The GDPR does not (yet) compute for IPs

Matt Jukes reports back on IP concerns about the upcoming General Data Protection Regulation (GDPR).

The latest round of European data protection regulation is touted on the EU GDPR portal as the most important change to data privacy regulation in 20 years. Ostensibly it is heavily targeted at the social media giants – entities that hold private and personal data on millions of individuals – but is bringing every business, organisation and public service across the EU along for the ride and the insolvency profession is no exception.

In Spring 2018, R3 played host to the inaugural meeting of the Insolvency GDPR Forum to bring members of the profession together to pool knowledge, eke out hidden answers to the burning data protection questions and establish how practitioners may be preparing for the regulation coming into force on 25 May this year.

Background

The GDPR updates the existing Data Protection Directive, which came into force in 1995, prior to the advent of the internet as a medium for mass communication and amusing cat videos. The regulation states that it aims to strengthen individuals' rights to be informed about the collection and use of their personal data, to request and receive such data held about them in a convenient format and to have the right to be forgotten should they choose. Data breaches will need to be reported within 72 hours to the Information Commissioner's Office (ICO) and data handling and protection processes will need to be clearly documented. A company found in breach of the GDPR may be fined up to four per cent of global turnover or a maximum of €20m, whichever is greater.

To read more about the background and impact of the GDPR, see Annabel Gillham and Mercedes Samavi's excellent article *GDPR: data protection detail* on page 15 of the Autumn 2017 issue of *RECOVERY*.

Knowing too much?

One of the key concerns raised at the Insolvency GDPR Forum was what data should be kept upon an appointment. As an office-holder you may be faced with hoards of data on day one that (under GDPR) may need to be used, passed on or destroyed according to the situation and data type – does the IP immediately assume accountability for all information held, past and present, upon appointment? Do the obligations differ depending on what type of appointment is made?

In such a situation Annabel Gillham, of counsel at Morrison & Foerster, suggests that you start by asking yourself questions: 'You do have an obligation to think about what data is flowing through an organisation as an IP. Ask yourself: do I need to be handling this data? And, what legal basis do I have?' suggests Gillham. 'The easiest basis is consent, but consent can be withdrawn. Then there is compliance with a legal obligation, which may be the case for many IPs in some situations. If it is pertinent for an IP to use that data to make and process claims, then it may fall into the category of "processed in order to comply with a legal obligation".'

> The question that needs to be asked is: have you, as the agent for the business, taken all the steps you reasonably can to keep the data safe?

Customer data that may be a prime candidate to be sold on by an office-holder, may require a certain degree of due diligence as well. Mercedes Samavi, an associate at Morrison & Foerster, recommends following the paper trail: 'Businesses should be writing to customers and other concerned individuals to obtain their customers' consent for selling their data. If a business has written to 10,000 customers, and it receives 2,000 replies negating consent but has 8,000 replies giving consent, you have a clear paper trail demonstrating that the appropriate steps have been taken regarding the data, and the business can sell those 8,000 customers' data in confidence,' says Samavi.

Breach of the (IPs') peace

Data breaches potentially pose a somewhat larger headache for IPs when taking a first look at the inventory. The issue arose at the Insolvency GDPR Forum in the form of a hypothetical question: you are appointed as liquidator over a small building company with listed assets of 23 laptops. When the inventory takes place, there are only 15 laptops listed. Does that count as a breach and how detailed do you have to be when reporting to the ICO?

The interpretation at the moment seems to be that it will involve a conversation with the ICO as soon as possible. 'If you are aware of a data breach then you have to report it,' says Gillham. 'You have a stricter obligation under GDPR to notify the ICO and the individuals whose data has been compromised.'

The accountability, not to mention the real capacity of the IP to act, is called into question again. Without the laptops, it may not be possible to determine the individuals that are affected. Likewise, the data may be encrypted, so anyone accessing the 'missing' laptops may not be able to see the data held on them. The question that needs to be asked is: have you, as the agent for the business, taken all the steps you reasonably can to keep the data safe?

No protection from data protection?

Much of the above will need clarification by the time the regulation comes into force in May. In what circumstances are directors truly entitled to the 'right to be forgotten'? To what degree does the GDPR determine a liquidator's responsibility as a data controller? Will IPs have to increase fees to account for the disposal of data? How will firms have to adapt their policies on the use of public wifi and company mobile phones? And, most importantly, to what degree will IPs be held accountable if a company has 'misplaced' data?

The Insolvency GDPR Forum deemed it unlikely that there will be dawn raids on the morning of 25 May 2018, so hopefully there will be more time to address such matters before the ICO breaks out its newly-polished battering ram. In the meantime, R3 will be hosting breakfast briefings on the GDPR on 13 March in London and 19 April in Manchester. You can also join the online discussion about the GDPR and how to comply as an insolvency practitioner at **insolvency-gdpr.co.uk**.

MATT JUKES is publishing manager of *RECOVERY* magazine.