THE BUSINESS PHONE LIMITED ("TBP")
DATA PROTECTION POLICY

TBP is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. It has therefore adopted the following principles and undertakings to underpin this

The principles for processing of personal data

Lawfulness, fairness and transparency

Personal data will be collected and processed in a lawful, fair and transparent manner to protect the individual rights of the data subjects.

Restriction to a specific purpose

Personal data will only be collected for specified explicit and legitimate purposes and will not be processed in a manner incompatible with those purposes.

Accuracy of Data

Personal data will be accurate and where necessary kept up to date. TBP will take all reasonable steps to erase or rectify errors or inaccurate information without delay.

Relevant Data

Personal data will be adequate, relevant and limited to what is necessary. Personal data will not be stored longer than necessary.

Rights of data subjects

TBP respects the rights of all data subjects including rights of access to their data, the right of restriction of processing or erasure, and the right of accuracy. TBP will provide clear and unambiguous information about how and why subjects' data are collected and processed.

Right to be Forgotten

Time limits for storage of personal data will be defined. TBP will erase personal data that is no longer necessary in relation to the purposes for which it has been collected or where the original consent or permission is withdrawn and no other legitimate purpose for processing applies.

Data security

Personal data will be processed securely. Measures will be taken against unauthorised processing or alteration, and against loss or destruction or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. TBP will seek to ensure ongoing integrity, availability, confidentiality and authenticity.

TBP will provide resilient systems and services when processing personal data.

In the event of an incident TBP will have the ability to restore the availability and access to data in a timely manner.

Data protection by design and by default

TBP will implement appropriate technical and organisational measures for ensuring that, by default, only personal data that is necessary for each specific purpose of the processing is processed.

Accountability

There shall be accountability in all processing activities.

This Policy defines requirements to ensure compliance with laws and regulations applicable to the TBP's collection, use, processing, and transfer of personal data throughout the world.

Scope

TBP is committed to complying with the applicable Data Privacy and Protection requirements in the countries in which it operates. Because of differences among these jurisdictions TBP has adopted a Data Protection policy which creates a common core of values, policies and procedures intended to achieve generic compliance, supplemented (where applicable) with additional guidance applicable in those jurisdictions which require such additional guidance.

This policy is based upon the UK Data Protection Act 1998 and the General Data Protection Regulation (GDPR) which operates within EU Regulation 2016/679, which provides a model for global Data Protection and privacy compliance. TBP has adopted this policy for TBP affiliated companies.

This Policy applies to all affiliates, suppliers and contacts who receive Personal Data from TBP, have access to Personal Data collected or processed by the TBP, or who provide information to the TBP, regardless of geographic location.

TBP will use reasonable efforts to correctly establish its status for all Data Processing as either a Data Controller, or Data Processor acting for another Data Controller.

Group Compliance

TBP is committed to ensuring the adherence to the policy and will implement procedures, as well as any duties required by applicable law, including:

determining whether notification to one or more Data Protection authorities is required as a result of the TBP's Data Processing activities, then making any required notifications, and keeping such notifications current.

designing and implementing ongoing programs for training employees in Data Protection rules and procedures.

establishing procedures and standard contractual provisions for obtaining compliance with this Policy by group companies, affiliates, suppliers, and third parties who receive Personal Data from TBP, have access to Personal Data collected or processed by TBP, or who provide information to TBP, regardless of geographic location.

establishing mechanisms for periodic audits of compliance with this Policy, implementing procedures, and applicable law.

establishing, maintaining, and operating a system for prompt and appropriate responses to Data Subject requests to exercise their rights.

establishing, maintaining, and operating a system for the prompt and appropriate automatic disclosure to the relevant authorities and Data Subjects of any loss of Personal Data.

informing senior managers, officers, and directors of TBP of breaches or suspected breaches to the policy.

ensuring that the risk management plans in relation to Data Protection are implemented effectively and promptly.

ensuring that adequate assurance regarding the effectiveness of Data Protection procedures and audits is provided to the Board, management and other stakeholders.

Data Protection Principles

TBP has adopted the following principles to govern its use, collection, and transmittal of Personal Data, except as specifically provided by this Policy or as required by applicable laws:

Personal Data shall only be processed fairly and lawfully.

Personal Data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes.

Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or processed.

