HML Group Data Protection Policy

We protect your property and your data!

1. Introduction

a. The EU General Data Protection Regulation (GDPR) becomes effective 25 May 2018. This legislation strengthens the rights that UK individuals have over their data, and creates a uniform data protection law across the European Union. These provisions supplement the requirements of the Data Protection Act (The Act).

b. HML manages the communal and amenity areas for a wide range of properties including blocks of flats, housing estates and mixed-use developments. HML has developed Data Protection policies and procedures to ensure that we and our clients comply with our Data Protection obligations.

2. HML's Services and Approach

a. HML acts as an agent and advisor to its client. Although primary legal responsibility for the management of the property and the control of records is with our client, part of HML's service is to ensure our clients' compliance with the law, their leases, and codes of practice. The client is however, responsible for setting policy and monitoring the work of their agent.

b. In order to perform the daily duties of running a property on behalf of the client, HML collects and uses certain types of information about leaseholders, tenants, clients and other service users. Data collected is also used to promote and advertise its services; maintain its own accounts and records; and support and manage its employees and contractors. In specific circumstances, HML gathers data for marketing its services but client and tenant information is not used for this purpose.

c. This personal information is collected and dealt with appropriately whether it is collected on paper, stored in a computer database or recorded on other material. HML has put in place safeguards to ensure this information is protected under the Data Protection Act 1998 and General Data Protection Regulation (GDPR).

d. Our data protection policy outlines what HML does with the data that is collected, who it will be shared with and how it will be stored using the agency based relationship between HML and its clients

3. HML's Commitment

a. HML complies with the GDPR regulations as a 'Data Processor' and where applicable as a 'Controller'. We will assist our clients wherever possible to meet their GDPR obligations.
b. This policy sets out HML's approach to the protection of data for all leaseholders, tenants, clients and other service users with whom we interact including our employees. HML wishes to stress the high level of importance that it places upon complying with the requirements of GDPR.

4. Data Controller and Data Processor

a. HML can be both a Data Processor and a Data Controller under the regulations. HML is a Data Processor when data is being processed on behalf of our instructing clients. This data includes anything to do with the management of our clients' buildings. We are the Data Controller under the Act when we create or collect personal data other than on behalf of our clients. This could be for example when HML is using the data for the purposes of its own communications. Interpretation of this difference could be difficult and in the event of any doubt HML's Data Controller should be contacted to provide clarification.
b. HML is also responsible for notifying the Information Commissioners Office (ICO) of the data it holds or is likely to hold, and the general purposes that this data will be used for. Our Registration number under the ICO is shown at the end of this document.
c. HML's Data Protection Officer (DPO), is responsible for ensuring that we comply with all provisions within this policy and the Act.

5. Data Protection Principles

a. HML regards the lawful and correct treatment of personal information as critical to maintaining the confidence of those with whom we deal.
b. To this end, HML will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998. Specifically, the Principles require that personal information:
    i. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
    ii. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with those purposes,
    iii. Shall be adequate, relevant and not excessive in relation to those purposes,
    iv. Shall be accurate and, where necessary, kept up to date,
    v. Shall not be kept for longer than is necessary,
    vi. Shall be processed in accordance with the rights of data subjects under the Act,
    vii. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information
    viii. Shall only be transferred to a country or territory outside the European Economic Area that subscribes to Privacy Shield; this policy allows US (and other no EEA based) companies to be deemed compliant under the GDPR, for further information please see the following link: www.privacyshield.gov/participant?id=a2zt0000000TO6hAAG

6. Disclosure

a. HML may share data, that it could reasonably be expected to with other agencies such as local authorities or the police.

b. The leaseholders, clients, and other service users will be made aware how and with whom their data will be shared via HML documentation which may include this policy, management agreements, works orders, resident's handbooks and welcome letters. There are circumstances where the law requires HML to disclose data (including sensitive data) without the data subject's consent. These are:
   i. Carrying out a legal duty or as authorised by the Secretary of State
   ii. Protecting vital interests of an Individual/Service User or other person
   iii. The Individual/Service User has already made the information public
   iv. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
   v. Monitoring for equal opportunities purposes - i.e. race, disability or religion

c. Thirdly, HML may need to disclose data without the data subject's consent in order to allow HML to carry out our duties as a Data Processor and a property manager to clients. Examples of this include:
   i. Providing Individual/Service User's personal information in an emergency, such as contact details to a tradesman who needs to carry out urgent repairs on behalf of a client
   ii. Disclosing information to a debt collection company when a leaseholder is in service charge arrears
   iii. Data can be shared with clients' (the landlord or a client company director) where necessary in order for them to monitor our work and maintain the Data Processing obligation of the client and agent relationship. The relationship is based on the premise that documents which relate to the affairs of a client, resident management company or right to manage company are not the property of the managing agent and should always be handed over by HML on request. Examples where data may be shared with a client are set out below:
   iv. Legal proceedings brought against a client,
   v. Leaseholder not paying service charges,
   vi. Complaints from leaseholders regarding service levels,
   vii. Concerns raised by a tenant, lessee or freeholder in respect of matters relating to the management of a building.

d. Leaseholder account information is not divulged to other leaseholders, tenants or third parties. Members of a Residents Association or Committee are not considered Directors for this purpose therefore personal leaseholder information cannot be disclosed to them

e. There are circumstance where clients have a legal obligation to disclose data. This includes their obligations under S22 of the Landlord and Tenant Act 1985. (Receipts and invoices supporting service charge accounts).

f. Neither HML nor our clients should disclose any information that could not reasonably be expected to be disclosed in the normal course of duties.

