## FAQs on the GDPR: Practical considerations for insolvency practitioners (IPs)

*This content is not intended to constitute legal advice. Specific legal advice should be sought before taking or refraining from taking any action in relation to the matters outlined. All information is as of 25 May 2018.*

These FAQs are issued by:

- The Institute of Chartered Accountants in England & Wales (ICAEW)
- The Insolvency Practitioners Association (IPA)
- The Institute of Chartered Accountants of Scotland (ICAS)
- The Association of Chartered Certified Accountants (ACCA)
- Chartered Accountants Ireland (CAI)
- The Association of Business Recovery Professionals (R3)

### What changes do I need to make to my appointment notices for the GDPR?

Post 25 May 2018 your appointment notices need to include a privacy notice. A privacy notice is a document explaining to data subjects their rights and how you will use their personal data. Privacy notices are part of a data subject's right to be informed by an organisation on how their personal data will be used. A data controller has an obligation to provide 'fair processing information' to data subjects, typically through a privacy policy (e.g. on a website) or a privacy notice (e.g. a hard copy form).

It is best practice to include your privacy notice on your website. This privacy notice should cover and explain how you handle data and respect privacy of your clients across your accounting activities. For example it is expected that you would explain what data you collect, process and handle for the purposes of insolvency matters, but you may want to cover how you also handle data of prospective clients.

A key requirement of GDPR is that data controllers are required to provide the required privacy information to individuals at the time that their personal data is collected from them. This means that if you have a privacy notice on your website, you will need to make reference to it, and explain where it can be found, in your post-appointment notices or in any other forms and templates you may be using. We are aware that some firms are planning to include a sentence in their footer, to tell people where they can find their privacy notice.

It is common practice to include a short notice explaining the purpose of use within the collection channels and then refer to the longer privacy notice via a link, to ensure transparency.

The privacy notice will relate to the data you generate as office holder. The position is less clear cut for data generated by the company and held in its records.

GDPR also requires that if the data is obtained from another source and not directly from the individuals, data controllers need to provide the required privacy information to individuals within a reasonable period of obtaining the data and no later than one month. From an IP's perspective you are likely to be taking possession of data from within the company's records (company data) and also generating your own data as part of processing or adjudicating on employee or creditor claims. It is more than likely that this data will be obtained under legitimate basis.

In a privacy notice, you need to disclose to the data subject:

- your lawful basis for processing the individual's data
- the purposes of the processing
- your data retention periods
- contact details for the member of staff responsible for the GDPR at your practice, so that individuals can contact them to enforce their rights under the GDPR, and
- the individual's right to complain to the Information Commissioners Office (ICO) if they think there's a problem with the way you're handling their data.

Privacy notices are not new but the GDPR is more prescriptive as to what they should include and how they should be prepared. In particular they must be easy to understand and not excessively long. The ICO has provided guidance on privacy notices.

You may want to seek legal advice on your privacy notices to ensure they are compliant.

**Is there anything I particularly need to consider in relation to employees?**

Some information held in payroll records or collected during recruitment might fall within the definition of special category data. Special category data is personal data that the GDPR says is more sensitive and so needs more protection. It includes information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation

The payroll records you collect may, for example, include reference to an employee's religion or trade union membership.

The form of the data isn't relevant so bear in mind that photos could be personal data, if they identify any of the above. This may also be an issue, depending on the business you're dealing with.

If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data. The ICO has further information about special category data and the requirements.

It is generally advised as best practice to try and either minimise the data collected relating to special categories (i.e. collect only on if it is regulatory requirement) and also try to anonymise or segregate it from core individual records, for example if the data is required for statistical purposes.

**What steps do I need to consider before appointment?**

As part of your take on processes you should carry out a data security risk analysis, ideally by speaking to whoever is responsible for overseeing GDPR compliance at the insolvent entity. This might be the directors, the Data Privacy Officer (if there is one), the Data Protection Manager, the Head of Privacy or the Data Protection Contact.

You need to understand:

- what they have done in relation to the GDPR
- their processes and procedures
- the type and nature of the data the company holds
- whether any data needs to be securely destroyed
- whether they have a BYOD (bring your own device) policy and the implications of that
- whether they have any specific data retention requirements
- where the data is held. If it isn't held in the EU, then you should get confirmation from the storage provider that the data is being stored or transferred in accordance with the GDPR.

