



# IS213 Privacy Notice

---

To the requirements of ISO 27001:2013 and the EU General Data Protection Regulation (GDPR)

## Classification: **Public**

As a public document, this document may be shared with and viewed by any member of the general public.

### **Dial-a-Cab Limited**

Dial-a-Cab House  
39-47 East Road  
London  
N1 6AH

Tel: 0207 251 0581

Web Site: [www.dialacab.co.uk](http://www.dialacab.co.uk) [www.encompassgt.com](http://www.encompassgt.com)

Created by:	John Bankes on 19/12/2017
Approved by:	John Bankes on 19/12/2017
Owner:	IT Director
Revision Date:	22/03/2018
Review Date:	22/03/2019
Revision:	<b>2.2</b>

## Table of contents

<b>1. REFERENCES</b>	<b>3</b>
1.1. ISO / IEC 27001:2013	3
1.2. OTHER REFERENCES	3
<b>2. INTRODUCTION</b>	<b>4</b>
<b>3. PURPOSE</b>	<b>4</b>
<b>4. SCOPE</b>	<b>4</b>
<b>5. WHO WE ARE</b>	<b>4</b>
<b>6. HOW YOUR INFORMATION WILL BE USED</b>	<b>4</b>
<b>7. THE INFORMATION WE COLLECT AND HOLD</b>	<b>5</b>
7.1. PERSONALLY IDENTIFIABLE INFORMATION (PII)	5
7.2. PERSONAL DATA ASSOCIATED WITH PII	5
7.3. ACQUISITION AND COLLECTION OF DATA	5
<b>8. LEGAL BASIS FOR PROCESSING</b>	<b>6</b>
<b>9. WHO WE WILL SHARE YOUR INFORMATION WITH</b>	<b>6</b>
9.1. TAXIS	6
9.2. ENCOMPASS	6
9.3. ADFLEX	6
9.4. GOVERNMENT AND LAW ENFORCEMENT	7
<b>10. THE SECURITY OF YOUR INFORMATION</b>	<b>7</b>
10.1. CYBER ESSENTIALS	7
10.2. ISO/IEC 27001 ISMS	7
10.3. PHYSICAL SECURITY	7
10.4. PERIMETER AND NETWORK SECURITY	7
10.5. APPLICATION SECURITY	7
10.6. DPIA AND RISK ASSESSMENTS	8
10.7. SECURITY AWARENESS TRAINING	8
10.8. COMPLIANCE WITH EU GDPR AND PCI DSS	8
<b>11. DATA RETENTION POLICY</b>	<b>8</b>
<b>12. YOUR RIGHTS</b>	<b>8</b>
12.1. PRIVACY BUTTON	8
<b>13. COOKIES</b>	<b>9</b>
<b>14. CONTACTING DIAL-A-CAB ABOUT YOUR INFORMATION</b>	<b>9</b>
<b>15. REVISION HISTORY</b>	<b>10</b>
<b>16. DOCUMENT META DATA</b>	<b>10</b>

## 1. REFERENCES

### 1.1. ISO / IEC 27001:2013

A.18.1.4 Privacy and protection of personally identifiable information

### 1.2. Other references

- EU General Data Protection Regulation Portal ([www.eugdpr.org](http://www.eugdpr.org))
- Information Commissioners Office GDPR guide ([Link](#))
- Information Commissioners Office Advice on Privacy Notices under GDPR ([Link](#))

## 2. INTRODUCTION

Dial-a-Cab Limited operates two brands, Dial-a-Cab and Encompass. Both brands use the same IT infrastructure and as such, both brands are covered by this document. At Dial-a-Cab we take your privacy seriously and will only use your personal information to administer your account and to provide the services you have requested from us.

## 3. PURPOSE

The purpose of this document is to disclose the ways that Dial-a-Cab gathers, processes, discloses, and manages your personal data. It will also set out our cookies policy and to make you aware your rights under the current and upcoming Data Protection legislation most notably the EU General Data Protection Regulation (GDPR) which comes into effect on May 25<sup>th</sup> 2018.

## 4. SCOPE

The scope of this policy extends to all Dial-a-Cab Limited departments, employees, contractors, vendors, customers and partner agencies that use/access Dial-a-Cab Limited's information assets.

## 5. WHO WE ARE

Dial-a-Cab is a limited company registered in England with the registration number 10456162. We are registered as a data controller with the UK Information Commissioner's Office. Our data protection registration number is ICO:00040461379.

Dial-a-Cab was established in 1953 and has always prided itself on the innovation of its technology and the security and safety of its customers.

Dial-a-Cab Headquarters is based at:

Dial-a-Cab House  
39 – 47 East Road  
London  
N1 6AH

Telephone:

020 7251 0581

Email:

[info@dialacab.co.uk](mailto:info@dialacab.co.uk)

Web:

[www.dialacab.co.uk](http://www.dialacab.co.uk)

[www.encompassgt.com](http://www.encompassgt.com)

## 6. HOW YOUR INFORMATION WILL BE USED

The information held by Dial-a-Cab will only be used for the purpose of providing seamless joined up ground transportation services to you and your company. Your data will identify you to our system to make sure that your account is not used fraudulently. We will also report back to you and to your company on the trips you have taken with us by way of providing Management Information reports. These reports will be delivered securely to authorised personnel within your company. This is usually the Travel Management Team.

