CONTENTS

1. POLICY STATEMENT

PROCABS HACKNEY SERVICES LTD, as a controller and processor of personal data, needs to collect personal information from employees, customers, suppliers and clients to effectively carry out our everyday business functions and activities and to provide a taxi booking service. In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations.

We are committed to processing all personal data in accordance with the General Data Protection Regulation (GDPR), Irish data protection laws and any other relevant codes of conduct.

The Company adopts a 'Privacy by Design' approach to minimise the risk of breaches and uphold the protection of personal data. We have implemented data management systems and processes to protect personal information, including policies, procedures, records and control measures. We undertakes staff training, audits and risk assessment to ensure maximum and continued compliance with data protection laws and principles.

This policy also serves as a reference document for employees and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

2. SCOPE

This policy applies to all staff within the Company i.e. permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

3. GENERAL DATA PROTECTION REGULATION (GDPR)

As the Company processes personal information regarding individuals (data subjects), we are obligated under the General Data Protection Regulation (GDPR) (EU 2016/679), to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

PERSONAL DATA

Information protected under the GDPR is known as "personal data" and is defined as*: "Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

4. OBJECTIVES

We ensure all personal data is processed in accordance with data protection laws and principles, and any associated regulations and/or codes of conduct laid down by the Supervisory Authority and Irish law. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

We have developed objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements. The Company ensures that:

- We protect the rights of individuals with regards to the processing of personal information
- We develop, implement and maintain a data protection policy, procedure, audit plan and training programme for compliance with the data protection laws
- Business practices and process are monitored for compliance
- Personal data is processed, only where we have verified and met the lawfulness of processing requirements
- When relevant, we record consent at the time it is obtained and evidence such consent to the Data Protection Commissioner when requested.
- Where consent is not a requirement, we establish and verify the legitimate basis for collection and processing of personal data.
- Employees are aware of their data protection and are provided with relevant training in data

protection laws, principles, regulations and how they apply to their role and the Company

- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws
- We maintain a continuous programme of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary
- We monitor the Supervisory Authority, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements
- We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting breaches or complaints with regards to data protection
- We perform regular audits and assessments on how the personal data we process is obtained, used, stored and shared. The audit programme is reviewed against our data protection policies, procedures and the relevant regulations to ensure continued compliance
- We provide clear reporting lines and supervision with regards to data protection
- We store and destroy personal information, in accordance with our data retention policy
- Information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible and easily accessible form
- Employees are aware of their own rights under the data protection laws
- We maintain records of processing activities
- We have developed and documented appropriate technical and organisational measures and controls for personal data security and have a robust Information Security programme in place

5. GOVERNANCE PROCEDURES

5.1 ACCOUNTABILITY & COMPLIANCE

We carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of personnel data processing.

We have implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the data protection laws and can evidence such measures through our documentation and practices.

The technical and organisational measures in place to safeguarding of personal data and to ensure and demonstrate compliance with data protection laws, regulations and codes of conduct are detailed in this document and associated policies / procedures.

5.2 PERSONAL INFORMATION INVENTORY

We record and categorise all personal information obtained, processed and shared and have compiled a Data Inventory which includes: -

- The personal data we hold
- From where it came
- With whom it is shared
- The legal basis for processing
- The retention format
- The person(s) responsible
- Disclosures and Transfers

5.3 PRIVACY BY DESIGN

We operate a 'Privacy by Design' approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We have developed controls and measures, which help us enforce this ethos.

5.4 DATA MINIMISATION

Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws. We obtain, retain, process and share only the data which is essential to carry out our services and/or meet our legal obligations and retain data only for as long as is necessary.

Measures to ensure that only the necessary data is collected includes: -

- Electronic collection (i.e. forms, website, mobile app etc.) only have the fields relevant to the purpose of collection and subsequent processing.

  We do not include 'optional' fields regarding the collection of data necessary to provide a taxi booking service; optional denotes that collection of this data is not necessary to fulfil the service
- Physical collection (telephone etc.) is supported using scripts and/or computer systems where the required data collection is ascertained using predefined fields.
- We have SLAs and bespoke agreements in place with third-party controllers who send us personal information (either in our capacity as a controller or processor). Only relevant and necessary data related to the processing activity is provided
- We have documented destruction procedures in place where a data subject or third-party provides us with personal information that is surplus to requirement
- Forms, contact pages and any documents used to collect personal information are reviewed regularly to ensure they are fit for purpose and only obtaining necessary personal information in relation to the legal basis being relied upon and the purpose of processing

5.5 ENCRYPTION

We utilise encryption as a further risk prevention measure for securing the personal data we hold. Encryption is used to make data indecipherable unless decryption of the dataset is carried out using an assigned key/code.