**What do I need to do post-appointment?**

You should consider the physical security of the premises and any building where records are stored. If you store information in systems as electronic records, you should also ensure that appropriate security controls are in place to prevent unauthorised access of these records.

If the system or physical storage facility is supplied by an external provider you will need assurances from them contractually that they have appropriate security in place.

You will need to document the data you are holding and the basis, or bases, on which you are holding it. You can do this using case-type specific proformas for each different type of insolvency appointment, which document the reasons for processing that data, as most cases should follow the same model. However if you have a case, which you consider to be higher risk, which may therefore not fall within your usual processes, you should specifically document the position on that case. The ICO have published guidance about which processing activities need to be documented and the requirements.

## What do I need to do if I'm trading a business?

Before you consider trading, you need to take steps to identify whether the entity is GDPR-compliant by getting comfort from them as to whether:

- contract clauses ensure that where data is shared with others, the contract is GDPR-compliant
- clients / customers understand how the entity will use their personal data
- employees have been told of their right to complain to the ICO if they believe that their personal data isn't being used appropriately or held securely, and
- marketing contracts are GDPR-complaint.

If you conclude that the entity is not GDPR-compliant, you will need to consider how this can be addressed and whether you can trade in a GDPR-compliant manner. You should document the GDPR risks and how they have been mitigated.

We are seeking clarification as to whether during a period of trading the company needs to continue to be registered as a data controller or whether the IP's registration will suffice.

The nature of some businesses may mean that they are holding special category data. This includes information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation

If the business is processing special category data it needs to identify both a lawful basis for general processing and an additional condition for processing this type of data. The ICO have published guidance about special category data and the requirements.

## What about the company's books and records?

As an IP you have a number of regulatory responsibilities, including collecting a company's books and records so you can fulfil your SIP 2 obligations, and potentially pursue antecedent transactions.

You can't disclaim books and records or computer equipment holding an entity's data because you perceive GDPR to impose onerous obligations. You need to have possession of the relevant records to be able to fulfil your investigatory obligations. If you are satisfied that you have all the electronic records you need, or have taken a back up of or have imaged the entity's computer system (which you can access), and are disposing of computer equipment, you need to ensure that all data is wiped. The ICO has guidance on disposing of electronic equipment.

Whereas in the past on certain cases you might have taken control of all a company's records up front for ease, post-GDPR you:

- need to ensure that personal information is only collected and used for appropriate purposes;
- need to ensure that personal information is deleted when no longer needed;
- need to take a more considered approach to ensure you only take information relevant to your role and responsibilities; and
- should ensure you have a process for deleting personal data when it is no longer needed. That said, we would however expect IPs to retain information to support employee and creditor claims for the life of the case, and for the usual retention periods.

You do though need to ensure you have recovered sufficient records (both hard copy documents and also computerised records) to be able to effectively discharge your statutory obligations.

You need to consider the position with any books and records that you aren't taking into your control, as they may contain personal data. The ICO hasn't yet updated its guidance about disposing of IT equipment for the GDPR and in the meantime is referring people to its guidance under the 1998 Data Protection Act legislation.

However as the GDPR covers both paper and electronic data, you will need to be careful how you deal with any hard copy company records that you aren't intending to take into your control. While the company is likely to be the data controller for any pre insolvency records, that doesn't mean to say that you should leave the records in an empty property, without arranging for secure destruction. As agent of a company, IPs still need to take an informed view of data risks as they must ensure the company's compliance with its obligations.

For cases in England and Wales, section 5.6 of R3's Technical Bulletin 104 sets out the retention periods for company records, which in the case of administrations moving to dissolution or voluntary liquidations, can be destroyed at any time after the expiry of a year after the company's dissolution. In bankruptcies and compulsory liquidations, the officeholder can, on the authorisation of the Official Receiver, sell, destroy or otherwise dispose of the entity's records at any time. When seeking authorisation, the Insolvency Service ask that IPs submit a completed Form BPDC.

In Scotland, a company's books and records may be disposed of in accordance with the timescales and approval processes set out in rule 7.34 of the Insolvency (Scotland) Rules 1986. In personal insolvencies, guidance issued by the Accountant in Bankruptcy provides for a debtor's records to be disposed of when the trustee has no further use for them.

**What do I need to think about when employing third parties?**

It is currently unclear whether an office holder is a data processor or data controller of the company's books and records.

