Data Protection Policy

KEY FACTS

StaffCircle's Data Commissioner Registration Number is ZA302977 and we confirm we have a data protection officer. As a Data Controller and Data Processor, StaffCircle aims to be compliant with the GDPR with regard to its policies and procedures around the management of client data. A designated officer ("the Designated Officer") within the Company is appointed with the specific responsibility of overseeing data protection and ensuring compliance with the Legislation. A data subject may make a subject access request ("DSAR") at any time to see the information which the Company holds about them StaffCircle ensures that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of the Company comply with this policy when processing and / or transmitting personal data.

PURPOSE OF THIS POLICY

This document sets out the obligations of StaffCircle Ltd. ("the Company") with regard to data protection and the rights of people with whom it works in respect of their personal data under The Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679 ("GDPR"). This Policy shall set out procedures which are to be followed when dealing with personal data. The procedures set out herein must be followed by the Company, its employees, contractors, agents, consultants, partners or other parties working on behalf of the Company. The Company views the correct and lawful handling of personal data as key to its success and dealings with third parties. The Company shall ensure that it handles all personal data correctly and lawfully.

DATA PROTECTION PRINCIPLES

The GDPR outlines six data protection principles we must comply with when processing personal data. These principles relate to:

- **Lawfulness, fairness and transparency** - we must process personal data lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation** - we must only collect personal data for a specific, explicit and legitimate purpose. We must clearly state what this purpose is, and only collect data for as long as necessary to complete that purpose.
- **Data minimisation** - we must ensure that personal data you process is adequate, relevant and limited to what is necessary in relation to your processing purpose.
- **Accuracy** - we must take every reasonable step to update or remove data that is inaccurate or incomplete. Individuals have the right to request that you erase or rectify erroneous data that relates to them, and you must do so within a month.
- **Storage limitation** - we must delete personal data when you no longer need it. The timescales in most cases aren't set and will depend on the business' circumstances and the reasons why we collect this data.
- **Integrity and confidentiality** - we must keep personal data safe and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

RIGHTS OF DATA SUBJECTS

Under the GDPR, data subjects have the following rights:

- The right to be informed that their personal data is being processed.
- The right to access any of their personal data held by the Company within 30 days of making a request.
- The right to prevent the processing of their personal data in limited circumstances.
- The right to rectify, block, erase or destroy incorrect personal data.
- The right to object
- The right for data portability

PERSONAL DATA

1. Personal data is defined by the GDPR as data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

2. The GDPR also defines “special category data” as personal data relating to the racial or ethnic origin of the data subject; their political opinions their religious (or similar) beliefs; trade union membership; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

3. The Company only holds personal data which is directly relevant to its dealings with a given data subject. That data will be held and processed in accordance with the data protection principles and with this Policy. The following data may be collected, held and processed by the Company from time to time:

- Customer credit card and bank account data for the purposes of payment for services provided by StaffCircle
- Customer contact details, names, addresses, e-mail addresses, telephone numbers
- Employee information relating to their work and basic person information
- Commercial information gathered as a result of e-mail based communications with its customers
- Customer credit check information and results; Data related to the nature of the customer’s business and CRM system

PROCESSING PERSONAL DATA

1. Any and all personal data collected by the Company is collected in order to ensure that the Company can facilitate efficient transactions with third parties including, but not limited to, its customers, partners, associates and affiliates and efficiently manage its employees,

contractors, agents and consultants. Personal data shall also be used by the Company in meeting any and all relevant obligations imposed by law.

2. Personal data may be disclosed within the Company. Personal data may be passed from one department to another in accordance with the data protection principles and this Policy. Under no circumstances will personal data be passed to any department or any individual within the Data Protection Policy Company that does not reasonably require access to that personal data with respect to the purpose(s) for which it was collected and is being processed.

3. The Company shall ensure that:

- All personal data collected and processed for and on behalf of the Company by any party is collected and processed fairly and lawfully
- Data subjects are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used
- Personal data is only collected to the extent that is necessary to fulfil the stated purpose(s)
- All personal data is accurate at the time of collection and kept accurate and up-to-date while it is being held and / or processed
- No personal data is held for any longer than necessary in light of the stated purpose(s)
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data in so far as those measures can be applied to StaffCircle's own systems
- All personal data is transferred using secure means, electronically or otherwise
- No personal data is transferred outside of the UK or EEA (as appropriate) without first ensuring that appropriate safeguards are in place in the destination country or territory
- All data subjects can exercise their rights set out above and more fully in the Legislation.

DATA PROTECTION PROCEDURES

The Company shall ensure that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of the Company comply with the following when processing and / or transmitting personal data:

- All emails containing personal data must be encrypted
- Personal data may be transmitted over secure networks only – transmission over unsecured networks is not permitted in any circumstances
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted
- Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data
- Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient. Using an intermediary is not permitted
- All hardcopies of personal data should be stored securely in a locked box, drawer, cabinet or similar
- All electronic copies of personal data should be stored securely using passwords and suitable data encryption, where possible on a drive or server which cannot be accessed via the internet
- All passwords used to protect personal data should be changed regularly and should not use words or phrases which can be easily guessed or otherwise compromised.

ORGANISATIONAL MEASURES

The Company shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

- A designated officer ("the Data Protection Officer") within the Company shall be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the legislation.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company are made fully aware of both their individual responsibilities and the Company's responsibilities under the Legislation and shall be furnished with a copy of this Policy.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be appropriately supervised.
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
- The Performance of those employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract. Failure by any employee to comply with the principles or this Policy shall constitute a disciplinary offence. Failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Policy shall constitute a breach of contract. In all cases, failure to comply with the principles or this Policy may also constitute a criminal offence under the GDPR.
- All contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR.
- Where any contractor, agent, consultant, partner or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

ACCESS BY DATA SUBJECTS

A data subject may make a subject access request ("DSAR") at any time to see the information which the Company holds about them.

- DSARs can be made verbally or in writing
- Upon receipt of a DSAR the Company shall have a period of 30 days within which to respond and this can be extended up to 2 months in certain circumstances. The following information will be provided to the data subject:
    - Whether or not the Company holds any personal data on the data subject.
    - A description of any personal data held on the data subject.
    - Details of what that personal data is used for
    - Details of any third-party organisations that personal data is passed to
    - Details of any technical terminology or codes.

NOTIFICATION TO THE INFORMATION COMMISSIONER'S OFFICE

- As a data controller, the Company is required to notify the Information Commissioner's Office that it is processing personal data. The Company is registered in the register of data controllers.
- Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.
- Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.
- The Data Protection Officer shall be responsible for notifying and updating the Information Commissioner's Office.

IMPLEMENTATION OF POLICY

- This Policy shall be deemed effective as of 1st November 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.
- This policy applies to data collected by StaffCircle as part and parcel of its normal commercial operations. StaffCircle cannot be held responsible for the security of data that is held outside its own systems.