Chartered Accountants Ireland or CCAB-I material

Technical Releases

TR 02/2019 - GDPR Guidance for Insolvency Practitioners (updated October 2022)

This publication has been jointly developed by the member bodies of the Consultative Committee of Accountancy Bodies – Ireland (CCAB-I), being the Institute of Chartered Accountants in Ireland, The Association of Chartered Certified Accountants, The Institute of Certified Public Accountants and Chartered Institute of Management Accountants.

Issued May 2019

Updated October 2022

Disclaimer

This publication has been jointly developed by the member bodies of the Consultative Committee of Accountancy Bodies – Ireland (CCAB-I), being the Institute of Chartered Accountants in Ireland, The Association of Chartered Certified Accountants, The Institute of Certified Public Accountants and Chartered Institute of Management Accountants.

The content of this publication is provided as a guide only and does not purport to give professional advice. It should, accordingly, not be relied upon as such. No party should act or refrain from acting on the basis of any material contained in this publication without seeking appropriate professional advice. While every reasonable care has been taken by the member bodies of the Consultative Committee of Accountancy Bodies – Ireland (CCAB-I) in the preparation of this publication we do not guarantee the accuracy or veracity of any information or opinion, or the appropriateness, suitability or applicability of any practice or procedure contained therein. The member bodies of the CCAB-I are not responsible for any errors or omissions or for the results obtained from the use of the information contained in this publication.

To the fullest extent permitted by applicable law, the member bodies of the CCAB-I exclude all liability for any damage, costs, claims or loss of any nature, including but not limited to indirect or consequential loss or damage, loss of business profits or contracts, business interruption, loss of revenue or income, loss of business opportunity, goodwill or reputation, or loss of use of money or anticipated saving, loss of information or loss, damage to or corruption of data, whether arising from the negligence, breach of contract or otherwise of the member bodies of the CCAB-I, their committee members, employees, servants or agents, or of the authors who contributed to the text, even if advised of the possibility of such damages.

Similarly, to the fullest extent permitted by applicable law, the member bodies of the CCAB-I shall not be liable for any indirect or consequential losses including but not limited to, loss of business profits or contracts, business interruption, loss of revenue, loss of business opportunity, goodwill or reputation, or loss of use of money or anticipated saving, loss of information or damage to or corruption of data, nor shall it be liable for any damage, costs or losses of any nature (whether direct or indirect) occasioned by actions, or failure to act, by users of this publication or by any third party, in reliance upon the contents of this publication, which result in damages or losses incurred either by users of this publication, for whom they act as agents, those who rely upon them for advice, or any third party, or for any breach of contract by the member bodies of the CCAB-I in respect of any inaccurate, mistaken or negligent misstatement or omission contained in this publication.

Any issues arising out of the above will be governed by and construed in accordance with the laws of Ireland and the courts of Ireland shall have exclusive jurisdiction to deal with all such issues.

Table of Contents

A.Introduction

1.This Technical Release highlights features of the General Data Protection Regulation (the "**GDPR**") (Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) which are of particular importance to insolvency practitioners ("**IPs**"). It is not intended as a substitute for the formation and implementation of policies for compliance generally with GDPR by IPs and their firms. It contains general guidance only and legal and other professional advice should be obtained on any particular issue that arises in practice.

2.The guidance relates to the duties and responsibilities of practitioners in their capacity as appointed insolvency office holders, and does not extend to the application of GDPR to the firms of which practitioners are members.

3.The GDPR entered into force on 25 May 2018. As an EU Regulation it has direct effect in every Member State within the EU.

4.The Data Protection Act 2018 entered into force in Ireland on 25 May 2018 and gave effect to and implemented the GDPR in the Republic of Ireland, with some permitted exceptions / derogations. This Act and the Data Protection Acts 1988 and 2003 may be cited together as the Data Protection Acts 1998 to 2018 (the "**Act**").

5.The GDPR is a comprehensive scheme of rules governing the protection of natural persons with regard to the privacy and security of their Personal Data. It imposes obligations on all entities who are Data Controllers or Data Processors of Personal Data and establishes a regime for the protection of the privacy rights of Data Subjects, both by regulatory powers vested in the Data Protection Commission (the Irish data protection supervisory authority) and by the statement of civil remedies available to persons whose rights are infringed.

6.**Administrative Fines:** The administrative fines for breach of the GDPR are significant. For the most serious breaches, the **fines can be up to €20 million or 4% of the worldwide annual revenue of the prior financial year, whichever is higher.**
7.**Cost of Rectifying GDPR Breach:** There are certain circumstances in which an IP will be required to rectify a GDPR breach. Depending on the case and the circumstances of the particular breach, it should also be noted that the cost of rectifying such a breach can be considerable and it is a material issue that an IP needs to concern himself or herself with.
8.CCAB-I consulted with the office of the Data Protection Commission in the development of this Technical Release.
9.Finally, where the IP has to deal with significant amounts of Personal Data or any particularly sensitive Personal Data, it is advisable that the IP seek specific advice in relation to any particular issues that arise.

B.Key definitions
10.Reference should be made to Article 4 of the GDPR and Section 2 and other parts of the Act for key definitions. A summary of the most important definitions is set out below.

