mobile mini
Secure Container & Site Accommodation Hire

Mobile Mini UK Ltd.
Privacy Policy

Spring 2018

Contents

Mobile Mini UK Ltd.
Data Protection Policy

Context & Overview

Key Details

- Policy Prepared on: April 25, 2018
- Approved by the board and management team on: May 25, 2018
- Policy operational on: May 25, 2018
- Next review date: May 25, 2019

Introduction

Mobile Mini UK Ltd. ("Mobile Mini UK") respects the privacy rights of individuals and is committed to handling Personal Data responsibly, in accordance with applicable law and Mobile Mini UK's commitment to the protection of Personal Data is described below. Our policy sets forth Mobile Mini UK's principles for the treatment of Personal Data subject to the General Data Protection Regulation ("GDPR") and related data protection legislation.

Our policy also establishes the legal basis for cross-border transfers of Personal Data within the Mobile Mini Group. Moving forward, the Mobile Mini will be adopting Privacy Shield Certification. Additionally, Mobile Mini UK may carry out onward transfers of Personal Data to third parties outside the Mobile Mini Group in accordance with applicable law. Mobile Mini will handle Personal Data in accordance with this policy where applicable, unless in conflict with stricter requirements of local law, in which case local law will prevail.

Why this policy exists

This data protection policy ensures Mobile Mini UK:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers, and partners
- Is open and transparent about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

On May 25, 2018, the European Union's General Data Protection Law ("GDPR") comes into effect. The GDPR applies to any company that offers goods or service to data subjects ("natural persons") located within the European Union. The regulation dictates that individuals (a/k/a: "data subjects") have the right of privacy. The regulation affords European-based data subjects with various rights. This includes: The right to erasure (the "right to be forgotten"), the right to know how their information is processed, and the right of access to their personal data. The GDPR provides penalties for failing to comply and can be as high as 4% of the company's worldwide gross revenue. These rules apply regardless of whether data is stored electronically, on recorded devices, or on paper. To comply with the law, Personal Data must be collected and used fairly, transparently, and stored safety. In addition, it may not be disclosed unlawfully.

GDPR Accountability Principles

The GDPR is underpinned by six key accountability principals:

- Data must be processed and utilized fairly, transparently, and lawfully.
- Data must be obtained only for a specific, explicit, and legitimate purpose and not further processed in a manner that is incompatible with those purposes.
- Data collection must be relevant and not excessive.
- Data must be accurate and kept up to date. Inaccurate information is to be erased or rectified without delay.
- Data must not be retained for any longer than necessary.
- Data must be processed in a manner that ensures security including: unauthorized or unlawful processing, accidental loss, destruction, damage, or using appropriate technological or organizational measures.

The Purpose of the Processing

Information about Mobile Mini UK. purchases are maintained in association with an individual profile account. The Personal Data Mobile Mini UK collects from data subjects is stored in one or more databases hosted by third parties located in the United States. These third parties do not use or have access to a data subject's Personal Data for any purpose other than cloud storage and retrieval. On occasion, Mobile Mini UK engages third parties to obtain publicly available information for the purposes of targeted marketing campaigns. This information is cross checked externally and internally to ensure the collected data is not subject to: (1) individual do not call registers, (2) corporate do not call registers, and (3) internal do not call suppression lists.

Mobile Mini UK observes the following principles when processing Personal Data:

Fairness: Mobile Mini UK will process Personal Data fairly and lawfully.

Purpose: Mobile Mini UK will limit the processing of Personal Data to the fulfillment of Mobile Mini UK's specific, legitimate purposes. Mobile Mini UK will only carry out processing that is compatible with such purposes unless Mobile Mini UK has the unambiguous consent of the individual to process the data for unrelated purposes.

Proportionality: Mobile Mini UK limits the processing of Personal Data to that which is adequate, relevant and not excessive in relation to the purposes for which Mobile Mini collects and uses it. Further, Mobile Mini UK will make reasonable efforts to limit Personal Data to the minimum necessary for these purposes.

