Data Protection, Data Privacy and Compliance

CPB UK Ltd was formed in 1998 to provide outsourced marketing services to technology suppliers and manufacturers. In supplying this document, the CPB Board of Directors hopes to allay any potential fears that clients and suppliers may have around non-compliance, misuse of information and lack of security procedures.

Should you have any points that you wish to clarify, these should be addressed to the CPB Data Protection Officer, Jon Pritchett, by email to jon@cpbuk.co.uk, or by calling 01295 263410.

Contents:

1) Privacy Statement

CPB UK Limited ("the company") is a business-to-business based marketing services agency offering a range of outsourced, sales support services to suppliers of technology and communications. Registered as a limited company in England (3907803), the company is committed to uphold the privacy rights of individuals, and to protect the intellectual property of our clients.
This privacy statement details our approach to the capture and processing of personal information in accordance with the requirements of current legislation (e.g. Data Protection Act, GDPR, PECR, ePrivacy Regulation).
The company is registered as a Data Controller with the UK Information Commissioner's Office under reference ZA230015.

Should you need to clarify any aspects that you consider are not covered sufficiently within this statement, please contact the company's Data Protection Officer (Jon Pritchett – jon@cpbuk.co.uk).

Information processed

Personal information that may be collected are the name, business email address and business title/position of individuals employed within UK based organisations. The personal information we may gather, and store originates from:

- Marketing assignments delivered for CPB clients
- CPB's own commercial activity

1a) Marketing assignments delivered for CPB clients

Assignments we deliver for our clients will usually involve an agreed target audience, and the data used for direct marketing purposes in such assignments will be supplied by the client, a third-party organisation, or a combination of the two.

Personal information will be updated as part of the assignment and an updated list of contact information will be returned to the client at the end of the assignment. A copy of these lists is held by CPB for a period of 12 months after the end of the assignment.

CPB staff are instructed to make it clear to all contacts that we are acting on behalf of our client and where necessary, we give assurance to contacts who are asked to confirm personal information that their details will be processed and stored in a compliant manner by our clients.

Information supplied by a client or third party, and any further information captured during an assignment will be treated as confidential, as will any other information supplied by a client as part of an assignment briefing. Information will not be shared with any individual or organisation other than nominated employees and agents of the client.

1b) CPB's own commercial activity

We collect information from visitors to our website through URL IP tracking, from an enquiry form on the website and we collect information when you email us with an enquiry, or indeed via a telephone enquiry.

Information is also collected via a New Customer Information Form for administrative and invoicing purposes at the beginning of a new trading relationship.

We process this information, which will include personal information, for the purposes of:

- Providing intelligence about our services
- Dealing with your enquiries and requests
- Administering orders, invoicing and supplier transactions

Your personal information will not be shared with any individual or organisation other than nominated CPB employees and the information will never be sent to countries outside of the European Union.

If at any point you wish to opt-out of communications from us, or request details of what personal information is held, please contact our Data Protection Officer, Jon Pritchett: jon@cpbuk.co.uk.

2) Cookie Policy

Our websites use cookies – small text files that are placed on your computer to help the website provide a better user experience. In general, cookies are used to retain user preferences, to store information for things like shopping carts and to provide anonymised tracking data to third party applications like Google Analytics.

The company does not capture any personal information through website cookies.

As a rule, cookies will make your browsing experience better, however, you may prefer to disable cookies on this site and others. The most effective way to do this is to disable cookies within your browser. If this is your aim, we suggest consulting the *Help* section of your browser or take a look at websites such as *About Cookies* which offers guidance for most of the popular browsers.

3) IT and Data Security Policy

CPB UK Limited ("The Company") use hosted applications and cloud based systems to deliver marketing assignments on behalf of clients. The assignments regularly involve the capture and export of personal data as specified within the EU General Data Protection Regulation ("GDPR"). The purpose of this document is to supply reassurances on the infrastructure, policies and procedures adopted by The Company in providing a protected and compliant environment to deliver services to clients.

The Board of Directors of The Company are committed to the implementation, staff awareness and ongoing management of a secure IT and Data Policy.

3a) Key Objectives:

The Company is committed to:

- maintaining the highest possible standards of integrity, confidentiality and security when processing personal data
- ensuring that suppliers, contractors, and support organisations have high levels of appropriate data security in place
- a continual awareness programme for all staff to encourage commitment, at all levels within The Company, to current data protection obligations
- regular audits of data protection procedures and processes

3b) Outline of IT Infrastructure:

The Company is contracted to use the amenities of two IT service providers in delivering services to clients. Acteol Support Services Ltd provides a cloud based application that manages the delivery of clients marketing assignments. BrightCloud Technologies Ltd provides hosted hardware, network and general applications support (e.g. email and file structure), again in a cloud based environment. Both organisations use highly secure data centres.

The IT Security policies of both of the above organisations have been thoroughly reviewed and are considered to be within current legislative requirements. The storage and backups of data at both organisations are carried out to ISO27001:2013 accredited standards and the Directors of The Company therefore acknowledge that the procedures and facilities used in supporting CPB UK Ltd's business activities are clearly defined and robust.

