What is personal information?

Personal information is data that can be used to identify or contact a single person. You may be asked to provide (if required for the type of event you are booking with us) your personal information or your guests personal information any time you are in contact with Pure Communications Group. You are not required to provide the personal information that we have requested, but, if you choose not to do so, in many cases we will not be able to provide you with our products or services or respond to any queries you may have.

Here are some examples of the types of personal information Pure Communications Group may collect and how we may use it:

What personal data will Pure Communications Group collect from me?

When you consent to use Pure Communications Group services, contact us or complete an online form, we may collect a variety of information, including, but not limited to; your name, mailing address, telephone number, email address, credit/debit card or bank details.

How will we use your personal information?

The personal information we collect allows us to keep you informed and may include communication by post, telephone, SMS or email, about us and our content, products, services and events. If you wish to adjust what information we use or choose to opt out, you can do so at any time by contacting us on gdpr@purecommsgroup.com

The personal data we collect will be used to provide you with services specified in the booking form relating to your contracted event or for updates about Pure Communications Group.

From time to time, we may use your personal information to send important notices, such as communications about changes to our terms, conditions, and policies.

Pure Communications Group may securely transfer data inside and outside the United Kingdom and the EU, including for the purposes of your event.

When will Pure Communications Group contact me?

In relation to any service, activity or online content you have signed up for in order to ensure that Pure Communications Group can deliver services specified in the booking form and relating to your event.

In relation to any correspondence we receive from you or any comment or complaint you make about Pure Communications Group.

To keep you informed periodically on relevant products and services that we think may be of interest to you.

Types of communication include occasional newsletter updates If you wish to adjust what information we use or choose to opt out, you can do so at any time by contacting us on gdpr@purecommsgroup.com

How long will Pure Communications Group keep my personal data?

We retain your event related personal information as long as it is necessary and relevant for our operations but no longer than 30 days post event. After it is no longer necessary for us to retain your personal information, we dispose of the data in a secure manner.

In regards to marketing communications we will retain your information as long as it is relevant and you choose not to notify us in regards to removing your consent by unsubscribing to any Pure Communications Group communications.

Will Pure Communications Group share my personal information with anyone else?

At times Pure Communications Group may make certain personal information available to strategic suppliers that work with Pure Communications Group to provide products and services. Such as when we share your personal information with an airline in order to book your flight, hotel to book your accommodation, venues to provide conference or dining services. Pure Communications Group will never sell your Personal information or it will not be shared with third parties for their marketing purposes.

Does Pure Communications Group ever have to disclose my personal information?

It may be necessary − by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence − for Pure Communications Group to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate. We may also disclose information about you if we determine that disclosure is reasonably necessary to enforce our terms and conditions or protect our operations or users. Additionally, in the event of a reorganisation, merger, or sale we may transfer any and all personal information we collect to the relevant third party.

Can I find out what personal information Pure Communications Group holds about me?

You can help ensure that your contact information and preferences are accurate, complete, and up to date by informing us. For other personal information we hold, we will provide you with access for any purpose including; requesting we correct inaccurate data or deleting data if Pure Communications Group is not required to retain it by law or for legitimate business purposes.

Access, correction, or deletion requests can be made by contacting our Data Protection team on gdpr@purecommsgroup.com

Can I delete my data?

Yes, please contact our Data Protection team at gdpr@purecommsgroup.com

Will Pure Communications Group employees have access to my personal data?

To make sure your personal information is secure we communicate our privacy and security guidelines to all Pure Communications Group employees and strictly enforce privacy safeguards within the company.

How do I contact Pure Communications Group?

For any queries or comments about this privacy policy or updates, amendments and corrections to your records, or for personal information requests, please contact gdpr@purecommsgroup.com or by post to: Data Protection Team, Pure Communications Group, Alliance House, 12 Caxton Street, London, SW1H 0QS

If you wish to make a complaint about how we use your information, please contact our Data Protection team, in the first instance, and we will do our best to help. If you are still unhappy, you can contact the Information Commissioner's Office via their website: www.ico.org.uk

We will occasionally update this privacy policy. We will post a notice of any material changes on our website prior to implementing the changes, and, where appropriate, notify you using the contact details we hold for you for this purpose. We encourage you to periodically review this policy to be informed of how we use your information.

Data Security

As such we have tried and will continue to implement the most appropriate security options we can for our hardware.

Server

Our server is protected by our IT supplier's software and passwords which are not held on-site at Pure.

Server Backups Encrypted

Our server is backed up daily to encrypted hard drives which are taken off site in the event of a fire or catastrophic event at the office.

Laptops encrypted

All staff and on site laptops have encrypted hard drives requiring a primary login as well as a secondary password login.

Encrypted USB drives

We only use encrypted USB drives on site which work on fingerprint recognition.

Secure WeTransfer site

All files are sent via WeTransfer site and are individually password protected.

As part of the transfer, a password is applied to the "transfer" itself as well.

Mobile phones

Staff mobile phones use PIN or biometric log ins.

Staff mobile phones have no VPN access only Outlook functionality.

Personal laptops

Staff personal laptops have no remote VPN access to the Pure server and network.

Data Protection Officer (DPO)

Pure Communications Group does not have a Data Protection Officer but has nominated its CEO as the key person responsible for Data issues along with one of the Senior Event Managers.

Please note anyone wishing to contact or liaise with the Pure Data Team must do so via gdpr@purecommsgroup.com and not via any other email addresses for the individuals.

Data Breaches and Notification

A Data Protection breach is the result of an event or series of events where Personally Identifiable Information (PII) Personal Data is exposed to unauthorised or inappropriate processing that result in its security being compromised. The extent of damage or potential damage caused will be determined by the volume, sensitivity and exposure of the PII.

Breach management is concerned with detecting, reporting and containing incidents with the intention of implementing further controls to prevent the recurrence of the event.

The key actions in a breach scenario are to:

- Notify Senior Management and/or the company DPO or nominated person
- Create a full report on what happened

In the event of a breach the Data Owner should immediately notify Senior Management and log the breach in the Personal Data Incident Log excel document located on the server.

- Once In the Personal Data Incident Log - assign a Breach number and complete the basic fields in the document.
- Then, make a copy of the Folder named “PDB_[Breach Reference Number]” and rename it with the assigned breach reference number.
- Then open the Word file “PURE COMMUNICATIONS GROUP Data Breach Report_Template” and make a copy and rename the copied file with word “template” replaced with the Breach Number.
- Then read and complete all the relevant fields with as much detail and information as possible in the renamed Data Breach Report Document.
- Save the completed and renamed Data Breach Report and all other relevant files and emails into the renamed Breach Number Folder.
- Let Senior Management know as soon as this is complete – ideally within 24hr of discovering the breach.

Staff Training

All employees of Pure Communications Group are required to understand our data protection policies and procedures as part of their induction process. All staff undergo updates and reminders at least annually.