Information Quality: Mobile Mini UK will take reasonable steps to ensure that Personal Data is accurate and kept up to date, to keep Personal Data only for as long as necessary for the purposes for which it is collected and used, and to delete or to render it anonymous after such retention requirements have been met.

Transparency: Where required by applicable law, Mobile Mini UK will make available to individuals at the point of collection, or within a reasonable period of collection, information about Mobile Mini UK's identity; the purposes and nature of processing their Personal Data; intended recipients and cross border data transfers; source(s) of Personal Data; how individuals may exercise their rights regarding Personal Data; and additional explanations as needed to ensure fair processing. Where Mobile Mini UK collects Personal Data through the Internet or other electronic means, Mobile Mini UK will post an easily accessible privacy notice with these elements.

Confidentiality: Mobile Mini UK will maintain the confidentiality of Personal Data it processes, except where disclosure is required by an applicable operational or legal requirement. This obligation will continue even after the relationship with the individual has ended.

Security: Mobile Mini UK strives to Protect Information with appropriate technical and organizational measures to ensure its integrity, security, availability, and resilience.

Legitimate Basis for Processing Personal Data: Mobile Mini UK processes personal data for legitimate business purposes, to comply with a contract or legal obligation, or with the explicit "opt-in" consent of the data subject. Mobile Mini UK considers the rights of the data subject and ensures the nature, scope, context, and purposes of processing align with the General Data Protection Regulation.

People, Risks, & Responsibilities

Policy Scope

This policy applies to:

- The head office of Mobile Mini UK.
- All branches of Mobile Mini UK
- All staff of Mobile Mini UK
- All contractors, suppliers, and third-party vendors working on behalf of Mobile Mini UK
- It applies to all data that the company holds relating to identifiable individuals.

The Data We Collect

We make every attempt to minimize the scope and nature of the data we collect. However, there will be times when, during the regular course of business, we are required to keep the following types of personal data.

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Financial information
- Emergency Contact Information
- Photos used for employee access badges
- Medical Information (for employment benefit processing)
- IP addresses

Data Protection Risks

This policy is designed to protect Mobile Mini UK from some very real data security risks, including:

- **Breaches of Confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer Choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Data Privacy Team Responsibilities

Everyone who works for or on behalf of Mobile Mini UK has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that personal data is handled and processed in line with this policy and data protection principles. Failure to do so is grounds for discipline.

The **board of directors** of Mobile Mini UK is ultimately responsible for ensuring that Mobile Mini UK. meets its legal obligations.

The appointed **interdisciplinary data privacy team, comprised of global directors from HR, IT, Legal, and Marketing** is responsible for the following (some of which may be delegated to UK management):

- Keeping the Board updated about data protection responsibilities, risks, and issues.
- Reviewing all data protection procedures and related polices, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Mobile Mini UK holds about them. (Also called “Data Subject Access Requests”)
- Reviewing and approving material contracts or agreements with third parties that may handle the company’s sensitive data.
- Regularly reviewing and updating the company’s Records of Processing Activities
- Overseeing third party call list reviews.

The **US and UK IT manager(s)** is/are responsible for:

- Ensuring all systems, services and equipment used for storing data meet company-adopted security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.

- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

The **US and UK Marketing Manager(s)** is/are responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalist or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by the company's adopted data protection principles. This includes regularly reviewing internal systems responsible for reviewing third party call lists against individual do not call registers, corporate do not call registers, and internal suppressed user lists.
- In the event of a data breach, the marketing manager will support the board of directors and senior management as requested in developing an appropriate crisis communication plan and strategy.

The **Chief Legal Officer** is responsible for:

- Final approval of data subject access requests.
- Ensuring that jurisdictional data privacy regulations are being followed.
- Ensuring that cross-border transfer mechanisms are in place.
- Assisting auditors in the event of regulatory audit.
- Ensuring the vendor risk management program is monitored.
- Ensuring Processor and Controller contracts have been reviewed and where necessary, amended to reflect GDPR principles.

