Data Protection Policy

(Revised 20th October 2023)

Aim and Scope of Policy

This policy applies to the processing of personal and customer data in physical and electronic form either kept by the organisation, or that the organisation has access or visibility to in its day-to-day business. It also covers our response to any data breach and other rights under the General Data Protection Regulations.

This policy applies to the personal data of individual contacts at clients, potential clients, suppliers, competitors, website visitors, office visitors, job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

Glossary

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion or trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Personal Data Register" is the central register that records:

- For Personal Data: The categories of individuals we hold data for, the type of data held, why the data is held and processed, where the data is sourced from, whether consent is required, where the data is held, the lawful basis on which the data is processed, who the data is shared with and the retention period
- The approved 3rd Party Processors
- The digital file structure and access rights
- The locations to save regular documents
- The details of any data breach

Our Commitment

We commit to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws.

We commit to ensuring that the physical and digital data of our customers is protected to the same standard as GDPR legislation.

All our employees conduct themselves in line with this, and other related, policies.

We do not collect, hold or process the data of children.

We do not carry out profiling and/or automated decision-making using personal data.

We have completed the ICO registration self-assessment and we do not have to register with the ICO.

Where third parties process data on our behalf, we will ensure that the third party takes such measures in order to maintain our commitment to protecting data. In line with GDPR, we understand that we are accountable for the

processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Our overriding principle is that we will only use personal data in a way that an individual would reasonably expect and that we will never use customer without consent. For example, client email addresses only to communicate out the service we provide or staff ID documents to prove right to work in the UK.

Types of Data Held

Personal data is kept in both paper and electronic files and/or within our software systems.

The following types of data may be held by us, as appropriate, on relevant individuals:

From Clients, Potential Clients and Suppliers:

- individual names, phone numbers, email addresses and social media accounts
- correspondence
- We have access and visibility to:
    - Intellectual property
    - Documents and files (digital and physical)
    - Other information staff may see or overhear on Client's site

From Job Applicants:

- personal information including nationality, normal CV information and application form answers
- correspondence
- information about their current package
- interview notes
- medial history
- referee responses
- psychometric test results

From Employees and Sub-Contractor Employees - same as from Job Applicants plus:

- proof of ID and right to work in the UK
- proof of address
- P45, NI number, tax code and other normal tax information
- bank account details
- emergency contacts
- normal HR records
- correspondence
- emails sent and received
- details of any RIDDOR incidents on client sites
- timesheet data of hours worked as well as authorise and unauthorised absence

From Competitors:

- individual names, phone numbers, email addresses and social media accounts
- correspondence

From Head Office Visitors:

- personal details
- details of any RIDDOR incidents

From Website Visitors:

- device and IP address information held in a cookie
- personal details entered into web forms

Please refer to the Clean Space Privacy Notice for more information on the reasons for our processing activities, the lawful bases we rely on for data processing, when we collect data and our data retention periods.

A copy of our employee privacy notice can also be found at www.thecleanspace.com/privacy.

Data Protection Principles

All employee personal data obtained and held by us will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes it is collected and processed
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- comply with the relevant GDPR procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

Procedures

We have taken the following steps to protect the personal data of relevant individuals and customers, which we hold or to which we have access:

- we appoint employees with specific responsibilities for:
    a. the processing and controlling of data
    b. the comprehensive reviewing and auditing of our data protection systems and procedures
    c. monitoring the effectiveness and integrity of all the data that must be protected.
    d. There are clear lines of responsibility and accountability for these roles.

- we provide information to our employees on their data protection rights, how we use personal and customer data, and how we protect it. This information includes the actions relevant individuals can take if they think that their data has been compromised in any way
- we provide our employees with information and training to make them aware of the importance of protecting personal and customer data, to teach them how to do this, and to understand how to treat information confidentially
- we can account for all personal and customer data we hold, where it comes from, who it is shared with and also who it might be shared with
- we carry out risk assessments as part of our normal activities to identify any vulnerabilities in the handling and processing of personal and customer data, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal and customer data in and by the organisation.
- we conduct Data Privacy Impact Assessments for any major project we undertake to ensure "data protection by design and default"
- we recognise the importance of seeking individuals' and customers consent for obtaining, recording, using, sharing, storing and retaining some types of personal data, and regularly review our procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. We understand that any consent must be freely given, specific, informed and unambiguous. We will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time
- we have the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. We are aware of our duty to report significant breaches that cause significant harm to the affected individuals and customers to the Information Commissioner, and we are aware of the possible consequences of non-compliance.

