# The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR')

## The Data Protection Act 2018 ('DPA 18')

## Introduction

This guidance note addresses the dual capacities in which as an IP, you are required to consider your GDPR responsibilities. Firstly your firm needs to be GDPR compliant and this note considers to what extent your IPA monitoring visits will address this. Secondly you should consider the GDPR position of any entity to which you are appointed as officeholder and identify and address potential areas of risk.

This is not a definitive guide and if in doubt you should seek expert advice or access the information available on the Information Commissioner's Office (ICO) website, details of which are provided below.

## GDPR/DPA 18

The GDPR took effect in the UK from 25 May 2018. Its terms have been incorporated into the Data Protection Act 2018. The data processing regime exists to ensure that the rights of any EU individual in respect of data processing are protected and applies where the entity holds and/or processes personal data, of which some may be classed as special category.

Article 4 GDPR defines "personal data" as any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location, data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special category data is defined as: health (including mental health); crimes/criminal activity (alleged or proven); sexual orientation and activity; religion and philosophical beliefs; political opinions; racial and ethnic origins; trade union membership and biometric and genetic data.

A Data Controller is defined as: natural or legal person, public authority, agency or body which alone or jointly with another, determines the purposes and means of processing personal data.

Data Processor is defined as: natural or legal person, public authority, agency or other body, which processes personal data on behalf of a controller.

Any Data Processor dealing with EU residents must comply with EU GDPR regardless of where the Data Processor is located. There is an adequacy decision by the European Commission in respect of the USA to the effect that it is deemed to provide an adequate level of protection for personal information.

Under GDPR both Data controllers and Data Processors may be jointly and severally liable in the case of any breach. If you are in any doubt as to the capacity in which you or the entity in insolvency acts, you are recommended to take independent legal advice.

## What are the legal bases for holding data?

- Consent: The individual has given clear consent for you to process their personal data for a specific purpose. Consent must be freely given, specific, informed and unambiguous. It cannot be taken from silence, pre-ticked boxes or inactivity.
- Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
- For the performance of a contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- For the performance of a public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- To comply with a legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.

## Demonstrating compliance

GDPR requires organisations to be able to demonstrate compliance with the principles set out in the legislation. In essence you need to review the data you hold and demonstrate that:

- The information is needed
- The data held is relevant and accurate for that purpose
- The data is held securely
- The data is only held for as long as is necessary
- It is clear to people how and why you hold the data
- It is only shared as necessary

## What do I need to do as a business?

Your business needs to document what personal data it holds, on what basis and in what capacity, and by whom it will be processed. As a minimum you will need to maintain a Data Processing Register, Register of Data Processors and a Data Breach Register. Depending on the size of the organisation within which you operate, you may have a Data Protection Officer who can assist you with your insolvency-specific data requirements.

Your business will need to consider policies to deal with: data confidentiality and security; data breaches, data retention and destruction, data subject access requests, special category data; staff member data protection; supplier oversight and vulnerable clients.

Privacy notices setting out your approach to data handling should be available to cover the various parties whose personal data you may handle as an office holder, and you should consider privacy notices for the following: business contacts and customers; debt advice and personal insolvency clients; directors, shareholders and business owners; staff members and job applicants and stakeholders generally. You should also have an up-to-date Privacy Notice on your firm's website.

You may consider completing a Data Protection Impact Assessment (DPIA). This will allow you to demonstrate that you know what data you hold, how you hold it and why. This needs to be documented together with any actions you need to take to secure data and ensure you have the appropriate consents, where applicable.

## Do I need a Data Protection Officer (DPO)?

A DPO is required if you are a public authority, or if you carry out regular and systematic processing of data on a large scale; large scale processing of special data or data relating to criminal convictions. It is likely therefore that large practices and volume providers will require to appoint a DPO.

For a smaller insolvency practice, a DPO is not required but we recommend that a member of your organisation is responsible for GDPR and actively monitors GDPR and data protection compliance, ensuring registers, policies and notices are up to date, and that suitable staff training and awareness is embedded in the organisation.

If your organisation is appointing a DPO it is important to note that it should not be a senior board member or director, unless they also have a compliance role, as this may give rise to conflicts of interest.

Do I need to notify all creditors, debtors and directors that I am holding their personal information following an appointment?

Ideally you will have a privacy notice that deals with this. This information can be on your firm's website, and referenced in your communication with these parties. You do not have to send the data subjects a copy of the relevant privacy notice, unless you think it is appropriate to do so.

## Pre-appointment

Any letter of engagement that your practice issues should include or reference the appropriate privacy notice.

