Hygenisys Environmental Health Ltd

Data Protection & Privacy Policy

1. Introduction

Hygenisys Environmental Health Ltd is committed to data security and the fair and transparent processing of personal data. This Privacy Policy sets out how we will treat the personal data that is provided to us in compliance with applicable data protection law, in particular the General Data Protection Regulation (EU) 2016/679 (GDPR).

The Policy contains important information about who we are, how and why we collect, store, use and share personal data, the rights in relation to personal data and how to contact us and the regulatory authorities to report a concern about the way in which we process personal data.

2. Who are we?

Hygenisys Environmental Health Ltd is registered with Companies House, number 8081166. Our registered address is Bury House 31 Bury Street London EC3A 5AR

For the purposes of the GDPR, Hygenisys Environmental Health Ltd is the 'Controller' of the personal data provided to us in the course of our business operations. Any queries about this Policy, the way in which the company processes personal data, or about exercising personal rights, should be directed by e-mail to: **dataprotection@hygenisys.com**

3. What personal data do we collect?

We may collect and process the following types of personal data provided to us by our clients in the course of our normal business operations and under our service agreements and contracts to provide consultancy services:

- names;
- e-mail address;
- postal address;
- telephone numbers;
- medical information and
- job roles.

This information will normally be received:

- in person;
- by telephone;
- by e-mail, or
- in writing;

The Company also collects, uses and processes a range of personal information from sub contractors This can include:

- your contact details, including your:

  - name;
  - address;
  - telephone number and
  - personal e-mail address

- personal information included in a CV, any application form, covering letter or interview notes;
- references;
- information about your right to work in the UK and copies of proof of right to work documentation;
- copies of qualification certificates;
- copies of membership certificates of professional bodies;
- copy of driving licence;
- other background check documentation (e.g. Disclosure & Barring Service (DBS) checks);
- details of your skills, qualifications, experience and work history with previous employers;
- information about your current salary level, including benefits and pension entitlements;
- National Insurance number

4. Personal information we collect

We only collect personal information that is provided to us that is deemed necessary to carry out the legitimate functions of the business, i.e. providing consultancy services or offer employment to sub contractors or consultants.

5. Information we receive from other sources

We may also receive information from other sources, e.g. a client's appointed representative or agent, other employers, their employees, other businesses and connected service providers, when they enter into an agreement with us or our clients and receive our services directly or indirectly as part of a third-party service agreement.

Under our agreements to provide consultancy services to our clients, we expect that they will also comply fully with the requirements under the GDPR and have obtained all necessary consents to share third party data with us for the mutual legitimate needs of our respective business operations.

6. Information about other people

Where information is provided to us about any other person(s) (e.g. employees, consultants, contractors, next of kin, advisers, suppliers, business associates etc.) the persons providing that information must ensure that they understand how it will be used, and that permission has been obtained for the information to be disclosed to us and for all parties to allow us, and any associated outsourced service providers and advisors, to use it.

7. Sensitive personal data

It is not expected under the normal course of our business that we will collect any sensitive personal data (i.e. information about racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or genetic or biometric data). If in the future this should change for any reason then we will only collect, process and retain this information on the basis of explicit consent first being obtained.

8. How do we use personal data?

Any personal data requested by us and supplied by our clients or third parties is required to enable us to undertake our legitimate business operations and consultancy service provision and for no other purpose. Any request for such information will always be made in this context and for no other reason.

Contract performance: We may use personal data to:

- deliver our consultancy services;
- fulfil a contract, or where it may be linked to a client's contract with a third party;
- communicate with clients in relation to the provision of the contracted services;
- provide administrative engagement such as accounts, security, and responding to any issues;
- provide professional information related to the services provided by the Company.
- Offer employment to sub-contractors

Legitimate interests: Where this is necessary for purposes that are in our interests, the interests of our clients or the aligned interests of any third parties.

These interests include communicating with clients and third parties in relation to any service provision, issues, complaints, or disputes.

Individuals have the right to object to the processing of their personal data on the basis of legitimate interests as set out below, under the heading 'Individual's rights under GDPR'.

Where required by law: We may also process personal data if required by law, including responding to requests by government or law enforcement authorities, or for the prevention of crime or fraud.

9. Who do we share personal data with?

We take all reasonable steps to ensure that personal data is protected and are aware of the information security obligations under the GDPR. We limit access to personal data to those who have a genuine and legitimate business need to know it.