Where you are acting as a data controller and employ third parties to assist with aspects of a case, which would involve processing personal data (such as solicitors, agents, debt collection or ERA specialists), the third party may be either a data controller or a data processor in relation to the personal data supplied to them. Where the third party acts as a data processor you will need to ensure that a written contract reflects the GDPR.

Such contracts must now include certain specific terms, as a minimum. These terms are designed to ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure).

The contract should specify:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

The contracts should also include the following compulsory terms:

- that the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
- that the processor must ensure that people processing the data are subject to a duty of confidence;
- that the processor must take appropriate measures to ensure the security of processing;
- that the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- that the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller as requested at the end of the contract; and
- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

You may also want to include a provision for the third party to indemnify you against any breach.

As a matter of good practice, you may also want to consider including a statement that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR.

When the contract comes to an end, you need to ensure that the third party has complied with any agreement to destroy data.

On pre-25 May 2018 cases where agents are continuing to process personal data, you should vary the contract to reflect the above requirements.

**Can I still maintain an interested party database?**

Many IPs keep a database of potentially interested parties, which they will then use when marketing businesses for sale.

As with other data that you hold, you will need to consider the lawful basis on which you process this data. It may be that the parties on the database have consented to the use of their data for such purposes; but bear in mind that consent requires a positive opt-in and you can't use pre-ticked boxes or any other method of default consent.

It may be that you consider that the legitimate interest basis could apply. This is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests. There are three elements to the legitimate interests basis. You need to:

- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

The ICO has recently introduced guidance on legitimate interest.

If you consider that the legitimate interest basis applies, you should keep a record of your legitimate interests assessment to help you demonstrate compliance if required. And you must include details of your legitimate interests in your privacy information.

You also need to bear in mind the Privacy and Electronic Communications Regulations (PECR), which give people specific privacy rights in relation to electronic communications. The EU is in the process of replacing the e-privacy Directive with a new e-privacy Regulation to sit alongside the GDPR. However, the new Regulation is not yet agreed. For now, PECR continues to apply alongside the GDPR.

PECR covers:

- marketing by electronic means, including marketing calls, texts, emails and faxes.
- the use of cookies or similar technologies that track information about people accessing a website or other electronic service.
- security of public electronic communications services.
- privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (eg caller ID and call return), and directory listings.

While some of the rules only apply to organisations that provide a public electronic communications network or service, PECR will apply to businesses who:

- market by phone, email, text or fax;
- use cookies or a similar technology on their website; or
- compile a telephone directory (or a similar public directory).

PECR will apply even if the business isn't processing personal data, as many of the rules protect companies as well as individuals, and the marketing rules apply even if you cannot identify the person you are contacting.

If you send electronic marketing or use cookies or similar technologies, from 25 May 2018 you must comply with both PECR and the GDPR. The ICO have further information on PECR.

**What about an individual's rights in relation to the deletion of data?**

The GDPR introduces a right for individuals to have personal data erased. But this is not absolute. This right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing and you have one month to respond to a request.

The right is not absolute and only applies in certain circumstances, if:

- the personal data is no longer necessary for the purpose which it was originally collected or processed for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the first principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

You can refuse to comply with a request for erasure if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. In such cases you can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case you will need to justify your decision.

Office holders' rights and obligations override an individual's rights to deletion. You need to ensure that you retain sufficient documentation to support any claims that the estate has against any parties. GDPR can't be used as a tool to erase evidence.

**What about company laptops and mobile devices?**

IPs should take all reasonable steps to locate and secure company laptops and other mobile devices. In some cases it may be that the holder of the equipment is interested in acquiring it from you, and that might maximise realisations from it. But you will need to be careful about the company data held on the device as allowing that data to remain in a third party's possession could result in a security breach.

You should carry out a risk analysis and document any decisions for collecting in equipment, or deciding not to do so. As part of this you should consider whether the entity's laptops are encrypted and any ability to shut down or restrict access remotely.

You should ascertain whether the entity has a BYOD policy and the implications and extent of that, including understanding what data could be held outside an entity's systems. The ICO has a helpsheet on BYOD.

We are seeking clarification as to whether, despite having taken all reasonable steps, an inability to recover all IT equipment or mobile equipment is always a data breach which needs to be reported to the ICO, particularly as in such cases the officeholder may not be aware of the nature and extent of the data held on such devices, whose data was held and so would be unable to report the security breach to those affected.

**Are there any particular issues when I am marketing a business for sale?**

You will need to ensure compliance with GDPR during a due diligence process. Personal data should be kept secure and redacted where appropriate to ensure it isn't disclosed.

