Practical aspects of the General Data Protection Regulation for insolvency professionals

Produced in partnership with Patrick Elliot of Cubism Law

What is the GDPR?

The General Data Protection Regulation (GDPR) ***Regulation (EU) 2016/679***, in force from 25 May 2018, replaces the **Data Protection Act 1998** (**DPA 1998**) and, at least for the time being, will remain in force post-Brexit. The GDPR applies to the processing of personal data and its objective is to protect individuals in this regard while promoting the free movement of personal data.

Insolvency professionals process personal data as partners/employees/consultants of their respective organisations but also by virtue of their appointments as office-holders. They are subject to the requirements of the GDPR in both capacities.

In this note we provide a brief overview of the requirements of the GDPR as well as some practical considerations for insolvency professionals. Professionals include insolvency practitioners, legal advisers and other professional advisers (eg financial advisers, Chief Turnaround Officers etc).

Key Terms under the GDPR

Personal data means any information relating to an individual *(**Article 4(1)** of Regulation (EU) 2016/679, GDPR)*.

Special categories of personal data include racial or ethnic data, political opinions, religious beliefs, trade union membership and health and sexual information *(**Article 9** of Regulation (EU) 2016/679, GDPR)*.

Controller means the legal entity which, alone or jointly with others, determines the purposes and means for processing *(**Article 4(7)** of Regulation (EU) 2016/679, GDPR)*.

Processor means a legal entity processing on behalf of a data controller *(**Article 4(8)** of Regulation (EU) 2016/679, GDPR)*

Applicable principles under the GDPR

In order to process personal data a number of key principles need to be complied with *(**Article 5** of Regulation (EU) 2016/679, GDPR)*. These provide for processing to be:

- lawful, fair and transparent
- limited in purpose
- limited in scope
- accurate
- carried out for only as long as necessary
- secure and confidential
- accountable

In addition, processing will only be lawful if one of the following applies:

- the data subject has provided actual and informed consent
- it is pursuant to contractual obligations
- to comply with a legal obligation
- to protect the vital interests of a data subject
- in performance of a task carried out in the public interest
- for the purposes of the legitimate interests of the controller or a third party

Right to process

Insolvency professionals, like any other professionals, must only process personal data if they have the right to do so. This means that they must abide by the principles set out above and also be able to justify their activities when/if one of the Article 6 conditions apply.

Their activities are most likely to be justified when complying with a legal obligation (eg managing an insolvency/bankruptcy), performing a task in the public interest (eg winding up a company) or acting in pursuit of their legitimate interests. They may also be protecting individual creditors' interests with the consent of creditors and/or bankrupts.

Unlike under **DPA 1998**, if an insolvency professional wishes to rely on consent this will need to be explicit rather than implied (Article 7). In addition, it should be informed, freely given, unambiguous and revocable. A record should be kept of the consents obtained (***Article 7*** *of Regulation (EU) 2016/679, GDPR)*.

Insolvency professionals are likely to have client details on databases and to undertake business development activities. They must ensure that they have consent to carry out this activity to the extent it goes beyond providing client-specific or industry information.

To process special categories of personal data (see below) or criminal information, insolvency professionals will need to have an Article 6 justification and an Article 9 or 10 justification respectively.

Article 9 of Regulation (EU) 2016/679, GDPR justifications are:

- where explicit consent has been given
- necessary processing pursuant to the rights of the data controller or data subject in the employment or social protection context
- to protect vital interests where the data subject cannot give consent
- where carried out by foundations or associations
- where the data is public
- in relation to legal proceedings
- in the public interest
- for medical purposes, and
- for public interest, scientific or historical archiving purposes

Article 10 requires processing under the control of official authority or where it is authorised under law with appropriate safeguards *(**Article 10** of Regulation (EU) 2016/679, GDPR)*.

While **DPA 1998** made it a criminal offence if data controllers failed to register with the Information Commissioner's Office (ICO), the GDPR does not include this requirement.

However, regulations made **under section 108** of the Digital Economy Act 2017 require data controllers to pay a fee to the ICO and the ICO will continue to require registration by data controllers.

Data Controller or Data Processor?

When considering whether to register with the ICO or not, insolvency professionals will need to determine whether they are data processors or data controllers.

