

HAZA CONSULTING LIMITED

GDPR & DATA PROTECTION POLICY

1. INTRODUCTION

Haza Consulting is committed to carrying out its business in compliance with all relevant data protection laws and regulations and according to the highest ethical standards.

This policy establishes the expected behavior of Haza Consulting Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure, and destruction of Personal Data belonging to a Haza Consulting Contact (the Data Subject).

Personal Data means any information (including opinions and intentions) that identifies or can be used to identify a Natural Person. It is protected by the Data Protection Laws and subject to certain restrictions on how an organization may process it. An organization that processes Personal Data and determines how it is used is called a Data Controller. Haza Consulting, as a Data Controller, is responsible for ensuring that Personal Data is handled in accordance with this policy and with the requirements of the Data Protection Laws. Failure to comply may result in complaints, regulatory action, fines, and/or damage to the reputation of Haza Consulting.

The management of Haza Consulting is committed to the continued and effective implementation of this policy. Haza Consulting's leadership expects all Haza Consulting employees and third parties to share this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

2. SCOPE

This policy is applicable to all Haza Consulting Entities that process a Data Subject's Personal Data:

In relation to the business activities of the Haza Consulting Entity.

For the delivery of services to either individuals or businesses by Haza Consulting or its Entities

To actively observe the behaviors of people.

Monitoring the behavior of individuals includes using data processing techniques such as persistent web browser cookies or dynamic IP address tracking to profile an individual with a view to deciding between them.

This policy applies to any processing of personal data in electronic form (including electronic mail and documents prepared with word processing software), as well as manual files that are designed to give easy access to information about individuals.

HAZA CONSULTING LIMITED

This policy is intended to set a global standard for the processing and protection of personal data by all Haza Consulting and its Entities. Where national law imposes a requirement that is more stringent than this policy, such requirements must be met. Furthermore, if a condition imposed by national law is not addressed in this policy, the applicable national legislation must take precedence. If there are conflicting requirements in this policy and national law, the Data Protection Team must be contacted for further guidance. If this policy's requirements contradict national legislation, contact the Data Protection Team for clarification.

This policy does not apply to the protection of Personal Data belonging to employees of Haza Consulting.

3. DEFINITIONS

- **Employee:** an individual who works part-time or full-time for Haza Consulting under a contract of employment, whether oral or written, express or implied, and has recognized rights and duties (Including temporary employees and independent contractors)
- **Third Party:** An external organization with which Haza Consulting conducts business and is also authorized to, under the direct authority of Haza Consulting, Process the Personal Data of Haza Consulting Contacts.
- **Personal Data:** Any information (including opinions and intentions) that relates to an identified or Identifiable Natural Person.
- **Contact:** Any past, current, or prospective Haza Consulting customer.
- **Identifiable Natural Person:** Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controller: A natural or legal person, Public Authority, Agency, or other body that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- **Haza Consulting Entity:** A Haza Consulting establishment, including subsidiaries and joint ventures over which Haza Consulting exercises management control.
- **Data Subject:** The identified or Identifiable Natural Person to which the data refers.
- **Process, Processed, Processing:** Any operation or set of operations performed on Personal Data or sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- **Data Protection:** The process of safeguarding Personal Data from unauthorized or unlawful disclosure, access, alteration, Processing, transfer, or destruction.
- **Data Protection Authority:** An independent public authority responsible for monitoring the application of the relevant data protection regulations set forth in national law.
- **Data Processors:** A natural or legal person, Public Authority, Agency, or other body that Processes Personal Data on behalf of a Data Controller.
- **Consent:** Any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by an explicit affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