5.6 RESTRICTION

The Company's processes, systems and structure ensures that only those with authorisation and/or a relevant purpose, have access to personal information.

5.7 HARD COPY DATA

Where information is retained in paper format, it is stored in secure locked cabinets.

6. COMPLIANCE OFFICER

We have appointed a Compliance Officer who takes overall responsibility for implementation and ongoing compliance with data protection laws, actively stays informed and up-to-date with all legislation and changes relating to data protection and ensures all processes, systems and staff are compliant and operating within the requirements of the data protection laws and its principles.

7. LEGAL BASIS FOR PROCESSING

Prior to any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using that which is most appropriate

The legitimate basis is documented on our Personal Data Inventory and, where applicable, is provided to the data subject and Supervisory Authority. Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where:

- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

  OR

  The data subject has given consent to processing of their personal data for specific purposes
- Processing is necessary for compliance with a legal obligation to which we are subject
- Processing is necessary to protect the vital interests of the data subject or of another person
- Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a

third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data).

7.1 PROCESSING SPECIAL CATEGORY DATA
We do not process any special category personal data or information relating to criminal convictions.

8. RECORDS OF PROCESSING ACTIVITIES
As an organisation with less than 250 employees, we may not maintain records of all processing activities, except for those required as a Taxi Dispatch operator.

For the purpose of providing a taxi booking service, we maintain records of processing activities, maintain records on computer systems and, for some purposes, in hard copy, in a clear a format and readily available, on request.

9. THIRD-PARTY PROCESSORS
The Company may utilise external processors for processing certain activities.

We use information audits to identify, categorise and record all personal data which may be processed on servers, outside of the company, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible.

We have strict due diligence measures in place and review, assess and evaluate all processors prior to forming a business relationship. We may obtain company documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task employed. We assess their processes and activities prior to and during the contract period to ensure compliance.

10. DATA RETENTION, ERASURE & DISPOSAL
10.1 RECORDS STORAGE & ACCESS
PROCABS HACKNEY SERVICES LTD retains records and personal information about the persons we employ, work with or have a business relationship with for legitimate or legal business reasons only. In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations. Personal data, which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed and required by regulation / legislation.

Electronic and hard copy documents containing personal data, and associated correspondence and internal memoranda, are always retained in a secure location, with controlled and authorised access.

10.2 DESTRUCTION AND DISPOSAL OF RECORDS & DATA
When the retention period shown on the Personal Data Inventory has elapsed, all personal data, on paper or electronic media, is disposed of in a manner which protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion). Electronic records will be deleted in a secure manner so that it cannot be reconstructed. Hard copy documents will be shredded

On occasions, the data may be anonymised.

10.3 EQUIPMENT DISPOSAL
Where possible, information is wiped from the equipment through use of software and formatting, however this can still leave imprints or personal information that is accessible and so we ensure the secure disposal of all assets.

10.4 SUSPENSION OF RECORD DISPOSAL FOR LITIGATION OR CLAIMS
If we are served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against our firm, we will suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

11. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

The Company will conduct a Data Protection Impact Summary in advance of introduction of new systems or technology which have an impact on personal data processed or stored. DPIA, We continually monitor all activities against the GDPR Article 35 requirements and have robust DPIA procedures already developed, should they be necessary.

12. DATA SUBJECT RIGHTS PROCEDURES

Data protection law defines consent as: *"Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*.

Optional provision of personal data is not an option in booking a taxi service; it is a requirement of contract fulfilment. Providing the minimum personal data, necessary for service, is deemed as consent.

Where processing is based on consent, *COMPANY NAME* ensures that consent requests are transparent, using plain language. Pre-ticked, opt-out boxes are not used. Consent is always freely given (telephone, in writing - documented affirmative action, email, website, booking app). Evidence of all consent or request for service is retained.

Electronic methods of providing personal data and/or gaining consent (i.e. website or mobile app) are regularly reviewed to ensure that a compliant Privacy Notice is accessible and that consent is clear.

