Hosted Desktop UK Limited

DATA PROTECTION POLICY

CONTENTS

1. INTRODUCTION

This policy governs the use of personal information within Hosted Desktop UK Limited (the company) so that all of our team members, individual contractors and other workers (Personnel) will have a clear idea of the limits of use of personal information, and where to go for further advice.

1.1 Purpose

This policy lays down the principles for the processing of personal information, whether it relates to team members, suppliers, guests, customers or others. Personal information means any information relating to a living, natural person, who can be identified either directly or indirectly. Processing personal information includes the obtaining, handling, processing, transporting, storing, destruction and disclosure of personal information.

It is not designed to replace practical advice from the Data Manager. Nor is it intended to provide all the answers to questions concerning the use of personal information in particular areas, such as HR, IT or marketing.

Additional Guidance notes on specific issues (e.g. Subject Access Rights) are also available from the intranet.

1.2 Summary

The company will use the personal information of individuals fairly, lawfully, transparently and in a manner consistent with its valid business interests and at the same time, respecting the fair and lawful privacy requirements of those individuals concerned.

1.3 Status of this policy

This policy has been approved by the board of Hosted Desktop UK Limited. Personnel who process personal information on behalf of the company must adhere to the terms of this policy and any breach will be taken seriously and may result in formal disciplinary action.

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with your line manager, HR team or the Data Manager.

Any Personnel who consider this policy has not been followed should raise this matter with their relevant head of his/her function within the company, or (if an employee related issue) the HR Team.

1.4 Further advice

Further advice may be obtained from the Data Manager at Contact@hosteddesktopuk.co.uk.

2. GOVERNING PRINCIPLES

2.1 Principles

Personal information will be used within the company by its Personnel according to the principles of applicable data protection legislation (the "**DP Legislation**"), meaning the General Data Protection Regulation ("GDPR"), the Data Protection Act ("DPA") and the Privacy and Electronic Communications Regulations ("PECR"). The principles require that personal information will be:

1. Lawfulness, fairness & transparency	The DP Legislation seeks to ensure that processing is carried out lawfully, fairly and transparently without adversely affecting the freedoms, interests and rights of the individual concerned. For personal information to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the individual data subject has consented to the processing, or that the processing is necessary for the performance of the contract with the individual, for compliance with a legal obligation, the vital interest of the data subject, or the legitimate interest of The company or the party to whom the information is disclosed. DP Legislation imposes specific requirements in relation to electronic marketing (e.g. email, Apps, social media and SMS), telephone marketing and the use of tracking or profile analysis technology (e.g. to deliver targeted online advertising). It is very important that you seek advice from internal teams, including the Data Manager before undertaking such activities on behalf of the company. Before personal information is passed to third parties, including law enforcement agencies, government bodies, investigators or anyone else, it is important that full consideration is made of the possible data protection implications of doing so. Again, please contact the Data Manager if you have any questions or are in any doubt regarding a particular request.
2. Purpose limitation	Personal information may only be processed for the specific purposes notified to the individual when the information was first collected or for any other purposes specifically permitted by the DP Legislation. This means that personal information must not be collected for one purpose and then used for another, unless the other purpose is also specified.
3. Data minimisation	Only personal information that is necessary for the purposes specified should be collected. Any data which is not necessary for that purpose should not be collected in the first place.

4. Accuracy	Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal information at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date information should be securely destroyed.
5. Storage limitation	Personal information should not be kept longer than is necessary for the purpose for which it was collected. This means that data should be destroyed or erased from our systems when it is no longer required.
6. Integrity and confidentiality	We must ensure that appropriate safeguarding measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Individual data subjects may apply to the courts for compensation if they have suffered damage or distress from such a loss. From May 2018 tough new obligations to notify, in certain situations, regulators (and affected individuals) will be introduced if the above mentioned safeguarding measures fail to protect personal information. It is therefore very important that you immediately report any suspected incident to the Data Manager. The DP Legislation requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction, be it paper-based or in electronic format. Personal data may only be transferred to a third-party data processor (such as a supplier or service provider to the company or a group company) if they agree to comply with those procedures and policies, or if they put in place adequate measures. DP Legislation also requires the company to have a written contract in place with all suppliers or service providers who will process their personal information. It is therefore important that procurement are involved in all such arrangements, that the correct procurement templates are used and/or that internal legal teams are consulted prior to the engagement of suppliers and partners who will either process personal information per our instructions or jointly process personal data.
7. Accountability	We must ensure that we are able to evidence that we comply with DP Legislation. For example, that all the above principles have been applied, documentation is up to date, training on data protection and privacy has been completed, and security measures are complied with.