Article 28 Contract	A contract that every IP should ensure is put in place with Data Processors, whether those Data Processors be existing service providers to the debtor entity whose services are being continued, or service providers engaged by the IP following his or her appointment.
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes or a statement of affirmative action by which he signifies agreement to the Processing of Personal Data relating to him or her.
Data Controller(s)	The natural or legal person(s) which, alone or jointly with others, determine(s) the purpose and means of the Processing of Personal Data.
Data Processor(s)	A natural or legal person(s) which processes Personal Data on behalf of a Data Controller.
Data Subject(s)	An identified or Identifiable Natural Person(s).
Filing System	Any structured set of Personal Data which are accessible according to specific criteria.[1]
Identifiable Natural Person	A person who can be identified directly or indirectly, in particular by reference to an identifier such as a name or identification number, location data or one or more factors specific to the physical, physiological, genetic, mental, economic culture or social identity of that person.
Personal Data	Any information relating to an identified or Identifiable Natural Person.[2]
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.
Processing	Any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as the following: •collection; •recording; •organisation; •structuring; •storage; •adoption or alteration;

	•retrieval; •consultation; •use; •disclosure; •dissemination; •alignment or combination; •restriction; •erasure; •destruction.
Profiling	Any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymisation	The Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information.[3]
Special Categories of Personal Data	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

C.Insolvency Practitioners – General

11.No guidance has been issued by the Data Protection Commission concerning the application of the GDPR or the Act to the performance of the functions of insolvency practitioners.

12.It is important to remember that the GDPR and the Act relate only to the protection of the Personal Data of natural persons. Certain information obtained, accessed and utilised by an insolvency officer holder will relate to commercial and business counterparties of the entity to which they are appointed and therefore do not attract the protection of GDPR. However, in most assignments, the information and data utilised will include Personal Data relating to natural persons and therefore vigilance and awareness of the GDPR is essential.

13.Whether or not acting as agent of the entity to which they are appointed and whether in the exercise of their functions, IPs are Data Controllers or Data Processors and so it is imperative that IPs make themselves aware of the fundamentals of GDPR and put in place systems to ensure that they and their employees, agents and service providers adhere to the GDPR and the Act. Therefore IPs should consistently and continuously refer to the core principles (paragraph 31 below) of the GDPR and the duties and obligations of both Data Controllers and Data Processors (paragraphs 46 – 53 inclusive).

14.Whether an insolvency practitioner ("**IP**") becomes a Data Controller depends on whether he is a person who determines the purpose and means of the Processing of Personal Data.

15.Even if the IP is an agent of the relevant entity, if the IP makes decisions as to the purpose and means of the Processing of Personal Data, the IP will be subject to the obligations of a Data Controller. If the IP or his or her firm process Personal Data, the IP or his or her firm will assume the obligations of a Data Processor. Whilst the status of agent may in certain limited cases protect the IP against civil liability, it will not relieve the IP of the obligation to observe the laws of GDPR and the Act.

16.Every IP should ensure that there is in place a binding Article 28 Contract (see paragraphs 49 and 51) with Data Processors, whether those Data Processors be existing service providers to the debtor entity whose services are being continued or service providers engaged by the IP following his or her appointment. These binding Article 28 Contracts are designed to ensure that Processing carried out by a Data Processor meets all the requirements of the GDPR (not just those related to keeping Personal Data secure).

17.The requirements of the GDPR concerning such matters as informing Data Subjects of the data being held and processed and of their rights in relation to such data can be complied with by appropriate clear text in the IP's first communication informing creditors, debtors, employees and others of the appointment.

18.Where an IP is performing functions which are particular to his or her role as IP, it is likely that the IP will have become a controller of data obtained and utilised by him or her in the performance of those functions. The description of the IP as acting at all times for and on behalf of the company to which he or she has been appointed will not relieve the IP of the obligations attaching to the performance of those functions under the GDPR or the Act. The most common forms of data obtained by an IP under this heading would be employee related data, information obtained in response to communications requesting creditors and potential creditors to submit particulars of their claims for the purpose of adjudication of claims and the calculation of dividends, questionnaires to directors and officers and others concerning the affairs of the company for the purpose of:

a. the IP's own investigation and as to potential remedies against relevant parties, and
b. reporting to the Director of Corporate Enforcement and others.

Therefore IPs should be ready to issue, as part of the first communication with relevant parties informing them of the appointment, a compliant privacy notice which refers to the privacy policy being adopted by the IP. IPs should ensure that their privacy notices are specific and relevant to their engagement and should not use generic privacy notices. This is further discussed at paragraphs 63 to 70 below.

D. Liquidators

19.Where a liquidator accesses and retains Personal Data which was held by the company on the day of his or her appointment, he or she generally does so in his or her capacity as agent of the company. This will apply to such matters as the continuance of the business of the company. However once the liquidator commences determining the purpose and means of Processing of data following his or her appointment in the context of performing his or her functions of investigation or the adjudication of claims, the liquidator will become a Data Controller.

20.In connection with the performance of functions unique to the role of a liquidator, such as the gathering of information for the purpose of his or her investigations, statutory reporting, adjudication of claims, it is probable that the liquidator will himself or herself become a Data Controller.

21.The liquidator's firm is likely to become a Data Processor of relevant data as will any service providers to the liquidator. It is critical therefore that an Article 28 Contract be put in place between the Data Controller (whether acting through its duly appointed liquidator or otherwise) and every Data Processor.