The data privacy team may be reached at:

dataprivacyteam@mobilemini.com

General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work.**
- Protected data **should not be shared without a business purpose**. When access to confidential information is required, employees can request it from their line managers.
- Employees should **keep all data secure** by taking sensible precautions and following guidelines below.
- Passwords should never be shared or displayed in your workspace area.
- Personal **data should not be disclosed** to unauthorized people.
- Employees **should request help** from their manager or the data protection officer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where protected personal data should be safely stored. When we say "data" below, we mean protected data under the GDPR guidelines. Questions about storing data safety can be directed to the IT manager or members of the data privacy team.

- When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it should be protected from unauthorized access, accidental deletion and malicious hacking attempts.
- Passwords should not be shared between employees.

- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should not be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Accuracy

The law requires Mobile Mini UK to take reasonable steps to ensure data is kept accurate and up to date.

- It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
- Data should be held in as few places as necessary.
- Mobile Mini UK will endeavor to make it easy for data subjects to update the information Mobile Mini UK holds about them.
- Data should be updated as inaccuracies are discovered.
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Data Subject Access Requests

All UK and EU individuals who are the subject of personal data held by Mobile Mini UK are entitled to:

- Ask what information the company holds about them and why (purpose and categories of personal data.)
- Ask how the company obtained the data and with whom it has shared the data with
- Ask how the data is stored and secured
- Ask how long the data is retained
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

If some individual contacts Mobile Mini UK requesting this information, the individual has triggered a 'Data Subject Access Request'. Data Subject Access Requests from individuals should be made by email, addressed to the data controller at the following email address: datasubjectaccessrequest@mobilemini.com.

In addition, they may contact our data privacy team at the following address:

Email: DataPrivacy@MobileMini.com

Mobile Mini can supply a standard request form, although individuals do not have to use this. Mobile Mini UK will aim to provide the relevant data in an easy to read format without undue delay. A Data Subject Request shall be processed within thirty days from the time of receipt. Please note, Mobile Mini UK will always verify the identity of anyone making a data subject request before records are released. If the identity of the person requesting the Data Subject Access Request cannot be validated, the information will not be released.

Disclosing Data & Sharing Personal Data to Third Parties

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without consent of the data subject. Under these circumstances, Mobile Mini UK will disclose requested data. However, Mobile Mini UK will attempt to ensure the request is legitimate, seeking assistance from the Board and from the company's legal advisers where necessary. Under the Privacy Shield Principles, Mobile Mini may be liable in the

event that a service provider to whom Mobile Mini transfers personal data uses such personal data in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage. An individual with an inquiry or complaint may contact us using the mailing or email address below:

datasubjectaccessrequest@mobilemini.com

In addition, Mobile Mini UK may share or transfer Personal Data in the following circumstances:

- Personal Data may be shared within the Mobile Mini Group for the purposes specified above, provided the Mobile Mini entity processing Personal Data adheres to the policy standards.
- Mobile Mini UK may transfer Personal Data to third parties hired to perform services on Mobile Mini UK's behalf, subject to applicable law. For example, a pre-employment screening company hired to perform a drug screening test may obtain your name and contact information for the purposes of conducting a drug screening test. The third parties will have access to Personal Data solely for the purposes of performing the specified services and may transfer Personal Data globally in accordance with the principles specified in this Policy and with Mobile Mini UK's instructions, including an applicable data transfer mechanism. Mobile Mini will select reliable third parties and will strive to ensure that new supplier engagements provide for processing and security of Personal Data in accordance with this privacy policy and applicable law.
- Mobile Mini UK may disclose Personal Data to credit reference agencies (e.g., Experian) for purposes including, but not limited to, assessing creditworthiness, checking your identity, managing your account, tracing and recovering debts, preventing criminal activity, settling accounts and notifying when debts are not paid on time. Credit reference agencies may use and share your data with other third-party organizations. For information on the ways credit reference agencies use and share Personal Data, please visit their websites.
- Mobile Mini UK may disclose Personal Data to other third parties where required by law, to protect Mobile Mini UK's legal rights, or in an emergency where the health or security of any person is endangered.

