BERNARDI'S

Data privacy & PROTECTION.

Dining Theory Ltd Data Privacy Policy
Effective from 25th May 2018

DINING THEORY LIMITED

DATA PRIVACY AND PROTECTION

Introduction

Dining Theory Limited ("Dining Theory") has a continuing commitment to privacy and data protection compliance. This document, together with the Employee Privacy & Data Protection Policy set out in Schedule One, the Privacy Notices in Schedule Two (Employees) and Schedule Three (Customers) and the Data Audit in Schedule Four now constitutes our company-wide Data Protection Rules ("the Rules").

The Rules express the commitment of our employees and Board of Directors to data privacy and to protecting all information relating to identified or identifiable natural individuals (known as "Data Subjects"). Dining Theory processes certain information about Data Subjects while operating its business (known as "Personal Data"). The Rules set out Dining Theory's overall approach to privacy and data protection and emphasise the key role our employees play in protecting Personal Data.

Data protection laws give Data Subjects certain rights regarding how their Personal Data is handled.

The Scope of the Rules

The Rules apply to all Personal Data used and collected by Dining Theory.

Categories of Data Subjects and Purposes of Processing and Transfers

Dining Theory processes and transfers Personal Data (potentially including Sensitive Personal Data) relating to the following types of Data Subjects:

- Our customers relating to the provision of services ("Customer Information");
- Individuals making payment transactions;
- Dining Theory employees, contractors, and consultants in connection with their working relationship or application for employment ("Employment Data");
- Other persons as appropriate to conduct its business such as suppliers, partners, contractors and contingent workers and prospective customers of Dining Theory.

"Sensitive Personal Data" in relation to the Rules means any Personal Data about a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data about health or sex life, criminal record data, social security numbers and other national identifier numbers.

The processing and transfers undertaken by Dining Theory relating to the types of Data Subjects discussed above include processing for the following business purposes:

- Employee recruitment;
- Employee performance management and professional development;
- Payroll and administration of employee benefits;
- Research and development;
- Business development;
- Maintaining and building upon customer relationships;
- Business planning;
- Facilities management;
- Maintaining technology infrastructure and support;
- Database management;
- Training;
- Maintaining the security of data collected and processed;
- Fulfilling a transaction initiated by or involving a Data Subject;
- Fulfilling a transaction with or for our customers;
- For fraud prevention or investigation, or other risk management purposes;
- For identification and information verification purposes;
- For protecting Dining Theory's legal rights or assets;
- Facilitating the acquisition or disposition of Dining Theory businesses, including providing Personal Data to prospective purchasers;
- Enforcing our rights or the rights of other persons in a financial transaction;
- In response to a lawful request from a court or government agency or to otherwise comply with applicable law or compulsory process;
- On the written request of the Data Subject, where appropriate;
- In emergencies where the health or safety of a person is endangered;
- Other purposes required or permitted by law or regulation;
- Our processing also includes the use of CCTV systems for the prevention and prosecution of crime.

Nature of Data Transferred

Dining Theory reserves the right to process and transfer a broad range of Personal Data between Dining Theory entities and to third parties. The types of Personal Data include:

- *Employment Data:* This includes data relating to health records, benefit information, staff development records, attendance records including any days off due to illness, salary remuneration and expenses information, immigration status, equal opportunities management, grievance and disciplinary procedures, employee share equity holdings, employment termination information, names, addresses, date of birth, work location, employee performance, trade union membership and next of kin.
- *Other Personal Data:* Dining Theory also processes contact information of the employees of its suppliers and vendors and independent contractors including name, e-mail address, work location and telephone numbers and such other personal data as may be required in order for Dining Theory to conduct business with such suppliers, and vendors and independent contractors.

Applicable Law

We will handle Personal Data (including Sensitive Personal Data) in accordance with these Rules and all applicable local data protection and privacy laws and regulations including, but not limited to, the European Union Data Protection Directive (Directive 95/46/EC) and the General Data Protection Regulations (numbered Regulation 2016/679). The Rules must be interpreted in accordance with all applicable data protection and privacy laws and regulations.

Where applicable data protection and privacy laws provide less protection than those granted by the Rules, the Rules will apply. Where applicable data protection and privacy laws provide a higher protection, they will take precedence over the Rules.

Dining Theory does not assume any responsibility for compliance requirements that apply to its customers, suppliers, or contractors.