We may also share personal data with trusted third parties including:

- legal and other professional advisers, consultants and professional experts;

- service providers contracted to us in connection with the provision of our services, such as providers of IT services.

We will ensure there is an agreement in place with the categories of recipients listed above, which include obligations in relation to the confidentiality, security, and lawful processing of any personal data shared with them.

We do not envisage sharing personal data with any third party recipient located outside the European Economic Area; however, should this situation arise due to the needs of a client, we will ensure that the transfer of personal data will be protected by appropriate safeguards, namely the use of standard data protection clauses adopted or approved by the European Commission where the data protection authority does not believe that the third country has adequate data protection laws.

We will share personal data with law enforcement or other authorities if required by applicable law.

10. How long will we keep personal data?

Where there is a contract in place, personal data will be retained for the duration of the contract, and for a period of six years following its termination or expiry, to ensure we are able to comply with any contractual, legal, audit, insurance and other regulatory requirements, or any orders from competent courts or authorities.

11. Where do we store personal data and how is it protected?

We store personal data securely at our registered address in the UK. We take reasonable steps to protect personal data from loss or destruction, including:

- the regular backup of electronic data;
- using a GDPR compliant IT service provider;
- operating secure and encrypted servers through the IT provider;
- ensuring that any hard copy information is stored securely with restricted access to unauthorised persons.

We have procedures in place to deal with any suspected data security breach and we will notify clients and any applicable regulator of a suspected data security breach where we are legally required to do so.

The transmission of information via the internet cannot be considered to be completely secure. Although we will do our best to protect personal data, we cannot guarantee the security of personal data transmitted to our e-mail addresses and any transmission is at the client's own risk. Once we have received any personal data, we will use the procedures and security features outlined above to prevent unauthorised access.

12. Individual's rights under the GDPR

Individuals have various rights with respect to our use of personal data.

Individuals have the right to request a copy of the personal data that we hold about them by contacting us at the e-mail or postal address given above. Any persons making such a request for information must be able to verify their identity. We will respond within forty calendar days as a maximum. However, there are exceptions to

this right and we may be unable to make all information available if, for example, making the information available would reveal personal data about another person, if we are legally prevented from disclosing such information or if the request is manifestly unfounded or excessive.

Right to rectification

We aim to keep any personal data accurate and complete. We encourage clients to contact us, using the contact details provided above, to let us know if any of personal information held is inaccurate or has changed, so that we can keep this up-to-date.

Right to erasure

Individuals have the right to request the deletion of their personal data where, for example, the personal data is no longer necessary for the purposes for which it was collected, where consent to processing is withdrawn, where there is no overriding legitimate interest for us to continue to process the personal data, or the personal data has been unlawfully processed. Clients can request that personal data is erased using the contact details provided above.

Right to object

In certain circumstances individuals have the right to object to the processing of their personal data where, for example, it is being processed on the basis of legitimate interests and there is no overriding legitimate interest for us to continue to process that personal data. Where clients would like to object to the processing of personal data they can contact us using the contact details provided above.

Right to restrict processing

In certain circumstances individuals have the right to request that we restrict the further processing of personal data. This right arises where, for example, an individual has contested the accuracy of the personal data we hold about them and we are verifying the information, they have objected to processing based on legitimate interests and we are considering whether there are any overriding legitimate interests, or the processing is unlawful and they elect that processing is restricted rather than deleted. In any such cases clients can contact us using the contact details provided above.

Right to data portability

In certain circumstances individuals have the right to request that some of their personal data is provided, or to another data controller, in a commonly used, machine-readable format. This right arises where personal data has been provided to us, the processing is based on consent or the performance of a contract, and processing is carried out by automated means. If an individual would like to request that their personal data is ported to them, they must contact us using the contact details provided above. The GDPR sets out exceptions to these rights and if we are unable to comply with a request due to an exception we will explain this in our response.

13. Contact

In the event of any queries about this Policy, the way in which Hygenisys Environmental Health Ltd processes personal data, or about exercising any personal rights, please send an e-mail to **dataprotection@hygenisys.com**

15. Changes to our Policy

Any changes we may make to our Policy in the future will be communicated directly to our clients, subcontractors and consultants.

Hygenisys Environmental Health Ltd
General Data Protection Regulations 2016 (GDPR)
Data Protection & Privacy Policy **25th May 2018**