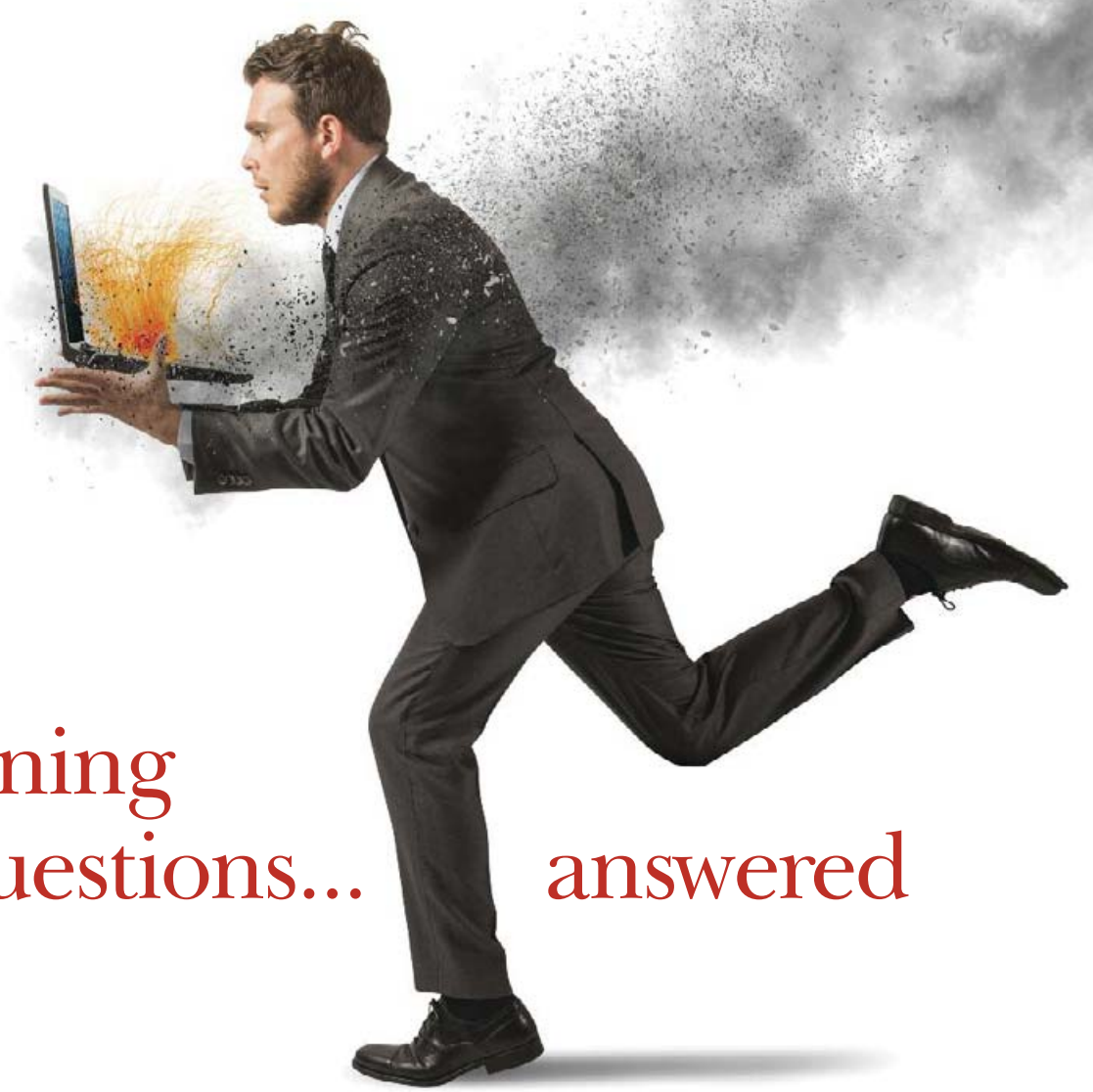

Your burning GDPR questions... answered

Annabel Gillham and **Mercedes Samavi** have been listening to IPs voice their GDPR concerns and have come back with some key guidance.

The GDPR is now in effect, as of 25 May, but – as many readers will know – this is just the beginning. Many companies and firms may have already put in place the initial framework for the new data protection regulation, but insolvency in the UK is a highly specialised area with its own challenges, and IPs are asking fundamental questions about their role and relationship with insolvent companies in the light of data protection and its related requirements.

> **An agent IP will have an ongoing duty to ensure that the company complies with all applicable laws (including the GDPR).**

In this article, we deal with the questions that have dominated the conversation among IPs in the run-up to the GDPR's implementation.

Am I a data controller or a data processor?