Changes to these Rules and Transparency

Dining Theory may change the Rules, or any relevant underlying documents from time to time. Current versions of the Rules will be available from head office and we will clearly indicate the date of the latest revision to the Rules.

Compliance and Dispute Resolution

If you have questions, concerns, or a complaint about Dining Theory's compliance with the Rules, you are encouraged to contact **Marcello Bernardi** (contact details at the end of this document) who will work with you to attempt to resolve the issue to your satisfaction. We will strive to resolve any issues within five business days. Where that is not possible, for example due to the nature and complexity of the issue, we will keep in regular contact until the issue is resolved.

If the issue is not resolved to your satisfaction you can:

- raise the issue before the competent Data Protection Authority; or
- bring the issue before either the courts of England and Wales.

The rights contained in the Rules are in addition to any other legal rights or remedies that you may otherwise have, including the right to compensation if appropriate.

Data Audit

Dining Theory has carried out a detailed audit of the data which is held by Dining Theory, including, amongst other things:

- the nature and extent of data held
- how it is acquired
- how it is managed and by whom

Details of the audit are set out in Schedule Three. Dining Theory has reviewed the data audit with a view to assessing the basis upon which the date is held and processed.

Lawful basis for processing data

Under the General Data Protection Regulations, there are six lawful bases for processing data, namely:

(a) **Consent:** the individual has given clear consent for Dining Theory to process their personal data for a specific purpose.

(b) **Contract:** the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

(c) **Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).

(d) **Vital interests:** the processing is necessary to protect someone's life.

(e) **Public task:** the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Dining Theory has determined that:

(a) **Employee and Consultant data** is held pursuant to paragraphs (b) and (c) above. It would not be possible to run the business of Dining Theory without the employment of our many employees and it is essential to have appropriate contact and other details to enable us to fulfil this obligation and on the

grounds of welfare, health and safety of our employees and, of course, to ensure that they receive their remuneration into their nominated bank accounts. We also need to hold their employment records (including details of any disciplinary action) to safeguard the company's legal interests.

(b) **Customer data** is held for marketing purposes pursuant to paragraph (f) above, because Dining Theory believes that our customers have a particular interest in what we offer at our venues, details of forthcoming events and other activities in which we are engaged. We encourage customers to actively opt in to our marketing activities but we are satisfied that we have a legitimate interest in keeping our customers advised of forthcoming events, for the reasons set out above. We also ensure that the procedure for unsubscribing and/or removing customer data is clear on our website and in our communications.

(c) **Supplier data** is held pursuant to paragraphs (b) and (c) above, as such activities arise in the ordinary course of our business with third party suppliers, for the proper and efficient operation of our business interests. Such involvement needs to be secured by way of contract, hence the need to hold appropriate data.

Communication of Dining Theory's Data Rules

All Dining Theory employees who handle Personal Data must comply with the Rules and will receive training on the Rules. Dining Theory will also make physical copies of the Rules available at its head office. In addition, a copy will be sent to you on request.

Dining Theory's Privacy Principles

All Dining Theory employees will abide by the following principles when processing Personal Data.

- *We process Personal Data fairly and lawfully.*

Dining Theory processes Personal Data fairly and lawfully, in accordance with all applicable laws and regulations.

- *We obtain Personal Data only for carrying out lawful business activities.*

Dining Theory collects, transfers, holds and processes Personal Data only for explicit and legitimate purposes as set out in the Rules. Dining Theory will not process Personal Data in ways incompatible with those purposes. Where we obtain Personal Data from third parties (including our customers) and publicly available sources, we always endeavour to use only reliable and reputable sources.

- *We limit our access to and use of Personal Data.*

Dining Theory limits access to Personal Data to those employees, contractors, agents and suppliers who reasonably need access to this data to fulfil their responsibilities and forbids employees from accessing or using this data for personal reasons or for any purposes other than fulfilling their Dining Theory responsibilities. We require our contractors, agents and suppliers to adopt a similar approach to Personal Data they access in connection with providing services to Dining Theory.

Dining Theory processes Personal Data in accordance with its written agreements or with instructions from our business partners, in compliance with applicable laws and our policies. In addition, our contracts and applicable laws govern our use of Personal Data received from vendors or other third parties.