## Risk assessment

If possible, understand and assess the risks that GDPR presents to the entity to which you are to be or have been appointed, and whether these are material or can be mitigated. Your firm's checklists or work programmes should reflect your considerations of GDPR and its potential impact, and document any decisions or outcomes. You should be able to demonstrate that the entity's current GDPR approach has been assessed, any risks arising from its being held or processed are identified, and wherever possible minimised.

If personal data processing will continue post-appointment, for example by way of trading, you will need to assess the GDPR risks and requirements and ensure that the entity has in place the necessary consent and appropriate controls and policies surrounding its handling of personal data.

If personal data is likely to be transferred as part of a going concern sale, you should consider checking whether any personal data is transferable and whether consent to transfer has been given or is set out in the privacy notices of the entity.

You may be required to notify the individuals of the impending transfer, giving them the opportunity to consent or have their data removed. We would recommend specialist advice and consideration of a DPIA in these circumstances.

Any data acquired that is outside of the insolvent's accounting ledgers falls under the Mergers and Acquisitions section of the Data Sharing Code of Practice of the current and future Data Protection Bill. This means that for an interim period you are able to share data from the company for which you have been appointed and yourselves without having to notify the individuals provided that the use of personal data continues to be fair. The ICO have yet to issue updated guidance on this area.

## Data breaches

All breaches of personal data must be recorded in the relevant Data Breach Register. Reportable breaches must be notified to the ICO within 72 hours of a breach being identified. The ICO need not be notified if an objective assessment determines that the breach is likely to result in no harm to the individual data subjects.

If the breach is serious, and there is a risk of harm to individuals, there will be an obligation to notify the individuals personally as well as the ICO.

You should be able to demonstrate that your firm has the appropriate policies and processes in place for dealing with data breaches. You should also be able to demonstrate that you have considered the risk of data breach in relation to each entity to which you have been appointed, and that that entity has in turn the appropriate policies and processes in place for dealing with breaches, where required.

## Do I still need to be registered as a Data Controller?

Formal registration as a Data Controller is no longer required. Your role in holding or processing data determines whether you are a Data Controller or Data Processor, not whether you are voluntarily registered.

Going forward all Data Controllers will pay a fee to the ICO based on turnover and number of employees. Your firm will be assessed on expiry of its current annual registration.

You will also need to check the ICO status of any entity when appointed, and whether its fees are up to date.

Our understanding is it is a criminal offence not to pay your data protection fee.

Our previous recommendation has always been that the firm should also be registered to cover those situations where you may no longer be in office but data is held. This has not changed.

## Existing cases: what are my GDPR responsibilities?

Following the commencement of GDPR, we recommend that you notify any personal data subjects of any changes to the relevant privacy policy by way link to your website (or other manner as appropriate) on the next occasion on which you are communicating with them.

You do not need to contact individual data subjects in closed cases. You are, however, required to consider how you will deal with any Subject Access Requests relating to these appointments and satisfy yourself that the data in question is securely stored.

We would also draw your attention to s93(4)(b) DPA 18 that states you need not notify data subjects where it "would be impossible or involve disproportionate effort".

## What will the IPA be looking for on a monitoring visit?

Compliance with all aspects of the law is part of being a fit and proper person. You are, therefore, expected to be legally compliant as a business owner or operator. The IPA will not fulfil the role of the Information Commissioner. We will, however, take steps to evidence general compliance with GDPR, since we recognise that any significant breach in your systems may lead to investigation and penalty, leading to a financial or reputational compromise of your business. Likewise, you will be required to demonstrate that you have adequate procedures for assessing and managing GDPR related issues across your cases.

On a monitoring visit you are likely to be asked the following:

- Can we inspect your Data Registers, and check to see that you have privacy notices and policies in place?
- Have you completed a data protection impact assessment for your business line or your firm? (You may be asked to provide a copy)
- What steps have you taken to effect any recommendations?
- Is your enrolment with ICO up to date?
- Have you received any Subject Access Requests in the last twelve months? How and within what timescale were they dealt with? (Again you may be asked to evidence this).

If we are aware of a specific risk area you may be asked further questions or asked to provide documentary evidence however we expect this to the exception to the rule.

## Further queries

This is not intended as a definitive guide, and our guidance may change as issues become clearer once the legislation is in force.

Further information may also be obtained from the ICO website at:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

*IPA guidance does not constitute legal advice nor do they seek to instruct or direct Members to take, or avoid taking, any action. Members should be aware that any advice or assistance provided cannot fetter the authority of its regulatory and disciplinary committees to make determinations about a Member's conduct.*

*The IPA accepts no liability in respect of actions that Members may take in accordance with guidance issued as it must be for each Member to be satisfied that his/her conduct meets the legal and professional requirements placed upon Office-Holders/Members. Therefore, Members may consider it appropriate to seek independent professional advice in respect of the subject matter.*

Last revised 1 October 2018