E. Receivers

22.In most cases, the security pursuant to which a receiver has been appointed will declare the receiver to be acting as agent of the debtor. This will mean that in respect of data previously held by the company and of which the company is a Data Controller, the receiver will be acting as agent of that Data Controller. However, once the receiver commences to make decisions determining the purpose and means of Processing that data after his or her appointment, the receiver becomes a Data Controller and he or she must observe the rules regarding the obligations of a Data Controller and ensure that all Processing of Personal Data is compliant with the GDPR. In particular the receiver should ensure that an Article 28 Contract is in place with every Data Processor. It may be appropriate that, as with other contracts entered into by a receiver, the named Data Controller is still the company, now in receivership but acting through the receiver as its agent.

23.It is likely that the receiver's firm will be a Data Processor, as will any other service providers to the receiver.

24.The receiver's status could alter in cases where the agency terminates, for example on the winding up of the debtor company (save for NAMA statutory receivers).

25.The degree to which GDPR will directly affect the performance of functions of a receiver will vary depending on the precise nature and scope of the appointment, viz whether it is a full floating charge appointment or limited to fixed assets, and whether the receiver is agent of the company.

26.See also paragraphs 32 – 35 (inclusive) regarding lawfulness of Processing.

F. Examiners

27.An examiner generally is not agent of the company to which he or she is appointed. Therefore it is likely that in respect of Personal Data which the examiner takes into his or her possession or control the examiner will become a Data Controller.

28.Certain data will remain under the control of the company only, although the examiner will have rights of access thereto pursuant to the powers conferred on him or her by Part 10 of the Companies Act 2014 ("**CA 2014**"). For example, data of the kind which an investor may wish to access in the course of a due diligence, will typically remain within the control of the company. Even if the examiner does not become the Data Controller, if he or she facilitates access to data of the company in the context of a due diligence it is important to ensure that there is no ambiguity as to who is acting as Data Controller of the relevant data. In such circumstances the examiner

should ensure at least that the company puts in place measures to ensure that the GDPR and the Act are complied with in terms of confidentiality agreements etc.

29.The examiner may still become a Data Controller of Personal Data and it is likely that the examiner's firm will undertake certain Processing of Personal Data. Therefore an Article 28 Contract should be in place with the firm.

30.The position described above is unlikely to be any different in cases where the examiner applies under Section 528 (1) of the CA 2014 to exercise the powers of directors or under Section 528 (4) of the CA 2014 for the exercise of the powers of a liquidator.

G.The Seven Principles

31.Article 5 of the GDPR establishes the Seven Principles which govern the Processing of Personal Data. It provides that all Personal Data shall be:

a.processed lawfully, fairly and transparently;

b.collected for specified explicit and legitimate purposes and not further processed in a manner which is incompatible with those purposes;

c.adequate, relevant and limited to what is necessary for the purpose for which it is processed;

d.accurate and up to date;

e.stored for no longer than is necessary for the purpose for which it is processed;

f.processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage; and

g.the Data Controller is responsible for and must be able to demonstrate compliance with a. – f. above (inclusive) (the accountability rule). This is the Data Controller's obligation but relates both to the performance of functions by the Data Controller and Data Processors engaged by him or her.

H.Lawfulness of Processing (Non-Special Categories of Data)

32.Article 6 of the GDPR describes the conditions in which Processing is lawful when it comes to non-special categories of data (the Processing conditions for these categories are discussed further below). Under Article 6 of the GDPR, one of the following must apply:

a.the Data Subject has consented to the Processing;

b.Processing is necessary for the performance of a contract to which the Data Subject is party e.g. the loan agreement and security instrument entered into between a lender and a borrower;

c.Processing is necessary for compliance with a legal obligation of the Data Controller;

d.Processing is necessary to protect the vital interests of the Data Subject or of another natural person;

e.Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller; and

f.Processing is necessary in connection with and can be justified by reference to the legitimate interests pursued by the Data Controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data.

33.Legitimate Interests as a Lawful Basis (for Non-Special Categories of Data)

Legitimate interests is one of the six lawful bases for Processing non-special categories of Personal Data. As noted in paragraph 31, you must have a lawful basis in order to process Personal Data in line with the 'lawfulness, fairness and transparency' principle.

Article 6(1)(f) of the GDPR states that *"[P]rocessing shall be lawful only if and to the extent that…(f) [P]rocessing is necessary for the purposes of the legitimate interests pursued by the [Data] [C]ontroller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the [D]ata [S]ubject which require protection of [P]ersonal [D]ata, in particular where the [D]ata [S]ubject is a child."*

Legitimate interests is different to the other lawful bases as it is not centred around a particular purpose (for example, performing a contract with the individual), and it is not Processing that the individual has specifically consented to. Legitimate interests is more flexible and could in principle apply to any type of Processing for any reasonable purpose, provided that a balancing test can be met.

Essentially, because the legitimate interests legal basis can apply in a wide range of circumstances, the onus is on the Data Controller to conduct an analysis of the identified legitimate interests and consider the balancing of the necessity of Processing the Personal Data as weighed against the interests, rights and freedoms of the individual taking into account the particular circumstances.

The key elements of the legitimate interests provision and the associated balancing test can often be broken down into a three-part question test:

- •the purpose test – is there legitimate interests behind the Processing?
- •the necessity test – is the Processing necessary for that purpose? and
- •the balancing test – are the legitimate interests overridden by the individual's interests, rights or freedoms?

