BQC Assessment Pvt. Ltd.
Registered Office: 202 DLF Galleria Mayur Vihar Phase-1, Delhi, India

INDEPENDENT ASSESSOR'S REPORT
Based on
General Data Protection Regulation- (EU) 2016/ 679
For
HUMAN EDGE ADVISORY SERVICES PVT LTD (HUMAN EDGE)

Scope of services	**"MITO, an app that offers health and wellbeing solutions rooted in data, biology, and technology"**
Location from which the services are being provided	142, Persepolis Apartment, GD Somani Road, Cuffe Parade, Colaba, Mumbai 400005
Date(s) Assessment	July 07, 2023
Name of the Lead Auditor / Assessor	Jayshree Dutta
Audit Criteria	Operations of **Human Edge Advisory Services Pvt Ltd (Human Edge)** for Support Function of IT Infrastructure, Human Resources, Physical Security, Legal and Administration.

July 07, 2023

Human EdgePrivate Limited

142, Persepolis Apartment, GD Somani Road, Cuffe Parade, Colaba, Mumbai 400005

We have examined the design and controls of **"Human Edge Advisory Services Pvt. Ltd (Human Edge)"** as on July 07, 2023 against the requirements of **General Data Protection Regulation (EU) 2016/679**.

The Company's management is responsible for the adequate design of these controls and compliance with the GDPR requirements. Our responsibility is to express an opinion on the design of these controls and the Company's compliance based on our examination.

Our examination included:
(1) Interviewing Top Management, IT Administration Staff, HR Management Staff, General Administration Staff;
(2) Reviewing IT Assets;
(3) Obtaining an understanding of the design of the Company's controls over GDPR Principles;
(4) Technical and Non- technical controls adopted and Reviewing Related policies and procedures;

Because of inherent limitations, controls may not prevent, detect or correct errors or fraud which may occur. Also, projections of any evaluation of adequate design to future periods are subject to the risk that controls may become inadequate because of change in conditions, or that the degree of compliance with the policies and procedures may deteriorate.

In our opinion, as of July 07, 2023 the Company in all material respects has adequately designed controls to meet GDPR requirements

This report is intended solely for the information and use of **Human Edge Advisory Services Pvt Ltd (Human Edge)** and should not be used without prior authorization of **Human Edge Advisory Services Pvt Ltd (Human Edge).**

Jayshree Dutta
Assessor/Lead Auditor ISO 27001: 2013

1. GDPR Background

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.[1] Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements related to the processing of personal data of individuals (formally called data subjects in the GDPR) who are located in the EEA, and applies to any enterprise—regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of data subjects inside the EEA.

The GDPR was adopted on 14 April 2016, and became enforceable beginning 25 May 2018. The regulation applies if the data controller (an organisation that collects data from EU residents), or processor (an organisation that processes data on behalf of a data controller like **cloud service providers**), or the data subject (person) is based in the EU.

Under certain circumstances, the regulation also applies to organisations based outside the EU if they collect or process personal data of individuals located inside the EU. The regulation does not apply to the processing of data by a person for a "purely personal or household activity and thus with no connection to a professional or commercial activity.

2. GDPR Definitions

S.No	Definitions
1	**'personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
2	'**processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
3	'**restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;
4	**'profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;
5	'**pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
6	**'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
7	**'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
8	**'recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients;

9	**'third party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
10	**'consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
11	**'personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
12	**'genetic data'** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
13	**'biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
14	**'data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

3. Introduction-

Registered Company Name – **Human Edge Advisory Services Pvt Ltd (Human Edge)**

“MITO, an app that offers health and wellbeing solutions rooted in data, biology, and technology

The report reflects the controls of **Human Edge** as a **Processor** of data held within **Human Edge** facilities / cloud Infrastructure.

