Data Protection Policy

Version: 2

Date: 7th May 2018

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our customers, employees and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1 The types of personal data that som saa limited may be required to handle include information about current, past and prospective customers, employees and other third parties that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations.

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. All data subjects have legal rights in relation to their personal information.

som saa

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.6 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about any offence committed or alleged to have been committed by that person. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly and lawfully.

(b) Processed for limited purposes and in an appropriate way.

(c) Adequate, relevant and not excessive for the purpose.

(d) Accurate.

(e) Not kept longer than necessary for the purpose.

(f) Processed in line with data subjects' rights.

(g) Secure.

(h) Not transferred to people or organisations situated in countries without adequate protection.

5. FAIR AND LAWFUL PROCESSING

5.1 The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of business, we will ensure that those requirements are met.

6. PROCESSING FOR LIMITED PURPOSES

6.1 In the course of our business, we may collect and process the personal data set out in the Privacy Policy. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

6.2 We will only process personal data for the specific purposes set out in the Privacy Policy or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. NOTIFYING DATA SUBJECTS

7.1 If we collect personal data directly from data subjects, we will inform them about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

7.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

7.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

8. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9. ACCURATE DATA

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection. We will act promptly to correct any inaccuracies if notified that the personal data we hold is incorrect, taking all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. TIMELY PROCESSING

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

11. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

We will process all personal data in line with data subjects' rights, in particular their right to:

(a) Request access to any data held about them by us.

(b) Prevent the processing of their data for direct-marketing purposes.

(c) Ask to have inaccurate data amended.

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

12. DATA SECURITY

12.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

12.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

12.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

12.4 Security procedures include:

(a) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(b) **Passwords.** Passwords will be set on all drive locations, computers or applications on which personal data is stored.

(c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

13. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

13.1 We may also disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

13.2 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

13.3 We may also share personal data we hold with selected third parties for the purposes set out in the Privacy Policy.

14. DEALING WITH SUBJECT ACCESS REQUESTS

14.1 Data subjects must make a formal request for information we hold about them. This must be made in writing to the restaurant or by email to 'The Data Officer' at theoffice@somsaa.com. Employees who receive a written request should forward it The Data Officer.

14.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

14.3 Our employees will refer a request to their manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

15. EMPLOYEE RIGHTS AND DUTIES

15.1 Employees are entitled to access their employment files on making a reasonable request on reasonable notice.

15.2 To help us keep accurate information, employees must tell us of changes to their contact or payroll details or other details we hold about them.

15.3 Employees must also assist us to meet our obligations regarding handling personal data in accordance with the Act:

(a) Employees receiving requests to disclose information must be careful. All reasonable steps should be taken to confirm the requestor's identity and to ensure they are authorised to have that information.

(b) Employees handling personal information should only do so as required for their job and should take all reasonable steps to protect the security of the information.

(c) Managers collecting records about their teams should ensure they only do so when necessary and that they protect that information.

