Data Protection Policy

Data protection is a vital ingredient in running a successful business, particularly in light of the UK GDPR and Data Protection Act 2018. This document has been updated for compatibility with the UK GDPR and is ready for use from January 2021

Produced by

Compliance Unit

Version V01/21

January 2021

This document is issued by the Compliance Department of:
PJG Recovery (GB) Limited and PJG Recovery Limited
11 Coopers Yard, Curran Road, Cardiff, CF10 5NB

Registered in England & Wales with numbers 05580693 and 07962945 at the address above
Recognised Professional Body (RPB): IPA
Data Protection Registration Numbers: ZA261992 and Z329258X Web: www.pjgrecovery.com

Version Control

Versions	Author	Date	Approved
V0315	Melanie Giles	28/3/2015	Melanie Giles
V0121	Kevin Still	31/1/2021	Melanie Giles

Contents

Section	Section name	Page
1	Introduction	3
2	Definitions	3
3	Data Protection Officer (DPO) and scope of the policy	5
4	Data protection principles	5
5	The rights of data subjects	6
6	Lawful, fair and transparent data processing	6
7	Consent	8
8	Specified, explicit and legitimate purposes	8
9	Adequate, relevant and limited data processing	9
10	Accuracy of data and keeping data up-to-date	9
11	Data retention	9
12	Secure processing	9
13	Accountability and record keeping	10
14	DPIAs and privacy by design	11
15	Keeping data subjects informed	12
16	Data subject access	13
17	Rectification of personal data	13
18	Erasure/deletion of personal data	13
19	Restriction of personal data processing	14
20	Data portability	14
21	Objections to personal data processing	14
22	Automated processing, decision-making and profiling	15
23	Direct marketing	15
24	Personal data collected, held and processed	15
25	Transferring personal data to a country outside the UK	15
26	Data breach notification	16

1. Introduction

This Data Protection Policy sets out the obligations of PJG Recovery Limited, a company registered in Wales under number 07962945, whose registered office is at 11 Coopers Yard, Curran Road, Cardiff CF10 5NB ("PJG") regarding data protection and the rights of data subjects (e.g. Staff, customers, joint debtors, carers, business contacts) in respect of their personal data under UK Data Protection Legislation (defined below).

This Policy sets out PJG's obligations regarding the collection, processing, transfer, storage and disposal of personal data. The procedures and principles set out must be followed at all times by PJG, its employees, agents, contractors or other parties working on behalf of PJG.

2. Definitions

"consent"	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they (by a statement or by a clear affirmative action) signify their agreement to the processing of personal data relating to them;
"data controller"	means the person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, PJG is the data controller of all personal data (e.g. staff, customers, joint debtors, carers, business contacts) used in our business;
"data processor"	means a person or organisation which processes personal data on behalf of a data controller;
"Data Protection Legislation"	means all applicable data protection and privacy laws including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation;
"data subject"	means a living, identified, or identifiable individual about whom PJG holds personal data;

"EEA"	means the European Economic Area (EEA), consisting of all EU Member States, Iceland, Liechtenstein and Norway;
"personal data"	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;
"personal data breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
"processing"	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"pseudonymisation"	means 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, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and
"special category personal data"	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric or genetic data.

3. Data Protection Officer (DPO) and scope of policy

PJG's Data Protection Officer (DPO) is Melanie Giles. The DPO is responsible for administering this Policy and for developing and implementing any applicable related policies (including those referred to in this Policy), procedures and/or guidelines. PJG maintains a Data Processing Register, a register of Data Processors and a Data Breach Register.

The DPO and the company directors are responsible for ensuring that any employees, agents, contractors or other parties working on behalf of PJG comply with this Policy and, where applicable, must implement such practices, processes, controls and training as are reasonably necessary to ensure such compliance.

Any questions relating to this Policy, PJG's collection, processing, or holding of personal data or to the Data Protection Legislation should be referred to the DPO.

4. The Data Protection principles

The Data Protection Legislation sets out the following principles with which any party handling personal data must comply. All personal data must be:

- processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
- accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the Data Protection Legislation in order to safeguard the rights and freedoms of the data subject;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5. The Rights of Data Subjects

The Data Protection Legislation sets out the following key rights applicable to data subjects:

- The right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure (also known as the 'right to be forgotten');
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights with respect to automated decision-making and profiling.

6. Lawful, Fair, and Transparent Data Processing

The Data Protection Legislation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the processing of personal data shall be lawful if at least one of the following applies:

- the data subject has given consent to the processing of their personal data for one or more specific purposes;
- the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the data controller is subject;
- the processing is necessary to protect the vital interests of the data subject or of another natural person;
- the 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; or
- the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

If the personal data in question is special category personal data (also known as 'sensitive personal data'), at least one of the following conditions must be met:

- the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so);

- the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by law or a collective agreement pursuant to law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
- the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
- the processing relates to personal data which is manifestly made public by the data subject;
- the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;
- the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19 of the Data Protection Act 2018) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

7. Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

- Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.
- Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.
- Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.
- If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

If special category personal data is processed, PJG shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.