## 7. THE INFORMATION WE COLLECT AND HOLD

### 7.1. Personally Identifiable Information (PII)

The table below details the PII that is held by Dial-a-Cab in order to provide ground transportation for its customers.

Name	Mobile phone Device UUID	Home address (if provided by Data Subject)
Contact phone numbers	Mobile phone IP address	Email address
Employee number / Unique ID	Login	Home address

### 7.2. Personal Data associated with PII

The table below details the personal data that is associated with the PII documented in 7.1.

Trip pickup and destination	Trip pickup date and time	Trip purpose
Vendor who provided the trip	Registration of the vehicle	Passenger on Board time
Booker details	Drop off time	Location of vehicle (during trip)

### 7.3. Acquisition and collection of data

Most of the personal data held by Dial-a-Cab is transferred to us by the Data Subject's employer as part of the ground transportation service delivery agreement. This data is transferred to Dial-a-Cab through a secure and encrypted transfer method. The data enables Dial-a-Cab to identify and authenticate an individual to the system and set up a user profile. This user profile is maintained by the Data Subject or a delegate nominated by the Data Subject or the Data Subject's employer.

In the case where the PII data is sent to Dial-a-Cab by the customer, Dial-a-Cab assumes the role of Data Processor and the customer assumes the role of Data Controller. Dial-a-Cab will only use the information for the purpose specified in section 6 of this document.

Where the Dial-a-Cab systems collect the information directly from the users, for instance if a home address is added to the profile for speed of booking purposes, Dial-a-Cab assumes the role of Data Controller for that information but will still only use it for the purpose stated in section 6.

Dial-a-Cab expects that the customer, as the Data Controller that shares the information with Dial-a-Cab will notify the Data Subject that their data has been transferred to Dial-a-Cab along with the purpose for which it is shared and the lawful basis upon which it is being processed.

## 8. LEGAL BASIS FOR PROCESSING

The legal basis upon which we process your data is that of “Legitimate Interest”. This legal basis is detailed in the EU GDPR in Recital 47 and Article 6. Our legitimate interests in processing your data are listed below:

- To operate our business efficiently
- To offer work to our drivers
- To successfully fulfil our obligation to our customers

We have conducted a Legitimate Interest Assessment (LIA) and have concluded that the processing is legal on this basis. The fundamental findings from LIA are below:

- We have identified the legitimate interests.
- We have determined that the delivery of the service to you is not possible without processing your data and as such the processing is necessary.
- We have determined through our balancing test that your rights and interests do not override our legitimate interests.
- We only use your data in ways you would reasonably expect to deliver your service.

## 9. WHO WE WILL SHARE YOUR INFORMATION WITH

Dial-a-Cab will not disclose your information to any third party for any purpose except those listed below. Your data will not be transferred outside of the United Kingdom.

### 9.1. Taxis

For Dial-a-Cab taxi journeys, the details of your booking will be transmitted securely to the driver who will fulfil your booking. All of our drivers are aware of their responsibility to protect your data and to only use it for the purpose stated in section 6.

### 9.2. Encompass

For journeys booked through our Encompass ground transportation platform, the details of your booking will be securely transmitted to the service provider who will fulfil your booking. All of these transport service provider vendors have been approved by your company. All Encompass vendors must also undergo and successfully pass an information security audit administered by the Dial-a-Cab information security team.

### 9.3. Adflex

All financial transactions associated with trips you have booked with us are processed by our payment services provider, *Adflex*. You can review the provider's privacy policy at [www.adflex.co.uk](http://www.adflex.co.uk). We share information with our payment services provider only to the extent necessary to process payments and refunds for the transportation services you have used with us. We do not store any credit card information on our systems. All credit card details are securely tokenised by Adflex and only the tokens are stored on Dial-a-Cab systems.

## 9.4. Government and Law Enforcement

Dial-a-Cab will share your data with Government or Law Enforcement agencies only if it is required to do so by law or for regulatory or compliance purposes.

## 10. THE SECURITY OF YOUR INFORMATION

Dial-a-Cab makes all reasonable efforts to protect your information while it is in our care. Below are the measures that we take to ensure that your information is safe.

### 10.1. Cyber Essentials

The Cyber Essentials scheme has been developed by the United Kingdom Government and industry to fulfil two functions. It provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats, within the context of the Government's 10 Steps to Cyber Security. And through the Assurance Framework it offers a mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions.

Dial-a-Cab has achieved certification under the Cyber Essentials scheme. The Dial-a-Cab certificate number is **7241821519458983**.

### 10.2. ISO/IEC 27001 ISMS

Dial-a-Cab operates an ISO/IEC 27001 aligned Information Security Management System. The ISMS contains the policies, standards, procedures and guidelines under which all Information processing is performed by the company and its staff. Most of the ISMS documents are classified as 'Controlled' which means that they can be shared with interested third parties. If you would like to see any part of the system, please contact the Dial-a-Cab Information Security Officer at [iso@dialacab.co.uk](mailto:iso@dialacab.co.uk).