7. Data Collection

a. HML will ensure that data is collected within the terms set out in this policy. This applies to data that is collected in person, or in the written word from the completion of a form.

b. When collecting data, HML will ensure that the leaseholder, tenant, client and other service user clearly understands what the data will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing.

c. HML collects the type of information set out below to carry out our property management services as well as maintain our own records. These records include addresses, financial and bank details for the following groups:

i. Clients
ii. Tenants
iii. Leaseholders
iv. Professional advisers and consultants
v. Complainants, enquirers
vi. Suppliers/contractors
vii. Landlords

d. HML collects the following type of information to support and manage our employees and contractors.

i. Personal details
ii. Family details
iii. Lifestyle and social circumstances
iv. Employment and educations details
v. Goods and services
vi. Financial details
vii. All information contained in references
viii. HML also processes sensitive classes of information that may include:
ix. Racial or ethnic origin
x. Religious or other beliefs
xi. Trade union membership
xii. Physical or mental health details

8. HML Staff Roles and Responsibilities

Ensuring compliance with our statutory duties under GDPR is everyone's responsibility. To provide the leadership and overarching policy direction HML will appoint:

Data Protection Officer (DPO) who is responsible to the CEO for:

i. Ensuring staff and authorised users are aware of this policy;
ii. Monitoring compliance;
iii. Conducting regular review of all policies, having regard to any changes in contractual obligations, organisational changes, and legislation; and
iv. Ensuring there is clear direction and visible management support for security initiatives.
v. Chair bi-annual meetings with 'information owners' to review compliance and the HML Information Security risk register.

Information Owners
HML has designated information owners who are responsible for Data Protection compliance within their area. Designated information owners are:

Information/Data Area	Lead Department	Designated Information/Data Owner
Client Data	Operations	Heads of Property Management
New Business Pipeline Data	Business Development	Siân Lewis
Marketing Data	Business Development	Siân Lewis
Employee Data	HR	Richard Scott
Client Data Storage	IT	Sarah Longman
Finance/Payroll Data	Corporate Finance	James Hayles
Contractor Data	TAFS	Kate Bowes
3rd Party	Facilities	Hamilton Comely
Customer Services	Customer Services	Theo Delemos
Alexander Bonhill	AB	Danielle Williams
Lettings	HML Lettings	Linda Cole/Anthony Miller/ Simon Tarrant/Polly Dyer/Ryan Heap

Information Owners are responsible to the DPO for:

a. Completing a Privacy Impact Assessment (PIA) on systems/data when required. A PIA shall be performed for all information systems on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limit. Information owners must be satisfied that the controls will reduce any residual risk to an acceptable level.

b. Mitigate identified risks by ensuring information security is an integral part of information management, whether the information is held in electronic or hard-copy form. HML is committed to protecting the security of its information and information systems in order to ensure that

   i. The integrity of information is maintained, so that it is accurate, up to date and 'fit for purpose';
   ii. Information is always available to those who need it and there is no disruption to the HML Group business and operational activities;
   iii. Confidentiality is not breached, so that information is accessed only by those authorised to do so'
   iv. HML meets its legal and contractual requirements, including those applicable to personal data under GDPR; and
   v. The reputation of HML is safeguarded.
   vi. HML shall establish and maintain appropriate contacts with other organisations, regulatory bodies, and network/telecommunications operators in respect of its information security policy. Breaches of information security must be recorded and reported to the DPO, who will act and inform the relevant authorities.
   vi. Ensure 3rd parties that are used to support HML in conducting its functions are compliant with GDPR regulations.

Contractor Accreditation Team

a. Ensure that all suppliers on HML's Contractor Accreditation scheme will comply with HML's Data Protection Policy.

HML Managers are responsible for:

a. Ensuring that data protection requirements are observed;
b. Providing clear messages to their staff regarding appropriate processing of the personal data that they handle;
c. Identifying and addressing training needs within the team and informing the DPO if the available training will not address their needs;
d. Consulting the DPO before processing personal data for a new purpose;
e. Informing the DPO of any data subject requests or complaints;
f. Ensure staff are trained in Data Protection/Information security and have regular update training.

All employees are responsible for:

a. Complying with the data protection principles, as supported by the Policy, guidance on the application of the Policy and associated policies and guidance;
b. Contacting their manager or the DPO for guidance if they are in any doubt about how they should deal with certain personal data;
c. Only processing personal data in the manner that is authorised for the purpose of carrying out their responsibilities or with management authorisation.