4. GDPR AUDIT REPORT

GENERAL DATA PROTECTION REGULATION AUDIT CHECKLIST		
LEAD AUDITOR:	Jayshree Dutta	***DIRECTIONS:*** 1. *Answer each requirement based on your current process* 2. *Refer to the relevant GDPR Article if you need further clarification on meeting the standard or requirement (if the question relates to a specific Article, it is noted to the left of the question – those without Article references are suggested requirements or guidelines from the ICO orWP29)* 3. *Use the requirement number on the Action Plan where corrective actions or mitigating controls are required*
AUDIT DATE:	July 07, 2023	
AUDIT DESCRIPTION:	Review of policy and procedure documentation to ensure alignment to GDPR**.**	

1. GOVERNANCE & ACCOUNTABILITY							
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**
1.1	24	78	Do you have a Data Protection Policy?	✓			Data Protection aspects covered in multiple policies, at the same time data protection policy has been separately documented
1.2	24	78	Do you have a Clear Desk Policy?	✓			Clear desk policy in place and the same is documented

1.3	24	78	Do you have a Remote Access Policy?	✓			Remote access policy is documented and implemented. Remote access is via secure VPN connection.
1.4	32	78	Do you have Data Breach Incident & Notification Policy &Procedures?	✓			Incident management procedure has been documented detailing the handling of PII breaches.
1.5	24	78	Do you have a Records Management & Data Retention Policies?	✓			Data handling and storage policy is in place
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**
1.6	24	78	Do you have an Information Security Policy?	✓			Information security policy statement has been documented and hosted on the website. Apart from the above other IS security policies related to human resource, access control, physical, network, communications, secure development have been documented and implemented.
1.7	32	--	Do you have a documented Business Continuity Plan?	✓			Business continuity plan is documented.
1.8	24	78	Do you have documented procedures for obtaining, processing & storing personal data?	✓			Data handling and storage policy is implemented.
1.9	24, 25, 28, 32	74, 77, 78, 81, 83	Have you implemented appropriate technical and organizational measures to protect data & reduce risks?	✓			Required technical & organizational measures are in place including, data encryption, data retention, risk assessment, DPIA etc
1.10			Have you conducted an Information Audit?	✓			Internal audit has been conducted taking into account ISO 27001 requirements and GDPR

1.11			Does your Information Audit contain: - ● What personal data you hold? ● Where it came from? ● Who you share it with? ● Legal basis for processing it? ● What format(s) is it in? ● Who is responsible for it?	✓			Personal data is collected and processed as per the signed contract with the client. Presently there is no sensitive data being collected. Data comes directly from data subjects and secure APIs provided by the controller. Data is shared with the Data Controller, authorized parties by Data controller and internal authorized employees for data processing. Data is being processed as per legal requirements. Data is received over secure email which is encrypted upon storage. DPO is responsible for handling of PII.
1.12	4, 24, 28	74, 81	Have you assessed and documented whether you are a 'Data Controller', 'Data Processor' or both?	✓			**Human Edge** is a data processor and as per the customer requirement **Human Edge** in-house developed product access to various tolls are allotted as per the contract
1.13	25, 40, 42, 43	98, 99, 100	If you have obligations under any data protection Codes of Conduct or Certifications, do you disseminate these codes/requirements to all staff?	✓			No relevant data protection codes of conduct apply.

1.14	88	155	Have your HR policies and procedures been reviewed (and if applicable, revised) to ensure that employee's individual rights under the GDPR are considered and complied with?	✓			Yes, procedures and policies are in place related employee on-boarding (Back ground verification, employment contracts, health & safety, employee rights NDAs, induction programmes, trainings) and off – boarding (asset handing over).
2. DATA PROTECTION OFFICER (DPO							
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**
2.1	37	97	Have you allocated responsibility for data protection compliance to a designated person (i.e. DPO or suitable individual)?	✓			Yes, As part of CFT responsibilities.
2.2	38	97	Does the Data Protection Officer (DPO) have sufficient access, support and the budget to perform the role?	✓			Required support is provided by the top management.
2.3	38	97	Has the DPO identified, created and disseminated reporting lines for the data protection governance structure?	✓			As part of CFT Team DPO is defined. The regular reporting is during the management review meetings held bi-annually or whenever there are changes in the processes or people or hierarchy structure, infra etc. The emergency reporting structure is in case of a data breach.
2.4	38	97	Are all employees aware of the DPOs appointment & contact details?	✓			Yes, DPO contact has been shared on the privacy policy, available on the public domain
2.5	38	97	If the DPO has other tasks and duties, have they been assessed to ensure there is no conflict of interest?	✓			Non- conflicting role as a DPO.