There are at least two categories of data which are processed by office holders—those that are under their control by virtue of their appointment, for example customer lists of an insolvent company; and those collected during the term of appointment, for example, details of directors. In relation to some of this data, office-holders will be acting as agent, and therefore data processors, and for the rest they will have control over the data as data controllers.

In theory administrators and supervisors act as agents, and liquidators act as principals, but the lines are often blurred. In *Re Southern Pacific Personal Loans* Limited **[2013] EWHC 2485 (Ch)**, it was held that the liquidators received data as agents and were not therefore responsible as data controllers. However, it may be prudent for insolvency professionals to assume that they are data controllers and register as such.

In certain circumstances, insolvency professionals may be joint controllers of personal data in which case they should put in place joint controller agreements as well as register with the ICO *(**Article 26** of Regulation (EU) 2016/679, GDPR)*.

Purposes for processing

In order to comply with the limitation requirement of Article 6, insolvency professionals will need to identify the personal data they manage and the purposes for which they are processing it, and not stray beyond these. This may require conducting an audit (see compliance below).

The likely personal data held will include employee data, customer information and databases, details of debtors and creditors and information relating to directors. Some of this data might fall into the special category provisions (in Article 9).

The likely purposes will include reviewing the data on appointment; making contact with individuals, dealing with employees, helping and/or pursuing directors, chasing debtors, accounting to creditors and selling assets.

Control of data

Article 10 of the GDPR imposes an obligation on data controllers to maintain records of the processing activities under their responsibility. This must include the nature of the processing and its purpose as well as details of recipients, transfers, time-limits and security measures put in place to protect it.

Data processors also need to document their activities *(**Article 30** of Regulation (EU) 2016/679, GDPR)*.

Where there is a high risk to the rights of individuals from processing, data controllers must carry out an impact assessment in advance and document it *(Article 35 of Regulation (EU) 2016/679, GDPR)*.

A high risk might arise in a number of situations but an obvious example would be if there is an insolvent financial services business. The assessment would enable any appointee to demonstrate compliance if necessary (so long as it was followed through).

As already mentioned, maintaining the security of personal data is of fundamental importance under the GDPR. Section 2 of the GDPR requires controllers and processors

to *(**Articles 32–34** of Regulation (EU) 2016/679, GDPR):*

- ensure there is an appropriate level of security in place (Article 32)
- notify any breach of security to the ICO within 72 hours (Article 33), and
- notify the data subject(s) without delay (Article 34)

This means that insolvency professionals need to tighten up their security measures both on and offline. For data held in hard copy, appropriate storage with restricted access needs to be in place. Desk drawers, filing cabinets and access to offices should be suitably secure.

For data held electronically, password protection and access restriction should be in place.

The GDPR also requires processing (which includes storage) to only take place for as long as necessary (Article 6).

Insolvency professionals should therefore ensure that personal data is only held for as long as necessary and that any destruction of old data is carried out efficiently (particularly of electronic records where a 'cyber shredding' exercise should be utilised).

In the event of the sale of a business, including personal data, insolvency professionals will need to demonstrate compliance with the GDPR and the right to sell the data.

The same will apply in the event of a transfer overseas. There are stringent obligations under Chapter V of the GDPR relating to transfers and providing for the protection of the data subjects *(**Articles 44–50** of Regulation (EU) 2016/679, GDPR).*

In *Re Bernard L Madoff Investment Securities LLC **[2009] EWHC 442 (Ch)***, the court approved the transfer of personal data as part of a cross-border restructuring but insolvency professionals would be well-advised to ensure that any recipient of personal data is obliged to comply with the GDPR to the same degree as its own compliance (and to be able to demonstrate this).

Compliance

Compliance with the legislation has to be demonstrable. For those new to data privacy, it would be worthwhile to initially carry out an audit of the data held. This audit should be used to identify what data is held, from where it has been obtained, the circumstances under which it was obtained, what it is being used for, to whom it is being transferred, how it is being held and when it is being destroyed.

This will enable insolvency professionals to then implement the appropriate procedures to deal with individuals' rights (see below) and to comply with the provisions of the legislation.