Processing of Sensitive Personal Data

Where Mobile Mini UK processes and/or transfers Special Personal Data, Mobile Mini UK will conform to all applicable data privacy regulations

Privacy Program

Mobile Mini UK employee privacy practices are designed to support its compliance with this policy and applicable law, including privacy policies, education and awareness programs, incident response protocols, privacy impact assessments, and audits.

Individual Rights

Mobile Mini UK aims to ensure that individuals are aware as required by applicable law that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, an individual who has satisfactorily established his or her identity to Mobile Mini UK may exercise the following rights in relation to Personal Data Mobile Mini holds about him or her:

Access: Where required by local law, Mobile Mini UK will provide an individual Personal Data about him or her that Mobile Mini UK holds, including information concerning the source of the Personal Data, the purposes of any processing by Mobile Mini UK and the recipients, or categories of recipients, to whom such Personal Data is disclosed.

Correction and Deletion: Valid request for correction or deletion of Personal Data which is incomplete, inaccurate or excessive will be respected, except that deletion will not be performed where retention is required by the contractual relationship between Mobile Mini UK and the individual, in the context of a legal dispute or other legal retention requirement, or as otherwise required by law.

Complaints: Any individual who claims to have suffered damage because of non-compliance by a Mobile Mini, Inc. entity, including when committed by a Mobile Mini entity located outside the European Union or the United Kingdom, may file a complaint with the applicable Mobile Mini Privacy Leader or Compliance Officer, or with the Mobile Mini Complaint Handling Process available on Mobile Mini websites if other channels are unavailable or exhausted.

External and Internal Concern Reporting: datasubjectaccessrequest@mobilemini.com

Enforcement: An individual who has suffered damage because of an unlawful processing operation or a breach of applicable privacy law or of this policy, may have rights under the law an individual may seek to enforce his or her rights under applicable law by direct recourse to the courts or other judicial authority in the jurisdiction of the Mobile Mini UK entity exporting Personal Data or administratively before a competent Data Protection Authority. Where permitted under local law, Mobile Mini UK may specify alternative mechanisms for resolving disputes. Individuals also may be able to invoke binding arbitration, under certain circumstances where permitted by the Privacy Shield program, if the individual believes there has been a violation of Privacy Shield requirements that has not been appropriately addressed by Mobile Mini.

Cooperation with Supervisory Authorities: Mobile Mini UK will cooperate with any regulatory authority responsible for supervising applicable data protection laws that has good cause to question any processing of Personal Data by Mobile Mini UK and will comply with their legally binding decisions on issues related to this Policy. Mobile Mini also may be required to disclose personal data in response to lawful requests by public authorities, including disclosures to meet national security or law enforcement requirements. Mobile Mini's disclosure of personal data to third parties is governed by the Notice and Choice Principles described above, and, for the purpose of providing consumer reports to third parties, Mobile Mini complies with FCRA requirements.

Changes to the Policy

Mobile Mini UK reserves the right to modify this Policy at any time. Once adopted, changes will be promptly posted on Mobile Mini UK websites.

Mobile Mini Cookies Policy

In the European Union, cookies are, at present, governed by the E-Privacy Directive, Directive 2002/58/EC, as amended by Directive 2009/136/EC. The E-Privacy Directive (or EPD) is set to be replaced by the E-Privacy Regulation[1] (or EPR) sometime in 2018, with enforcement likely to begin in 2019.

A cookie is a piece of information contained in a very small text file that is stored in your internet browser or elsewhere on your hard drive. Cookies allow a website to identity a user's device whenever that user returns to the website and are commonly leveraged to make websites function more efficiently and enrich the user experience, as well as to provide information to the owners of the site.