2.6	37, 39	97	Has the DPO been assessed & verified as having adequate professional qualities and expert knowledge of data protection and the ability to fulfill the tasks referred to below? ● To inform and advise the business, management, employees & third parties who carry out processing, of their obligations under the GDPR ● To monitor compliance with the GDPR and with the firm's own data protection objectives ● Assignment of responsibilities, awareness-raising and training of staff involved in processing operations ● To provide advice where requested as regards the data protection impact assessment and monitor its performance ● To cooperate with the Supervisory Authority ● To act as the contact point for the Supervisory Authority on issues relating to processing	✓			DPO has undergone a general awareness training programme on GDPR and has planned to undergo training programme on GDPR Security Professional
2.7	38	97	Is the DPO bound by secrecy and/or confidentiality?	✓			DPO has signed a Confidentiality Agreement with **Human Edge**
2.8	37	97	Have you published the contact details of the Data Protection Officer?	✓			Yes, DPO contact has been shared on the privacy policy, available on the public domain
2.9	37	97	Have the DPO's contact details been communicated to the Supervisory Authority?			✓	Presently **Human Edge** is established in India. So no communication is sent to supervisory authority in Europe.
2.10	38	97	Does the DPO have access to suitable training materials, courses and workshops to support and improve their role & knowledge?	✓			DPO has access to the GDPR material available on the public domain.
2.11			Have reporting mechanisms been developed between the DPO and senior management?	✓			Yes The regular reporting is during the

							management review meetings held bi-annually or whenever there are changes in the processes or people or hierarchy structure, infra etc. The emergency reporting structure is in case of a data breach.
3. PRIVACY BY DESIGN & SECURE PROCESSING							
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES** **REVIEW DATE**
3.1	32	---	Are daily data backups performed and all back-ups kept in a secure, restricted access location?	✓			Back up and restoration testing policy is in place, required backups are being taken on AWS cloud.
3.2	24, 25, 28, 32	28,29, 78, 83	Do you utilize pseudonymisation and/or encryption methods to secure personal data?	✓			All Data is encrypted during the transit via SSL/TLS 1.2 During storage PII data is encrypted.
3.3	24, 25, 28, 32	28,29, 78, 83	Do you ensure that pseudonyms and their personal identifiers and/or encryption methods and their secret keys, are always kept separate and secure?	✓			Database is in AWS and encrypted
3.4	25	78	Do you advocate data minimization& only obtaining and processing the minimum information necessary for the purpose specified?	✓			No irrelevant data processed. Data is collected lawfully with definite purpose. **Human Edge** maintains the record of processing
3.5	25	78	Is data collected by electronic means (i.e. forms, website, surveys etc) minimized sonly the relevant fields are used, as relevant to the processing purpose?	✓			Data is collected though the website and in line GDPR principles

3.6	24, 25	78	Do you have documented destruction procedures in place for information that is no longer necessary, surplus to requirement or part of an individual's consent withdrawal or right to erasure?	✓			Policy for secure media disposal and policy for data handling and storage is available.
3.7	24, 25	78	If you must use hardcopy data for storing or processing, do you use redaction methods where possible to ensure data minimization?			✓	No hard copies of PII data are maintained.
3.8	24, 25	78	Do you enforce strong passwords across your organisation?	✓			Yes strong passwords are implemented (Min.8 characters, alpha numeric)
3.9	24, 25	78	Are passwords to networks, computers, backups, servers etc changed frequently?	✓			Yes, they are being changes in each frequency as detailed in access control policy for source code, AWS console. Access to production servers is via2 factor authentication/MFA.
3.10	24, 25	78	Do you restrict access to personal information to only those employees processing the data?	✓			Role based Access control policy has been implemented and is limited to DevOps team.
3.11	25, 32	78, 83	Do you activate strong security defaults on all systems and networks?	✓			Yes, password policy, session time out, account lock out etc has been implemented. Policies for the same are documented.
3.12	32	83	Do you carry out frequent audits & reviews to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services?	✓			Bi- annual internal audits have been planned.
3.13	32	83	Do you have documented; robust & tested business continuity plans to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident?	✓			Business Continuity Plan has been documented. Disruption scenarios have been identified, against which the testing shall be done.

