

Company of Cooks Limited

DATA PROTECTION POLICY

CONTENTS

1. Interpretation.....	1
2. Introduction	2
3. Scope.....	3
4. Personal data protection principles.....	4
5. Lawfulness, fairness, transparency.....	4
6. Purpose limitation.....	6
7. Data minimisation.....	6
8. Accuracy.....	6
9. Storage limitation.....	6
10. Security integrity and confidentiality	7
11. Transfer limitation	8
12. Data Subject's rights and requests	9
13. Subject Access Requests.....	9
14. Right to rectify inaccurate data or to complete incomplete data	11
15. Right to erase Personal Data	110
16. Right to restrict processing of Personal Data	11
17. Right to object to the processing of Personal Data.....	111
18. Right to data portability.....	111
19. Accountability	111
20. Penalties	114
21. Changes to this Data Protection Policy.....	14
15. Acknowledgement of receipt and review.....	15

This policy covers the Company's procedures for Data Protection, in accordance with the General Data Protection Regulation ((EU) 2016/679) (GDPR), relating to the obtaining, handling, processing, transporting and storage of Personal Data in the course of our operations and activities, including customer, supplier and employee data.

All employees, workers, contractors, agency workers, consultants, directors, casual workers, members and others are covered by this policy. It does not form part of the contract you have with us, but applies regardless of how long you have been with us.

The Company is committed to the lawful and fair handling of Personal Data and respecting the legal rights and privacy of the individuals that it deals with and in doing so will ensure compliance with this procedure, the relevant data protection legislation and the spirit of such legislation.

1. Interpretation

1.1 Definitions:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company name: Company of Cooks Limited, a company registered in England and Wales with company registration number 03395673 and whose registered address is Dephna House, 14 Cumberland Avenue, Park Royal, London NW10 7QL.

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, casual workers, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Manager: A mandatory Data Protection Manager has not been appointed, and so this term means the person appointed with responsibility for data protection compliance, that is Ian Stephenson, the Company's Data Protection Manager, [TELEPHONE] and ian.stephenson@companyofcooks.com

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Guidelines: the Company privacy/GDPR related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies.

Privacy Notices or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal 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 transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Company's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

2. Introduction

This Data Protection Policy sets out how Company of Cooks Limited ("we", "our", "us", "the Company") handles the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Data Protection Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Data Protection Policy may result in disciplinary action.

This Data Protection Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Data Protection Manager.

3. Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to €20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

The Directors are responsible for ensuring all Company Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The Data Protection Manager is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by Ian Stephenson, the Company's Data Protection Manager, [TELEPHONE] and ian.stephenson@companyofcooks.com

Please contact the Data Protection Manager with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the Data Protection Manager in the following circumstances:

- (a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see [section 5.1](#) below);
- (b) if you need to rely on Consent and/or need to capture Explicit Consent (see [section 5.2](#) below);
- (c) if you need to draft Privacy Notices or Fair Processing Notices (see [section 5.3](#) below);
- (d) if you are unsure about the retention period for the Personal Data being Processed (see [section 9](#) below);
- (e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see [section 10.1](#) below);
- (f) if there has been a Personal Data Breach ([section 10.2](#) below);
- (g) if you are unsure on what basis to transfer Personal Data outside the EEA (see [section 11](#) below);
- (h) if you need any assistance dealing with any rights invoked by a Data Subject (see [sections 12](#) to 18);

- (i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see [section 19.4](#) below) or plan to use Personal Data for purposes others than what it was collected for;
- (j) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see [section 19.5](#) below);
- (k) If you need help complying with applicable law when carrying out direct marketing activities (see [section 19.6](#) below); or
- (l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see [section 19.7](#) below).

4. Personal Data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

- (a) processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
- (b) collected only for specified, explicit and legitimate purposes (Purpose Limitation).
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
- (d) accurate and where necessary kept up to date (Accuracy).
- (e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
- (f) processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
- (g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
- (h) made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. Lawfulness, fairness, transparency

5.1 Lawfulness and fairness

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject. You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not

intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, which are set out below:

- (a) the Data Subject has given his or her Consent;
- (b) the Processing is necessary for the performance of a contract with the Data Subject;
- (c) to meet our legal compliance obligations.;
- (d) to protect the Data Subject's vital interests;
- (e) the Processing is necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the Data Controller; or
- (f) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

You must identify and document the legal ground being relied on for each Processing activity.