Mobile Mini's use of cookies

Mobile Mini collects information during a data subject's visit to the Mobile Mini website using cookies. We use these cookies for a variety of reasons, most commonly to distinguish the data subject from other users of our

[1] *See* https://iapp.org/media/pdf/resource_center/ePriv-reg_03-2018.pdf.

websites and help compile aggregate statistics about usage of our websites. We also use cookies to help us provide data subjects with a positive experience when browsing our website, to improve our content, and to personalize a data subject's visit.

Main Mobile Mini Cookies

Mobile Mini may use the following cookies. From time to time, this list may modify or be updated. We will update the list accordingly.

1. **Analytics Cookies.** These cookies are used to estimate our audience, identify usage patterns, and speed up searches.
2. **Session Cookies.** These cookies are used to maintain your transactions. Generally, your session cookies expire when your browser is closed. The use of the session cookies reduces the need for Mobile Mini to transfer your information over the internet.
3. **Functional Cookies.** These cookies are used to recognize repeat visitors to the site and allow the website to remember the choices you make (such as user name, language or the region you are in.) They are often used to record specific browsing information (including the way a data subject arrived at the site, the page you view, and options you select:
    a. **Country Preference Cookies.** Used to record your country preference.
    b. **Language Preference Cookies.** Used to record your preferred language.
    c. **Consent Management System Cookies.** Denotes the way the site is being viewed.
    d. **Authentication Management Cookies.** Contains your authentication ticket information.
4. **Tracking Cookies.** From time to time, we may leverage the relationships of carefully selected and monitored partners to assist in the delivery of a quality website. Some of those partners may set cookies during your visit to track the performance of marketing campaigns and/or meet contractual obligations with Mobile Mini. While these cookies do not store personal details relating to you, we do not have access or control over the cookies and similar technologies that our partners use.

Mobile Mini's Use of Web Beacons

Mobile Mini may also use tracking technologies called web beacons to collect information about your visit to Mobile Mini sites. These are small images embedded in web content and HTML-formatted email messages and are ordinarily not visible to users. Like cookies, this technology enables us to track pages and content accessed and viewed by users on Mobile Mini sites. Also, when we send HTML-formatted (as oppose to plain text) emails to our users, this technology may be embedded in such emails. Using web beacons allows us to determine whether emails have been opened or links were accessed, and identify aggregate trends, individual usage, and generate statistics about how our site is used. This enables Mobile Mini to provide our users with more relevant content and additional information about our services.

Web beacons are often used in combination with cookies; however, unlike cookies, web beacons cannot be declined when delivered via a regular web page. However, they can be refused when delivered via email. If you do not wish to receive this technology via email, configure your email software to disable HTML images or refuse HTML emails (selecting the option for text only viewing). Setting your browser to decline cookies or to prompt you for an opt in response before cookies are set will also reduce web beacons functionality.

Data Storage and Retention Policy

Like most corporate entities, Mobile Mini stores personal data in various locations. This may include: our own servers, third party servicers, email accounts, desktops, employee owned devices, backup storage, and/or paper files.

Mobile Mini UK's data retention periods can differ based on the type of data processed, the purpose of processing, and other factors. For example, whether any legal requirements apply for the retention of data. (i.e.: trade law, tax law, employment law, administrative law, or regulations regarding certain professions.)

In the absence of any legal requirement, personal data should only be retained if necessary for the intended processing.

From time to time Mobile Mini may leverage publicly available call and e-mail lists for direct marketing purposes. In keeping with e-Privacy regulations, Mobile Mini verifies publicly available call and e-mail lists against local do not call registers. In accordance with law, we complete this practice every six months.

Privacy Shield Statement

Mobile Mini, Inc. is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC). Mobile Mini, Inc. complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Mobile Mini, Inc. has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

In compliance with the Privacy Shield Principles, Mobile Mini, Inc. commits to resolve complaints about our collection or use of your personal information. EU individuals with inquiries or complaints regarding our Privacy Shield policy should first contact our data privacy team at: DataPrivacy@MobileMini.com.
To initiate a data subject access request, please email our data subject access request team at: datasubjectaccessrequest@mobilemini.com.

Mobile Mini, Inc., has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints concerning data transferred from the EU.