HAZA CONSULTING LIMITED

- **Special Categories of Data:** Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
- **Third Country:** Any country not recognized as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.
- **Profiling:** Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular, to analyze or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behavior, location, or movement.
- **Binding Corporate Rules:** The Personal Data protection policies used for the transfer of Personal Data to one or more Third Countries within a group of undertakings or groups of enterprises engaged in a joint economic activity.
- **Personal Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.
- **Encryption:** The process of converting information or data into code to prevent unauthorized access.
- **Pseudonymization:** Data is amended so that no individuals can be identified from it (directly or indirectly) without a "key" that allows the data to be re-identified.
- **Anonymization:** Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

4. POLICY

Governance

Data Protection Team

To showcase our dedication to data security and improve the efficacy of our compliance activities, Haza Consulting has formed a data protection team. The DP Team works autonomously and reports to Haza Consulting's Group Operations Director. The data protection team's responsibilities include:

- Informing and advising Haza Consulting and its Employees who carry out Processing pursuant to Data Protection regulations, national law, or union-based Data Protection provisions.
- Ensuring the alignment of this policy with Data Protection regulations, national law, or Union Data Protection provisions;
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);
- Determining the need for notifications to one or more DPAs as a result of Haza Consulting Ltd.'s current or intended Personal Data processing activities;
- Making and keeping current notifications to one or more DPAs as a result of Haza Consulting Ltd.'s current or intended Personal Data processing activities;
- The establishment and operation of a system providing prompt and appropriate responses to Data Subject requests;
- Informing senior managers, officers, and directors of Haza Consulting of any potential corporate, civil, and criminal penalties that may be levied against Haza Consulting and/or its Employees for violation of applicable Data Protection laws.
- Ensuring the establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any Third Party who:

HAZA CONSULTING LIMITED

- ★ provides Personal Data to a Haza Consulting Entity
- ★ receives Personal Data from a Haza Consulting Entity
- ★ has access to Personal Data collected or processed by a Haza Consulting Entity.

POLICY ENFORCEMENT

The management team of each Haza Consulting Entity must ensure that all Haza Consulting Ltd employees who are responsible for Personal Data Processing are aware of and follow the terms of this policy.

Furthermore, each Haza Consulting Entity will ensure that all Third Parties involved in processing personal data on its behalf (i.e., their data processors) will know about and fall in line with this policy. Each third party (whether a company or an individual) shall give such assurance in writing before they will be allowed to access any personal data under the control of Haza Consulting.

COMPLIANCE MONITORING

The Data Protection Team, in collaboration with key business stakeholders from each Haza Consulting Ltd Entity, will develop a plan with a timeline to address any gaps found within a specified and reasonable period of time. Significant gaps found will be escalated to and tracked by the Haza Consulting Executive Management team.

DATA PROTECTION PRINCIPLES

Haza Consulting has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

- **Principle 1:** Lawfulness, Fairness and Transparency
Personal Data shall be processed in a lawful, fair, and transparent manner in relation to the Data Subject. In other words, Haza Consulting must inform the Data Subject about what will happen to the Processing (transparency); the Processing must conform to what has been described to the Data Subject (fairness); and it must be for one of the purposes defined in the relevant Data Protection law (lawfulness).
- **Principle 2:** Purpose Limitation
The Data shall be collected for specified, explicit, and legitimate purposes and shall not be processed in a way that is incompatible with those purposes. In other words, Haza Consulting Ltd. has to specify what the collected personal data will be used for and limit the processing of such data only to the extent necessary to achieve such purpose.
- **Principle 3:** Data Minimisation
Personal Data shall be adequate, relevant, and limited to what is necessary for the purposes for which they are processed. This means Haza Consulting must not store any Personal Data beyond what is strictly required.
- **Principle 4:** Accuracy
Personal Data must be accurate and up to date. This means Haza Consulting needs to have processes in place to identify and deal with out-of-date, incorrect, and redundant personal data.
- **Principle 5:** Storage Limitation
Personal Data shall be kept in a form that allows identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed. That means Haza Consulting has to, as much as possible, store Personal Data in a way that limits or prevents the identification of the Data Subject.

