Privacy Policy

ThenMedia understands and appreciates the requirements of GDPR 2018. It stores personal data securely and treats it with respect at all times.

Personal data

ThenMedia stores personal data of staff, customers, suppliers and contacts.

Its legal basis for doing so is 'legitimate interest'.

It stores the data in order to efficiently deliver its services and provide support to its customers.

Personal data can include title, name, gender, postal address, phone numbers and email addresses.

ThenMedia makes every effort to maintain the accuracy of its personal records.

Access to the personal data is restricted to ThenMedia staff.

ThenMedia doesn't pass on any personal data to any third party.

Anyone wishing to view what ThenMedia is storing about them should make a data access request by emailing: data@thenmedia.co.uk.

Data storage

ThenMedia stores its data (including its own personal data and the personal data of its customers) using it's own web-based software.

This software runs on a bespoke version of Linux, with MariaDB and PHP/Javascript for storage and retrieval.

ThenMedia servers are protected by industrial strength firewalls and access to commonly exploited ports is restricted to ThenMedia office IPs.

ThenMedia servers are hosted securely at a GCP Data Centre in London.

ThenMedia servers are regularly backed-up at two offsite locations in Cheshire.

Cookies

ThenMedia hosts websites for itself and its customers. It uses cookies on these sites. Non-interactive sites (where a user is simply a visitor) use persistent cookies to monitor usage and so provide statistics on visits and pages viewed. This is achieved using Google Analytics. See https://www.google.com/analytics/terms/us.html for relevant terms and policies.

Interactive sites (where a user can sign-in) use session cookies to monitor the interaction and deliver data to the user without repeated requests for authorisation. Further information detailing how we store your data is included in our Data Security Policy below.

Data security

This document explains how and where your data is stored when you use ThenMedia Cloud, or a ThenMedia product such as Loudhailer or Chrestos. The information detailed in this document also applies to any bespoke project created by ThenMedia which uses our cloud system at its core. ThenMedia Limited operates a number of virtual & physical servers located at a data-centre in London. Our core cloud server features redundant power supplies along with battery

backup and a generator. The hardware itself is located in a secure facility with access closely monitored and strictly controlled. The servers we operate are owned and managed by ThenMedia Limited. No third party companies or organisations have access to our systems. However, it is sometimes necessary for independent data- centre engineers to be given temporary access to perform upgrades or essential maintenance.

Data protection

Our infrastructure is protected by industrial strength firewalls, with access to commonly exploited ports such as FTP (21) and SSH (22) restricted to ThenMedia's static IP addresses. All cloud data is managed using MariaDB and accessed via a CMS (content management system) developed by ThenMedia using an NGINX/PHP architecture. This infrastructure runs on a customised installation of Linux, chosen for its security, reliability and speed.

Data capture & storage

Captured data is stored using MariaDB and transmitted securely via 256 bit SSL. All our security certificates are independently A-rated by Qualys. They feature super-strong ciphers and 4096bit Diffie-Hellman keys for enhanced security.

By default, uploaded customer data is restricted to everyone except the cloud administrator. The cloud administrator will be allocated as your contract is finalised. Once allocated, this user can sign into our cloud using an encrypted password. They are then free to create additional users and grant permissions as required. ThenMedia cannot read any passwords, although we can reset them if required.

Once stored, all customer data is backed up securely at two independent locations. Backups are held in accordance with our GDPR policy (above), and are stored on NAS devices using RAID (redundant array of independent disks).

We take every care to ensure that your data is stored safely and securely. However, ThenMedia accepts no liability for any losses incurred through loss of data. Please make sure you keep local backups of all data you upload to our servers.

Access to customer data is logged and irregular sign-in requests are reported. Multiple incorrect attempts to access data will result in an IP block.

For more information on how we manage and protect your data, please email data@thenmedia.co.uk or alternatively phone 01244 478727.

PCI Compliance

Anyone involved with the processing, transmission, or storage of card data must comply with the Payment Card Industry Data Security Standards (PCI DSS). This is why ThenMedia uses Stripe's embeddable card-payment system, Stripe Checkout, to enable our clients to accept card payments on their website.

The simplest way to be PCI compliant is to never see (or have access to) card data at all. Stripe makes this easy as they do the heavy lifting to protect customers' card information. By using Stripe Checkout, payment information is securely transmitted directly to Stripe without it passing through our servers.

Stripe has been audited by a PCI-certified auditor and is certified to PCI Service Provider Level 1. This is the most stringent level of certification available in the payments industry. To accomplish this, Stripe use the best-in-class security tools and practices to maintain a high level of security at Stripe.