This means it is not sufficient for you to simply decide that it's in your legitimate interests and start Processing the data. You must be able to satisfy all three parts of the test prior to commencing your Processing.

I.Lawfulness of Processing (Sensitive Categories of Data)

34.Article 9(2) of the GDPR sets out the circumstances in which the Processing of sensitive Personal Data which is otherwise prohibited, may take place. The following categories of Personal Data are considered "sensitive" or "special", as set out in Article 9(1) of the GDPR:

a.racial or ethnic origin;
b.political opinions;
c.religious or philosophical beliefs;
d.trade union membership;
e.data concerning health;
f.data concerning sex life or sexual orientation; and
g.biometric data where processed to uniquely identify a person.

In order to process the above types of sensitive Personal Data one of the following legal bases under Article 9 of the GDPR must apply (and are all subject to further conditions):

a.the Data Subject has given explicit Consent;
b.the Processing is necessary in the context of exercising specific rights of the Data Controller or Data Subject in the field of employment, social security or social protection law;
c.the Processing is necessary to protect the vital interests of someone;
d.the Processing is necessary for the legitimate interests of a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim;
e.the Processing relates to Personal Data which is manifestly made public by the Data Subject;
f.the Processing is necessary for the establishment, exercise or defence of legal claims or in connection with courts acting in their judicial capacity;
g.the Processing is necessary for reasons of substantial public interest;
h.the Processing is necessary for the purposes of preventative or occupational medicine;
i.the Processing is necessary for reasons of public health;
j.the Processing is necessary for archiving purposes in the public interest, scientific, statistical or historical research purposes.

J.Lawfulness of Processing (Data Relating to Criminal Convictions and Offences)

35.Article 10 of the GDPR applies to Personal Data relating to criminal convictions and offences, or related security measures. This is an issue for the Office of the Director of Corporate Enforcement, the Companies Registration Office and / or the Courts Service regarding the publication of, for example, notices of disqualifications or restrictions or the publication of Court judgments. It is not an issue that insolvency practitioners are likely to come across. There must still be a lawful basis for the data Processing under Article 6 of the GDPR, in exactly the same way as for any other Personal Data. However, the difference is that if you are Processing personal criminal offence data, you will also need to comply with Article 10 of the GDPR. Article 10 of the GDPR in particular provides that such Processing can only be done in an official capacity as an authority or where the Act allows for such Processing.

K.Performance of a Legal Obligation or Exercise of Official Authority

36.Section 38(1)(a) of the Act provides that the Processing of Personal Data is lawful to the extent that such Processing is necessary and proportionate for: *"…the performance of a function of a [Data] [C]ontroller conferred by or under an enactment or by the Constitution…"*

The functions of insolvency office holders are not specifically referenced under Section 38 of the Act, but in so far as those functions are conferred on office holders by the CA 2014, they are conferred under an enactment. Therefore any Processing of Personal Data which is necessary and proportionate for the performance of such functions will be lawful by reference to Section 38 of the Act. This does not in any way mitigate the obligation of the office holder to ensure that Processing is compliant with GDPR and the Act.

37.Similarly, in respect of appointments over the charged assets of borrowers and obligors who are natural persons, the provisions of the loan agreement, the mortgage and the Land and Conveyancing Law Reform Act 2009, confer legal obligations on the appointed receiver and therefore any aspect of the performance of the functions of the receiver which is necessary and proportionate will be lawful, subject to compliance with the GDPR and the Act.

L.Rights of Data Subjects

38.The GDPR extends a number of rights that existed in the previous regime which individuals can exercise against Data Controllers, as well as having introduced certain new rights. The focus on individual rights, and on the transparency and accountability principles which underpin the GDPR, puts individuals and their rights at the heart of the GDPR. Data Controllers will need to consider all aspects of their Processing activities in light of the rights afforded to individuals, so that they will ultimately be in a position to demonstrate compliance not only when individuals seek to exercise those rights, but with their overall obligations under the GDPR.

39.Articles 12 to 22 and Article 34 of the GDPR govern the rights of Data Subjects which can be summarised as follows:

a.the right of access;
b.the right to be forgotten;
c.the right to restrict Processing;
d.the right to object;
e.the right to not be subject to automated decision making; and
f.the right to data portability.

40.None of these rights under GDPR are intended to be an absolute right and, in addition to the specific limitations set out in the GDPR, the Act provides for a number of additional restrictions in certain circumstances (discussed in further detail below).

M.Data Subject Access Requests

41.A Data Subject has the right to obtain from the Data Controller confirmation as to whether or not Personal Data concerning him or her is being processed and if so access to the Personal Data itself and comprehensive information concerning the purpose of the Processing, the categories of data concerned, recipients to whom such data will be disclosed, the period for which data will be stored, the existence of the right to request rectification or erasure, existence of the right to lodge a complaint with the Data Protection Commission, and the existence of automated decision making, including Profiling.

42.The Data Controller must, on request, provide a copy of the relevant Personal Data within one month (although Article 12 of the GDPR allows for this to be extended in certain scenarios). No charge can be imposed but for additional copies of the data a reasonable fee based on administrative costs may be charged. The Irish authorities have taken an extremely limited view of such administrative costs in the past.