You should also reflect the GDPR in the confidentiality agreements that you ask interested parties to sign.

**What about selling computer equipment?**

The ICO hasn't yet updated its guidance about disposing of IT equipment for the GDPR. In the meantime it is referring people to its guidance under the 1998 Data Protection Act legislation.

**Can I still sell a company database?**

GDPR won't stop you selling a database of customers or an in-house list of those who have registered on a website but you should ensure that the company has records of what individuals have consented to, including what they were told, and when and how they consented. The company's records should also show whether they have consent for texts, emails and automated calls, if relevant.

You can expect purchasers to carry out rigorous checks to satisfy themselves that the company obtained the data fairly and lawfully before completing a purchase. So it would be useful to establish the quality of the consents in place before you invest too much time in marketing a database as if the purchaser can't satisfy themselves that the company has the appropriate consents in place, the value of the database may be significantly depleted.

When you're selling a database you should check whether the database to be transferred will be used for the same or a similar purpose by the purchaser, as the purchaser can only use the data for the purposes for which it was originally collected. If the buyer wants to use the data for a new purpose then it will need to obtain the consent of the individuals on the database. Where appropriate, you should ensure that the contract reflects any obligation for the purchaser to seek consent as soon as possible.

The ICO has guidance on direct marketing.

**What about my pre-25 May 2018 appointments?**

**Existing appointments**

If you haven't previously informed creditors and employees that you are holding their data and the reasons for doing so, under the Data Protection Act 1998, you will need to notify them on open cases that pre-date 25 May 2018. From a practical perspective, the best timescale for notifying them of this would be at the time you next report to them. We are seeking clarification from the ICO that this would be acceptable.

Where you use a portal to host creditor reports, we would expect individuals on each case to be able to access either a privacy notice, or a link to your privacy notice.

**Closed cases**

You may also be holding data on individuals on closed cases. The definition of processing includes holding data.

Whether under GDPR you need to notify employees and creditors on closed cases that you are holding their data is something we are seeking to clarify with the ICO. However it may not be an issue if you previously notified them of the applicable privacy policies and told them how long you would retain their data for, under the Data Protection Act 1998.

**Do I need to update my engagement letters for new work?**

While not mandatory, engagement letters can be a useful way of ensuring that you have communicated key terms and the scope of your work to your client.

If you're issuing new engagement letters before 25 May 2018 incorporating the GDPR provisions, you will need to adapt the provision to refer to existing UK legislation (the Data Protection Act 1998). One way of doing this would be to ensure that the definition of 'data protection legislation' covers both the current and the post-GDPR position.

If you are amending an existing letter of engagement, the amendment should state that it takes effect on and from 25 May 2018. ICAEW and ICAS have some suggested wording for engagement letters that their members and IPs can access.

**Data breach notifications**

**What is a personal data breach?**

A personal data breach is the loss or disclosure of, unauthorised access, or unlawful destruction of personal information. It includes breaches that are the result of both accidental and deliberate causes, but it can also be the result of an operational breakdown or faulty procedures.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- leaving a hard copy document with personal information on a printer;
- computing devices containing personal data being lost or stolen;
- alteration or deletion of personal data without permission; and
- loss of availability of personal data.

**What policies or procedures do I need to have in place?**

You need to have policies and procedures in place to deal with any personal data breaches. These should cover how to identify and recognise a breach, and what you need to do if there is one. You should also have a register of breaches, as all breaches must be recorded.

### What should I do if a data breach has occurred?

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. You must notify the ICO unless the breach is *unlikely* to result in a risk to the rights and freedoms of individuals; if it's unlikely then you don't have to report it. But if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

You will need to report breaches to the ICO within 72 hours of becoming aware of them. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay. As a result it's important that staff know how to identify a breach and who to report it to. Given the short timeframe staff should also know who to contact if the main contract is away from the office.

When reporting a breach, the GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible the categories and approximate number of individuals concerned;
- and the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

The GDPR acknowledges that it won't always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. You can provide the required information in phases, but the subsequent reports need to be made without undue further delay.

The ICO has indicated a preference for breaches to be reported by phone. The ICO's guidance suggests that online reporting is appropriate where you are confident that you have dealt with a breach appropriately or if you are still investigating it and will be able to provide more information at a later date. The ICO has published guidance on reporting breaches (and their contact details).