2.2 Compliance with the principles

In order to meet the requirements of the principles the company will:

- observe the conditions regarding the fair, lawful and transparent collection and processing of personal information;
- meet its obligations to specify the purposes for which personal information is used;
- collect and process personal information only to the extent it is required for the company's valid business interests and where there is a legal basis for doing so;
- ensure the quality of the personal information used;
- adopt a data retention and disposal policy that includes the length of time personal information is held;
- ensure that the rights of individuals about whom personal information is held can be fully exercised under the respective DP Legislation;
- take appropriate technical and organisational safeguarding measures (which include strict Personnel access controls) to protect personal information including following the policy guidelines set out in Hosted Desktop UK Ltd IT Security Policy and IT Acceptable Use Guide;
- ensure that any contractor, agent or other third party who processes personal information on the company's behalf does so under a written contract requiring that third party to:
    - only process the personal information in accordance with the company's instructions; and
    - take appropriate technical and organisational security measures to safeguard personal information; and
    - ensure that personal information is not transferred outside the European Economic Area without suitable safeguards; and
    - confirms destruction of all information. This should include paper, electronic and consideration should be given to backup media; and
    - which contains additional data processing clauses which are specified in the DP Legislation.

2.3 Responsibility for compliance

The company is a data controller (and, in certain circumstances, also a processor) responsible for complying with the DP Legislation. It is the responsibility of each member of Personnel to comply with this policy when using personal information relating to team members, customers or others.

The Data Manager has responsibility for this policy and its review.

3. LEGAL BASIS

All processing must be lawful, which means that there must be one of the following legal grounds established before processing can take place:

3.1 Consent

When using consent, the company must be able to demonstrate that consent has been unequivocally given, not just implied. Consent cannot apply to children under 13 vis-à-vis online unless the holders of parental responsibility have provided it. Nor can consent be coerced, for example, forced consent as part of a contract. Consent is a valid legal basis for processing of special categories of personal information. Consent must be prominent in any privacy statement:

- freely given, specific, informed and unambiguous
- a clear affirmative action, signifying agreement to the processing of their personal information

When consent is given in the context of a statement which also concerns other matters, the request for consent needs to be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

When consent is provided, it must be able to be withdrawn at any time with as much ease as it was originally given. If withdrawn, the information must be erased[1].

When carrying out any direct marketing using personal information the company will:

- only market to those individuals under the correct legal basis, such as consent, and for the specific purposes notified to the guest or customer when the personal information was collected;
- use safeguarding measures such as the Telephone Preference Service, Mailing Preference Service and other third party suppression lists where appropriate;
- use standard Hosted Desktop UK Limited consent wording; and
- require our third party partners to use the an approach compatible with this document when capturing consents on our behalf.

Any use of personal information for direct marketing purposes which is not in accordance with the requirements set out above must be approved, in advance, by the Data Manager.

NB you must use the legal basis of consent for any direct marketing that involves electronic communications, including Apps, SMS, phone and / or email, and for the purpose of direct marketing using these channels, you cannot use legitimate interests.

3.2 Legitimate Interests

It is always important to demonstrate the necessity for the company to process personal information for its legitimate interests if relying on this legal basis.

[1] The right to data portability applies in the case of contract being the legal basis.

When using legitimate interests, the company must be able to demonstrate that there are no over-riding risks to the individuals' interests, rights or freedoms.

Therefore, the company's legitimate interests when weighed up against the risks to individuals must always be taken into account when conducting a data protection impact assessment (required for any new system or process – or a significant change). Similarly, the mitigating measures that are applied need to be documented.

3.3 Contract

When using contract as the legal basis, the company must be able to demonstrate that the necessity of the performance of a contract (or negotiation of a contract) with the individual, for example, employee, supplier or customer / guest[2].

NB - Consent is presumed not to be freely given if it does not allow separate consent to be given if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

3.4 Legal Obligation

When there is a statutory obligation, The company must be able to demonstrate for the specific purposes of processing personal information what that legal obligation is, third parties who receive the personal information under the auspices of the obligation, and any retention obligations required.

3.5 Vital Interests

When using vital interests, The company must be able to demonstrate that there is a necessity to process personal information in the vital interests of the individual concerned. For example, capturing allergy information when taking a table booking.

3.6 Public Interest

When using public interest, The company must be able to demonstrate that there is a need to store personal information in the interests of the public. For example, for public safety and security purposes, retaining staff information to pass to emergency services personnel given some event.

4. REQUIREMENTS

4.1 Notices

Individuals have the right to be informed regarding the specific purposes that their personal information is being processed before processing takes place, for how long the information will be stored and processed, who it is being shared with (including internationally), and if there is automated decision-making, including profiling.

---

[2] The right to not being subject to automated decision-making, including profiling, does not apply where there is a necessity for the purposes and legal basis of a contract (or entering into a contract).
The right to data portability applies in the case of contract being the legal basis.

