Data Protection Policy Statement

Reference: GDPR DOC 1.0

Issue No: 1

Issue Date: 15-05-18

Author: Alex Patrick-Smith

Content

Statement of Policy

Hinton Perry & Davenhill Ltd (the Company) is committed to full compliance with the requirements of the General Data Protection Regulation (GDPR). The Company comprises Dreadnought Tiles and Ketley Brick and the policy applies to the data collected for both entities. The GDPR and this policy apply to all of Hinton Perry & Davenhill Ltd's personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

Hinton Perry & Davenhill Ltd regards the lawful and appropriate treatment of personal information as very important to its successful operations and essential to maintaining confidence between the company and those with whom it carries out business. The Company therefore fully endorses and adheres to the Principles of the General Data Protection Regulation.

All data users who have access to any personal data held by or on behalf of the company are made fully aware of and are required to abide by their duties under the General Data Protection Regulation.

The Company needs to collect and use information about people with whom it works in order to operate and carry out its functions. In addition, the company may be required by law to collect and use information in order to comply with the requirements of government legislation. This personal information must be handled and dealt with properly however it is collected, recorded and used and whether it is on paper, in computer records or recorded by other means.

Following an audit for each type of personal data received, the Company has identified a lawful basis for holding or processing this information and determined what purposes personal information held, will be used for. The Company is registered with the Information Commission and has notified the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

Data collected by the Company shall be obtained and held for a defined purpose with an established lawful basis and shall not be processed in any manner incompatible with that purpose or those purposes. The data collected shall be necessary and proportionate in relation to those purposes.

Data collected shall be accurate and, where necessary, kept up to date and shall not be kept for longer than is necessary.

The lawful bases for collecting, holding and using data shall be either, Consent, Contract, Legal Obligation, Vital Interest, Public Task or Legitimate interest.

The Company understands 'consent' to mean that it has been explicitly and freely given and understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement. It is further understood that consent can be withdraw at any time. There must be some active communication between the parties to demonstrate active consent. In most instances, consent to process personal and sensitive data is obtained through standard documents such as when a new client places an order, agrees a contract, or when enquiries or requests for samples or information are received by the Company by prospective clients. For employees of the Company consent to hold personal data shall be obtained through signed consent forms.

All data handled by the Company shall be kept with appropriate technical and security measures to safeguard the information. Data that is no longer needed shall be destroyed securely.

Privacy Policy - How personal data is collected and used

The Company shall strive to collect and process only the data or information which is needed and only use personal data for such purposes as are described at the point of collection, or for purposes which are legally permitted and shall not keep information for longer than is necessary.

Employees

Personal data is collected on the company's employees, such data shall be held on the lawful basis of consent during their employment and once employment has ceased relevant information on their employment shall be retained on the basis of legitimate interest, for any legal requirements that may be necessary such as the defence on any claims brought against the Company. Data no longer required such as bank details shall be deleted within 12 months following the end of employment. Personal data on employees shall not be provided to 3rd parties except for legitimate requests from law enforcement bodies.

Customers and Potential Customers

Personal data collected on the company's customers and potential customers through enquiries by email, websites, trade shows and telephone calls, shall be on the basis of legitimate interest and used to service their enquiries and orders and shall be retained securely on the Company's data management system Microsoft Navision and email system. Paper records shall be kept securely on the Company's premises. Personal data such as email and addresses provided may be used for marketing purposes.

Details of orders placed with the Company including site details shall be retained for the anticipated life of the products supplied to ensure traceability and information is available for any potential performance related issues. In certain circumstances site addresses will be provided to 3rd parties where the site can be viewed without interfering with the privacy of the occupiers. Site addresses where privacy may be impacted will only be provided to 3rd parties with the consent of the occupiers. Personal data collected on the Company's customers and potential customers shall not be provided to 3rd parties without consent being granted.

