Mobunti Limited

GDPR COMPLIANCE

1st May 2018

Compliance Statement

The EU General Data Protection Regulation ("GDPR") comes into force across the European Union on 25th May 2018 and introduces the biggest change to data protection law in over 2 decades. The regulation provides a framework across Europe (including the UK after we leave Europe) to ensure that the same regulations exist in every European country and puts privacy of data, front and centre in an organisation

We have been registered under the data protection act since 2004 and have always taken a privacy based approach in our business dealings.

Mobunti Ltd is dedicated to safeguarding the personal information we hold. Our preparation for compliance is explained here

Information Audit

Analysing where we get data from, what we do with it, why it is processed and where it is stored, along with who it is shared with. Then confirming the location of any third party providers we use that process or store the data to confirm where they are and whether they are compliant with GDPR

Policies and Procedures

Updating our Privacy Notice and our cookie policy

Review Existing Data

We have reviewed our customers and prospects lists and where users are deemed to be unlikely to purchase again, we have removed their user accounts from our system, ensuring that we only hold access details for customers who have visited in the last 12 months or who are regular customers. Customers who have previously ordered who no longer hold user account records after the data review, now only have data in our accounts system under our legal obligations. We then got in touch with the customers who kept an account on our system to give them the opportunity to request that their account be removed if they felt it was no longer needed

1st May 2018

Reviewing existing email marketing procedures

As a general rule we do not carry out much email marketing, but after reviewing the customer and prospect lists, we then contacted each one to advise of the update in the privacy notice and to get a re-opt in to any marketing lists we do hold. We hold records of who has opted in to marketing requests and when they opted in, and who has opted out and when they opted out. Marketing via email is the only area of business where we rely on consent for the legal grounds of processing.

Data Transfers

We have reviewed where our data is stored and with whom it is shared and have ensured that all third parties are either within the EEA and so subject to GDPR or are within USA under the US-EU Privacy Shield. We do not transfer data, whether it holds personally identifiable data or not, outside of these 2 areas. Our primary off site storage/database services are European based Google Cloud Servers and European based (EEA) offsite backup servers.

Data Transfer Process

When data is transferred, either through a programming API or as part of a backup process, the data is transferred either securely through an ssh tunnel or, if over a web based protocol, data is transferred only when a SSL/TLS (https) certificate is in use to ensure end to end encryption is in place

Processor Agreements

Where we use third party services, such as accountants or other data processing services, we have prepared compliant Processor Agreements to ensure that they meet and understand their GDPR obligations

Special Categories Data

We have identified that we do not request, store or process any special categories data

1st May 2018

Review of Staff Access

We have reviewed staff access and confirm that as has been the case anyway, only people who have a need to see your personal data have that ability.

Privacy Notice

This document should be read in conjunction with our updated Privacy Notice

Subject Access Requests and Right of Erasure/Removal

Mobunti Limited fully complies with your rights for us to remove your data from our system, subject to any legal requirements that we may have - primarily relating to either accounting data or Money Laundering Regulations. You may email support@mobunti.co.uk to make this request

Data Retention

Mobunti Limited periodically reviews registered user accounts and if it sees there has been little or no access since registration, will contact you (under legitimate interest legal basis) to ask if you want your account removed. The email may remind you of the services we provide in case you had forgotten you registered with us, but it's aim will primarily be for data retention/removal purposes. If we get no response after 4 weeks, we reserve the right to remove your account from our system.

Network Security

Office machines are protected by a hardware firewall to protect from direct access from the internet. The office primarily uses Linux servers, workstations and laptops, but where Microsoft products are used, it is Windows 10. It is prohibited for any machine to have an operating system on that is not supported with security updates. All machines are protected by antivirus software and software based firewalls and all available patches and updates are applied as soon as they are available. All machines, whether server, desktop, laptop, mobile or tablet require password access (with automated screen lock after a period of inactivity) and mobiles have remote wipe facilities on them.

1st May 2018

Our internet servers are based at the Next Generation Data centre in Newport, Wales, and it is the largest data centre in Europe with access security meeting the government's highest standards. The servers are managed by a security focused team based nearby to the centre in Cardiff, who apply all available patches and configure the equipment with security at the forefront at all times. Any brute force attempt at a login prevents access to that IP address for 24 hours within seconds of the attempt. Any SSH access to the server requires locally stored security keys. It is not possible to login over SSH with just a username and password. All databases on the server require administrative password access. Backups of website data are taken daily and are rotated weekly.

Our systems are scanned daily for viruses and malware and we use secure cloud based email services to prevent zero day malware having access to local mail accounts

Office Backups

Backups of the main server in the office are taken every hour to an on-site storage facility and via an ssh public/private key pair to a backup server located within the EEA, also every hour. Local office based backups are kept for a 2 month period and off site backups are kept for 1 month.

Telephony Security

When liaising with a customer on the telephone, if the request relates to anything to do with a user's account, we will confirm your identity before allowing the call to continue. This will usually involve us checking the history of the account and asking questions that the account holder would know relating to what had been previously purchased for example, in combination with the usual confirmation of name and comparing the incoming caller ID details with the account. If we have any concerns, we would call the phone number we have on the account and ask to speak with the person who has just called in.

1st May 2018

Office Security

The office is accessed by one of two key holders. Paper documents with customer information are kept in customer/supplier folders in a locked filing cabinet, however much of our customer communication is electronic and so any electronic documents are stored within Google's GSuite services which are under the US-EU Privacy Shield.

Software

Mobunti Limited only uses fully licenced up to date software, or uses cloud based products, ensuring all applicable updates are applied to help prevent software exploits. Our website, including the company formation service is controlled using bespoke, custom written software. The software is primarily written in PHP, using the latest available version (7.2 at the time of writing) with all security patches applied. We do not use open source Wordpress websites or anything where the source code is easily viewable to exploit the software