DATA BREACH POLICY
May 2018

This document sets out the policy of LA Business Recovery Limited ("the Company") where there is a breach or suspected breach of confidentiality or data privacy.

Acting lawfully and protecting the privacy of our Staff Members, prospective clients and those involved in the formal insolvency appointments that we deal with is a responsibility that the Company takes seriously at all times.

This policy applies to any breach or suspected breach of the confidentiality and/or data privacy of all persons that the Company deals with.

Confidentiality and Data Privacy

Individuals, companies, partnerships and other artificial legal persons all have rights to confidentiality that the Company and Staff Members must respect. Individual living persons also have rights to data privacy in respect of their personal data, contained in the data protection legislation.

The nature of insolvency practice is such that confidential information (some of which may also be described as personal data) will come into our possession in the ordinary conduct of the Company's business activities.

A list of the different types of personal data ("data categories") that we deal with in respect of different individuals ("data subjects"), can be found in our Data Processing Register. This policy is available on request via virgil@labr.co.uk or to Virgil Levy in writing.

The Code of Ethics for Insolvency Practitioners requires Client Confidentiality and the Data Protection framework provides safeguards to protect the privacy of individuals' personal data.

Breaches of Confidentiality and/or Data Privacy

What is a breach?

A breach of confidentiality is the disclosure of confidential information to a person or persons who were not entitled to receive the information. Examples include sending a sensitive communication to the wrong recipient or the accessing of files or computer equipment by an unauthorised person.

A 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. It would include examples such as the above, but would also extend to other potential transgressions of an individual's rights – such as the processing of their data in a manner that is beyond the scope of the purpose for which it was provided (for example, using an Advice Client's contact details of unrelated marketing purposes, retaining their personal data for longer than is necessary or accidentally deleting their file).

Some breaches may be prospective in nature: for example, if a document containing personal data is left in a public place or a piece of computer equipment is stolen. While the finder/perpetrator might

not actually access the information the document or equipment contains, their potential ability to do so still amounts to a breach.

Breaches of confidentiality or data privacy may be accidental or deliberate (unlawful).

How can breaches be avoided?

The principle mechanism for avoiding a breach of confidentiality and/or data privacy is adherence to the policies and procedures that the Company has established to manage the potential risks of a breach. Of particular importance is the Confidentiality and Data Security Policy, which is available on request to virgil@labr.co.uk or to Virgil Levy in writing. Although there are a number of other policies which are relevant and reflect our commitment to privacy by design:

- Confidentiality and Data Security Policy
- Data Breach Policy
- Data Retention & Destruction of Records Policy
- Data Protection Checklist for Formal Appointments Policy
- Data Subject Access Policy
- Special Category Data Policy
- Supplier Oversight Policy

Training for Staff Members in relation to these policies is provided. If a Staff Member identifies or suspects a weakness or has a concern about the robustness of any process that they are asked to employ, they should raise that concern with their Line Manager. Any ideas or suggestions for how the Company can continue to protect or enhance our approach to confidentiality and data privacy are always welcomed.

When to report a breach internally?

Whenever a Staff Member becomes aware or suspects that a breach has occurred, they must report it as soon as they become aware of it.

During business hours, reports should be made to the Staff Member's Line Manager, by email. If the Line Manager is known to be absent from the business for any reason, a report may be made to an alternative Director who is known to be working within the business at the time. If the breach occurs outside of ordinary business hours and is considered potentially serious, it should be reported by text message or telephone call to a Director.

Staff Members should be aware that reporting a breach will not necessarily result in any disciplinary action (in the demonstrable absence of a breach of policy or procedure, or negligence or malpractice by the Staff Member). Prompt reporting will always be commended and may be a mitigating factor in any disciplinary action.

It is vital that breaches or suspected breaches are reported promptly. Failure to report a known breach is itself a disciplinary matter that the Company will take very seriously.

What will happen once reported internally?

When reported internally, the recipient of the breach report must record the breach in the Data Breach Register. Where the breach concerns an insolvency case, the Office Holder should also be advised.

Assessment of risks to rights and freedoms

When a breach report is received, the recipient must assess whether the breach is likely to result in a risk to any person's rights or freedoms. They may discuss this with Virgil Levy or David Hughes in formulating a view.

In assessing the risk to and rights and freedom, the focus should be upon the potential negative consequences for the individual concerned.

Examples of the types of harm that could be suffered include (but are not limited to) inability to access data, damage to reputation, loss of confidentiality or identity theft.