- *We transfer Personal Data only for limited purposes.*

Dining Theory transfers Personal Data only when:

  - all applicable legal requirements are met;
  - the transfer is based on a clear business need;
  - the receiving party has appropriate security;
  - in the case of all transfers to third parties there is a written contract
    - specifying that the receiving party will follow the exporting party's instructions;
    - setting out the rights and obligations of each party including provisions relating to security and confidentiality which they must follow; and
    - when transferring to a third-party entity, ensuring that it has adequate security measures in place.

Dining Theory does not disclose Personal Data except as set out in the Rules, its policies or as required or otherwise permitted by contract or applicable law.

- *We use appropriate security safeguards.*

Dining Theory employs appropriate technical, organisational, administrative and physical security measures to protect Personal Data against unauthorised or unlawful processing and against accidental loss or destruction. Dining Theory regularly reviews and, as appropriate, enhances its security systems, policies and procedures to take into account emerging threats, as well as emerging technological safeguards and precautions. Dining Theory will not transfer Personal Data to a country or territory which has inadequate data protection laws, unless adequate safeguards are in place.

When the processing of Personal Data is outsourced by Dining Theory to a third party, Dining Theory will select reliable third parties that have implemented appropriate security safeguards.

- *We provide transparency, choice and access as required by applicable data protection and privacy law.*

Dining Theory verifies, to the extent practicable in its capacity as data controller or data processor, that Personal Data is kept up-to-date and current, accurate, adequate, relevant, and limited to the purposes for which it is collected and processed. Dining Theory retains Personal Data only for the period of time that there is a business or legal need to do so.

Dining Theory will consider each reasonable request of a Data Subject for access to his or her own Personal Data and will provide, at no charge to the Data Subject, a copy of the Personal Data processed by Dining Theory about that person within **one month** of the date on which the request has been received (unless there is a compelling reason not to do so). Dining Theory reserves the right to refuse a subject access request (or make a charge) for requests that are manifestly unfounded or excessive.

If a Data Subject submits a valid claim that the Personal Data which Dining Theory maintains about him or her is incorrect, Dining Theory will endeavour to rectify the inaccuracy as promptly as reasonable practicable.

When a Data Subject believes that Dining Theory's processing of his or her Personal Data is likely to cause unwarranted substantial damage or distress, then the Data Subject may request in writing that Dining Theory stops or does not begin processing that Personal Data. Dining Theory will respond to such requests within 28 days.

- *We recognise a Data Subject's right to object to direct marketing by Dining Theory.*

Dining Theory engages in direct marketing in accordance with applicable laws. Dining Theory provides Data Subjects with the opportunity to opt out of marketing and honours any such requests.

- *Data Breaches*

Dining Theory will notify the ICO of any data breaches which will, or are likely to, result in a risk to the rights and freedoms of individuals, such as discrimination, damage to reputation, financial loss, loss of confidentiality or other significant or economic disadvantage.

In addition, Dining Theory will (in most cases) notify individuals concerned where a data breach is likely to result in a high risk to the rights and freedoms of individuals.

Dining Theory has considered whether or not a Data Protection Impact Assessment is required and has determined (at the date of adoption of this policy) that no such Assessment is required. This determination will be kept under review from time to time.

- *We recognise the importance of data privacy and hold ourselves accountable to our Rules.*

Dining Theory and its Board of Directors are committed to compliance with the Rules. All Dining Theory employees who handle Personal Data must understand and comply with the Rules. Any Dining Theory employee who materially violates any applicable data privacy or data protection laws or the Rules may face disciplinary action up to and including dismissal.

Contact Information

All data enquiries should be sent to:

Marcello Bernardi
Dining Theory Limited
First Floor, 105 Crawford Street
London W1H 2HT

Email: data@bernardis.co.uk

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

April 2018

SCHEDULE ONE

EMPLOYEE PRIVACY & DATA PROTECTION

Dining Theory Limited ("the Company") takes protection of the privacy of our job applicants, employees, former employees, dependents and beneficiaries of employees and former employees, contractors and contingent workers ("Data Subjects") very seriously.

The Company collects and processes information relating to Data Subjects relating to their working relationship or application for employment with the Company ("Employment Data").

The Company collects and processes Employment Data in compliance with applicable data protection laws, including the European Union's (EU's) Data Protection Directive (Directive 95/46/EC).

1. Notice and Choice

The Company provides Data Subjects with notice disclosing why Employment Data is collected and how it will be used. Employment Data is collected and used fairly and lawfully and in accordance with this Policy and the notices provided.