							Testing shall be conducted at least once in a year. **Human Edge** doesn't have any data available in physical; all data are being stored in AWS Cloud.
3.14	24, 25, 32	83	Do you have a documented audit & review process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing?	✓			Annual internal audits have been planned.
4. PRINCIPLES & PROCESSING ACTIVITIES							
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**
4.1	5	39, 60	Is personal information: - ● Processed lawfully, fairly and in a transparent manner? ● Collected for specified, explicit and legitimate purposes only? ● Adequate, relevant and limited to what is necessary? ● Accurate and, where necessary, kept up to date ● Kept only for as long as is necessary and only for the purpose(s) which it is processed? ● Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage?	✓			Data Privacy policy is documented. Data is collected and processed as per the contractual agreement with the controller. **Human Edge** maintains the record of PII collected on project basis. Data archiving is done as per the contractual agreement with the controller and / or as legally required to be maintained. Data is being processed as per legal requirements. Appropriate security measures like employment agreements, NDAs with employees processing the personal data, encryption, availability of data at DR site etc.
4.2	32	75, 76, 77	Have you carried out a risk assessment to identify, assess, measure and monitor the impact(s)of processing?	✓			Risk register and data protection impact assessment has been documented.

4.3	30, 32	82	Do you carry out internal audits of all processing activities?	✓			Annually
4.4	6	40-50	Do you identify and establish the legal basis for all personal data that you process?	✓			The present legal basis is Reasonable security practices and procedures for sensitive personal data or information rules 2011 under Indian IT act 2000
4.5	9	51-56	If you process special category, is it in compliance with one or more of the Article9 (2) conditions?	✓			No special data is being processed presently.
4.6a	30	13, 82	If you employee less than 250 people, do you maintain records of all processing activities where: - ● Processing personal data could result in a risk to the rights and freedoms of individual? ● The processing is not occasional? ● You process special categories of data or criminal convictions and offences?			✓	Organization does not employee any EU citizens.
4.6b	30	82	If you employee more than 250 people and act in the capacity as a controller (or a representative), do your internal records of the processing activities carried contain: - ● Your full name and contact details and the name and contact details of the Data Protection Officer? ● Where applicable, details of any joint controller and/or the controller's representative? ● The purposes of the processing? ● A description of the categories of data subjects and of the categories of personal data? The categories of recipients to whom the personal data has or will be disclosed (including any recipients in third Countries or			✓	Organization does not employee any EU citizens.

			international organisations)? ● Where applicable, transfers of personal data to a third country or an international organisation (including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)? ● Where possible, the envisaged time limits for erasure of the different categories of data? ● A general description of the processing security measures you have in place?				

NO	ARTICLE	RECITAL	REQUIREMENT	YES	NO	N/A	AUDITORS NOTES
4.6c	30	82	If you act in the capacity as a processor (or a representative) on behalf of a controller, do your internal records of the categories of processing activities carried out, contain: - ● Your full name and contact details? ● The full name and contact details of each controller on behalf of which you are acting? ● The name and contact details of the Data Protection Officer? ● The categories of processing carried out on behalf of each controller ● Where applicable, transfers of personal data to a third Country or an international organisation (including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)?			✓	**Human Edge** works in the capacity of a processor and all the activities are listed in the RoPA

			● A general description of the processing security measures you have in place?				
4.7	30	82	Do you ensure that the above records are: - ● Maintained in writing? ● Provided in a clear and easy to read format? ● Readily available to the Supervisory Authority upon request?	✓			**Human Edge** works in the capacity of a processor and all the activities are listed in the RoPA **Human Edge** presently is operating in India only. There is no supervisory authority in India. In case **Human Edge** Consumer Analytics operates in EU, then the supervisory authority within the EU shall be selected by the **Human Edge** and the reporting to the same shall happen
4.8	6	40-50	Prior to obtaining & processing personal information, do you carry out are view to verify compliance with one or more of the lawfulness of processing conditions?	✓			All the PII information collected in the platform is collected lawfully
5. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)							
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**
5.1	35	84, 90	When processing is likely to be high risk or cause significant impact to a data subject, do you carry out Data Protection Impact Assessments (DPIA)?	✓			**Human Edge** has conducted the DPIA based on PII processed.