HAZA CONSULTING LIMITED

- **Principle 6:** Integrity & Confidentiality

Personal Data shall be Processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful Processing and against accidental loss, destruction, or damage. Haza Consulting will take appropriate technical and organizational measures to ensure that the integrity and confidentiality of personal data are respected at all times.

- **Principle 7:** Accountability

The Data Controller will be accountable and able to prove compliance. In other words, Haza Consulting should demonstrate that all the six principles of Data Protection mentioned above are fulfilled regarding all kinds of Personal Data it is in charge of.

JUSTIFICATION FOR USING THE DATA

The requirements for processing are outlined in Schedules 2 and 3 of the Data Protection Act. Unless a relevant exception is applicable, at least one of the following requirements must be satisfied whenever we treat your personal data:

- **You have consented to the processing.**

The processing is necessary:

★ **in relation to a contract which we entered into; or**

★ **because you have asked for something to be done so we can enter into a contract.**

- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract)
- The processing is necessary to protect your “vital interests.”
- The processing is necessary for administering justice or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the “legitimate interests” condition.

We may get your CV data from external sources, such as LinkedIn, Job Boards, and/or referrals, and maintain it in our database for legitimate business purposes.

We may engage with you by sharing your CV with our Clients if you are looking for your next job, and we will always get your permission before doing so. We may engage in a formal contract that includes your express agreement to treat your data under one of the circumstances for data processing.

At the termination of the contract, we may still be legally required to process your data until the retention period expires. We will keep your data in line with our 10-year retention policy.

DATA SOURCES

Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates the collection of Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.
- If Personal Data is collected from someone other than the Data Subject, the Data

HAZA CONSULTING LIMITED

Subject must be informed of the collection unless one of the following applies:

- The Data Subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, Processing, or transfer of Personal Data.

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data
- At the time of first communication, if used for communication with the Data Subject
- At the time of disclosure, if it is disclosed to another recipient.

DATA SUBJECT CONSENT:

Each Haza Consulting Entity shall gather Personal Data only through authorized and fair procedures and, where applicable, with the individual's knowledge and consent. Haza Consulting is dedicated to getting an individual's consent before collecting, using, or disclosing their Personal Data.

The Data Protection Team, in collaboration with the Group General Counsel, the Operations Director, and other appropriate business officials, will create a system for obtaining and recording Data Subject Consent for the collection, processing, and/or transfer of their Data. The system must include provisions for:

- Determining what disclosures should be made in order to obtain valid Consent.
- Ensuring the request for consent is presented in a manner that is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the consent is freely given (i.e., it is not based on a contract that is conditional to the processing of personal data that is unnecessary for the performance of that contract).
- Documenting the date, method, and content of the disclosures made, as well as the validity, scope, and volition of the Consent given.
- Providing a simple method for a Data Subject to withdraw their consent at any time.

DATA SUBJECT NOTIFICATION:

Each Haza Consulting Entity shall provide Data Subjects with information about the purpose of the Processing of their Data as required by applicable law, contract, or where it believes it is reasonably acceptable to do so.

When the Data Subject is requested to provide Consent to the Processing of Personal Data, and any Personal Data is acquired from the Data Subject, all necessary disclosures will be provided in a way that draws attention to them unless one of the following applies:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given electronically or in writing. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

HAZA CONSULTING LIMITED

EXTERNAL PRIVACY NOTICES:

Each external website offered by a Haza Consulting Entity shall provide an online 'Privacy Notice' and an online 'Cookie Notice' that comply with relevant legislation. All Privacy and Cookie Notices must be authorized by the Data Protection Team before being published on any Haza Consulting external website.

DATA USE:

Haza Consulting uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of Haza Consulting Entities.
- To provide services to Haza Consulting Clients.
- The ongoing administration and management of customer services.

