data Privacy & Security

MEET THE TEAM

Andrew Hart

Co-Author, London

andrew.hart@bclplaw.com
+44 (0) 20 3207 1148

Kate Brimsted

Co-Author, London

kate.brimsted@bclplaw.com
+44 (0) 20 3400 3207