5.2	35	84, 90	Do you have a process and screening questions for determining whether a DPIA is required?	✓			Yes, Data Protection Impact Assessment is conducted
5.3	35	84, 90	Does this process utilize the Article 35 definitions of high risk processing?	✓			Yes, Data Protection Impact Assessment is conducted in line with Article 35 requirements
5.4	24		Do you have documented policies & procedures for completing a DPIA?	✓			Yes, there data protection impact assessment process is documented
5.5	35, 39		Is the DPO always involved in the assessment and mitigating action plan?	✓			Yes, DPO is involved in conducting DPIA
5.6	35	90	Does the DPIA contain: - ● A systematic description of the envisaged processing operations? ● The purposes of the processing? ● Where applicable, the legitimate interest pursued by the controller? ● An assessment of the necessity and proportionality of the processing operations in relation to the purposes? ● An assessment of the risks to the rights and freedoms of data subjects? ● The measures envisaged to address the risks (inc. safeguards, security measures and mechanisms to ensure the protection of personal data)?	✓			Yes, the required parameters are available in the DPIA.
5.7	35		Where appropriate, do you seek the views of data subjects or their representatives on the intended processing?	✓			Explicit consent is taken by the data subject and privacy policy is updated with the needful information

NO	ARTICLE	RECITAL	REQUIREMENT	YES	NO	N/A	AUDITORS NOTES
5.8	35, 36	90	Are mitigating measures proposed & actioned to reduce the impact of the risk?	✓			Required mitigation measures are being adopted in the risk register.
5.9			Are all DPIAs documented in writing?	✓			DPIA has been conducted at the organizational level.
5.10	35		Where there is a change to the risk posed by processing, is a review of the DPIA carried out?	✓			There is a process for reviewing the DPIA in case of any changes in the process, technology, PII type collected.
5.11	36	94, 96	Where measures fail, or cannot mitigate the risk, do you consult the Supervisory Authority prior to processing where a DPIA indicates that the processing would result in a high risk?	✓			Appropriate security and process level controls are implemented. The controls which are due implementation are updated in the risk register

5.12	36	94, 96	If consulting the Supervisory Authority, do you provide: - ● The respective responsibilities of the controller (if applicable)? ● Joint controllers and processors involved in the processing (if applicable)? ● The purposes and means of the intended processing? ● The measures and safeguards provided to protect the rights and freedoms of data subjects? ● The contact details of the Data Protection Officer? ● The data protection impact assessment? ● Any other information upon request?			✓	No contact been established with the supervisory authority yet, since business has operation only in India.

6. CONSENT & INFORMATION DISCLOSURES							
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**
6.1	7	32, 42, 43	Are you always able to demonstrate that consent has been given?	✓			Yes consent is recorded
6.2	7, 12	32, 42, 60	Where processing is based on consent, is the request in a clear and transparent format, using plain language and avoiding any illegible terms or jargon?	✓			Yes, consent is recorded. Explicit consent is taken at the time of data collection