The use of a Contact's information should always be examined from their perspective, including if it will meet their expectations or if they are likely to object. For example, it would be reasonable for a Contact to expect Haza Consulting Ltd to use their information to reply to a Contact request for information about the services offered. However, it will be beyond their reasonable expectations for Haza Consulting to release their information to third parties for marketing reasons.

Each Haza Consulting Entity shall process Personal Data in compliance with all relevant laws and contractual obligations. More precisely, Haza Consulting Ltd will not handle Personal Data unless at least one of the following conditions are met:

The Data Subject has been authorized to process their personal information for one or more stated purposes.

- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the Data Controller.
- Processing is necessary for the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

In some instances, Personal Data may be processed for purposes other than those for which it was gathered. When determining the compatibility of the new reason for processing, the Office of Data Protection must provide guidance and permission before any processing may begin.

In the event that Consent has not been obtained for the specific Processing in issue, Haza Consulting will consider the following additional factors to establish the fairness and transparency of any Processing beyond the original reason for which the Personal Data was collected:

HAZA CONSULTING LIMITED

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing.
- The context in which the Personal Data has been collected, in particular regarding the relationship between the Data Subject and the Data Controller.
- The nature of the Personal Data, in particular, whether Special Categories of Data are being Processed or whether Personal Data related to criminal convictions and offenses is being Processed.
- The possible consequences of the intended further Processing for the Data Subject:
- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation, or Pseudonymization.

SPECIAL CATEGORIES OF DATA:

Haza Consulting shall Process Special Categories of Data (also referred to as sensitive data) only when the Data Subject gives explicit consent to such Processing or where one of the following conditions is applied:

- The Processing relates to Personal Data, which has already been made public by the Data Subject.
- The Processing is necessary for the establishment, exercise, or defense of legal claims.
- The Processing is specifically authorized or required by law
- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.

Further conditions, including constraints, are dependent on national laws governing the processing of genetic data, biometric data, or health-related data.

In any case where Special Categories of Data are to be processed, prior clearance from the Data Protection Team is required, and the rationale for processing must be explicitly documented with the Personal Data in question.

Where Special Categories of Data are processed, Haza Consulting will implement additional safeguards. Each Haza Consulting Entity may further take extra steps to meet local customs or social expectations for the processing of Special Categories of Data.

CHILDREN'S DATA:

Children cannot consent to the processing of personal data for information society services. Consent must be obtained from the person with parental responsibility for the child. It should be highlighted, however, that where processing is permissible under other grounds, the child or the holder of parental responsibility does not need to provide consent.

If any Haza Consulting Entity anticipates the need to get parental agreement for information society services provided directly to a child, guidance and approval must be obtained from the Office of Data Protection before any processing of a child's personal data can begin.

HAZA CONSULTING LIMITED

DATA QUALITY:

Each Haza Consulting Entity shall take all necessary steps to ensure that the Personal Data it collects and processes is complete and accurate in the first place and that it is updated to reflect the Data Subject's current position.

- The measures adopted by Haza Consulting to ensure data quality include Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading, or outdated, even if the Data Subject does not request rectification.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.

Restriction, rather than deletion of Personal Data, insofar as:

- A law prohibits erasure.
- Erasure would impair the legitimate interests of the Data Subject.
- The Data Subject disputes that their Personal Data is correct, and it cannot be clearly ascertained whether their information is correct or incorrect.

PROFILING & AUTOMATED DECISION-MAKING:

Haza Consulting will only engage in profiling and automated decision-making if it is required to provide you with our services or if it is permitted by law. Each Profiling involving a Data Subject must be based on reliable information.

We will occasionally send promotional or direct marketing materials to a Haza Consulting Ltd contact via digital channels like email, the Internet, and mobile phones without first getting their consent. This will only be done if it's required to provide our services to you, like advertising a job that they might be interested in. Any Haza Consulting Ltd. entity that wants to run a digital marketing campaign without first getting the data subject's consent must first get the Office of Data Protection's approval. The data subject must be made aware of their right to object at any time to the processing of their data for digital marketing purposes where the processing of their personal data is authorized for such purposes. In the event that a data subject objects, processing of their personal data connected to digital marketing must stop right away, and instead of being erased entirely, their information shall be retained on a suppression list with a record of their opt-out choice.