Personal Data shall not be collected or processed unless one or more of the following apply:

the Data Subject has provided Consent;

processing is necessary for the performance of a contract directly with the Data Subject, or to which the Data Subject is an affiliate of a party;

processing is necessary for compliance with a legal obligation;

processing is necessary to protect the vital interests of the Data Subject;

processing is necessary for legitimate interests of TBP or by the third party or parties to whom the Data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject.

The appropriate physical, technical, and procedural measures shall be taken to:

prevent and/or to identify unauthorised or unlawful collection, Processing, and transmittal of Personal Data; and

prevent accidental loss or destruction of, or damage to, Personal Data.

Transfers to Third Parties

Personal Data shall not be transferred to another entity, country or territory, unless reasonable and appropriate steps have been taken to establish and maintain the required level of Data Security.

Personal Data may be communicated to third persons only for reasons consistent with the purposes for which the Data were originally collected or other purposes authorised by law.

All transfers of Personal Data to third parties for further Processing shall be Subject to written agreements supporting the security of the data transfer.

EU Personal Data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless the transfer is made to a country or territory recognised by the EU as having an adequate level of Data.

Subject to the provisions of the above, Personal Data may be transferred where any of the following apply:

The Data Subject has given Consent to the proposed transfer;

The transfer is necessary for the performance of a contract between the Data Subject and TBP;

The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between TBP and a Third Party;

The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defence of legal claims;

The transfer is required by law;

The transfer is necessary to protect the vital interests of the Data Subject.

Sources of Personal Data

Personal Data shall be collected only from the Data Subject unless the nature of the business purpose necessitates collection of the Data from other persons or bodies.

If Personal Data are collected from someone other than the Data Subject, the business unit collecting the Data must have confirmation, in writing, from the supplier of the Data that the Data Subject has provided Consent to the transfer to TBP.

Data Subject Rights

Data Subjects shall be entitled to obtain the information about their own Personal Data upon a request made in writing to TBP who will establish a system for logging each request under this Section as it is received and noting the response date

TBP shall provide its response to a request above within 40 days from the date of the written request, or within a shorter timescale if required by any country legislation.

Data Subjects shall have the right to require TBP to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

TBP may establish reasonable fees to cover the cost of responding to requests from non-employee Data Subjects.

Sensitive Data

Sensitive Personal Data should not be processed unless:

processing is specifically authorised or required by law.

the Data Subject expressly and unambiguously Consents.

data relating to criminal offenses may be processed only by or under the control of the Legal Department.

Data Retention

Personal Data must be kept only for the period necessary for permitted uses. TBP has established local Record Retention Policies which determine applicable timescales for Data deletion.

Personal Data shall be erased if their storage violates any Data Protection rules or if knowledge of the Data is no longer required by TBP, or at the request of the Data Subject.

Intra-Group Processing

Where TBP relies on another group company to assist in its Processing activities, TBP will enter a data transfer process is in place with that other group company to ensure that responsibility for the data are clearly identified, as both parties may be considered as Data Controllers.

Where the other group company is located abroad, the group companies involved in the Processing shall be known as a Data Exporter and a Data Importer respectively, although there may be more than one Data Importer involved in the Processing.

Third Party Processors

Similarly, where TBP relies on third parties to assist in its Processing activities, TBP will choose a Data Processor who provides sufficient security measures and take reasonable steps to ensure compliance with those measures.

TBP will enter into a written contract with each Data Processor requiring it to comply with Data privacy and security requirements imposed on TBP under local legislation.

Audits of Third Party Data Processors

As part of TBP's internal Data auditing process, TBP shall conduct periodic checks on processing by third party Data Processors which will included reconfirming current security measures.

Notice to Directors, Managers, and Officers for Non-Compliance

The compliance team shall notify directors, managers, and other officers of TBP that:

failure to comply with relevant Data Protection legislation may trigger criminal and civil liability, including fines, imprisonment, and damage awards; and

they can be personally liable where an offence is committed by TBP with their Consent or is attributable to any neglect on their part.

Data Security

TBP has documented Data Protection and Electronic Communications policies, under which it shall adopt physical, technical, and organisational measures to ensure the security of Personal Data, including the prevention of their alteration, loss, damage, unauthorised Processing or access, having regard to the nature of the Data, and the risks to which they are exposed by human action or the physical or natural environment. These measures will be documented within the Data Protection and Electronic Communications, which will be reviewed at least annually, or when necessary to reflect significant changes to security arrangements.