The Company collects and processes Employment Data only for purposes of administering the employment relationship, for carrying out of lawful business activities, when required by law, or for purposes relevant to Corporate policies. The Company will not process Employment Data in ways incompatible with those purposes.

The Company may disclose Employment Data to third parties only for purposes stated above. Examples of the types of third parties to whom the Company may disclose Employment Data include governmental entities, where required, and vendors serving the Company relating to the administration of employee benefits, training, performance management, security, data collection and similar matters.

The Company will seek consent from Data Subjects before using the Employment Data for any other purpose, apart from purposes for which the Company is required to process data by any legislative or regulatory requirement.

The Company will obtain the Data Subject's prior written consent before processing Sensitive Employment Data, except where the processing is necessary to carry out the Company's rights and obligations in the field of employment law or where consent is not required under applicable law.

The Employment Data collected by the Company is necessary for business purposes, including the administration of the employment relationship. Therefore, failure to provide necessary Employment Data may disqualify an individual from employment by the Company or from participation in certain Company programmes.

2. Onward Transfer

In the event that the processing of Employment Data is outsourced by the Company to a third party, the Company will select reliable third parties and processing will be subject to written agreements between the Company and the third parties processing the data. These written agreements specify the rights and obligations of each party and will provide that the third party has adequate security measures in place and will only process Employment Data on the specific written instructions of the Company. The Company may also transfer Employment Data to third parties as required by law or legal instrument, to protect the Company's legal rights or assets, to facilitate acquisition or disposition of Company businesses, and in emergencies where the health or safety of a person is endangered.

The Company does not sell, rent, share, trade or disclose any Employment Data it keeps relating to a Data Subject to any other parties without the prior written consent of the Data Subject, except for entities within the Company and any suppliers or vendors which the Company has engaged to provide services and are involved in the processing of Employment Data on the Company's behalf.

Personal data will not be transferred to a country or territory when collected in a country or territory that considers the receiving country or territory to having inadequate data protection law(s), unless adequate measures are in place to protect the rights and freedoms of data subjects in relation to the processing of personal data.

3. Access and Data Integrity

Data Subjects have the right to request access to Employment Data relating to them held by the Company. Upon request, and after providing proof of identity, individuals will be given access to their Employment Data, where proportionate and as required by applicable law.

The Company shall process access requests in the ordinary course of business and pursuant to applicable law and will ensure that any reasonable requests for information will be handled promptly and fairly.

The Company will exercise reasonable efforts to ensure that Employment Data is accurate, adequate, relevant, and not excessive for the purposes for which it is processed.

The Company will exercise reasonable efforts to ensure that Employment Data is retained for no longer than is necessary for the purpose for which it is being processed.

4. Security

The Company implements technical, physical, and organisational measures to protect Employment Data against accidental or unlawful destruction, or accidental loss or alteration, or unauthorised disclosure or access (in particular where the process involves transmission of Employment Data over a network).

The Company ensures a level of security appropriate to the risk represented by the process and nature of the Employment Data to be protected, with all due regard to the state of the art and cost measures.

The Company will not transmit Employment Data across the public Internet using a method that is not reasonably secure from parties who may attempt to intercept it. Employment Data will not, therefore, be transmitted in unencrypted form in the body of or in an attachment to an Email message that will be transmitted unencrypted across the public Internet.

5. Treatment of Sensitive Employment Data

"Sensitive Employment Data" for the purposes of this Policy means any Employment Data relating to a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life, criminal record data, National Insurance and/or PAYE numbers and other national identifier numbers.

Access to Sensitive Employment Data will be limited to Company employees and third-party processors that:

- the Company authorises to have access to Sensitive Employment Data;
- need access to such data to perform normal job responsibilities or to provide services to the Company; and
- are bound by company policy, contract or other legal obligation to use and disclose the data only as authorised by the Company.

Sensitive Employment Data must only be used as needed to satisfy the required responsibilities of the personnel authorised to access it. Sensitive Employment Data will be disposed of in accordance with the Company's Information Security Policy. All Sensitive Employment Data will be encrypted if transmitted electronically or secured in packaging if hard copy is sent by post or courier.

The Company takes compliance with its data protection obligations very seriously. Employees will receive training regarding data privacy rights and obligations, as appropriate.