5.2 Consent

A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be able to withdraw their Consent to Processing easily and at any time, and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data.

Where Explicit Consent is required, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents so that the Company can demonstrate compliance with Consent requirements.

5.3 Transparency (notifying data subjects)

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR

including the identity of the Data Controller and Data Protection Manager, how and why we will use, Process, disclose, protect and retain that Personal Data through Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

6. Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

7. Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

8. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

9. Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with the Company's guidelines on Data Retention.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

10. Security integrity and confidentiality

10.1 Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- (a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
- (b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- (c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

10.2 Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so:

- (a) All Personal Data Breaches must be reported immediately to the Company's Data Protection Manager.
- (b) If a Personal Data Breach occurs and that Personal Data Breach is likely to result in a risk to the rights and freedoms of a Data Subject (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Manager must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of the Personal Data Breach.
- (c) In the event that a Personal Data Breach is likely to result in a **high risk** the rights and freedoms of a Data Subject, the Data Protection Manager must ensure that all affected Data Subjects are informed of the Personal Data Breach directly and without undue delay.
- (d) Personal Data Breach notifications to the Information Commissioner's Office shall include the following information:
 - i. the categories and approximate number of Data Subjects concerned;
 - ii. the categories and approximate number of Personal Data records concerned;
 - iii. the name and contact details of the Company's Data Protection Manager;
 - iv. the likely consequences of the Personal Data Breach;
 - v. details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Data Protection Manager. You should preserve all evidence relating to the potential Personal Data Breach.

The Data Protection Manager will maintain a central register of the details of any Data Protection Breaches.

11. Transfer limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

- (a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- (b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Data Protection Manager;
- (c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- (d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where

the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

12. Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- (a) withdraw Consent to Processing at any time;
- (b) receive certain information about the Data Controller's Processing activities;
- (c) request access to their Personal Data that we hold;
- (d) prevent our use of their Personal Data for direct marketing purposes;
- (e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- (f) restrict Processing in specific circumstances;
- (g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- (h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- (i) object to decisions based solely on Automated Processing, including profiling (ADM);
- (j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- (k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- (l) make a complaint to the supervisory authority; and
- (m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format (data portability).

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the Data Protection Manager.

13. Subject Access Request

A Data Subject may make a subject access request ("SAR") at any time to find out more about the Personal Data which the Company holds about them. The Company is normally required to respond to SAR within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the Data Subject shall be informed of the need for the extension).

All SARs received must be forwarded to Ian Stephenson, the Company's Data Protection Manager, [TELEPHONE] and ian.stephenson@companyofcooks.com

The Data Subject will not have to pay a fee to access to their Personal Data (or to exercise any of the other rights). However, we may charge a reasonable fee if the request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

The Company must verify the identity of the Data Subject making a SAR or exercising any of the rights set out in section 12 and may need to request specific information to help to confirm the Data Subject's identity. This is another appropriate security measure to ensure that Personal Data is not disclosed to any person who has no right to receive it. The Company does not allow third parties to persuade it to disclose Personal Data without proper authorisation

14. Right to rectify inaccurate data or to complete incomplete data

If a Data Subject informs the Company that Personal Data held by the Company is inaccurate or incomplete, requesting that it be rectified, this request will be dealt with by the Data Protection Manager.

Following receipt of such a request, from a Data Subject, the Personal Data in question shall be rectified, and the Data Subject informed of that rectification, within one month of receipt the Data Subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the Data Subject shall be informed of the need for the extension).

In the event that any affected Personal Data has been disclosed to third parties, those parties shall be informed of any rectification of that Personal Data.

15. Right to erase Personal Data

Data Subjects may request that the Company erases the Personal Data that it holds about them in the following circumstances:

- a) where it is no longer necessary for the Company to hold that Personal Data with respect to the purpose for which it was originally collected or processed;
- b) where the Data Subject wishes to withdraw their consent to the Company holding and processing their Personal Data;
- c) where the Data Subject objects to the Company holding and processing their Personal Data (and there is no overriding legitimate interest to allow the Company to continue doing so);
- d) where the Personal Data has been processed unlawfully;
- e) where the Personal Data needs to be erased in order for the Company to comply with a particular legal obligation.

All requests, in accordance with clause 15, will be sent to the Data Protection Manager.