4.2 Transfers

The DP Legislation prohibits us from transferring personal information to countries outside the European Economic Area (EEA), unless we first put in place additional safeguards.

For example, before transferring information, we may need to enter into contracts with recipients in non-EEA countries which incorporate Standard Contractual Clauses approved by the EU Commission.

Any such transfers should be notified to the Data Manager stating who the data is being shared with, and if it is subject to any automated decision-making, including profiling.

4.3 Data Protection by Design / Data Protection by Default - Approach

We must ensure that our policies reflect processes and a culture of respecting privacy. This includes ensuring that we are each accountable for the security and other safeguarding measures are adhered to, as well as collecting, processing storing, and only sharing it with those authorised and required to use it, only the personal information that is required, and only for as long as it is required for.

4.4 Data Protection Impact Assessment (DPIA)

DPIA guidance is to undertake an assessment from a risk-based perspective.

Any new process or system that includes innovative technologies or processing personal information or monitoring individuals on a large scale, where there is a higher risk to rights and freedoms of individuals affected.

5. DATA SUBJECT RIGHTS

5.1 Summary of Rights

The subjects of personal information held by, or on behalf of, the company ("Data Subjects") have a wide range of rights granted to them under the DP Legislation. Whilst we can make use of personal information for specific purposes and where we can lawfully justify such use, an individual can still exercise significant control over what we do. We need to operate our business and process personal information in a way which facilitates the rights of individuals to exercise this control.

Today's DP Legislation significantly enhances the rights available to individuals. A summary of each of the rights is set out below.

It is important that requests from individuals wishing to exercise any of the rights below are quickly identified and sent to the appropriate person for preparing a response. Personnel should not respond to such requests without first discussing the matter with your line manager, who may refer the matter to the Data Manager.

5.2 Right to be informed

Individuals have the right to be informed of how their personal information is being processed.

This must be provided in a privacy notice – the notice may be in the form of:

- a privacy statement or privacy policy, separate to a cookie policy (which is also required);
- an email signature, other correspondence, or information board in a public area;
- a privacy clause in an Employee Handbook; or
- a clause within the Terms and Conditions of a contract.

In general, individuals must be informed about:

- the purpose for processing their personal information,
- what information is processed, and
- for how long.

The notice should also include the contact details of the company and our Data Manager.

Within the privacy notice, individuals also have the right to be informed whether any third parties are to be recipients of their personal information.

Similarly in the same notice, individuals have the right to be informed whether their personal information will be transferred to 3rd countries or international organisations – generally outside the European Economic Area not covered by the 'adequacy' regime or other safeguards, such as Binding Corporate Rules or Standard Contract Clauses.

5.3 Right of access ('Subject Access Requests')

Individuals have the right to request that we:

(i) confirm, amongst other things, whether we are holding their personal information;

(ii) provide them with a copy of that information, and

(iii) provide them with supporting (and detailed) explanatory materials.

We must comply with Subject Access Requests without undue delay and at the latest within one month of the request (although this can be extended in limited circumstances), and we cannot charge individuals for making a request (except in specific situations). Particular care should be taken if a request from one individual would result in personal information of another individual being disclosed. [seek advice from the Data Manager about whether such information should be redacted or its disclosure justified]

Please contact the data manager if you receive a request for the release of personal information.

5.4 Right to rectification

Individuals have the right to require us to rectify inaccuracies in personal data held about them. In some circumstances, if personal information records are incomplete or

inconsistent, individuals have the right to require us to complete the data, make it consistent, or to record a supplementary statement correcting it.

Advice should be sought from the Data Manager if uncertain.

5.5 Right to erase ('the right to be forgotten')

Individuals have the right to have their personal information erased in certain specified situations – in essence where the continued processing of it does not comply with DP Legislation.

Where an individual makes an erasure request, we must respond without undue delay and in any event within one month (although this can be extended in limited circumstances).

There are a number of exemptions which apply to such requests, and you should not assume that you should delete personal information simply because you have received a request of this nature.

Such a request should be referred to the Data Manager as soon as it is received.

5.6 Right to restriction

This right allows individuals, in certain situations, to restrict our use of their personal information. This might result in our use of it being limited to storage only, and could mean we have to move personal information to separate IT systems, or temporarily block access to it.

This issue could arise in a situation where an individual is disputing the accuracy of information we hold, or where they are objecting to our right to continue to use their information and we need to take some time to establish whether we have a right to continue to do so.

Such a request should be referred to the Data manager as soon as it is received.

Advice should be sought from the Data Manager if uncertain.

5.7 Right to data portability

Data portability goes beyond rights of access and requires us to provide, on request, information to individuals in a structured, commonly used and machine-readable format. We could also be asked by an individual to transmit personal information directly to another data controller in the same format.