43.Where requests from a Data Subject are manifestly unfounded or excessive, the Data Controller may either charge a reasonable fee taking into account the administrative costs of providing the information, communication or taking the action requested; or refuse to act on the request. However, the Data Controller bears the burden of demonstrating how the request was manifestly unfounded or excessive. The terms manifestly unfounded and excessive are not defined in the GDPR, however historically regulators and supervisory authorities have very narrowly interpreted restrictions when it comes to Data Subject access rights.

N.Restrictions on Exercise of Rights of Data Subjects

44.Section 60 (6) of the Act provides that the Minister may make regulations / statutory instruments restricting the exercise of certain rights of Data Subjects where such restrictions are necessary for the purpose of safeguarding of important objectives of general public interest. A regulation / statutory instrument are likely to be required from the Minister in order to prescribe such restrictions in detail. However, for the time being, Section 60 (7) of the Act defines "important objectives of public interest" to include the following:

i.financial loss or detriment due to the dishonesty, mal-practice or other improper conduct of, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services, or in the management of bodies corporate or other entities;
ii.financial loss or detriment due to the conduct of individuals who have been adjudicated bankrupt, or
iii.financial loss or detriment due to the conduct of individuals who have been involved in the management of a body corporate which is the subject of a receivership, examinership or liquidation under the CA 2014.

45.No regulations or statutory instruments have been made by the Minister under Section 60 (6) of the Act and therefore no specific restrictions apply to exercise of Data Subject rights against insolvency office holders.[4]

O.Responsibilities of Data Controllers

46.Every Data Controller is required to ensure and be able to demonstrate that Processing of data is performed in accordance with the GDPR. This must be done by implementing appropriate technical and organisational measures, including formulating and maintaining appropriate data protection policies.

47.Where two or more Data Controllers jointly determine the purposes and means of Processing they are joint controllers. Joint controllers are required to transparently determine their respective responsibilities for compliance with the GDPR. Data Subjects may exercise their rights against each of the Data Controllers, irrespective of the terms of the arrangement between them.

48.A Data Controller may only use Data Processors who provide sufficient guarantees to implement appropriate technical and organisational measures to ensure the Processing meets the requirements of the GDPR and the protection of the Data Subject.

49.Every engagement of a Data Processor must be subject to a binding contract between the Data Processor and the Data Controller stipulating the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects, and the rights and obligations of the Data Controller (Article 28 of the GDPR). See also paragraphs 93 – 100 (inclusive).

50.The Data Controller must carry out a Data Protection Impact Assessment, prior to certain Processing, when the Processing uses new technologies that could potentially impact upon the Data Subject's privacy, taking into account the nature, scope, context and purposes of the Processing, is likely to result in a high risk to the rights and freedoms of natural persons (Article 35 of the GDPR).

P.Responsibilities of Data Processors

51.The Data Processor shall only process data having been authorised to do so by the Data Controller, pursuant to a binding contract providing, in particular for the following:

a.that data should only be processed on documented instructions from the Data Controller;

b.that persons authorised to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c.shall comply with the obligation to ensure appropriate security of Processing;

d.shall engage another Data Processor only where authorised to do so and for specific activities, and will ensure that such other Data Processor is bound by corresponding obligations;

e.assist the Data Controller by appropriate measures for the fulfilment of the Data Controller's obligations to respond to Data Subject access requests and to ensure compliance with obligations concerning notifications of Personal Data Breaches;

f.appropriately disposes of all Personal Data after the end of the provision of Processing services;

g.makes available to the Data Controller all information necessary to demonstrate compliance with the GDPR.

52.A Data Processor shall not engage with another Data Processor without prior specific or general written authorisation of the Data Controller.

53.Every Data Processor must maintain a record of all categories of Processing activities it performs.

Q.Security of Processing

54.Every Data Controller and Data Processor must implement measures to provide a level of security appropriate to the risk in respect of Personal Data for which it is responsible.

R.Data breaches

55.Every Data Controller must notify a Personal Data Breach to the Data Protection Commission unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The notification must be made without undue delay and where feasible not later than 72 hours after becoming aware of it.

56.Where a Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons the Data Controller shall communicate the data breach to the Data Subject without undue delay. This obligation does not arise where the Data Controller has implemented appropriate protection measures, in particular those which render the Personal Data unintelligible to any person not authorised to access it, subject to encryption, or the Data Controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialise or notification would involve disproportionate effort. In such a case there must instead be a public communication or similar measure.

57.A Data Processor must notify the Data Controller without undue delay after becoming aware of any Personal Data Breach.

S.Border Transfers of Personal Data

58.Where a Data Controller or Data Processor intends to transfer Personal Data to a country outside the EU or to an international organisation special rules apply requiring the Data Controller and Data Processor to safeguard the protections for Data Subjects afforded by the GDPR and the Act.

59.As a general rule under the GDPR, there is a restriction on the transfer of Personal Data to countries outside of the European Economic Area ("**EEA**") (so called "**third countries**", which includes the UK).

60.The GDPR permits this restriction to be circumvented subject to appropriate safeguards, for example through the use of a legitimising transfer mechanism such as (1) Standard Contractual Clauses ("**SCCs**") (pre-approved model contracts for data transfers), (2) Binding Corporate Rules ("**BCRs**") (which are internal corporate rules, typically for use within multinational companies or (3) an adequacy decision.