In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that PJG can demonstrate its compliance with consent requirements.

8. Specified, explicit and legitimate Purposes

PJG collects and processes the personal data. This includes:

- personal data collected directly from data subjects; and
- personal data obtained from third parties (e.g. creditors).

PJG only collects, processes and holds personal data for the specific purposes and for other purposes expressly permitted by the Data Protection Legislation (e.g. Anti-Money Laundering obligations).

Data subjects must be kept informed at all times of the purpose or purposes for which PJG uses their personal data.

9. Adequate, relevant and limited data processing

PJG will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 8, above.

Employees, agents, contractors or other parties working on behalf of PJG may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

10. Accuracy of data and keeping data up-to-date

PJG shall ensure that all personal data collected, processed and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 17, below.

The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. For customers in a debt solution, this will be at least annually. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate. This policy is aligned with PJG's Vulnerability Policy, which can involve the collection, processing and retention of special category data that may need to be assessed more frequently.

11. Data retention

PJG shall not keep personal data for any longer than is necessary taking account of the purpose or purposes for which that personal data was originally collected, held and processed. This reflects any regulatory requirements in respect of data retention and record keeping.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details of PJG's approach to data retention, including retention periods for specific personal data types held by PJG, please refer to our **Data Retention Policy**.

12. Secure processing

PJG shall ensure that all personal data collected, held and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the technical and organisational measures which shall be taken are provided in PJG's **Data Security Policy**.

All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.

Data security must be maintained at all times by protecting the confidentiality, integrity and availability of all personal data as follows:

- only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;
- personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and
- authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

13. Accountability and record keeping

The DPO is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

PJG shall follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments (DPIAs) will be conducted if any processing presents a significant risk to the rights and freedoms of data subjects (please refer to Part 14 for further information).

All employees, agents, contractors or other parties working on behalf of PJG shall be given appropriate training in data protection and privacy, addressing the relevant aspects of the Data Protection Legislation, this Policy, and all other applicable PJG policies.

PJG's data protection compliance shall be regularly reviewed and evaluated by means of data protection internal audits using an experience compliance and data protection expert.

PJG shall keep written internal records of all personal data collection, holding and processing, which shall incorporate the following:

- the name and details of PJG, its DPO and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);
- the purposes for which PJG collects, holds and processes personal data;
- PJG's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data;
- details of the categories of personal data collected, held and processed by PJG, and the categories of data subject to which that personal data relates;
- details of any transfers of personal data to non-UK countries including all mechanisms and security safeguards;

- details of how long personal data will be retained by PJG (please refer to PJG's Data Retention Policy);
- details of personal data storage, including location (e.g. in cloud); and
- detailed descriptions of all technical and organisational measures taken by PJG to ensure the security of personal data.

14. DPIAs and privacy by design

In accordance with privacy by design principles, PJG shall carry out Data Protection Impact Assessments (DPIA) for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a higher risk to the rights and freedoms of data subjects (e.g. Debt Respite Scheme assessments for mental health crisis moratoriums).

The principles of privacy by design is followed at all times when collecting, holding, and processing personal data. The following factors are routinely taken into consideration:

- the nature, scope, context and purpose or purposes of the collection, holding and processing;
- the relevant technical and organisational measures to be taken;
- the cost of implementing such measures; and
- the risks posed to data subjects and to PJG, including their likelihood and severity.

DPIAs are overseen by the DPO and address the following:

- the type(s) of personal data that will be collected, held, and processed;
- the purpose(s) for which personal data is to be used;
- PJG's objectives;
- how personal data is to be used;
- the parties (internal and/or external) who are to be consulted;
- the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- risks posed to data subjects;
- risks posed both within and to PJG; and
- proposed measures to minimise and handle identified risks.

15. Keeping data subjects informed

Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection. Any letter of engagement that PJG issues references our Privacy Notice.

Personal data processing will continue post-appointment and continue to assess the data protection risks and requirements and ensure that PJG has in place the necessary consent and appropriate controls and policies surrounding its handling of personal data.

Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

- if the personal data is used to communicate with the data subject, when the first communication is made; or
- if the personal data is to be transferred to another party, before that transfer is made; or
- as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided in PJG's **Privacy Notice**:

- details of PJG including, but not limited to, contact details, and the names and contact details of any applicable representatives and its DPO;
- the purpose(s) for which the personal data is being collected and will be processed and the lawful basis justifying that collection and processing;
- where applicable, the legitimate interests upon which PJG is justifying its collection and processing of the personal data;
- where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- where the personal data is to be transferred to one or more third parties, details of those parties;
- where the personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place (see Part 25 of this Policy for further details);
- details of applicable data retention periods;
- details of the data subject's rights under the Data Protection Legislation;
- details of the data subject's right to withdraw their consent to PJG's processing of their personal data at any time;
- details of the data subject's right to complain to the ICO;
- where the personal data is not obtained directly from the data subject, details about the source of that personal data;
- where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

- details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

16. Data Subject Access

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which PJG holds about them, what it is doing with that personal data, and why.