6.3	7, 12	42	Is the request in an easily accessible format with the purpose for data processing attached to that consent?	✓			Yes	
6.4	7	42	Where consent is requested in the context of a written declaration which also concerns other matters, is the request always presented in a manner which is clearly distinguishable from the other matters?	✓		✓	Yes, Data subject access request procedures are established	
6.5	7, 17	42, 65	Is the data subjects' right to withdraw consent at any time made clear?	✓		✓	Yes, Data subject access request procedures are established	
6.6	7	42, 65	Is the process for withdrawing consent simple, accessible and quick?	✓		✓	Yes, Data subject access request procedures are established	
6.7	8	38	Where personal information is obtained and/or processed relating to a child under 16 years (13 years for DP Bill in UK), do You ensure that consent is given and documented by the holder of parental responsibility over the child?			✓	**Human Edge**doesn't collect any children's data	
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
6.8	8, 12	38, 58	Where services are provided to children, does your communication information and privacy notice provide clear & plain information that is easy to understand by a child?			✓	**Human Edge** doesn't collect any children's data	
6.9			When physically collecting personal information (i.e. face-to-face, telephone etc), are supporting scripts used to remind staff of the conditions for consent and an individual's right to be informed?			✓		

6.10	7		Do you have clear audit trails to evidence consent and where it came from?	✓			Yes consent is recorded
6.11	13, 14	42, 60, 61	Do you utilise a Privacy Notice/Policy (on your website, contracts, emails etc) to ensure compliance with the conditions for consent and information disclosure rules?	✓			Yes, Privacy Policy is updated on the website
6.12	13	42, 60, 61	Where personal data is collected directly from the data subject, do you ensure that the below information is provided at the time of consent: - Identity and contact details of the controller(or controller's representative)? Contact details of the Data Protection Officer? Purpose of the processing and the legal basis for the processing? The legitimate interests of the controller or third party? Any recipient or categories of recipients of the personal data? Details of transfers to third country and safeguards? Retention period or criteria used to determine the retention period? The existence of each of data subject's rights? The right to withdraw consent at anytime, where relevant? The right to lodge a complaint with a supervisory authority? Whether the provision of personal data par to Statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data?	✓			Yes all the provisions are made to ensure GDPR principles are followed

6.13	14	61	Where personal data has not been obtained directly from the data subject, do you ensure, in addition to the above disclosures, that you also provide: - The categories of personal data? The source the personal data originates from and whether it came from publicly accessible sources?			✓	**Human Edge** doesn't collect any data indirectly	
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
6.14			Do you test, review &; audit Privacy Notices to ensure adequacy, effectiveness and data subject understanding?	✓			Yes all the provisions are made to ensure GDPR principles are followed	
6.15			Are final Privacy Notices authorised by Senior Management/Director and the DPO before being activated?	✓			Yes all the provisions are made to ensure GDPR principles are followed	
6.16	7, 13, 14	32	Is the Privacy Notice displayed clearly and prominently?	✓			Yes all the provisions are made to ensure GDPR principles are followed	
6.17	7, 13, 14	32	Are individuals asked to positively opt-in?	✓			Yes all the provisions are made to ensure GDPR principles are followed	
6.18	7, 13, 14	32	Does the Privacy Notice give the individual sufficient information to make an informed choice?	✓			Yes all the provisions are made to ensure GDPR principles are followed	
6.19	7, 13, 14	32	Does the Privacy Notice explain the different ways that you will be using the personal information?	✓			Yes all the provisions are made to ensure GDPR principles are followed	

6.20	7, 13, 14	32, 60	Have you provided a clear and simple way for individuals to indicate that they agree to different types of processing?	✓			Yes all the provisions are made to ensure GDPR principles are followed
6.21	7, 13, 14	32	Does the Privacy/Consent Notice include a separate un ticked opt-inbox for direct marketing?	✓			Yes all the provisions are made to ensure GDPR principles are followed
6.22	6, 7, 13, 14	32	Does your Privacy Notice clearly define the lawful basis for processing?	✓			Yes all the provisions are made to ensure GDPR principles are followed

7. DATA SUBJECT NOTIFICATIONS, REQUESTS & COMMUNICATION

NO	ARTICLE	RECITAL	REQUIREMENT	YES	NO	N/A	AUDITORS NOTES
7.1	12	60	Where you act on a data subjects request under Articles 15 to 22, do you provide information on the actions taken in writing (i.e. data erasures, rectifications etc)?	✓			**Human Edge** has implemented procedure to handle Data subject request. However, have not received data subject request
7.2	12	58, 60	For information disclosures (Articles 13 & 14) and communications relating to Articles 15-22 & 34, are responses and information sent to individuals in a concise, transparent, intelligible and easily accessible form?	✓			**Human Edge** has implemented procedure to handle Data subject request. However, have not received data subject request
7.3	12	59	Is requested/required information sent free of charge (unless a specific GDPR requirement states otherwise)?	✓			**Human Edge** has implemented procedure to handle Data subject request. However, have not received data subject request