Failure by any Company employee to comply with this Policy and all applicable privacy laws, or to undergo training, as appropriate, will amount to a serious disciplinary offence, subject to discipline that may include termination of employment.

If anyone has any questions or concerns regarding this Policy or the Company's privacy policies and practices, please contact Marcello Bernardi (marcello@bernardis.co.uk).

SCHEDULE TWO

PRIVACY NOTICE (EMPLOYEES)

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the information alone or in conjunction with any other information. The processing of personal data is governed by the Data Protection Bill/Act 2017 the General Data Protection Regulation 2016/679 (the "GDPR" and other legislation relating to personal data and rights such as the Human Rights Act 1998).

Who are we?

This Privacy Notice is provided to you by Dining Theory Limited ("the Company"), which is the data controller for your data. A description of what data is processed and for what purpose is set out in this Privacy Notice. This Privacy Notice is sent to you by the Company.

How do we process personal data?

The Company will comply with its legal obligations:

- To keep personal data up to date;
- To store and destroy it securely;
- Not to collect or retain excessive amounts of data;
- To keep personal data secure; and
- To protect personal data from loss, misuse, unauthorised access and disclosure and to ensure that appropriate technical measures are in place to protect personal data.

We use personal data for some or all of the following purposes:

- Employee recruitment;
- Employee performance management and professional development;
- Payroll and administration of employee benefits;
- Research and development;

- Business planning;
- Facilities management;
- Maintaining technology infrastructure and support;
- Database management;
- Training;
- Maintaining the security of data collected and processed;
- Fulfilling a transaction initiated by or involving a Data Subject;
- For fraud prevention or investigation, or other risk management purposes;
- For identification and information verification purposes;
- For protecting Dining Theory's legal rights or assets;
- Facilitating the acquisition or disposition of Dining Theory businesses, including providing Personal Data to prospective purchasers;
- Enforcing our rights or the rights of other persons in a financial transaction;
- In response to a lawful request from a court or government agency or to otherwise comply with applicable law or compulsory process;
- On the written request of the Data Subject, where appropriate;
- In emergencies where the health or safety of a person is endangered;
- Other purposes required or permitted by law or regulation;
- Our processing also includes the use of CCTV systems for the prevention and prosecution of crime.

What data does the Company process? It will process some or all of the following data where necessary for the proper performance of its business:

- Names, titles, and aliases, photographs.
- Contact details such as telephone numbers, addresses, and email addresses.

- We may process demographic information such as gender, age, date of birth, marital status, nationality, education/work histories, academic/professional qualifications, employment details, hobbies, family composition, and dependants/next of kin.

- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, employee identification numbers, tax reference codes, and national insurance numbers.

- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.

- Financial information such as salary, bonus, record of earnings, tax code, tax and benefits contributions, expenses claimed, creditworthiness, car allowance (if applicable), amounts insured, and amounts claimed.

- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.

- Other employee data (not covered above) including emergency contact information; gender, birth date, referral source (e.g. agency, employee referral); level, performance management information, languages and proficiency; licences/certificates, citizenship, immigration status; employment status, retirement date; billing rates, venue location, skills; prior job history, employment references and personal biographies.

What is the legal basis for processing your personal data?

Most of our data is processed because it is necessary for our legitimate interests, or the legitimate interests of a third party. An example of this would be fulfilling our obligations as an employer. We will always take into account your interests, rights and freedoms.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract (such as making a reservation or booking a function at one of our venues).

Where your information is used other than in accordance with one of these legal bases, we will first obtain your consent to that use.

Sharing your personal data

Your personal data will be treated as strictly confidential. It will only be shared with third parties where it is necessary for the performance of our tasks or where you first give us your prior consent. It is likely (or at least possible) that we will need to share your data with some or all of the following (but only where necessary):

- Accounting and payroll processing firms;

- Our professional advisers (accountancy, tax, immigration, health and safety, employment, etc)

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC audits. In general, we will endeavour to keep data only for as long as we need it. This means that we may delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data. When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. The right to access information we hold on you

At any point you can contact us to request the information we hold on you as well as why we have that information, who has access to the information and where we obtained the information from. Once we have received your request we will respond within one month.
There are no fees or charges for the first request but additional requests for the same data may be subject to an administrative fee.

2. The right to correct and update the information we hold on you

If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3. The right to have your information deleted

If you feel that we should no longer be using your data or that we are illegally using your data, you can request that we erase the data we hold.

