GENERAL DATA PROTECTION REGULATION (GDPR) STATEMENT

Introduction

The new EU General Data Protection Regulation (GDPR) came into force on 25 May 2018 (including in the UK regardless of its decision to leave the EU) and will impact every organisation which holds or processes personal data. It has introduced new responsibilities, including the need to demonstrate compliance, more stringent enforcement and substantially increased penalties than the current Data Protection Act (DPA) which it will supersede.

Our Commitment

Rotherhill Developments Ltd, and its associated companies ('we' or 'us' or 'our' or 'the company' or 'Rotherhill') are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection Bill

Rotherhill (and its associated companies) are focusing on the following GDPR requirements.

These are being implemented by Rotherhill:

- Ensuring Privacy by design is implemented in all new projects, services and tools.
- Fine tuning processes to ensure they meet GDPR requirements, for example DSARs (data subject access requests), our Data Breach process and Privacy Impact Assessments.
- Data Retention & Erasure – we have updated our retention policy and schedule to ensure that we meet the *'data minimisation'* and *'storage limitation'* principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new *'Right to Erasure'* obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
- Data Breaches – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.

- Employee Terms and Conditions - All employee contracts have been updated to reflect the changes under GDPR and how personal data is held and processed by the company
- Contract Terms and Conditions - We have updated our contract terms and conditions to reflect GDPR requirements, these show in detail how personal data is held and processed by the company and how long the data will be held for.
- Privacy Policy – we have revised our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- Legal Basis for Processing - we are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- *Direct Marketing* - we have revised the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.
- Subject Access Request (SAR) – we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.
- Data Protection Impact Assessments (DPIA) – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).
- *Special Categories Data* - where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.
- *Obtaining Consent* - we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they

are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.

Rotherhill have worked with our IT Management Company to ensure that data:

- is protected as it arrives with the company.
- is held securely whilst in the company.
- access is controlled whilst stored in all Rotherhill (and its associated companies) systems.
- is secured when it is sent to a third party where required.
- finally, that the data is securely destroyed once it is no longer required.

Rotherhill has policies in place that have been updated and reviewed to ensure the requirements of GDPR are addressed. The following key policies are in place: Non-Contractual Information Technology Policy, Data Protection Policy. These provide the governance to ensure the Personally Identifiable Information data is handled correctly.

Information Security & Technical and Organisational Measures

Rotherhill takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including: -

Security measures include, but are not limited to Data access control measures, password policies, encryptions, physical data storage security, mobile device management, authentication, encrypted data transport.

These measures are reviewed on a regular basis and are updated in consultation with our IT advisors.

GDPR Roles and Employees

Rotherhill have designated the company directors as our Data Protection Officers (DPO) who are responsible for the implementation of the new data protection Regulation. The directors are responsible for promoting awareness of the GDPR across the company, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

Rotherhill understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans. We have implemented an employee training program which forms part of our induction and annual training program.

If you have any questions about our preparation for the GDPR, please contact the company using the information in part 1 of our Privacy Policy.