It should be emphasized that when digital marketing is carried out in a 'business to business' setting, there is no legal necessity to get an indication of consent to carry out digital marketing to individuals, as long as they are given the option to opt-out.

DATA RETENTION:

In order to maintain equitable processing, Haza Consulting will not keep personal data for longer than is required for the reasons for which it was first gathered or for which it has since been processed.

The minimum and maximum retention periods specified in the schedule are influenced by contractual and legal restrictions, which are taken into consideration when determining how long Haza Consulting Entities must keep personal data. Once it has been established that there is no longer a need to keep any personal information, it should be promptly erased or destroyed.

HAZA CONSULTING LIMITED

DATA PROTECTION:

To guarantee the security of personal data, every Haza Consulting Entity will implement organizational, technical, and physical safeguards. This includes preventing loss or destruction, illegal alteration, access, or processing, as well as any other hazards that may arise from human activity or the environment. Below is a summary of the security measures pertaining to personal data:

- Prevent unauthorized persons from gaining access to data processing systems in which Personal Data are Processed.
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorizations.
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified, or removed without authorization.
- Ensure that access logs are in place to establish whether and by whom the Personal Data was entered into, modified, or removed from a data processing system.
- Ensure that in the case where a Data Processor carries out Processing, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that Personal Data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can be processed separately.
- Ensure that personal data is not kept for longer than necessary.

DATA SUBJECT REQUESTS:

The Data Protection Team will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing.
- Objection to automated decision-making and profiling.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

Let's say someone requests something related to any of the aforementioned rights. Then, in compliance with all relevant data protection laws and regulations, Haza Consulting Ltd will evaluate each such request. Unless the request is judged to be superfluous or excessive, there will be no administration cost for reviewing and/or granting it. Data subjects are entitled to the following details regarding their own personal data, provided they successfully verify their identity and submit a written request to the Office of Data Protection:

- The purposes of the collection, Processing, use, and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.
- The use of any automated decision-making, including Profiling.

HAZA CONSULTING LIMITED

The right of the Data subject to:

- Object to Processing their Data.
- Lodge a complaint with the Data Protection Authority.
- Request rectification or erasure of their Data.
- Request a restriction on processing their data.

All inquiries about access to or correction of personal data must be sent to the Office of Data Protection via email, and they will be recorded as soon as they are received. After the written request from the Data Subject is received, a response will be given within 30 days. The requestor must be identified as the Data Subject or their designated legal representative by appropriate verification. The right to request that Haza Consulting Ltd. update or rectify inaccurate, deceptive, out-of-date, or incomplete personal data belonging to data subjects. Suppose Haza Consulting cannot respond fully to the request within 30 days. In that case, the Office of Data Protection shall nevertheless provide the following information to the Data Subject or their authorized legal representative within the specified time: I An acknowledgment of receipt of the request.

- Any information located to date.
- Details of any requested information or modifications that will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g., where the request is excessive in nature).
- The name and contact information of the Haza Consulting individual who the Data Subject should contact for follow-up.

There may be circumstances in which giving a data subject the information they have requested might reveal personal information about another person. To safeguard that person's rights in such situations, the material must be redacted or withheld as may be required or appropriate.

4.8 LAW ENFORCEMENT REQUESTS & DISCLOSURES

Under some conditions, sharing personal information without a data subject's knowledge or consent is allowed. This occurs when any of the following reasons necessitate the disclosure of personal data:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If a Haza Consulting Entity Processes Personal Data for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

Suppose any Haza Consulting Entity receives a request from a court or any regulatory or law enforcement authority for information relating to a Haza Consulting Contact. In that case, you must immediately notify the Office of Data Protection, which will provide comprehensive guidance and assistance.