- we are aware of the implications of the transfer of personal data internationally
- we have written procedures for how we respond to any request of an individual or customer to exercise their rights under GDPR
- we have written a procedure for how to deal with a data breach

Access to Data

Relevant individuals and customers have a right to be informed whether we process data relating to them and to access the data that we hold about them. Requests for access to this data will be dealt with under the following summary guidelines:

- To make a subject access request an email must be sent to info@thecleanspace.com
- we will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request.
- we will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals and customers must inform us immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. We will take immediate steps to correct the information.

Data Disclosures

We may be required to disclose certain data to a 3rd party. The circumstances leading to such disclosures include:

- use of IT systems and software to run or day-to-day business (e.g. Microsoft, Sage Payroll, a 3rd party IT support company)
- at the request of relevant government agencies when required to do so (e.g. HMRC, The Home Office)
- when our professional service providers need the information to provide their services to us (e.g. lawyers, accountants, bank)
- when using 3rd party marketing providers (e.g. Google, Digital Marketing Agency)
- when using sub-contractors who deliver elements of our service
- where we have outsourced any various HR Services to an external provider
- where we require advice on a specific HR issue from an external provider (e.g. sharing health data when we are obtaining advice as to whether a disabled individual requires reasonable adjustments to be made to the working environment)
- sharing health data to comply with health and safety or occupational health obligations towards the employee

These kinds of disclosures will only be made when strictly necessary.

Data security

We adopt procedures to maintain the security of data when it is stored and transported.

In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- follow the guidelines for where regular documents are saved in the filing system to ensure the correct access rights are applied
- not email any personal data outside of the organisation unless absolutely necessary and in any instance only to approved 3rd Party Data Processors as defined in the Data Register
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- ensure that all files, photos and scanned documents are deleted from local devices in line with the retention policy on the Data Register
- check regularly on the accuracy of data being entered into computers
- always use the passwords provided to access the computer system and not share passwords with people who should not have them

- use computer screen blanking to ensure that personal and customer data is not left on screen when not in use.

Data relating to employees or customers should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by Charlie Mowat. Where such data is held on any such device it should be protected by:

- ensuring that it is held on such devices only where absolutely necessary
- ensuring that it is held in the correct location on the filing system (not on the desktop or in personal folders)
- ensuring that laptops or USB drives are not left lying around where they can be stolen
- deleting personal and customer data from devices promptly after use

Failure to follow these rules on data security may lead to disciplinary action including dismissal with or without notice dependent on the severity of the failure.

International Data Transfers

The organisation may be required to transfer personal data to a country outside of the EEA. This is because our marketing and software providers may operate outside of the EEA. Where this occurs, safeguards are adopted through the 3rd Party Data Processor Addendum to our agreement with the supplier.

Breach Notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals or a risk to the business of customers, it will be reported to the Information Commissioner within 72 hours of the organisation becoming aware of it and may be reported in more than one instalment.

Individuals and customers will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual or in a high risk to their business.

If the breach is sufficient to warrant notification to the public, we will do so without undue delay.

Data Protection Training

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

Our nominated data protection officer / lead Charlie Mowat, Founder & CEO is trained in the requirements of the GDPR and is available to help you with any questions you have on the subject.

All employees who need to use our computer systems are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the organisation of any potential lapses and breaches.

Data Protection Compliance

Our Data Protection Lead subject matter expert is Charlie Mowat, Founder & CEO and can be contacted on info@thecleanspace.com or 020 7091 9721.

Version control

Issue	Page(s)	Issue Date	Additions/Alterations	Initials
1.0	All	22 June 2017	Data Protection Policy First Authorised Issue	AB
2.0	All	24 May 2018	Changed to be compliant with GDPR	AB
3.0	All	8 October 2019	Document reviewed, no amendments	SF
4.0	All	20 October 2020	Amended to include customer data protection	SF

5.0	All	20 October 2021	Document reviewed, no amendments	SF
6.0	All	20 October 2022	Document reviewed, no amendments	SF
7.0	4	20 October 2023	Removed reference to Dropbox	SF