61.Countries that have been approved pursuant to an adequacy decision by the European Commission are considered to have legal frameworks equivalent to those that safeguard personal data in the EU / EEA, as set out under the provisions of the GDPR. Since June 2021, an adequacy decision is in place for the UK under the GDPR, which means that Personal Data can (continue to) flow freely from an EU / EEA country to the UK, because it benefits from an essentially equivalent level of protection to that guaranteed under EU law.[5]

T.Data Protection Officers

62.Article 37 of the GDPR provides that where Processing is carried out by a public body (except courts acting in their judicial capacity), or where the core activities of the Data Controller or the Data Processor consists of Processing activities which, by virtue of their scope and/or purposes require regular and systematic maintaining of Data Subjects on a large scale, or their core activities consist of Processing on a large scale of Special Categories of Personal Data, the Data Controller and the Data Processor must designate a data protection officer. The terms "core activities" and "large scale" are not defined in the GDPR.

While there is no explicit requirement in the GDPR or the Act for Data Controllers or Data Processors to register with the Data Protection Commission (DPC), Article 37 of the GDPR provides that Data Controllers and Data Processors (who are required to have a Data Protection Officer (DPO)) shall publish the contact details of the DPO and communicate such details to their supervisory authority. In this regard, the DPC has established a mechanism/register for the registration of appointed DPOs (which the DPC has said is a mandatory registration requirement). Therefore in cases where an organisation, being either a Data Controller or Data Processor, appoints a DPO under Article 37 of the GDPR that appointment should be registered with the DPC.

If a DPO has been appointed in a company, consideration could be given by the IP to retaining and engaging the services of such a DPO (where such a DPO is independent of the shareholders, directors etc. of the company) when the relevant company is in liquidation or receivership.

63.The core tasks of a data protection officer are:

a.to inform and advise the Data Controller or the Data Processor and their relevant employees of their obligations pursuant to the GDPR and the Act;

b.to monitor compliance with the GDPR and the Act and with the policies of the Data Controller or the Data Processor;

c.to provide advice where requested as regards data protection impact assessments;

d.to cooperate with the Data Protection Commission; and

e.to act as the contact point for the Data Protection Commission.

U.Codes of Conduct

64.The GDPR provides for the drawing up of codes of conduct intended to contribute to the application of the GDPR taking account of the specific features of various Processing sectors and the needs of micro, small and medium-sized enterprises. Associations and other bodies representing categories of Data Controllers or Data Processors may prepare such codes of conduct and submit them to the DPC for approval, registration and publication. A code of conduct must provide mechanisms for mandatory monitoring by an appropriate body of compliance by Data Controllers or Data Processors who undertake to apply it, and for accreditation of that monitoring body by the DPC.

The following section of the document is based on the Consultative Committee of Accountancy Bodies (CCAB) document '*FAQs on the GDPR: Practical considerations for insolvency practitioners (IPs)*'. The member bodies of the Consultative Committee of Accountancy Bodies – Ireland (CCAB-I) acknowledges the permission given by CCAB for the use of their document in the development of this Technical Release.

V.FAQs for IPs

65.The following FAQs have been amended from a ROI perspective and are issued by CCAB-I.

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

66.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 notice (e.g. on a website or by hard copy form).

67.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 all your firm's accounting activities. It is expected that this would include a description of what data you collect, process and handle for the purposes of insolvency matters, but you should cover how you also handle data of prospective clients. Consideration should also be given to including a separate privacy notice on your website bespoke to insolvency matters.

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. Some firms include a sentence in their footer, to inform readers where they can find their privacy notice.

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

69.The privacy notice will relate to the data you collect and generate as office holder.

70.GDPR also requires that if the data is obtained from another source and not directly from the Data Subject, Data Controllers need to provide the required privacy information to the Data Subject 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.

71.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 Data Subjects can contact them to enforce their rights under the GDPR; and
- •the Data Subject's right to complain to the DPC if they consider there is a problem with the way you're handling their data.

72.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.

73.You should seek legal advice on your privacy notices to ensure they are compliant.

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

74.Some information held in payroll records or collected during recruitment might fall within the definition of special category data. Processing of special category data is prohibited unless certain very strict conditions are fulfilled. The strict conditions for Processing special category data should be examined carefully to establish that such Processing is lawful (see Article 9 of the GDPR).

75.Special category data is Personal Data the GDPR deems to be more sensitive and needs more protection. It includes information about a person's:

- •race;
- •ethnic origin;
- •politics;
- •religion;
- •trade union membership;
- •genetics;
- •biometrics (where used for ID purposes);
- •health (including incapacity to work, disability, sickness records);
- •sex life;
- •sexual orientation.

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

77.Crime related data is also subject to special conditions.
78.The form of the data isn't relevant so bear in mind that photos or security recordings could be Personal Data.
79.It is generally advised as best practice to try and either minimise the data collected relating to special categories (i.e. collect only 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. Encryption is recommended for as much Personal Data as possible.

What steps do I need to consider before appointment?

80.The extent of preparations which can be undertaken by a practitioner will depend on the nature and timing of the appointment and whether the practitioner has the facility to inform the scope and timing of the appointment.
81.As part of your take on processes you should carry out a GDPR risk analysis, ideally by speaking to whoever is responsible for overseeing GDPR compliance at the insolvent entity. This might be the directors, the Data Protection Officer (if there is one), the Data Protection Manager, the Head of Privacy or the Data Protection Contact.
82.You need to understand:

- what they have done in relation to the GDPR;
- their processes and procedures, including risk assessments already made;
- the type and nature of the data the company holds;
- whether any data needs to be securely destroyed;
- whether they have a bring your own device ("BYOD") 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?