9. Data Storage

a. HML is accountable to maintain control of confidentiality of its and its clients' records. HML must therefore take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. HML undertake as and when necessary Privacy Impact Assessments to access the risk to individual's rights when using new or enhanced systems. The following measures are taken:
    i. Using lockable cupboards (restricted access to keys)
    ii. Archived data is kept off site with a secure third-party storage company
    iii. Password protection on personal information files
    iv. Setting up computer systems to allow restricted access to certain areas
    v. Copies of programs or data must not be taken or removed from HML's premises without the express permission of a line manager. However, when data is taken off site on laptops and mobiles, HML aims to protect the data on these medias by instructing staff to log-on to the network using their own account and keeping their passwords confidential.
    vi. Back up of data on computers kept on separate hard drives on a secure server on site
    vii. A clear desk and screen culture
b. Information will be stored for only as long as it is needed as laid out in HML's Data Retention Policy, or as required by statute, and will be disposed of appropriately.
c. It is HML's responsibility to ensure all personal and company data is non- recoverable from any computer system previously used within the organisation, which has been passed to a third party.

10. Data Access and Accuracy

a. Service users whose personal information are processed by HML have the right to know:
   i. What information we hold and process on them
   ii. How to gain access to this information
   iii. How to keep it up to date
   iv. What controls we have in place to ensure we comply with the Act.
b. Service users also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information determined to be wrongfully collected.
c. Service users have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to the Data Protection Officer (set out in (i) below).
d. The following information will be required before access is granted:
   i. Full name and contact details of the person making the request
   ii. Their relationship with HML
   iii. Any other relevant information - e.g. timescales involved
   iv. Reference number held on record by HML - e.g. T reference or company reference
   v. photographic identification - e.g. Passport, drivers licence.
e. HML may also require proof of identity before access is granted.
f. Queries about handling personal information will be dealt with swiftly and politely.
g. HML will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request.
h. This policy was last updated in March 2020 and will be reviewed regularly and updated as necessary to reflect any additional regulatory requirements as well as best practice in data management, security and control.
i. In case of any queries or questions in relation to this policy please contact HML's Data Protection Officer.

11. Compliance

HML takes data protection compliance very seriously; any breach of data protection legislation, local data protection procedures and/or the provisions of the Data Protection Policy may render staff liable to internal disciplinary proceedings (staff handbook on HML HR site). Staff should be aware that it is a criminal offence to breach certain provisions of the Act and GDPR regulations. Knowingly or recklessly obtaining or disclosing personal data may leave an individual employee liable to prosecution.

12. Policy Subdivision

This policy is the overarching foundation where all other subdivisions of HML information security policy shall conform to. While most policies are department specific there is a small subset below which will be applicable to all HML staff:

- Clear Desk and Screen Policy
- Document Retention Policy
- Privacy Policy

Glossary of Terms

The Act

a. Data Protection Act. The UK legislation that provides a framework for responsible behaviour by those using personal information.
b. Agent - Individual/company instructed to act on behalf of the client when it comes to day to day management of their development. In relation to this policy the agent is HML.
c. Client - This term refers to any one of the following property owners or landlords; freeholder, resident management company (RMS), right to management company (RTM) or developer which instructs HML.
d. Data Controller - The person who (either alone or with others) decides what personal information HML will hold and how it will be held or used.
e. Data Protection Officer - The person responsible for ensuring that HML follows its data protection policy and complies with the Data Protection Act 1998.
f. Explicit consent - is a freely given, specific and informed agreement by an Individual/ Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.
g. GDPR. General Data Protection Regulations.
h. HML is the agent working on behalf of the client and includes all the trading names within the HML Group.
i. Individual/Service User - The person whose personal information is being held or processed by HML for example: a client, an employee, a leaseholder, a tenant, a contractor, and a supplier etc.
j. Information Commissioner - The UK Information Commissioner responsible for implementing and overseeing the Act 1998.
k. Notification - Notifying the Information Commissioner about the data processing activities of HML.
l. Personal Information - Information about living individuals that enables them to be identified - e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees of HML.
m. Processing - means collecting, amending, handling or storing personal information.
n. Sensitive data - refers to data about
    i. Racial or ethnic origin
    ii. Political affiliations
    iii. Religion or similar beliefs
    iv. Trade union membership
    v. Physical or mental health

HML Company Details:

HML PM Limited
94 Park Lane
Croydon
CR0 1JB
Data Protection registration No: Z9099520

HML Holdings Plc
9-11 The Quadrant
Richmond
TW9 1BP
Data Protection No: ZA226890

HML Shaw Limited
Data Protection No: Z5541333

Shaw & Company (Surveyors) Limited
Data Protection No: ZA155848

Alexander Bonhill Limited
Data Protection No: ZA155848

Faraday Property Management Limited
Data Protection No: Z9628495