Employees wishing to make a SAR should do so using a Subject Access Request Form, sending the form to PJG's DPO.

Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to 2 months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

All SARs received shall be handled by PJG's DPO and in accordance with PJG's **Data Subject Access Request Policy & Procedure**. As a small firm this has been kept as simple as possible and to maintain a very personal service with a named contact at PJG.

PJG does not charge a fee for the handling of normal SARs. PJG reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

17. Rectification of personal data

Data subjects have the right to require PJG to rectify any of their personal data that is inaccurate or incomplete.

PJG shall rectify the personal data in question and inform the data subject of that rectification, within one month of the data subject informing PJG of the issue. The period can be extended by up to 2 months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

18. Erasure/deletion of personal data

Data subjects have the right to request that PJG erases the personal data it holds about them in the following circumstances:

- it is no longer necessary for PJG to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- the data subject wishes to withdraw their consent to PJG holding and processing their personal data;
- the data subject objects to PJG holding and processing their personal data (and there is no overriding legitimate interest to allow PJG to continue doing so) (see Part 21 of this Policy for further details concerning the right to object);
- the personal data has been processed unlawfully; or
- the personal data needs to be erased in order for PJG to comply with a particular legal obligation.

Unless PJG has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to 2 months in the case of complex requests. If such additional time is required, the data subject shall be informed. In the event that any personal data that is to be erased in response to a SAR has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

19. Restriction of personal data processing

Data subjects may request that PJG ceases processing the personal data it holds about them. If a data subject makes such a request, PJG shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

20. Data Portability

PJG processes personal data using automated means.

21. Objections to personal data processing

Data subjects have the right to object to PJG processing their personal data based on legitimate interests and for direct marketing (including profiling) purposes.

Where a data subject objects to PJG processing their personal data based on its legitimate interests, PJG shall cease such processing immediately, unless it can be demonstrated that PJG's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims. Where a data subject objects to PJG processing their personal data for direct marketing purposes, PJG shall cease such processing promptly.

22. Automated processing, automated decision-making and profiling

Not applicable.

23. Direct Marketing

PJG is subject to certain rules and regulations when marketing its products and services. Some of these relate to operating as an insolvency practice.

The prior consent of data subjects is required for electronic direct marketing including email, text messaging and automated telephone calls subject to the following limited exception:

PJG may send marketing text messages or emails to a customer provided that that customer's contact details have been obtained in the course of a sale, the marketing relates to similar products or services, and the customer in question has been given the opportunity to opt-out of marketing when their details were first collected and in every subsequent communication from PJG.

The right to object to direct marketing shall be explicitly offered to data subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve its clarity.

If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal data may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.

24. Personal data collected, held and processed

For details of data retention, please refer to PJG's Data Retention Policy.

25. Transferring personal data to a country outside of the UK

PJG may, from time to time, transfer ('transfer' includes making available remotely) personal data to countries outside of the UK. The Data Protection Legislation restricts such transfers in order to ensure that the level of protection given to data subjects is not compromised.

Personal data may only be transferred to a country outside the UK if one of the following applies:

- The UK has issued regulations confirming that the country in question ensures an adequate level of protection (referred to as 'adequacy decisions' or 'adequacy regulations'). From 1 January 2021, transfers of personal data from the UK to EEA countries will continue to be permitted. Transitional provisions are also in place to recognise pre-existing EU adequacy decisions in the UK.

- Appropriate safeguards are in place including binding corporate rules, standard contractual clauses approved for use in the UK (this includes those adopted by the European Commission prior to 1 January 2021), an approved code of conduct, or an approved certification mechanism.
- The transfer is made with the informed and explicit consent of the relevant data subject(s).
- The transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between the data subject and PJG; public interest reasons; for the establishment, exercise, or defence of legal claims; to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent; or, in limited circumstances, for PJG's legitimate interests.

26. Data breach notification

All personal data breaches must be reported immediately to PJG's DPO.

If an employee, agent, contractor or other party working on behalf of PJG becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the DPO must ensure that the ICO is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 26.3) to the rights and freedoms of data subjects, the DPO must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of PJG's data protection officer (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by PJG to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Reference material

IPA – October 2018

https://insolvency-practitioners.org.uk/uploads/documents/efe03f9987513fae5a37f9bd54f8ff4b.pdf

This Policy shall be deemed effective as of 31/1/2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Melanie Giles FIPA FABRP
Licensed Insolvency Practitioner

o +44 (0) 29 20346530 f +44 (0) 29 20346531
e melaniegiles@pjgrecovery.com w www.pjgrecovery.com
d +44 (0) 29 20346532 m +44 (0) 7713 739583