



CORPORATE AND COMMERCIAL

Data Protection Considerations for Liquidators

by Jane O'Grady, Clare Dowling, Jill Callanan, Jeanne
Kelly

Data Protection Considerations for Liquidators

23rd October 2020 | by Jane O'Grady, Clare Dowling, Jill Callanan, Jeanne Kelly

Most companies now hold large volumes of personal data – it is almost inevitable due to the interplay between technology and business. This includes companies that become insolvent, but what obligations does a liquidator have in relation to the personal data held by a company?

In data protection law, any party that holds or uses personal data is either a “controller”, a “joint controller” or a “processor”, of that personal data. The concepts of “controller”, “joint controller” and “processor” are crucial to determining a party’s legal obligations in relation to the personal data it holds and uses, and to assessing potential liability where an individual’s rights are infringed.

The terms “controller” and “processor” are defined in the General Data Protection Regulation (GDPR). In September 2020, the European Data Protection Board (EDPB) which is the body responsible for data protection at an EU level, published draft guidelines on the concepts of controller, joint controllers and processor. In a nutshell, a “controller” determines the purposes and means of the processing, i.e. the why and how of the processing whereas a “processor” processes personal data on behalf of the controller.

- Two basic conditions for qualifying as a processor exist: that it is a separate entity in relation to the controller and that it processes personal data on the controller’s behalf.
- In some circumstances, multiple entities may be joint controllers of the personal data. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in determining the purposes and means of a data processing operation. The EDPB has stated in its draft guidelines that joint participation can take the form of a common decision taken by multiple entities or result from converging decisions by two or more entities, where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing.

The role of a controller is legally more onerous because they are required to comply with the full scale of obligations arising under the GDPR. In contrast, processors’ legal obligations are much more limited under the GDPR. To a certain extent parties may contractually allocate responsibility as to whether the controller or the processor carries out mandatory data protection obligations but, as discussed further below, there is a risk that the courts and regulators will reject the validity of such contractual provisions.

Controller or processor: What is a liquidator’s status?

An insolvent company can be a controller as long as it remains in existence without being dissolved. However, once appointed, a liquidator has a duty to take custody and control of all the assets of the company. This will include any assets containing personal data such as databases, customer lists, customer accounts and marketing lists. The determination of whether a liquidator is a processor or controller of that personal data will depend on the nature of the role the liquidator is exercising and to what extent, if any, the liquidator decides why that personal data is processed.

The liquidator as a processor of personal data

In Ireland, where a liquidator is acting as agent of the distressed company for business continuation, it is

likely that the liquidator will be a processor of the personal data on behalf the company. In those circumstances the company as controller will continue to be responsible for the personal data it holds.

This position has been adopted by the English courts in *Re Southern Pacific Personal Loans Limited* [2013] EWHC 2485 (Ch), which ruled that in the same way that directors are not the controllers (because they act as agents of the company), a liquidator is not regarded as a controller in respect of personal data processed by the company.

The Irish courts have yet to rule definitively on the role of liquidators under data protection law. In *In the Matter for Mount Carmel Medical Group (South Dublin) Ltd (In Liquidation)* [2015] IEHC 450, the Irish High Court considered the decision in the *Southern Pacific* case but it did not rule on the issue because on the facts of that case, it was not disputed that the insolvent company was the controller of certain medical records. The issue before the High Court in *Mount Carmel Medical Group* was whether the transfer of the statutory role of controller in relation to those medical records to another entity, by way of a contract was permissible under data protection law. It is noteworthy that in *Mount Carmel Medical Group*, the Data Protection Commission (DPC) supported the granting of the declaration sought by the liquidators to transfer controllership of personal data from one company to another company. Notwithstanding this, the question of whether liquidators are controllers or processors remains unanswered by the Irish courts or by the DPC.

In addition to the *Southern Pacific* case, last year the English High Court in *Green v. Group Limited Covid-19* confirmed that administrators and liquidators are not controllers of personal data held by an insolvent company. This case is significant because it was decided after the GDPR became law. Due to our similar legal systems, it remains to be seen whether the case law of the English courts will prove persuasive when the courts in this jurisdiction rule on this question.

Even where a liquidator is a processor of the company's personal data, it will have an ongoing duty to ensure that the company complies with the GDPR and the Data Protection Acts 1988 to 2018. Since liquidators step into the shoes of directors as agents of insolvent companies, under section 146 of the Data Protection Act 2018 they may be liable for offences committed by the company under that Act.

The liquidator as the controller of personal data

Where a liquidator processes personal data in connection with the performance of functions unique to its role, it is likely that the liquidator does so as a controller of that personal data. There are a number of key compliance measures that a liquidator will have to adhere to when it processes personal data as either a controller or a joint controller with the company to avoid falling foul of data protection law. Liquidators should be cognisant that as controllers of company data, they may be held civilly and criminally liable for failure to comply with data protection law. The obligations of a liquidator, as controller include:

Establishing valid legal basis

Where a liquidator processes personal data as a controller, it cannot simply process personal data because it wishes to do so. It can only process personal data if it first establishes one of the legal bases set out in Article 6, and when dealing with special category personal data, a second lawful condition under Article 9 of the GDPR.