Where the IP is appointed as a liquidator or administrator and acts as the company's agent, the company (not the IP) is data controller of company data, and so the responsibility for company data still lies with the company. That position (following the case of *Re Southern Pacific*[1]) does not change under the GDPR. Nevertheless, an agent IP will have an ongoing duty to ensure that the company complies with all applicable laws (including the GDPR). Where an IP is acting as principal (for example, a trustee in bankruptcy where the bankrupt's assets vest in the trustee), the IP will likely be the data controller in respect of personal data processed in the business/estate. IPs will also be data controllers in respect of practitioner data, which will include creditor data (such as creditor claims and proofs of debt), internal marketing lists, records of appointment (including personal data on directors) and data used in court proceedings specific to IPs (eg to set aside preferences or transactions at an undervalue).

What are my registration requirements?

Heads up: the registration requirements for the Information Commissioner's Office (ICO) have changed under a new payment model, which is underpinned by the Digital Economy Act. Data controllers are still obliged to pay the ICO a fee, depending on the size of their organisation, however there is no longer a requirement to provide the ICO with details of the processing activities.

> **Trustees in bankruptcy should be aware that they could well be held responsible for failure to comply with the GDPR as a controller of company data.**

You should register with the ICO as a data controller of practitioner data. In addition, any company or sole trader for which you are appointed as liquidator or administrator should maintain a registration with the ICO – at least for as long as the business continues to trade.

What documents should I provide to individuals when I am appointed?

Privacy notices. For any individual whose personal data you handle as data controller (such as individual creditors, company directors or bankrupts), you should provide him or her with a notice, setting out (among other things):

- Who you are.
- What personal data you hold on him or her.
- Why you are processing his/her data, and on what lawful basis under the GDPR.
- Whether you are disclosing his/her data to any third parties, or making any cross-border transfers.
- That individuals can exercise their rights over their personal data (eg the right to access data or the right to be forgotten).
- How he/she can contact you if they have any questions or objections to your processing activities.

> **Data controllers are still obliged to pay the ICO a fee… however there is no longer a requirement to provide the ICO with details of the processing activities.**

Service provider contracts. If, in your capacity as a data controller, you are entering into any contracts with third-party vendors, such as payroll providers or secure asset-disposal providers, you should make sure that you incorporate the GDPR's article 28 processor obligations into the contract; this is a requirement under the GDPR, and has been introduced to ensure that data processors only process personal data in accordance with the data controller's explicit instructions.

In some situations, the privacy notice and service-provider contracts will need tailoring to the specific individual or third-party service provider (as the case may be); however, in most situations, you will be able to rely on template language to help speed up the process and, importantly, keep you GDPR-compliant.

What do I do if I receive a subject access request?

As a first step, you should consider whether you are data controllers in respect of all or part of the data requested, having regard to the *Southern Pacific* principles. So, where requests are made for data being processed as part of the insolvency proceedings (eg by directors, creditors or bankrupts), IPs will be controllers of that data and responsible for responding. Where the request is for company data, IPs should consider (as an agent of the company) the company's response.

IPs should then:

- If there are doubts, confirm the identity of the person requesting data (eg by requesting identification documentation). The one-month deadline for responding runs from when identity of the requestor is confirmed.
- Consider whether the request is manifestly unfounded or excessive – if so, write to the individual requesting clarification of the request, or consider not responding on that basis.
- Consider whether it will take more than one month to respond to the request; the deadline can be extended by up to two months if the request is complex or the individual has sent a number of requests.
- Consider whether any exemptions apply that will restrict the scope of the response. These exemptions are set out in section 15 and schedule 2 of the current draft data protection bill (which at the time of writing we expect to become the Data Protection Act 2018) and may exempt an IP from responding where (for example) there is a duty to protect the public from financial loss due to the conduct of a bankrupt, or from dishonesty or where the data is covered by legal privilege.
  - If no exemptions apply, individuals have the right to access their personal data and to be informed about:
    a) the purposes of the processing
    b) the categories of personal data processed
    c) the recipients to whom personal data is disclosed
    d) the envisaged retention period
    e) the existence of any automated decision-making.
  - If the IP concludes that there is a reason not to provide the personal data requested, let the individual know why (within one month) and inform the individual of the right to complain to the ICO or enforce legal rights.

Remember that no fee can be charged to the individual for dealing with the request, unless the request was manifestly unfounded or excessive (for example, large quantities of repeat requests).

Responding to data-subject access requests will remain a potentially time-consuming and costly task. As a practical point – to minimise cost and exposure – upon appointment as liquidators, IPs should prioritise ensuring that the company only retains personal data which is required for the purposes of the liquidation (including dealing with any claims that might be made in the liquidation).