### 10.3. Physical Security

All processing of data takes place in a single location within the United Kingdom. Dial-a-Cab House, located on East Road in London houses the company's secure data centre, contact centre and administrative operations. The building is protected 24 hours a day by patrolling security guards, CCTV and card swipe access to all areas.

### 10.4. Perimeter and Network Security

Dial-a-Cab's network perimeter is protected by state-of-the-art firewalls, intrusion prevention systems and anti-virus/ anti-malware systems. The network is regularly penetration tested with the last test performed in January 2018.

### 10.5. Application Security

All Dial-a-Cab developers are fully aware and practiced in secure application development. OWASP 10 code reviews are carried out with each release of software. The system has been subjected to an intensive 5 day application penetration test after which all vulnerabilities and method flaws were remedied. Dial-a-Cab subscribes to the Veracode (<https://www.veracode.com/>) static code analysis tool which constantly monitors development for coding flaws and identifies them to the programmer.

## 10.6. DPIA and Risk Assessments

Based on the requirements of GDPR Article 35(3), it is not a requirement for Dial-a-Cab to perform a Data Protection Impact Assessment (DPIA). However, the management of Dial-a-Cab have decided to include a DPIA in the company's Risk Treatment programme. Regular Information Security Risk Assessments are carried out against all information assets but a specific DPIA Risk Assessment will now be carried out within the normal risk treatment cycle.

## 10.7. Security Awareness Training

Each Dial-a-Cab staff member is required to attend security awareness training on an annual basis. Each member of staff is also required to read and agree by signing an Acceptable Use Policy. The Dial-a-Cab Acceptable Use Policy has been specifically tailored to include the requirements of the GDPR. The Acceptable Use Policy is essentially a summary of all Dial-a-Cab information security policies that relate to members of staff. Any breach of this policy or any other Dial-a-Cab security policy can result in disciplinary action being taken against the employee.

Full copies of the detailed security policies are available to members of staff on the company's intranet.

## 10.8. Compliance with EU GDPR and PCI DSS

Dial-a-Cab is compliant with both the EU GDPR and the PCI DSS standard. This compliance is monitored, reviewed and assessed on an ongoing basis in accordance with the Dial-a-Cab's Information Security Management System and its Internal Audit and Improvement Policies.

## 11. DATA RETENTION POLICY

The Dial-a-Cab Data Retention Policy states that data will be retained on our systems for 7 years after the data subject ceases activities with us.

## 12. YOUR RIGHTS

The EU GDPR has been specifically designed to put the Data Subject in control of his/her own data. Dial-a-Cab will honour those rights and provides a mechanism for the Data Subject to exercise those rights.

### 12.1. Privacy Button

Dial-a-Cab online systems provide a 'Privacy' button which is accessible to all online users of Dial-a-Cab and Encompass systems. The button, named 'Privacy', is located in the Profile Maintenance section of the web application. It provides a means for a Data Subject to perform the following tasks.

- Contact the Dial-a-Cab Information Security Officer at [iso@dialacab.co.uk](mailto:iso@dialacab.co.uk)
- Raise an objection to the processing of their data
- Request a copy of all PII held by Dial-a-Cab relating to the Data Subject
- Request that all PII held by Dial-a-Cab relating to the Data Subject be destroyed
- Request that all PII held by Dial-a-Cab relating to the Data Subject be corrected
- Download a copy of the Dial-a-Cab Privacy Notice



## 13. COOKIES

Dial-a-Cab uses Cookies on our web application to enhance your experience.

A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.

Cookies may be either "persistent" cookies or "session" cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.

Cookies do not typically contain any information that personally identifies a user, but personal information that we store about you may be linked to the information stored in and obtained from cookies.

We use only session cookies on our web applications. The names and content of the cookies that we use on our web applications are encrypted using AES256.

## 14. CONTACTING DIAL-A-CAB ABOUT YOUR INFORMATION

If you have any questions about the PII that Dial-a-Cab hold, please contact the Information Security Officer (ISO) using one of the methods below.

Email: [iso@dialacab.co.uk](mailto:iso@dialacab.co.uk)

Telephone: 0207 251 0581 - Ask to speak to the Information Security Officer.

Letter Addressed to:  
Information Security Officer  
Dial-a-Cab House  
39 – 47 East Road  
London  
N1 6AH

## 15. REVISION HISTORY

This document is reviewed periodically, at least annually, and is retained for a period of 2 years. The history of amendments and the issue of revisions are recorded below.

Date	Revision	Summary	Author	Approved By
22/03/2018	2.2	Update for GDPR	John Bankes	John Bankes

## 16. DOCUMENT META DATA

<b>File Name</b>	IS213 Privacy Notice.docx
<b>Location:</b>	L:\Documentation\ISMS\DocSource\IS213 Privacy Notice.docx
<b>Template:</b>	L:\Documentation\Templates\DaC_Document.dotx