THE BUREAU

Privacy policy

May 2018

At The Bureau we are committed to being transparent about the data we hold and how we work with that data. When dealing with personal data we are guided by the eight rights of individuals as laid out in the GDPR legislation.

Access to personal data
Requests for copies of any personal data that we hold, as well as requests for deletion of personal data, should be made by email to admin@thebureaulondon.com. We commit to responding within five working days.

Data breaches
If we discover a data breach on any of our systems, we will conduct an impact assessment and communicate this to any affected clients within 24 hours.

Subcontracting services
We subcontract software services such as cloud storage, email, hosting infrastructure and project management to third parties. All of our suppliers have committed to meeting the requirements of the GDPR legislation.

Project data
We store a shared set of client project files such as contracts, information architecture documents and design files with a major cloud storage provider whose servers are in the US and who adheres to the EU-US Privacy Shield. All files stored are encrypted and we require all our staff and subcontractors to activate two-factor authentication before accessing this service. We do not store any personal data of our clients' users - such as website account details - on this service. This service stores 30 days of versions for our files. Files are retained until they are deleted.

Email
We conduct project correspondence via email using a major US-based provider with servers worldwide who adheres to the EU-US privacy shield agreement. We require all staff and subcontractors to enable two-factor authentication on their accounts. Emails are kept until they are deleted.

Hosting
We use two major hosting infrastructure providers, one for live sites and another for backups and static sites. We only commission servers physically located in Ireland from both of these providers. Live sites contain the vast majority of the personal data that we store in the form of website accounts. All website accounts are password protected, and access permissions to sensitive functionality such as listing user accounts is tightly controlled. We activate two-factor authentication on all account dashboards with our hosting providers and live servers are only accessible using SSH key-based authentication. Files are kept until they are deleted. Live site backups are kept for 30 days.

Project management
We use a number services for project management. The only personal data these services keep are user accounts and on the services where our clients have user accounts they have full control of their own data.

Hardware
We store every kind of data mentioned above on our computers, the hard drives of which are encrypted using Apple's FileVault 2. If a device is lost or stolen we have the ability to remotely wipe the hard drive. We have encrypted Time Machine backups of our hard drives. Files on the hard drive are stored until they are deleted, and backup versions are stored until the backup disk is full.

We store contact details of our clients and our emails on our phones. Data is encrypted on our phones and is protected with passcodes and biometric fingerprint data. We can also remotely wipe any lost or stolen phones.

Staff members are required to immediately report lost or stolen hardware and potential unauthorised access to that hardware. In each case we will conduct an impact assessment and communicate this to any affected clients within 24 hours.

End of contract arrangements
If our relationship with a client ends, we will add all project files, emails and hosting files to an archive file. This archive will be retained for a minimum of six years to reflect time limits in legal cases.