For internal purposes, it would also be wise to adopt clear privacy policies which are then disseminated to staff (and clients if necessary).

For external purposes, for instance when engaging professional advisers, insolvency professionals must ensure that governing contracts contain sufficient data privacy clauses so that recipients of data they control comply with the requirements of the GDPR.

The GDPR, at Section 4, provides for the appointment of a data protection officer (DPO). While small organisations which don't carry out largescale processing or the processing of special category and/or criminal records data are exempt from having to make a formal appointment, most organisations would benefit from having a nominated person as responsible for matters to do with data privacy. A significant part of their work will

relate to data subject rights and the exercise of them*(Articles 37–39 of Regulation (EU) 2016/679, GDPR)*.

Individuals' rights

Chapter III of the GDPR provides data subjects with a number of rights. While many are familiar from the requirements of **DPA 1998**, there are additions and subtle changes *(Articles 12–20 of Regulation (EU) 2016/679, GDPR)*

These rights include:

- an obligation on data controllers to be transparent (Article 12)
- access to data held (Articles 13, 14 and 15)
- the right to rectification of inaccurate data (Article 16)
- the right to erasure where data is no longer needed (Article 17)
- the right to restrict processing (Article 18)
- the right to data portability (Article 19)

Data subject access requests are not new. Under the GDPR a one-month time-limit for the response is required and fees may no longer be charged. Some of the other rights are new such as the right to be forgotten, which is included in data protection legislation for the first time.

In order to efficiently respond to requests made by data subjects pursuant to these articles, insolvency professionals will need to have established processes in place with agreed responsibilities. These should be outlined in privacy policies and staff should understand how to respond to data subjects. Any DPO is likely to be ultimately responsible.

Special category data

As mentioned on a number of occasions above, there are additional requirements throughout the legislation in relation to special category data (defined above in the key terms). Processing of this data is not allowed unless one of the provisions in Article 9 applies.

For insolvency professionals, the most relevant exemptions include where processing:

- is carried out with a data subject's explicit consent
- is necessary for employment purposes
- is necessary to protect the data subject's vital interests
- is necessary for legal claims (bringing and defending)
- is necessary for reasons of substantial public interest

As well as provisions relating to special category data are provisions relating to children (Article 8). Where a child is less than 16 years old, parental/guardian consent must also be obtained.

This provision is unlikely to arise in most insolvency situations but may do so in bankruptcies.

Failure to comply with the GDPR

The sanctions for failing to comply with the legislation under the GDPR are much greater than under **DPA 1998**. Article 84 of the GDPR allows each Member State to decide on its own penalties.

The maximum penalty which the ICO will impose for any failure to comply with the principles or the rights of individuals or in relation to transfers to third countries is €20m or 4% of turnover, whichever is the higher.

For other infringements, the ICO can impose fines of €10m or 2% of turnover, whichever is higher.

In practice, the number of fines imposed by the ICO to date has been small both absolutely and relatively to the number of investigations made and this is likely to continue to be the case.

However, these significant penalties are there for a reason and insolvency professionals should beware accordingly.

In addition to the ICO taking action, data subjects are able to bring private claims for breach of the legislation pursuant to Article 82.

Whereas under **DPA 1998** claims could only be brought against data controllers they can now also be brought against data processors and where there are many potential infringers, a data subject can select which one to pursue and the defendant will have to seek contribution or compensation from any others involved.

Under **DPA 1998**, a data subject could obtain damages for misuse of data, as well as material damages (see *Vidal-Hall v Google Inc* ***[2014] EWHC 13 (QB)***). The GDPR specifically allows for the recovery of non-material damages which might include, for example, reputational damage.

With the above in mind, it is worth reviewing insurance policies to ensure that breaches of the GDPR are covered

If you would like to contribute to Lexis®PSL Restructuring and Insolvency please contact:

Amy Himsworth
LexisNexis
Lexis House
30 Farringdon Street
EC4A 4HH

amy.himsworth@lexisnexis.co.uk
+44 (0)207 400 2934

For more information, see Lexis PSL Restructuring & Insolvency.
Not a subscriber? Go to
http://www.lexisnexis.co.uk/en-uk/products/campaign/psl-randi-free-trial.page
for a free trial.