HAZA CONSULTING LIMITED

The right of the Data subject to:

- Object to Processing their Data.
- Lodge a complaint with the Data Protection Authority.
- Request rectification or erasure of their Data.
- Request a restriction on processing their data.

All inquiries about access to or correction of personal data must be sent to the Office of Data Protection via email, and they will be recorded as soon as they are received. After the written request from the Data Subject is received, a response will be given within 30 days. The requestor must be identified as the Data Subject or their designated legal representative by appropriate verification. The right to request that Haza Consulting Ltd. update or rectify inaccurate, deceptive, out-of-date, or incomplete personal data belonging to data subjects. Suppose Haza Consulting cannot respond fully to the request within 30 days. In that case, the Office of Data Protection shall nevertheless provide the following information to the Data Subject or their authorized legal representative within the specified time: I An acknowledgment of receipt of the request.

- Any information located to date.
- Details of any requested information or modifications that will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g., where the request is excessive in nature).
- The name and contact information of the Haza Consulting individual who the Data Subject should contact for follow-up.

There may be circumstances in which giving a data subject the information they have requested might reveal personal information about another person. To safeguard that person's rights in such situations, the material must be redacted or withheld as may be required or appropriate.

4.9 DATA PROTECTION TRAINING

All Haza Consulting employees who have access to Personal Data will be briefed on their obligations under this policy during their personnel induction. Furthermore, each Haza Consulting Entity will give regular data protection training and procedural guidance to their employees.

The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- The Data Protection Principles are set forth in Section 4.2 above.
- Each employee has to use and permit the use of personal data only by authorized persons and for authorized purposes.
- There is a need for the proper use of the forms and procedures adopted to implement this policy.
- The correct use of passwords, security tokens, and other access mechanisms.
- Limiting access to personal data, such as by using password-protected screen savers and logging out when systems are not being attended to by an authorized person.
- Securely store manual files, printouts, and electronic storage media.
- There is a need to obtain appropriate authorization and utilize appropriate safeguards for all transfers of personal data outside of the internal network and physical office premises.
- Proper disposal of personal data using secure shredding facilities is also important.
- Any special risks associated with particular departmental activities or duties.

HAZA CONSULTING LIMITED

4.10 DATA TRANSFERS

Haza Consulting Entities may transfer Personal Data to internal or third-party receivers in another country that is regarded as providing acceptable legal protection for the rights and freedoms of the relevant Data Subjects. Transfers to nations without an acceptable level of legal protection (i.e., Third nations) must follow an established transfer method. Haza Consulting Entities may only transmit Personal Data if one of the following transfer circumstances applies:

- The Data Subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise, or defense of legal claims.
- The transfer is necessary to protect the vital interests of the Data Subject.

TRANSFERS BETWEEN HAZA CONSULTING ENTITIES

In order for Haza Consulting to operate successfully across its different Haza Consulting Entities, it may be required to transfer Personal Data from one Haza Consulting Entity to another or to grant access to Personal Data from an overseas location. Should this happen, the Haza Consulting Entity that sent the Personal Data will still be responsible for guaranteeing its protection.

Haza Consulting uses the Binding Corporate Rules transfer mechanism to transfer personal data between Haza Consulting Entities when the destination entity is located in a third country. Binding Corporate Rules offer Data Subjects legally binding, enforceable rights regarding the processing of their Personal Data, which must be enforced by all certified Haza Consulting Entities, including their employees. When transferring personal information to another Haza Consulting Entity based in a third country, you must:

- Ensure that the recipient Haza Consulting Entity is included on the approved list of Haza Consulting Entities subject to Haza Consulting 'Binding Corporate Rules Agreement'. The approved list is held and maintained by the Office of Data Protection.
- Only transfer the minimum amount of Personal Data necessary for the particular purpose of the transfer (for example, to fulfill a transaction or carry out a particular service).
- Ensure adequate security measures are used to protect the Personal Data during the transfer (including password protection and Encryption, where necessary).