This right only applies to electronic records which have been provided to us by the individual themselves, or generated from their activity or are our observations of their activity (but not subsequent analysis of such activity), and only where we hold the personal information because we have the individual's consent or because we are fulfilling a contract with them.

Such a request should be referred to the Data manager as soon as it is received.

5.8 Right to object

Individuals have an absolute right to object to their personal information being processed for the purpose of direct marketing. If we receive any such objection we must immediately cease such marketing activities in respect of that individual.

Individuals have a wider right to object to processing we undertake which is justified on the basis that it is in our legitimate interests (rather than because we have their consent). If we receive an objection of this nature we must assess the objection and carefully consider if we can demonstrate compelling legal grounds to continue to process the personal information.

Such a request should be referred to the Data manager as soon as it is received.

5.9 Rights in relation to automated decision-making, including profiling

Individuals have rights which apply if we take decisions about them which are based solely on automated processing (i.e. without human intervention) and which produce significant or legal effects on the individuals. An example of this would be the use of an algorithm to analyse alumni data and decide which groups of people receive preferential promotional offers.

We can use such automated decision making in circumstances where we need to do so in order for us to enter into a contract with the individual, or where we have their explicit consent. However, we need to be transparent with individuals about what decisions are taken in this way, and we may need to put in place additional protective measures to protect the individuals concerned.

Such a request should be referred to the Data manager as soon as it is received.

5.10 Right to complain

Individuals have the right to bring a complaint to the Information Commissioner, or other supervisory authority.

5.11 Right to bring legal proceedings

Individuals have the right to seek judicial remedy through the Courts.

5.12 Requests

Team members, customers and other subjects of personal information held by, or on behalf of the company may exercise any of the rights specified above. These rights are subject to certain exemptions which are set out in the DP Legislation.

Any team member, customer or other subject of personal information wishing to exercise any of these rights should make the request in writing to the Data Manager.

The company aims to comply with any requests in relation to personal information as quickly as possible and in any event within the time specified by DP Legislation.

5.13 Personnel responsibilities

All Personnel are responsible for:

- checking any personal information which they provide to the company is accurate and up to date;

- informing the company of any changes to personal information which they have provided, for example change of address; and

- checking any information that the company may send out from time to time, for example giving details of personal information that is held by the company.

If, as part of their responsibilities, Personnel have access to or use personal information about other people as part of their employment duties (for example, customer or guest personal information) they must comply with this policy and in the company's other policies and procedures for processing personal information.

All Personnel are responsible for ensuring that any personal information which they hold or process is kept secure and is not disclosed either orally or in writing or otherwise to any unauthorised third party and transferred internationally without checking first that the right safeguards are in place.

Only those Personnel who strictly require access to personal information for their role should have such access, and all Personnel must make sure that personal information is not shared with Personnel who do not need to see it.

Personal information about Personnel and others may include special categories of personal information or other information that needs to be treated sensitively. This is personal information relating to an individual's:

- racial or ethnic origin;

- political opinions;

- religious beliefs or other beliefs of a similar nature;

- membership of a trade union;

- physical or mental health or condition;

- sexual life;

- biometric or genetic data (e.g. facial or iris imaging, or biological sample information.)

- commission or alleged commission of an offence;

- any proceedings for any offence or alleged offence, the disposal of such proceedings or any sentence imposed by a court

Particular care must be taken when dealing with any personal information falling under one or more of these headings. If in doubt, do take advice from the Data Manager or (if an employee related issue) the HR Team. In general, such personal information must be kept very secure and must only be allowed to be seen by a restricted number of people who need to know it. The Data Manager will act as an intermediary between the company, employees, suppliers, customers, partners and others.

5.14 Email

Due to the ease with which large quantities of personal data can be accidentally or inappropriately exposed when using email staff should be particularly careful to use email in a considered manner. In particular:

- Email to addresses outside the "@company.com" domain should not include personal data beyond simple contact information (name, email, telephone, address, job title and place of work). If more extensive data needs to be provided an encrypted attachment can be used (MS Office encryption is adequate for low risk data) or a specialised secure transfer option may be used in high risk cases.

- If using an encrypted email attachment to send personal data o not include the password in the same email and preferably use a different communication method to send the password (eg SMS).

- Emails sent from "@company.com" addresses to "@company.com" addresses are restricted to the secure environment and may include personal data.

- Do not include any personal information in the "Subject" field of email regardless of the recipient, in particular do not include names or other potential identifiers.

- Staff should make it a habit to preferentially use "Bcc" rather than "Cc", "Cc" should only be used where it is necessary for all recipients to see replies.

- When using Distribution Lists to send emails to those outside the company, ensure that email addresses are not shared. Use the "Bcc" facility so that email addresses are not displayed.