When we receive your request, we will confirm whether the data has been deleted or the reason why it cannot be deleted (for example because we need it for our legitimate interests or regulatory purpose(s)).

4. The right to object to processing of your data

You have the right to request that we stop processing your data. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have legitimate grounds to continue to process your data. Even after you exercise your right to object, we may continue to hold your data to comply with your other rights or to bring or defend legal claims.

5. The right to data portability

You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. **The right to withdraw your consent to the processing at any time for any processing of data to which consent was sought.**

   You can withdraw your consent easily by email, or by post (see Contact Details below).

7. **The right to object to the processing of personal data where applicable.**

8. **The right to lodge a complaint with the Information Commissioner's Office.**

Transfer of Data Abroad

Any electronic personal data transferred to countries or territories outside the EU will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the information we hold about you or to exercise all relevant rights, queries or complaints at:

Marcello Bernardi, Dining Theory Limited
First Floor, 105 Crawford Street, London W1H 2HT

Email: data@bernardis.co.uk

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

SCHEDULE THREE

PRIVACY NOTICE (CUSTOMERS)

Privacy Policy

This privacy policy explains how we use any personal information we collect about you when you use our website or make a booking at one of our venues.

Topics

- What information do we collect about you?
- How will we use that information about you?
- Marketing
- Access to your information and correction
- Cookies
- Other websites
- Changes to our privacy policy
- How to contact us

What information do we collect about you?

We collect information about you when you register with us, book a function or make a reservation at one of our venues. We also collect information when you voluntarily complete customer surveys, provide feedback and participate in competitions. Website usage information is collected using cookies.

How will we use the information about you?

We collect information about you to process your order, manage your account and, if you agree, to email you with our newsletter and to inform you about events, special offers, and other products and services we think may be of interest to you.

We will not share your information with third parties outside our group.

In processing your data, we may send your details to, and also use information from, credit reference agencies and fraud prevention agencies.

Marketing

We would like to send you information about our venues, our special offers, events, new openings, details of other products and services of ours and other companies in our group which may be of interest to you. If you have registered your details with us, we believe we have a legitimate interest in advising you, through our informative newsletters, about new events, venue openings and general news about our business.

You have a right at any time to stop us from contacting you for marketing purposes or giving your information to other members of our group.

If you no longer wish to be contacted for marketing purposes, please email us at this address: data@bernardis.co.uk.

Access to your information and correction

You have the right to request a copy of the information that we hold about you. If you would like a copy of some or all of your personal information, please email data@bernardis.co.uk or write to us as at the following address: First Floor, 105 Crawford Street, London W1H 2HT.

We want to make sure that your personal information is accurate and up to date.

You may ask us to correct or remove information you think is inaccurate.

Cookies

Cookies are text files placed on your computer to collect standard internet log information and visitor behaviour information. This information is used to track visitor use of the website and to compile statistical reports on website activity.

You can set your browser not to accept cookies, but you may find that some of our website features may not function as a result.

Other websites

Our website contains links to other websites. This privacy policy only applies to this website so when you link to other websites you should read their own privacy policies.

Changes to our privacy policy

We keep our privacy policy under regular review and we will place any updates on this web page.

This privacy policy was last updated in April 2018.

How to contact us

Please contact us if you have any questions about our privacy policy or information we hold about you:

- by email data@bernardis.co.uk
- or write to us: First Floor, 105 Crawford Street, London W1H 2HT

April 2018

SCHEDULE FOUR

Data Audit as at April 2018

DINING THEORY LIMITED - DATA ANALYSIS (April 2018)

	DATA											WHERE HELD	
CATEGORY	**Name**	**Address**	**Phone**	**Email**	**Photos**	**ID**	**Next of kin**	**Passport, visa**	**NI No & tax code**	**Employment terms/Potentially sensitive information**	**Booking history**	**Server**	**Access**
Employees	x	x	x	x	x	x	x	x	x	x		x	Accounts/HO Managers Senior Chefs
Customers/Agents	x	x	x	x							x	Hubspot/OpenTable/Dropbox	SS and DS
Suppliers/Advisers	x	x	x	x									

Contacts include:
- **Venue regulars**
- **Hospitality Contacts**
- **Press Contacts**
- **Design supplier Contacts**
- **Photographer Contacts**
- **Events Logs**
- **Website Subscriber List**
- **Vuelio Expors (media contacts)**