Having established that a legal basis under Article 6 for processing personal data applies, before processing special categories of personal data, a liquidator will also need to ensure that a specific condition for processing special categories of personal data applies. There are ten lawful bases that may apply to special categories of personal data; these are set out in Article 9 of the GDPR.

Establishing a valid legal basis under Article 6 and, where necessary, under Article 9, applies to all processing activities where a liquidator is controller. This includes what legal basis is valid to sell customer and marketing assets and to process personal data gathered as a consequence of a liquidator's appointment.

- Carrying out DPIAs. If in the course of carrying out their functions as liquidator, a new processing operation is applied to a company's personal data or it becomes evident that a processing operation (meaning any activity that includes processing personal data) that is modified is likely to present a

high risk to the rights and freedoms of individuals, having regard to its nature, scope, context and purposes, a liquidator as controller must ensure a data protection impact assessment (DPIA) is carried out.

- Contract issues. Where a liquidator enters into any contracts with third-party suppliers vendors such as secure asset-disposal providers, it should ensure that those contracts include the processor obligations mandated by Article 28 of the GDPR.
- Furthermore, a liquidator should exercise extreme caution prior to sharing any personal data with claims management providers and should not do so unless they have established a valid legal basis for such data sharing. Liquidators should remember that they cannot contract out of their obligations as a controller or those of the insolvent company by transferring them to another entity, because this tactic has been invalidated by the Irish courts in the Mount Carmel Medical Group case. In that case, Keane J. held the legal significance of the term “data controller” derives from the legal relationship it connotes between controllers and data subjects. The term has no meaningful application to the relationship between a controller and a third party.
- Compliance with data subject rights. Liquidators must comply with requests from data subjects exercising their data protection rights in accordance with GDPR requirements and within statutory deadlines. This obligation applies regardless of whether the request is made prior or subsequent to a liquidator’s appointment. The ability and freedom of data subjects to exercise their rights was central to the High Court’s refusal to transfer controllership from Mount Carmel Hospital to St James’s Hospital in the Mount Carmel Medical Group case. Keane J. ruled that there was "a clear danger of overlapping and unworkable jurisdictions" if he granted the declarations sought because to do so would deprive data subjects of any meaningful right to make a complaint to the DPC concerning Mount Carmel Hospital’s processing of their personal data.

Conclusion

Regardless of whether liquidators act as controllers or processors when processing personal data held by an insolvent company, they must demonstrate ongoing compliance with data protection law. To assist them in this regard, liquidators should follow a few practical steps.

- At the outset of their appointment, liquidators should establish a system for the active management and governance of data. They should ascertain the status of personal data held by the company because this may be pivotal in determining the company’s compliance with data protection law and mitigating against fines, civil claims and criminal prosecution.
- As part of their management of company data, liquidators should maintain a subject access register and ensure personal data is securely held and if necessary restrict who has access to it.
- It is equally important to ensure that any person a liquidator is responsible for is trained on data protection requirements and knows the policies and processes to follow in the event of a data subject request or a data breach.

These are very pertinent and topical matters for liquidators given that most retailers offer an online shopping experience and commercial businesses are increasingly facilitating online business trade, all resulting in the handling of personal data. Specialist legal advice regarding that data handling is recommended to ensure liquidators are fully aware of the extent of their data protection obligations in the carrying on of their duties.

Details for Jane O’Grady at jogrady@lkshields.ie, Clare Dowling at cdowling@lkshields.ie, Jill Callanan at jcallanan@lkshields.ie or Jeanne Kelly at jkelly@lkshields.ie.

About the Authors



Jane O'Grady
Associate Solicitor

Jane is dual qualified as a solicitor and a trade mark and design attorney, with many years private practice and in-house experience advising on commercial contracts, intellectual property, commercial agency and all aspects of technology law.

T: +353 1 637 1554 E: jogrady@lkshields.ie



Clare Dowling
Associate Solicitor

Clare practises in commercial litigation, specialising in corporate insolvency and restructuring and commercial disputes.

T: +353 1 637 1532 E: cdowling@lkshields.ie



Jill Callanan
Partner

Jill advises on all aspects of commercial litigation and dispute resolution specialising in insolvency and corporate recovery.

T: + 353 1 637 1551 E: jcallanan@lkshields.ie



Jeanne Kelly
Partner

Jeanne is a partner in our Intellectual Property, Technology and Privacy team. She advises public and private clients in relation to technology law and data privacy law.

T: +353 1 637 1530 E: jkelly@lkshields.ie