Dine Contract Catering

Information Data Protection Policy

Version: 1.0

Author: Ian Roberts

Information Security Officer: Ian Roberts

Email: i.roberts@dine.org.uk

Version History

Version	Date	Author	Description
1.0	30/04/2018	Ian Roberts	Initial Version

INTRODUCTION

Dine Contract Catering Limited (**"The Company"**) has responsibilities in relation to the Data Protection Act 1998 and the EU directive for General Data Protection Regulation (GDPR EU 2016/679) regarding the collection, storage, processing and destruction of data relating to individuals.

RESPONSIBILITY

The Company Directors are ultimately responsible for ensuring that information security is properly managed. The **Information Security Officer** is responsible for:

- The development and upkeep of this policy and its associated usage policies
- Ensuring this document is supported by appropriate documentation where required.
- Ensuring that documentation is relevant and kept up-to-date.
- Ensuring this policy and subsequent documentation is communicated to all applicable staff in a timely manner.

OBJECTIVE

This policy defines how the company operates on the principals of the UK Data Protection Regulations and EU General Data Protection Regulation, including;

- Striving to always provide data protection by design and by default
- Informed Consent – to ensure all individuals for who personal data is stored, is made aware of what data is stored, why the data is needed, and how it will be used.
- Access to data – the right to access, free of charge, all data which is being stored, with information about how it is being used.
- Correction – the right to request the correction of data if it is incorrect.
- Erasure and Right to be Forgotten (RTBF) – the right of an individual to have their data removed if no longer required for essential business or legal requirements.
- Data Portability – Ensure that when any personal information is sent to third party organisations for processing or storage an agreement is in place regarding how that data is handled.

DATA PROCESSING

Where **The Company** operates as **The Data Processor** accepting data from our clients ("**The Data Controller**"), the company will;

- Secure the storage of, access to, and timed deletion of any stored data in line with all relevant company policies and any relevant client agreements.
- Act only upon the instruction of the Data Controller when processing data or sharing data with a 3rd party to use ("**Sub-Processor**").
- Ensure any **Processor** or **Sub-Processor** used adheres to the same level of compliance and security by way of a **Data Processor Agreement**
- Assist all relevant authorities and **The Data Controller** with any queries or audits
- Inform **The Data Controller** within 48 hours of the discovery of a data breach by the company or any sub-processor.

DATA COLLECTION AND STORAGE

The company will only gather data from individuals relevant to completing a given task of which the individual is aware at the point of gathering. All information stored has been reviewed to ensure the reason for collection and storage are defined and relevant. Where details about individuals is obtained from other sources (e.g. public information) and consent is not required for initial contact, a controlled process will be in place to allow individuals to request no further contact.

DATA ACCESS

Upon receipt of a formal Subject Access Request from an individual the company will respond to this request within one calendar month of receipt once the identity of the individual has been confirmed.

Ensure that the all staff are aware of and adhere to the company policies relating to data protection and security. Secure access to all personal data, both electronic and physical by means of appropriate physical and logical security measures to restrict access to staff who require it.

BREACH PROCEDURE

Any individual who accesses, uses or manages the company's data is responsible for reporting data breach and information security incidents immediately to the Information Security Officer and the IT department.

Under current Industry Regulations and applicable laws, the company has a responsibility to deal with any suspected breach in a controlled manner to ensure it is dealt with in the correct manner. Dine Contract Catering Limited has a Data Breach Procedure to deal with this situation and ensure that correct process is followed. This follows the structure defined in the Data Protection Act and subsequent Data Breach Guidelines of the GDPR.

Containment and Recovery

Immediate response on discovery and reporting of the breach to contain the breach and put in place a recovery plan to stop any further breach of data.

Assessment of Risk

Evaluation of the scale of the breach, the data which has been breached, the individuals affected, and the possible effect on those individuals. Approximate figures may need to be used depending on the timescales available.

Notification of Breach

From the assessment of risk, the scale of the breach will be used to determine the appropriate notification procedures to be followed. From internal reporting to Senior Management and/or the Board of Directors, to a situation where the breach poses a risk to the rights and freedoms of the individuals, when the ICO (Information Commissioner's Office) must be informed within 48 hours of the discovery of the breach.

Evaluation and Response

Following the breach, it is essential to evaluate the cause and identify any processes or procedures which need to be changed to ensure they cannot cause another breach.