Where consent is obtained through direct telephone call by an individual, we utilise scripts and/or computer systems, using predefined fields, which show the required data to be collected to fulfil the contract request. A record of each phone call is retained as evidence.

We ensure that withdrawing consent is as easy. Consent withdrawal requests are processed immediately and without detriment

12.1 INFORMATION PROVISION / PRIVACY NOTICE

Where personal data is obtained directly from the individual (i.e. through consent by employees, written materials and/or electronic formats (i.e. website, mobile booking app etc.)), we make our privacy notice available in an appropriate manner.

Privacy Notices provide individuals with the necessary and legal information about how, why and when we process their data, along with their rights and obligations:

- The contact details of our data controller and compliance officer
- The purpose of the processing for which the personal information is intended
- The legal basis for the processing
- The recipients or categories of recipients of the personal data (if applicable)
- The criteria used to determine that period for which the personal data will be stored.
- The existence of the right to request access to and rectification or erasure of personal data
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with the Supervisory Authority
- Notification that providing personal data is a requirement necessary for booking of the taxi service and of the consequences of failure to provide such data

Records pertaining to the consent obtained are maintained and stored for 7 years from the date of consent, unless there is a legal requirement to keep the information for a longer period.

12.2 PERSONAL DATA NOT OBTAINED FROM THE DATA SUBJECT

The Company only processes and stores personal data which is obtained directly from a data subject, except in circumstances where it is necessary for fulfilment of a taxi booking service.

12.3 EMPLOYEE PERSONAL DATA

We do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated to ensure that employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with a Privacy Notice specific to the personal information we collect and process about them.

12.4. CONTRACTED DRIVER PERSONAL DATA

We do not use consent as a legal basis for obtaining or processing driver personal information. Our Driver Contract has been updated to ensure that drivers are provided with the appropriate information disclosure and are aware of how we process their data and why.

The Driver Contract informs them of their rights under the data protection laws and how to exercise these rights and are provided with a Privacy Notice specific to the personal information we collect and process about them.

12.5. THE RIGHT OF ACCESS

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide:

- The purposes of the processing
- The categories of personal data concerned
- The recipients / categories of recipient to whom the personal data have been or will be disclosed
- The envisaged period for which the personal data will be stored.
- The existence of the right to request rectification or erasure of personal data
- The right to lodge a complaint with a Supervisory Authority

Requests are passed to the Compliance Officer as soon as received and a record of request noted.

Under normal circumstances, the requested information is provided free of charge, at the earliest convenience, but at a maximum of 30 days from the date the request is received. In exceptional circumstances and where the retrieval or provision of information is particularly complex or subject to a valid delay, the period may be extended by two months. The data subject will be informed of any delay.

Release of information is subject to subject to prior verification of the identity of the Data subject.

12.6. CORRECTING INACCURATE OR INCOMPLETE DATA

To the extent possible, data held by the Company is reviewed and verified as being accurate. Where inconsistencies are identified and/or where the data subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to correct inaccuracies with immediate effect.

The Compliance Officer will be notified of the data subject's request; will, as necessary, validate the information and rectify errors as directed by the data subject.

12.7 THE RIGHT TO ERASURE

In specific circumstances, data subjects' have the right to request that their personal data is erased, however, the Company recognise that this is not an absolute *'right to be forgotten'*. Data subjects only have a right to have personal data erased and to prevent processing if one of these conditions apply:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent for retention
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed

- The personal data must be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

When a request to erase data is received, it is recorded on the Erasure Request Register. We first ensure that no other legal obligation or legitimate interest applies. If we are confident that the data subject has the right to have their data erased, all data relating to that individual will be erased within 30 days of the request being received.

The data subject will be notified, in writing, that the erasure has been completed, providing details of the information erased and the date of erasure or that it is not possible to act in response to the request, providing an explanation and informing of the right to complain to the Data Protection Commissioner and to a judicial remedy.

12.8. THE RIGHT TO RESTRICT PROCESSING

An erasure request is the best course of action to restrict processing of retained personal information. Processing of personal data is necessary to fulfil and retain evidence of fulfilment of contract.

The Company has legitimate grounds to override a restriction request to the extent that retention of information is required by law / regulation,

13. SECURITY & DATA BREACH MANAGEMENT

A personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

13.1 BREACH MONITORING & REPORTING

All data breaches are reported to the Compliance Officer, with immediate effect, even in instances where notifications and reporting are not required.