Can I sell the company's marketing lists?

Yes, subject to certain conditions. The ICO has stated that *'if a business is insolvent, or being closed down or sold, its customer database can be sold on without prior consent'*. However, you must make sure that the buyer understands that it can only use the information for the same purpose for which it was collected by the original business. In other words, the buyer's use of the information must be within the reasonable expectations of the individuals within the marketing list. For example, if the marketing list contains information originally obtained for marketing health insurance to individuals, the list should only be sold to another health insurance business providing similar health insurance products; the list shouldn't, for example, be sold to a pet insurance company.

> **In most situations, you will be able to rely on template language to help speed up the process and, importantly, keep you GDPR-compliant.**

How does the GDPR affect the due diligence I need to do on an insolvent company?

Data protection compliance should be towards the top of your checklist when considering whether to take an appointment. If a company or sole trader »

has complied with the GDPR, it will have the records and policies in place to show compliance, so an assessment can be made fairly quickly. Administrators seeking to sell the business should be aware that data protection compliance will be at the top of a potential purchaser's due diligence list (particularly in data-heavy organisations) and will affect pricing. Liquidators should be aware of the risk that trading on a business, or making long-term decisions over the use of personal data, could lead to the risk of accepting more liability for data protection compliance (similar to environmental claims – although the position has not yet been tested in respect of data protection compliance).

Is it my responsibility to secure or securely destroy personal data contained in the company's assets?

The practical answer is *yes*. The GDPR has not changed this. From an insolvency perspective, it is your duty as an IP to:

- Secure books and records; evaluating a company's personal data will be part of this.
- Investigate what assets there are and what recoveries can be made.

> Responding to data-subject access requests will remain a potentially time-consuming and costly task.

In terms of data management, you may be required to discard personal data that is not required for the purposes of a liquidation; for example, you will not be required to satisfy a subject access request where the company no longer retains the relevant personal data (see our response to question four above).

And of course, there are potential reputational ramifications if there is a data breach on your watch, both for the company and, potentially, for you as the IP.

Will I be made responsible if the company is penalised by the ICO?

Trustees in bankruptcy should be aware that they could well be held responsible for failure to comply with the GDPR as a controller of company data. If a bankrupt has failed to comply with the GDPR, the trustee should put in place a compliance programme as a priority. The trustee would be well advised to have template paperwork that can be quickly tailored (such as privacy notices, emails seeking fresh consent where necessary, etc). Liquidators and administrators step into the shoes of directors (for data protection purposes) as agents of the insolvent business. There is potential liability under the incoming UK Data Protection Act similar to the current position, whereby directors, managers, officers or 'any person acting in that capacity' could be held liable for an offence committed by a company with their 'consent, connivance or neglect'.

What should I do if I become aware that company devices containing personal data may have been stolen or lost?

As a result of the GDPR, all data controllers in the UK now have an obligation to notify the ICO (and other EU regulatory authorities if the breach occurs in another EU country) if there is a personal data breach, *unless* the breach is unlikely to result in a risk to the rights and freedoms of individuals. Such notification has to be made within 72 hours after becoming aware of the breach. In addition, data controllers should notify affected individuals if the risk to their rights and freedoms is considered to be high.

In practice, this means that you should assess whether any personal data breach (eg as a result of a device being stolen, lost or destroyed) is sufficiently significant to trigger the GDPR notification requirements for the company. Nowadays, it's more and more common for company devices to contain a lot of personal data; therefore, even the loss of one laptop or phone could cause significant data issues.

Do I need to change my practices in relation to my own marketing contacts?

Not necessarily. If you have previously obtained your own contacts with valid consent, you have a record of this and you have given them adequate opportunity to unsubscribe, you may not need to ask those individuals for fresh consent under the GDPR to send them marketing materials. For GDPR purposes, you can consider relying on the 'legitimate interests' basis for marketing activities in a business-to-business context.

> To try to mitigate your risk of complaints, always include an easy, accessible and free opt-out mechanism in each marketing communication.

To try to mitigate your risk of complaints, always include an easy, accessible and free opt-out mechanism in each marketing communication.

You should note that electronic direct marketing (such as email, SMS or social media) is predominantly governed by the Privacy and Electronic Communications Regulations, which are due to be replaced by the ePrivacy Regulation within the next year. So the rules for your marketing practices could change in the near future.

Because of the generality of this article, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. □

[1] *Re Southern Pacific Personal Loans Ltd* [2013] EWHC 2485 (Ch)

ANNABEL GILLHAM (LEFT) is of counsel at Morrison & Foerster (UK) LLP.

MERCEDES SAMAVI (RIGHT) is an associate at Morrison & Foerster (UK) LLP.