TRANSFERS TO THIRD PARTIES

Each Haza Consulting Entity will only send Personal Data to or grant access to Third Parties if it is confident that the information will be processed properly and appropriately by the recipient. Where Third Party Processing occurs, each Haza Consulting Entity shall first determine whether the Third Party is a Data Controller or a Data Processor of the transmitted Personal Data under relevant law.

HAZA CONSULTING LIMITED

If the Third Party is determined to be a Data Controller, the Haza Consulting Entity will enter into an appropriate agreement with the Controller, in collaboration with the Office of Data Protection, to explain each party's duties in relation to the Personal Data transferred. If the Third Party is determined to be a Data Processor, the Haza Consulting Entity will enter into an appropriate Processing Agreement with the Data Processor in collaboration with the Office of Data Protection. The agreement must compel the Data Processor to preserve the Personal Data from further disclosure and only to process it in accordance with Haza Consulting's instructions. Furthermore, the agreement will oblige the Data Processor to adopt sufficient technological and organizational safeguards to secure Personal Data, as well as processes for notifying Personal Data Breaches. When a Haza Consulting Entity outsources services to a Third Party (including Cloud Computing services), it will determine whether the Third Party will Process Personal Data on its behalf and if the outsourcing will result in any Third Country transfers of Personal Data. In either scenario, it will work with the Office of Data Protection to incorporate necessary measures in the outsourcing agreement for such processing and third-country transfers. Haza Consulting has a 'Standard Provisions for Outsourcing Agreement' document that can be utilized for advice.

The Office of Data Protection shall conduct frequent audits of Third Parties' Processing of Personal Data, particularly with regard to the technical and organizational protections in place. Any significant flaws found will be reported to and monitored by the Haza Consulting Executive Management team.

4.11 COMPLAINTS HANDLING

Data subjects who have a complaint regarding the processing of their data can submit it in writing to the Data Protection Team. An investigation of the complaint will be conducted to the extent necessary, depending on the facts of the particular situation. The Data Protection Team will notify the Data Subject of the status and resolution of the complaint within a reasonable time frame.

Suppose the issue cannot be resolved through consultation between the Data Subject and the Office of Data Protection. In that case, the Data Subject has the option of seeking redress through mediation, binding arbitration, litigation, or a complaint to the Data Protection Authority in the applicable jurisdiction.

4.12 BREACH REPORTING

Any individual who feels a Personal Data Breach has happened as a result of the theft or exposure of Personal Data must notify the Data Protection Team immediately, providing a detailed account of the incident. Notifications about the occurrence can be sent by email: **dpo@hazaconsulting.co.uk** or by calling: **020 8163 2880**

The Data Protection Team will review all reported occurrences to determine whether a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Data Protection Team will follow the appropriate permitted procedure based on the severity and quantity of the Personal Data concerned. In the event of a significant Personal Data Breach, the Operations Director of Haza Consulting Ltd Group shall form and lead an emergency response team to coordinate and manage the response.

HAZA CONSULTING LIMITED

5. POLICY MAINTENANCE

All concerns about this policy, including requests for exceptions or amendments, should be addressed to the Data Protection Team via e-mail: **(E-mail Address)**

5.1 PUBLICATION

This policy will be made available to all Haza Consulting employees via the Haza Consulting Ltd Policy intranet or through other channels as determined by the Data Protection Team.

5.2 EFFECTIVE DATE

This policy is effective as of March 19th, 2018, and is revised annually.

5.3 REVISIONS

The Office of Data Protection is in charge of keeping this policy current and accurate. Significant adjustments will be communicated to Haza Consulting employees through the Human Resources department. Changes to this policy will go into effect when published on the website.