Review meetings with Acteol Support Services Ltd and BrightCloud Technologies Ltd take place at 3 monthly intervals with IT and Data Security procedures being a permanent agenda item.

Information Security is regularly discussed at board meetings and the Directors of The Company foster a collective responsibility across all members of staff, not just the senior management team. From the induction programme for new recruits to regular departmental and company meetings, all staff are made aware of policy and encouraged to demonstrate a practical application of the key objectives throughout their daily duties.

3c) Information Management:

All staff have access to the servers housing the company's file structure, email, client reference and marketing automation system. Access levels are issued relevant to job roles. Client data is processed within separate databases for each client with security partitions between client data sets which are programmatically set for each new client created. The client data is sorted into the correct import format and input by the Campaign Delivery team. Where an assignment involves telemarketing, members of the Call Room team will be given access to data for assignments that they alone are allocated to. The Campaign Management team have access to all of their clients' databases as do the Systems Support team.

Passwords for this controlled access are renewed every 3 months and are maintained in a secure register by the Systems Director. Best practice with respect to client password administration is enforced through a minimum requirement for password strength.

3d) Breaches:

All staff are mandated to immediately notify the CPB Data Processing Officer and those Campaign Managers whose assignments are thought to be affected by any breach of security. The Data Processing Officer, or in his/her absence a nominated Company Director, will then validate the seriousness and potential impact of the breach. He/she will then immediately notify the client of any breach in security that has had, or is likely to have had, any illicit access to their data.

Should there also be obligations to notify any statutory authorities (i.e. Information Commissioner's Office), the Data Processing Officer, or in his/her absence a nominated Company Director, will report any breach in overall data security.

3e) Transfer of Data:

As noted in the introduction, data that is used and captured during marketing assignments will normally be exported to a CPB client at the end of an assignment. Such a transfer of data will be done using a Secure File Transfer Protocol method of delivery (i.e DropBox). Staff involved in the transfer of data will be instructed to adhere to this at all times.

Sales leads that are identified as part of a Prospecting assignment are held in a secure portal for clients to access on demand. This portal is housed on Acteol servers in a secure data centre environment, as referred to in 3b above.

4) Data Retention policy

CPB UK Ltd is a business-to-business (B2B) based marketing services agency and, as an integral part of our activity, we process personal information (referred to as "data" herein).
The management of the company is committed to a policy of compliance with the obligations of the EU General Data Protection Regulation 2016 (GDPR), across all data that is processed.
The data processed falls into five categories:

- Data processed on a client assignment within the Office file structure (Excel)
- Data processed on a client assignment within the campaign management system (Atreemo)
- Data held within CPB's customer and prospect management system (CRS)
- Data held within CPB's accounts system (Quickbooks)
- Staff data

Descriptions of these three categories are given below and the retention & archiving periods are shown on the table at the foot of this document.

4a) Data processed on a client assignment

Within Excel

- Targeted companies & contacts for assignments are typically received from clients in excel format (csv).
- Export of targeted companies & contacts upon assignment completion stored in csv format before onward transfer to client via secure SFTP (i.e. Dropbox)

Within Atreemo

Atreemo forms the hub of our assignment activity and the processing of data comprises of:

- Targeted companies & contacts imported from excel to an assignment database
- Sales lead reports produced on a designated Prospecting assignment are delivered to a client via a portal within Atreemo.

Contact lists and reports highlighted above are processed electronically and are not converted to printed copy by CPB.

4b) Data held within Client Reference System (CRS)

The CRS system is used for:

- Recording the details and parameters of client assignments
- Storing CPB client contact data
- Storing data of potential CPB clients

4c) Data held within Quickbooks

This system is used for invoicing and accounts reconciliation. There is data stored within Quickbooks, primarily purchase ledger contacts of our clients.

4d) Staff data

Data referring to current and past CPB employees is held in two areas:

- Personnel file. A manual, hard copy record of all HR related detail (i.e. application form, appraisals, next-of-kin, disciplinary issues, etc)
- The CRS system which is used for ready access to necessary contact information of current staff (i.e. telephone extension and mobile telephone number) and for the management of holiday entitlements

Data retention table

Data location	Retention period	Archive period
Excel – contact lists	2 years	+ 5 years
Atreemo – assignment database	2 years	+ 5 years
Atreemo – sales lead reports	3 years	+ 4 years
CRS – client data	2 years after trading	+ 4 years
CRS – prospective client data	2 years	deleted
Quickbooks	7 years	+ 3 years
Staff data - CRS	Whilst employed	+ 5 years
Staff data – Personnel file	Whilst employed	+ 7 years

All archiving above is done electronically to hosted, secure servers with the exception of Personnel files that are stored in a secure, off-site location.

Backups

Incremental and full backups of all data are carried out each day and are held for a period of one year in a hosted, off-site, secure location.