Security measures should include all the following:

prevention of unauthorised persons from gaining access to Data Processing systems in which Personal Data are processed.

preventing persons entitled to use a Data Processing system from accessing Data beyond their needs and authorisations.

ensuring that Personal Data during electronic transmission during transport or during storage on a Data carrier cannot be read, copied, modified or removed without authorisation.

ensuring Personal Data is protected against undesired destruction or loss.

ensuring data collected for different purposes can and will be processed separately.

Ensuring data not kept longer than stipulated in the Data Retention Policy, including by requiring that Data transferred to third persons be returned or destroyed.

Compliance Measurement.

TBP shall establish a schedule for and implement a Data Protection compliance audit for all locations. TBP shall devise a plan and schedule for correcting any identified deficiencies within a fixed, reasonable time.

TBP shall review annually its Data collection, Processing and Security practices. Subject to these reviews it shall determine what Personal Data the business unit is collecting including that held in manual systems that constitute "Relevant Filing Systems"

Information collected in this annual review shall be reviewed and appropriate action including, without limitation, the following:

recommendations relating to improvement to policies and procedures to improve compliance with this Policy and applicable law.

satisfying the requirements for self-certifying compliance within local Data Protection Authorities.

Access

This Policy shall be available at TBP's website. This Policy may be revised at any time but at least annually and the latest copy will be website.

Glossary

Consent means any freely given specific and informed indication of his wishes by which the Data Subject signifies agreement to Personal Data relating to him being processed. Consent may be obtained by a number of methods. These may include clauses in contracts, check boxes on replies to application or forms, click boxes contained in online forms/forums where Personal Data is entered.

In most European Union countries, Consent to the Processing of Sensitive Personal Data needs to be clear and unequivocal. This generally means that some form of specific, active Consent) is required. This requirement is sometimes found to be less unequivocal beyond the EU.

Data (whether or not having an initial capital letter) as used in this Policy shall mean information which either:
is being processed by means of equipment operating automatically in response to instructions given for that purpose;
is recorded with the intention that it should be processed by means of such equipment;
is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System;
does not fall within any of the above, but forms part of a readily accessible record covering an individual.

Data therefore includes any digital Data by computer or automated equipment, telephone recordings, and any manual information which is part of a Relevant Filing System.

Data Controller means a person who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed.

Data Exporter means the Data Controller or Data Processor who transfers the personal data abroad.

Data Importer means the Data Controller or Data Processor who agrees to receive from the Data Exporter personal data for further processing in accordance with the terms of this Policy and the relevant Data Transfer Agreement.

Data Processor means any person, other than an employee of the Data Controller, who processes the Data on behalf of the Data Controller. A company may be a Data Processor if defined as such under contractual terms with the Data Controller.

Data Subject means the person to which Data refers. Data Subjects include customers and web users, individuals on contact /e-mailing lists or marketing Databases, employees, affiliates, contractors and suppliers.

Personal Data means Data related to a living individual who can be identified from the Data or from the Data and other information in the possession of, or likely to come into the possession of, a Data Controller or Data Processor. Personal data does not include information that has been anonymized, encoded or otherwise cleaned of its identifiers, or information which is publicly available, unless combined with other non-public personal information.

Processing covers a wide variety of operations relating to Data, including obtaining, recording or holding the Data or carrying out any operation or set of operations on the Data, including:

organisation, adaptation, or alteration;

disclosure by transmission, dissemination, or otherwise; and

alignment, combination, blocking, erasure, or destruction.

Relevant Filing System means any set of information relating to individuals, whether kept in manual or electronic files, structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to an individual is readily accessible.

Therefore, any digital Database and/or organised manual files relating to identifiable living individuals fall within the scope of Data Protection laws and regulations, while a Database of pure statistical or financial information (which cannot either directly or indirectly be related to any identifiable living individuals) will not.

Sensitive Data means Personal Data containing information as to the Data Subject's:

Race or ethnic origin;

Religious beliefs or other beliefs of a similar nature;

Political opinions;

Physical or mental health or condition;

Sexual history or orientation;

Trade union membership.

Commission or alleged commission of any offence and any related court proceedings.

Technology: Technology is to be interpreted broadly, to include any means of collecting or Processing Data, including, without limitations, computers and networks, telecommunications systems, video and audio recording devices, biometric devices, closed circuit television, etc.

Privacy Statement*

Collection of personal data

As a visitor to our websites you are generally in control of the personal data shared with us. We may capture limited personal data automatically via the use of cookies on our website.