- ***Low risk – unlikely to result in harm to rights and freedoms:*** Where a breach is prospective (such as the loss of a password protected smartphone), or capable of full remedy (such as the accidental deletion of data that can be readily restored), it will less likely result in harm, particularly where acted upon promptly. Similarly, where the nature of the data concerned is not sensitive or is otherwise already a matter of public record (such as the name and address of a bankrupt), it is unlikely that there will be negative consequences from a breach to the individual concerned. In such circumstances, risk may be assessed as low.

- ***Medium risk - likely to result in harm to rights and freedoms:*** Where there is an actual (rather than potential) breach of security leading to the disclosure of, or access to, personal data the severity of the risk will be greater. The nature of the personal data involved will be particularly relevant to the risk assessment and breaches in relations to special categories of data (see Special Category Data Policy, which is available on request via virgil@labr.co.uk or to Virgil Levy in writing) will always present such a risk. Sending a communication containing sensitive information to the incorrect recipient would be likely to fall into that category, where that information is not already in the public domain.

- ***High risk – high risk to rights and freedoms*:** The most serious breaches would include the hacking of our computer systems or the loss of a case file. Breaches in relation to the inappropriate disclosure of special categories of information may also fall into this category.

The risk assessment should be conducted within 24 hours of receipt of the breach report. Once completed, the outcome of that risk assessment should also then be recorded in the Data Breach Register.

In all cases, the Company will consider whether any alterations to policy or procedure are warranted to avert any future breach of the type that has occurred.

External Reporting Requirements

The external reporting requirements upon the Company will depend upon the level of risk identified and the capacity in which we are processing the data concerned.

When acting as Data Controller

In most instances, the Company will be acting as Data Controller or Joint Data Controller with the Office Holder, Official Receiver, Accountant in Bankruptcy (AiB), or the insolvent entity itself (in respect of corporate insolvency appointments).

Following the breach risk assessment:

- If the risk assessment indicates that the risk of harm to rights and freedoms is **unlikely** (i.e. low risk), no further action beyond the remedy of the breach (where possible) and the recording for the breach in the Data Breach Register is be required;

- Where a breach is identified as **likely** to result in a risk to a person's rights and freedoms (i.e. medium risk) then the breach must be recorded in the Data Breach Register and notification sent to the Information Commissioners Office (ICO). Breaches can be reported online at: https://ico.org.uk/for-organisations/report-a-breach/

Breaches must be reported to the ICO without undue delay, but not more than 72 hours of the Company becoming aware of it.

- Where the is a **high risk** to rights and freedoms, in addition to recording the breach and notifying the ICO, the individual(s) who may be affected must also be notified of:
  - The nature of the breach;
  - The contact details of the Staff Member who can supply further information;
  - A description of the likely consequences; and
  - The measures taken, or proposed to be taken, to deal with the breach and, where appropriate, to mitigate any possible adverse effects.

When acting as Data Processor

Given that insolvency practice is a professional service, it is likely that in most instances and insolvency practice will be a Data Controller in respect of the data it holds within its files and systems. However, in some limited circumstances, the Company may be acting as a Data Processor for an insolvent entity, or under contract for another firm or insolvency practitioner or the Accountant in Bankruptcy.

When acting as Data Processor, the all breaches must be reported without undue delay to the relevant Data Controller.

When acting as Agent of an Insolvent Company

There is legal precedent suggesting that an insolvency practitioner is neither a Data Controller nor Data Processor when acting purely as an agent of an insolvent company over which they have been appointed, when dealing with the data which that company holds.

Agency status will not apply to the information contained in the insolvency practitioner's files or on their own Company's computer system.

When acting as Agent, reference should be made the insolvent entity's confidentiality and data protection arrangements and to our Data Protection Checklist for Formal Appointments. This is available on request made to Virgil Levy at virgil@labr.co.uk or in writing.

Requirements on Staff Members

In all circumstances, Staff Members are expected to apply the appropriate standards of care, confidentiality and privacy to avert possible data breaches, whether the Company, as Data

Controller or Data Processor, or when acting as Agent for an insolvent company that is itself a Data Controller or Data Processor.

If a Staff Member becomes aware of any breach confidentiality or data privacy, they must report it as soon as they become aware of it, even where doing so may implicate themselves in some failing or potential misconduct.

Any failure to follow the procedures and guidance laid out in this Policy may lead to disciplinary action which could result in termination of employment.

The Company reserves the right to pursue a claim for recovery of costs incurred where a Staff Member fails to adhere to this Policy and the Company suffers loss or damage.