83.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.
84.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.
85.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.

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

86.Even where the IP is acting as agent of the debtor entity, that fact will not render the IP immune from the obligation to take steps to identify whether the entity is GDPR-compliant by getting comfort 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 DPC if they believe that their Personal Data isn't being used appropriately or held securely; and
- marketing contracts are GDPR-complaint.

87.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.
88.The Data Protection Act 2018 repealed the requirement for certain Data Controllers and Data Processers to register with the Data Protection Commissioner. In Ireland there is now no such requirement to register.
89.If the business is holding or Processing special category data it needs to identify both a lawful basis for general Processing and an additional pre-condition for Processing this type of data (see also paragraph 34).

What about the company's books and records?

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

91.You cannot 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 backup 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 Personal Data is wiped.

92.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
- ensure you have a process for deleting Personal Data when it is no longer needed. That said, IPs should retain information to support employee and creditor claims for the life of the case, and for the usual retention periods.

93.You 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.

94.As the GDPR covers both paper and electronic data, you will need to be careful how you deal with any hard copy company books and records that you do not intend to take into your control. While the company is likely to be the Data Controller for any pre-insolvency records, that does not mean 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 and ensure the company's compliance with its obligations.

95.As regards retention of company records, reference should be made also to Section 707 of the Companies Act 2014 and in the case of a receiver to SIP 1B 'A receiver's responsibility for the mortgagor's records – Republic of Ireland (Updated 1 June 2015)'.

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

96.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 other specialists), the third party may be either a Data Controller or a Data Processor in relation to the Personal Data supplied to them. In certain circumstances the third party may be a joint controller with you. In that event an arrangement must be made regarding your respective functions as regards the data (see Paragraph 49). Where the third-party acts as a Data Processor you will need to ensure that a written contract reflects the GDPR (an Article 28 Contract).

97.Article 28 Contracts are designed to ensure that Processing carried out by a Data Processor meets all the requirements of the GDPR (not just those related to keeping Personal Data secure).

98.The Article 28 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 Data Controller.

99.The Article 28 Contract should also include the following compulsory terms:

- that the Data Processor must only act on the written instructions of the Data Controller (unless required by law to act without such instructions);
- that the Data Processor must ensure that people Processing the data are subject to a duty of confidence;
- that the Data Processor must take appropriate measures to ensure the security of Processing;
- that the Data Processor must only engage a sub-processor with the prior Consent of the Data Controller and a written contract;
- the Data Processor must assist the Data Controller in providing subject access and allowing Data Subjects to exercise their rights under the GDPR;
- that the Data 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 Data Processor must delete or return all Personal Data to the Data Controller as requested at the end of the contract; and
- the Data Processor must submit to audits and inspections, provide the Data Controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and inform the Data Controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or of a Member State.

100.It may be appropriate to include a provision for the third party to indemnify you against any breach.

101.It is advisable to include a statement that nothing within the contract relieves the Data Processor of its own direct responsibilities and liabilities under the GDPR.

102.When the term of the contract expires the IP should ensure that the third party has complied with any agreement to destroy data. This is especially important in the case of liquidations. Any agreements in place with Data Processors should be reviewed and a contingency agreement should be put in place in relation to the data to be destroyed (and the cost of same) once the liquidation of the relevant company has completed.

103.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?

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

105.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 Consent requires a positive opt-in and you cannot use pre- ticked boxes or any other method of default Consent.

106.You may consider that the legitimate interests basis applies. This is likely to be most appropriate where you use a person'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 assume the responsibility for considering and protecting the Data Subject's rights and interests. There are three elements to the legitimate interests basis. You need to:

- •identify the legitimate interests;
- •show that the Processing is necessary to achieve them; and
- •balance them against the individual's interests, rights and freedoms.

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

The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the "ePrivacy Regulations")

108.The 2002 ePrivacy Directive was implemented in Ireland through the 2011 ePrivacy Regulations. These regulations protect privacy rights in relation to electronic communications in Ireland. However 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, the ePrivacy Regulations continues to apply alongside the GDPR.

109.The ePrivacy Regulations covers:

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

110.While some of the rules only apply to organisations which provide a public electronic communications network or service, the ePrivacy Regulations 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).

111.The ePrivacy Regulations will also apply even if the business is not Processing Personal Data, as many of its rules protect companies as well as individuals, and the marketing rules apply even if you cannot identify the person you are contacting.

112.If you send electronic marketing or use cookies or similar technologies, from 25 May 2018 you must comply with both the ePrivacy Regulations and the GDPR.

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

113.The GDPR introduces a right for individuals to have Personal Data erased. This right to erasure is also known as 'the right to be forgotten'. Persons can make a request for erasure verbally or in writing and the Data Controller has one month to respond to a request.

114.The right of erasure 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 Data Subject withdraws their Consent;
•you are relying on legitimate interests as your basis for Processing, the Data Subject objects to the Processing of their data, and there is no overriding legitimate interests to continue this Processing;
•you are Processing the Personal Data for direct marketing purposes and the Data Subject objects to that Processing;
•you have processed the Personal Data unlawfully;
•erasure is necessary to comply with a legal obligation; or
•you have processed the Personal Data to offer information society services to a child.