Suppliers and Potential suppliers

Personal Data on suppliers shall be held on the basis of contract where supplies of goods and/or services to the Company have been made. Data provided by potential suppliers shall be held on the basis of consent.

Website

Dreadnought Tiles and Ketley Brick collect data from visitors throughout the website experience. This is largely to provide interactive functionality that would otherwise be impossible without collecting the minimum amount of data. Some data is also used to analyse the users experience anonymously to improve the website experience.

Dreadnought Tiles respects their website users privacy and will not sell data to third parties, or allow any access to the data that is not necessary to honour any other contracts we have in place or store excessive amounts of data we no longer need.

The data collected from the website session will likely be shared with:

Alphabet Inc (Google) – a suite of Google Tools is used by www.dreadnought-tiles.co.uk and www.ketley-brick.co.uk

Intergage Ltd – The websites and associated data are held securely on Intergage operated servers and are accessible to Intergage as the host and website service provider.

Our websites use a "session cookie" to identify the users browser "session" as they move between pages on the website and perform activities. The full policy is available to view on our websites.

Data Storage and security

All personal data is accessible only to those who need to use it. All personal data will be stored securely; in a lockable room with controlled access; and/or in a locked drawer or filing cabinet; and/or if computerised, password protected.

All personal data shall be kept secure by the Company with appropriate technical and other measures taken to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,

The Company has carried out a data audit that determines the business processes that use personal data, the source of personal data, the description of the personal data, the processing activity, the purpose(s) for which each category of personal data, the recipients, and potential recipients, of the personal data, the key systems and repositories and all retention and disposal requirements. This data audit is available to view on request to parties that the regulations are deemed to apply

The Company ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Company's business.

The Company shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

The Company shall take appropriate technical and organisational security measures to safeguard information including unauthorised or unlawful processing and accidental loss or damage of data. The Company shall apply password protection to computers including laptops and apply appropriate computer security procedures including, virus checking software and firewalls, role-based access rights including those assigned to temporary staff, security of local and wide area networks. Devices shall not be connected to the Company's network without appropriate authority.

Data which is no longer needed shall be securely destroyed, the retention period for each category of personal data is set out in the Data Audit.

Shall not be transferred to a country or territory outside the European Economic Area without suitable safeguards.

Rights and Data Access

Your principal rights under GDPR are:

(a) the right to access;
(b) the right to rectification;
(c) the right to erasure;
(d) the right to restrict processing;
(e) the right to object to processing;
(f) the right to data portability;
(g) the right to complain to a supervisory authority; and
(h) the right to withdraw consent.

The Company ensures that the rights of people about whom information is held can be fully exercised under the Regulation.

The Company strives to ensure personal data is accurate and kept up to date with every effort to erase or rectify without delay. Employees, customers and others should notify the Company of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Company to ensure that any notification regarding change of circumstances is recorded and acted upon.

CCTV

The Company operates a CCTV network for the purposes of crime prevention and detection, and Safeguarding. Where a data subject can be identified, images are processed as personal data.

Alex Patrick-Smith
Managing Director

Version 1
March 2018

Hinton, Perry & Davenhill Ltd
Dreadnought Road,
Pensnett,
Brierley Hill
DY5 4TH

01384 77405
www.dreadnought-tiles.co.uk
www.ketley-brick.co.uk

- Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.
- It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
- If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.
- Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.
- There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:
- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.
- The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
- The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
- You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.
- Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy notice.

Checklists

☐ We have checked that legitimate interests is the most appropriate basis.

☐ We understand our responsibility to protect the individual's interests.

☐ We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.

☐ We have identified the relevant legitimate interests.

☐ We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.

☐ We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.

☐ We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.

☐ We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.

☐ If we process children's data, we take extra care to make sure we protect their interests.

☐ We have considered safeguards to reduce the impact where possible.

☐ We have considered whether we can offer an opt out.

☐ If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.

☐ We keep our LIA under review, and repeat it if circumstances change.

☐ We include information about our legitimate interests in our privacy notice.