Unless the Company has reasonable grounds to refuse to erase Personal Data, all requests for erasure shall be complied with, and the Data Subject informed of the erasure, within one month of receipt of the Data Subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the Data Subject shall be informed of the need for the extension).

In the event that any Personal Data that is to be erased in response to a Data Subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Right to restrict Processing of Personal Data

Data Subjects may request that the Company ceases to process the Personal Data that it holds about them and if so, this request will be dealt with by the Data Protection Manager.

If a Data Subject makes such a request, the Company shall retain only the amount of Personal Data pertaining to that Data Subject that is necessary to ensure that no further processing of their Personal Data takes place.

In the event that any affected Personal Data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Right to Object to the Processing of Personal Data

Data Subjects have the right to object to the Company processing their Personal Data based on legitimate interests (including profiling), direct marketing (including profiling), this request will be dealt with by the Data Protection Manager.

Where a Data Subject objects to the Company processing their Personal Data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the Data Subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

Where a Data Subject objects to the Company processing their Personal Data for direct marketing purposes, the Company shall cease such processing forthwith.

18. Right to Data Portability

Where Data Subjects have given their consent to the Company to process their Personal Data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the Data Subject, the Data Subject has the right to receive a copy of that Personal Data and to use it for other purposes (namely transmitting it to other Data Controllers, e.g. other organisations).

To facilitate the right of data portability, the Company shall make available all applicable Personal Data to Data Subjects in a Comma Separated Value (CSV) file.

Where technically feasible, if requested by a Data Subject, Personal Data shall be sent directly to another Data Controller. Any such request will be dealt with by the Data Protection Manager.

All requests for copies of Personal Data shall be complied with within one month of the Data Subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

19. Accountability

19.1 The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Company must have adequate resources and controls in place to ensure and to document GDPR compliance including:

- (a) appointing a suitably qualified Data Protection Manager (where necessary) and an executive accountable for data privacy;

- (b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
- (c) integrating data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines and Privacy Notices;
- (d) regularly training Company Personnel on the GDPR, this Data Protection Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and
- (e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

19.2 Training and audit

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training.

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

19.3 Privacy By Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

- (a) the state of the art;
- (b) the cost of implementation;
- (c) the nature, scope, context and purposes of Processing; and
- (d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data controllers must also conduct DPIAs in respect to high risk Processing.

You should conduct a DPIA (and discuss your findings with the Data Protection Manager) when implementing major system or business change programs involving the Processing of Personal Data including:

- (a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- (b) Automated Processing including profiling and ADM;

- (c) large scale Processing of Sensitive Data; and
- (d) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- (a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
- (b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- (c) an assessment of the risk to individuals; and
- (d) the risk mitigation measures in place and demonstration of compliance.

19.4 Automated Processing (including profiling) and Automated Decision-Making

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

- (a) a Data Subject has Explicitly Consented;
- (b) the Processing is authorised by law; or
- (c) the Processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

19.5 Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

19.6 Sharing Personal Data

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our Company or Group Company (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

- (a) they have a need to know the information for the purposes of providing the contracted services;
- (b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- (c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- (d) the transfer complies with any applicable cross border transfer restrictions; and
- (e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

20. Penalties

It is important that you understand the implications for the Company if we fail to adhere to this Data Protection Policy and meet our Data Protection obligations. Failure to comply could result in any of, or a combination of, the following:

- (a) criminal and civil action;
- (b) fines and damages;
- (c) personal accountability and liability;
- (d) suspension/ withdrawal of the right to process Personal Data by the Information Commissioner's Office;
- (e) loss of confidence in the integrity of the Company's systems and procedures;
- (f) irreparable damage to the Company's reputation

21. Changes to this Data Protection Policy

We reserve the right to change this Data Protection Policy at any time without notice to you so ensure that you regularly obtain the latest copy of this Data Protection Policy. We last revised this Data Protection Policy in April 2018.

This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

22. Acknowledgement of receipt and review

I, [EMPLOYEE NAME], acknowledge that on [DATE], I received and read a copy of Company of Cooks Limited's Data Protection Policy, dated May 2018 and understand that I am responsible for knowing and abiding by its terms.

I understand that the information in this Data Protection Policy is intended to help Company Personnel work together effectively on assigned job responsibilities and assist in the use and protection of Personal Data.

This Data Protection Policy does not set terms or conditions of employment or form part of an employment contract.

Signed

Printed Name

Date