Please see the section on Cookies below for more information.

We receive personal data, such as name, title, company address, email address, and telephone and fax numbers, from website visitors; for example, when an individual registers on our website or subscribes to updates from us.

You are also able to send an email to us through the website. These messages will generally contain the user's screen name and email address, as well as any additional information the user may wish to include in the message.

We ask that you do not provide sensitive information (such as race or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; physical or mental health; genetic data; biometric data; sexual life or sexual orientation; and, criminal records) to us when using our website; if you choose to provide sensitive information to us for any reason, the act of doing so constitutes your explicit consent for us to collect and use that information in the ways described in this privacy statement or as described at the point where you choose to disclose this information.

Withdrawing Consent

Should you subsequently choose to unsubscribe from mailing lists or any registrations, we will provide instructions on the appropriate webpage, in our communication to the individual, or the individual may contact us by email to info@thebusinessphone.com.

Cookies

We use small text files called 'cookies' which are placed on your hard drives to assist in personalising and enriching your browsing experience by displaying content that is more likely to be relevant and of interest to you. The use of cookies is now standard operating procedure for most websites. However, if you are uncomfortable with the use of cookies, most browsers now permit users to opt-out of receiving them. You need to accept cookies in order register on our website. You may find other functionality in the website impaired if you disable cookies. After termination of the visit to our site, you can always delete the cookie from your system if you wish.

You can find out more details regarding our use of cookies on our Cookies page.

Links to Other Websites

This Privacy Statement applies only to this website. This website may contain links to other websites not operated or controlled by TBP ("Third Party websites"). Policies and procedures described in this Privacy Statement do not apply to third party websites.

TBP is not responsible for the contents of any linked site or any link contained in a linked website. Such links have been provided to you only as a convenience and the inclusion of a link does not imply endorsement by TBP of the website

Links from this website do not imply that TBP endorses or has reviewed the third-party websites. We suggest contacting those websites directly for information on their own privacy statements.

Use and protection of visitor's personal data

When a visitor provides personal data to us, we will use it for the purposes for which it was provided to us as stated at point of collection (or as obvious from the context of the collection). Typically, personal data is collected to:

register for certain areas of the site;

subscribe to updates;
enquire for further information;
distribute requested reference materials;
monitor and enforce compliance with our terms and conditions for use of our website;
administer and manage our website, including confirming and authenticating identity and preventing unauthorised access to restricted areas, premium content or other services limited to registered users; and
aggregate data for website analytics and improvements.
Registration details of professional advisors / intermediaries etc will be stored on a secure database.
Private individuals who try to register will have their applications rejected and their details will be deleted within 48 hours.
TBP relies on third parties to assist in its Processing activities, TBP choose Data Processors who comply with Data privacy and security requirements to a similar or equivalent standard and will take reasonable steps to ensure compliance with those measures.
Unless we are asked not to, we may also use your data to contact you with information about TBP's business, services and events, and other information which may be of interest to you.
Our websites do not collect or compile personal data for the dissemination or sale to outside parties for consumer marketing purposes or host mailings on behalf of third parties. If there is an instance where such information may be shared with a party that is not a TBP Company, the visitor will be asked for their consent beforehand.
TBP uses technical and organisational security measures to reasonably protect personal data against unauthorised access, accidental or intentional manipulation, loss and destruction.
The internet is not typically considered as a secure environment and therefore information sent can be accessed by unauthorised entities, potentially affecting the integrity of the communication itself.

Please note that TBP accepts no responsibility or liability for the security of your information whilst in transit over the internet. To protect your privacy, we would like to remind you that you may choose another means of communication if you deem it appropriate.

Data retention
Personal data collected via our websites will be retained by us for as long as it is necessary (e.g. for as long as we have a relationship with the relevant individual). By accessing the TBP Website, you are accepting this Privacy Statement and acknowledging the Data Protection Policy of TBP ("Statement").
If you do not agree to this Statement, do not proceed to further web pages of the TBP website or any associated TBP Company Website as listed within this site.
This Statement may be subject to change from time to time, therefore it is advised that you consult it on a regular basis.

This policy is based upon the UK Data Protection Act 1998 and the General Data Protection Regulation (GDPR) which operates within EU Regulation 2016/679, which provides a model for global Data Protection and privacy compliance. TBP has adopted this policy for TBP affiliated companies