He will raise a Data Breach Incident Report and take responsibility for conducting a full investigation. He/she may appoint appropriate persons to contain the breach, record the incident and/or make the relevant and legal notifications. Prior to investigation and initiation of breach procedures, measures will be taken to stop any further risk/breach.

13.2 DATA BREACH INVESTIGATION

The lead investigator will ascertain the information involved in the data breach and the subsequent steps required to remedy the situation and mitigate any further breaches:

- The type of information involved
- It's sensitivity or personal content
- The protections in place (e.g. encryption)
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications arising from the incident
- Keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

The completed incident form will be filed for audit and documentation purposes.

13.2 DATA BREACH RISK ASSESSMENT

HUMAN ERROR

Where the data breach is the result of human error, an investigation into the root cause will be conducted and a formal interview with the employee(s) held.

A review of the procedure(s) associated with the breach will be conducted and a full risk assessment completed. Any identified gaps found to have caused/contributed to the breach will be reviewed and risk assessed to mitigate any future occurrence of the same root cause.

Resultant employee outcomes of such an investigation can include, but are not limited to:

- Re-training in specific/all compliance areas
- Re-assessment of compliance knowledge and understanding
- Suspension from compliance related tasks
- Formal warning (in-line with the Company's disciplinary procedures)

SYSTEM ERROR

Where the data breach is the result of a system error/failure, the IT team will work, in conjunction with the Compliance Officer, to assess the risk and investigate the root cause. A gap analysis will be completed on the system(s) involved and a full report appended to the Breach Incident Report.

Any identified gaps found to have caused/contributed to the breach will be revised and risk assessed to mitigate and prevent any future occurrence. Full incident details will be determined and mitigating action taken to limit the impact of the incident. This may include:

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- Removing an employee from assigned task
- The use of back-ups to restore lost, damaged or stolen information
- Making the building secure
- If the incident involves any entry codes or passwords, then these codes must be immediately.

13.3 BREACH NOTIFICATIONS

– NOTIFICATION TO THE DATA PROTECTION COMMISSIONER

The Data Protection Commissioner must be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals i.e. situations which if the breach was ignored, would lead to significant detrimental effects on the individual.

Such notification must be made no later than 72 hours after the Company becoming aware of it. On completion of investigation, and during the investigation, if requested, a full report, including outcomes and mitigating actions will be provided within any specified timeframes. If notification of a breach is not possible within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for delay.

A notification to the Supervisory Authority will contain: -

- A description of the nature of the personal data breach
- The categories and approximate number of data subjects affected
- The categories and approximate number of personal data records concerned
- The name and contact details of our Compliance Officer and/or any other relevant point of contact (for obtaining further information)
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)

Where a breach is assessed and deemed to be unlikely to result in a risk to the rights and freedoms of persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

- DATA SUBJECT NOTIFICATION

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format. Notification to the data subject shall include:

- The nature of the personal data breach
- The name and contact details of our Compliance Officer and/or other relevant point of contact
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational measures which render the data unintelligible to any person who is not authorised to access it (i.e. encryption, data masking etc.) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

14 TRANSFERS & DATA SHARING

The Company takes proportionate and effective measures to protect personal data held and stored by us. Data is stored only within the EU.

15. AUDITS & MONITORING

We conduct regular audits and compliance monitoring to ensure the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The aim of internal data protection audits is to: -

- To test the application, adequacy and effectiveness of the policies and procedures implemented
- To detect breaches or potential breaches of compliance
- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and actions plans for improvement in protecting personal data
- To monitor compliance with the data protection laws and demonstrate best practice

16. TRAINING

We ensure all staff understand the requirements of data protection laws as they apply to their role. To ensure competence and adequacy for role, we provide ongoing training, support and assessments in data protection laws requirements and the Company's data protection objectives and obligations.

ASSOCIATED DOCUMENTS:

- PROCABS HACKNEY SERVICES LTD Privacy Notice
- PROCABS HACKNEY SERVICES LTD Terms & Conditions
- PROCABS HACKNEY SERVICES LTD Employee Privacy Notice
- PROCABS HACKNEY SERVICES LTD Driver Privacy Notice

RECORDS:

- Personal Data Inventory
- Data Breach Form
- DPIA Risk Assessment Form