115.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.

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

What about company laptops and mobile devices?

117.IPs should take all reasonable steps to locate and secure company computer equipment, 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.

118.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.

119.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.

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

120.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 is not disclosed. Encryption or Psuedonymisation may be appropriate measures.

121.You should also reflect the GDPR in the confidentiality agreements interested parties are requested to sign.

Can I still sell a company database?

122.GDPR does not preclude an IP from selling a database of customers or an in-house list of those who have registered on a website. However you should ensure that the company has records of what persons 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. Also, before selling a company's database, consideration should be given to the type of dataset being sold, for example, whether it contains Special Categories of Personal Data. If so, the IP should consider (i) doing a Data Protection Impact Assessment as to what safeguards can be done and (ii) redacting elements of the dataset in order to ensure that the data protection rights of individual employees or customers are not affected by the sale.

123.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. Therefore it would be important to establish the quality of the Consents in place before you invest time and cost in marketing a database. If a purchaser cannot satisfy itself that the company has the appropriate Consents in place, the value of the database may be significantly depleted.

124.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, because 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 persons on the database. Where appropriate, you should ensure that the contract imposes an obligation for the purchaser to seek Consent as soon as possible.

What about my pre-25 May 2018 appointments?

Existing appointments

125.If you have not previously informed creditors (being natural persons) and employees that you are holding their data and the reasons for doing so, 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.

126.Where you use a portal to host creditor reports, persons should be able to access either a privacy notice, or a link to your privacy notice.

Closed cases

127.You may also be holding data on persons in closed cases. The definition of Processing includes holding data. The first imperative is to establish whether there is any justification for continuing to hold such data. If so, and if not covered by a previous Privacy Notice, it may now be necessary to notify employees and creditors on closed cases that you are holding their data.

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

128.Engagement letters can be the most efficient method of ensuring that you have communicated key terms and the scope of your work to your client and of incorporating, at least by reference, a Privacy Notice.

Data breach notifications

What is a Personal Data Breach?

129.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.

130.Personal Data Breaches can include:

- •access by an unauthorised third party;
- •deliberate or accidental action (or inaction) by a Data Controller or Data 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?

131.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 to do if there is one. You should also have a register of breaches.

What should I do if a Personal Data Breach has occurred?

132.When a Personal Data Breach has occurred, you need to establish the likelihood and severity of the resulting risk to persons' rights and freedoms. You must notify the DPC within 72 hours of becoming aware of them unless the breach is unlikely to result in a risk to the rights and freedoms of persons. If you decide you don't need to report the breach, you need to be able to justify this decision, and you should document it.

133.If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those persons without undue delay. Therefore your staff should 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 contact is away from the office.

134.When reporting a breach, you must provide:

- •a description of the nature of the Personal Data Breach including, where possible the categories and approximate number of persons concerned;
- •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.

135.If it is not 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.

1 This Filing System does not have to be an IT based system and can include manual data.

2 The definition of Personal Data is a purposefully very broad one and in principle it covers any information that relates to an individual. A person's full name is an obvious likely identifier. But a person can also be identifiable from other information, including a combination of identification elements such as physical characteristics, pseudonyms, occupation, address etc. This definition is also technology neutral – it can be held in paper records, on an IT system or via another process such as CCTV or images.

3 This process is equivalent to "de-identifying" the data and essentially involves replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the Data Subject to be directly identified.

4 Section 60 (1) of the Act provides that certain rights and obligations towards Data Subjects are restricted to the extent specified in Section 60 (3) of the Act and may be restricted in regulations / statutory instruments made under Section 60 (5) or 60 (6). Section 60 (3) provides that subject to subsection (4) the rights of Data Subjects are restricted to the extent that the restrictions are necessary and proportionate for certain purposes, which include:

"(v)…for the enforcement of civil law claims, including matters relating to any liability of a [Data] [C]ontroller or [Data] [P]rocessor in respect of damages, compensation or other liabilities or debts related to the claim," and

"(vi) for the purpose of estimating the amount of the liability of a [Data] [C]ontroller on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of those rights or obligations would be likely to prejudice the commercial interests of the [Data] [C]ontroller in relation to the claim".

Section 60 (4) provides that the Minister may prescribe requirements to be complied with when the relevant rights and obligations are restricted. It may be argued that certain of the functions of an office holder fall within the purposes mentioned at (v) and (vi) above, in which case certain Data Subject rights, such as data access requests, may be capable of restriction provided the restriction is necessary and proportionate for the purpose of those functions. However, two considerations qualify this proposition:

A.The fact that Section 60 (6) expressly envisages the making of Ministerial regulations in respect of bankruptcy, receivership, examinership or liquidation matters, whereas no express reference to such processes is made in Section 60 (3) suggests that Section 60 (3) is not intended to apply to the functions of IPs.

B.Although the section speaks generally to the possibility of restrictions on the exercise of the rights of Data Subjects, it does not limit or mitigate the obligations of Data Controllers and Data Processors to adhere to the fundamental rules established by the GDPR.

5 The UK adequacy decision, however, includes a 'sunset clause', which limits the duration of adequacy to four years (i.e. 2025) and is designed as a safeguard in case of a divergence in the adequate level of data protection law in the UK. The European Commission continues to monitor the legal situation in the UK and could intervene at any point, if the UK deviates from the level of protection currently in place.