16. CHANGES TO THIS POLICY

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

Data Storage and Processing Activities

Data	Purpose	Source	Accessibility / Protection	Processing	Control	Duration	Access / Amendment / Erasure
Staff personal details and bank account details are held on Planday and Adobe Document Cloud	Compliance with HMRC and to ensure staff are paid	Provided by staff upon enrolment	Accessible by managers and protected by password.	The data is shared with Solutions for Caterers, our accountants, and with HMRC upon request for legal compliance	Data is controlled by the directors of som saa limited	HMRC requires payroll records to be kept for 3 years after the end of the tax year to which they relate.	We will delete all data three years after the end of the tax year to which they relate. Access and amendment can be requested at any time by contacting the restaurant and will be completed by the Data Officer.
Staff passport copies are held on Google Drive	Compliance with HMRC	Provided by staff upon enrolment	Accessible by managers and protected by password.	The data is not shared except with HMRC upon request for legal compliance	Data is controlled by the directors of som saa limited	HMRC requires payroll records to be kept for 3 years after the end of the tax year to which they relate.	We will delete all data three years after the end of the tax year to which they relate. Access and or updates can be requested at any time by contacting the restaurant and will be completed by the Data Officer.
Staff attendance, performace, disciplinary, grievance, medical and other records are held on Google Drive	To manage the workforce and comply with our obligations.	Entered by management. Medical information provided by staff	Accessible by managers and protected by password. G-Suite accounts conform to all data protection requirements.	We do not share the data with any third parties unless required to by law.	Data is controlled by the directors of som saa limited	Indefinite	Access is available at any time and will be completed by the data officer. Amendment and erasure will be at the company's discretion and we may keep records on file even after they have expired so that the company can demonstrate compliance.
Customer contact information and other information related to their visits to the restaurant is stored on the reservation system's cloud based operating system Opentable.	Enable us to make and confirm reservations, identify guests on arrival, note other information useful to the restaurant such as their dining habits.	Provided by customers by phone or email	Accessible by staff and password protected.	We do not share the data with any third parties unless required to by law.	Data is controlled by the directors of som saa limited	Indefinite unless requested	Access, amendment or erasure can be requested at any time by contacting the restaurant and will be completed by the Data Officer
Customer card details are stored on Opentable's PCI DSS Level 1 compliant system Braintree. This information is taken by the restaurant by phone and accessible through Opentable but is stored as an encrypted token with Braintree. We do not store the data directly at som saa	Enable us to charge £10 per head, donated to charity, for tables that do not honour reservation with little or no notice.	Provided by customers by phone	Accessible by staff and password protected.	We do not share the data with any third parties unless required to by law.	Data is controlled by the directors of som saa limited	Card details are held by Braintree for 7 days from the date of the booking and then automatically deleted	Deletion is automatic. Amendment is not applicable.

Customer contact information is stored on the Gmail system used by the restaurant for its business email accounts. In particular, when a customer emails data to reserve for a large group on our 'Sharing Menu' function sheet.	Enable us to make and confirm large party reservations.	Provided by customers by email	Accessible by staff and password protected.	We do not share the data with any third parties unless required to by law.	Data is controlled by the directors of som saa limited	Indefinite unless requested	Access, amendment or erasure can be requested at any time by contacting the restaurant and will be completed by the Data Officer
Customer contact details and the details of intended recipients are taken through our website as part of voucher sales. This is stored by Sitechef (our web developer), stored by Stripe (the payment processor) and the same information is emailed to our Gmail invoices account.	Enable us to receive voucher payments, post or email them to the correct recipients and then ensure the vouchers are redeemed by the correct customers.	Provided by customers through the website voucher system	The first two are accessible by directors only and the last accessible by management.	We do not share the data with any third parties unless required to by law.	Data is controlled by the directors of som saa limited	We will delete all records on our email system within one year of the expiry of the voucher unless requested	Access, amendment or erasure can be requested at any time after the expiry of the voucher by contacting the restaurant and will be completed by the Data Officer
Customer contact information is stored by Mailchimp after entry on the signup form on the som saa website	Enable us to send customers newsletters and updates by email	Provided by customers on the website sign up form	Accessible by managemnt and password protected.	We do not share the data with any third parties unless required to by law.	Data is controlled by the directors of som saa limited	Indefinite unless requested	Access, amendment or erasure can be requested at any time by contacting the restaurant and will be completed by the Data Officer. Customers can unsubscribe from the mailing list by following the link on each mailout
Personal details and employment records of prospective employees are stored on the Gmail system used by the restaurant for its business email accounts.	To allow us to evaluate and contact potential employees.	Provided by prospective employees through Indeed, Gumtree or other recruitment companies.	Accessible by managemnt and password protected.	We do not share the data with any third parties unless required to by law.	Data is controlled by the directors of som saa limited	We will delete all records on our email system within one year of the original application unless requested	Access, amendment or erasure can be requested at any time by contacting the restaurant and will be completed by the Data Officer.
CCTV records of the premises are recorded by a sytem maintained by Securaplace and stored on a hard drive on the premises.	For insurance, safety and compliance	CCTV cameras on the premises	Accessible by managemnt and passcode.	We do not share the data with any third parties unless required to by law.	Data is controlled by the directors of som saa limited	Data is stored for approximately 6 weeks before being auto-deleted	Access can be requested at any time by contacting the restaurant and will be completed by the Data Officer.