7.4	12	59	Is requested/required information sent within 30 days of receiving the data subjects' request/action?	✓			**Human Edge** has implemented procedure to handle Data subject request. However, have not received data subject request
7.5	12	59	Whereitisnotpossibletocomplywiththe30-daytimeframe for responding, do you inform the data subject(s) of the extensionwithin30daysofreceiptoftherequest,together with the reasons for the delay?	✓			**Human Edge** has implemented procedure to handle Data subject request. However, have not received data subject request
7.6	12	59	If you do not act on a request under a right exemption, do you inform the data subject within 30 days, of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy?	✓			**Human Edge** has implemented procedure to handle Data subject request. However, have not received data subject request
7.7	12	58, 60	Where communicating with a data subject, is the content always clear and using plain language?	✓			**Human Edge** has implemented procedure to handle Data subject request. However, have not received data subject request
7.8	12	58, 60	When requesting access to information or exercising a right, is the information provided to the individual in writing and/or by electronic means (where appropriate)?	✓			**Human Edge** has implemented procedure to handle Data subject request. However, have not received data subject request
7.9	12	64	If the data subject requests access to processing information and this is to be provided orally, do you verify the individual's identity by other means first?	✓			**Human Edge** has implemented procedure to handle Data subject request. However, have not received data subject request

7.10			Have you reviewed all existing data subject request processes and time frames and updated them to comply with the new deadlines and GDPR timeframes?	✓			**Human Edge** has implemented procedure to handle Data subject request. However, have not received data subject request
7.11	12, 15	59, 63	Do you have dedicated procedures for handling subject access requests and request refusals?	✓			**Human Edge** has implemented procedure to handle Data subject request. However, have not received data subject request
8. DATA SUBJECT RIGHTS							
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**
8.1	15	63, 64	Where a data subject exercises their Right of Access, do you ensure that they are provided with: - ● The purposes of the processing? ● The categories of personal data concerned ● The recipients or categories of recipient to whom the personal data has / will be disclosed? ● Whether the personal data has / will be transferred to a third countries or international organizations? ● Pursuant to the above, the right to be informed of the appropriate safeguards used? ● The envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period? ● The existence of the right to request rectification or erasure of personal data?	✓			Data Subject request procedure has been established to cater to Data Subject Rights

			● The existence of the right to restrict processing of personal data or to object to such processing? ● The right to lodge a complaint with a supervisory authority? ● Where the personal data was not collected directly from the data subject, information as to the source? ● The existence of automated decision-making (inc. profiling) and details of the logic involved, as well as any Significant/envisaged consequences of such processing?				
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTE**
8.2	16	65	Do you have a process for rectifying inaccurate personal data and/or completing incomplete personal data completed (inc supplementary statements)?	✓			Process is in place to rectify any in accurate data

8.3	17	65, 66	Where a data subject exercises their Right to Erasure, do you check the request against the below list before complying? ● The personal data is no longer necessary in relation to the purposes for which it was collected. ● The data subject with AWS consent on which the processing is based. ● The personal data has been unlawfully processed. ● The personal data must be erased for compliance with a legal obligation. ● The personal data has been collected in relation to the offer of information society services. ● The data subject objects, on grounds relating to their particular situation, to processing of concerning them which is based on points(e)or(f)ofArticle6(1). ● The data subject objects to the processing pursuant to Data being processed for direct marketing purposes.	✓			Process is in place to erase the data
8.4	17	65, 66	Where the data subject has a valid request to have personal data erased and that data has been made public, do you take every reasonable step, to request the erasure by such controllers of any links to ,or copy or replication of ,those personal data?	✓			Yes
8.5	18	67	Where the accuracy of the personal data has been contested by the data subject, do you restrict processing for a period to enable verification of the accuracy of the personal data?	✓			Yes

NO	ARTICLE	RECITAL	REQUIREMENT	YES	NO	N/A	AUDITORS NOTES	REVIEW DATE
8.6	18	67	Where processing is no longer necessary or lawful, do you have a process for restricting processing where requested this over erasure?	✓			Yes Data retention policy is established	
8.7	19	66	Do you notify any third party also processing such information about the restriction? (using the data from your Information Audit)			✓	No 3rd party involved. All the data on cloud is managed by **Human Edge**	
8.8	21		Where a data subject exercises rights of erasure, objection or rectification, do you restrict processing for a period to enable verification of the validity of the request?	✓			Done on the notification from the data controller.	
8.9	18	67	Do you ensure that where a data subject has obtained restriction of processing, they are informed in writing before the restriction is lifted?	✓				
8.10	20	68	Where possible, do you retain copies of personal data in a structured, commonly used and machine-readable format to comply with the Right to Data Portability?	✓				
8.11	20	68	If requested by a data subject, do you transmit personal data to another controller in a machine-readable format?	✓				
8.12	22	71, 72	Do you avoid using solely automated processing (inc profiling) in your decision-making processes, unless consent has been given by the data subject?			✓	No automated processing is conducted by **Human Edge**	
8.13	12	59	Do you have procedures and controls in place to ensure that all personal information can be provided electronically?	✓			Processes are in place to provide the data electronically	

8.14	21	70	Can individuals object to having their personal information processed for direct marketing?	✓			Yes	
9. TRANSFERS, SHARING & THIRD PARTIES								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
9.1	28	81	If you use a third party to process any personal information (e.g. I.T Services, HR Providers etc), do you carry out due diligence checks prior to selection?	✓			Cloud service providers like AWS are used for processing. Supplier management policy in place for supplier selection. **Human Edge** takes into consideration the following before on-boarding any supplier: Consent, Brand name, years of experience, legal conformances, any possible associated risks.	

9.2	28, 32	81	Do you have compliant Service Level Agreements (SLAs) and contracts with each third party processor, which outline: - ● Required skill, competency and knowledge? ● The processors data protection obligations? ● Your expectations, rights and obligations? ● The processing duration, aims and objectives? ● The data subjects' rights and safeguarding measures? ● The nature and purpose of the processing? ● The type of personal data & categories of data subjects? ● Frequency & type of ongoing due diligence & monitoring?	✓			Required SLAs/ contractual agreements in place and signed with the suppliers. Data Protection Agreement is in place covering all the required aspects
9.3	28, 32	81, 83	When transferring or disclosing personal information, do you encrypt the data and only send what is necessary?	✓			
9.4	32		Do you use secure data transfer methods for communications (i.e. emails, website forms, online payments)?	✓			All data is being transferred only over https.
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**

9.5	28, 32	78, 79, 81, 83	When sharing or disclosing personal information, do you carry out a data sharing assessment and identify and record: - ● The benefits and risks of sharing the data ● The objectives and goal of sharing ● What information needs to be shared ● Who requires access to the shared personal data ● How should it be shared ● Encryption methods and data minimization tools ● How to assess and monitor that the sharing is achieving its objectives? ● Due diligence checks of the entity or individual who will receive the personal information?			✓	No sharing or disclosure of data takes place without consent from the data controller.
9.6			Is the DPO (or appointed suitable individual) and I.T Manager/Department involved in the setup of any personal data transfers?			✓	No sharing or disclosure of data takes place without consent from the data controller. However, DPO shall be involved along with the authorized IT person when the data shall be transferred.

9.7	45, 46, 47, 48	101-107	Do you only effect a transfer of personal data to a third country or international organisation (outside of the EU), where one or more of the below conditions applies? **1.** Where the Commission has decided that the third country/organisation ensures an adequate level of protection (Adequacy Decision) **2.** In the absence of an Adequacy Decision, where you have provided appropriate safeguards and have ensured that enforceable data subject rights and effective legal remedies for data subjects are available **3.** With Supervisory Authority authorization, transfers can take place where there are:- **(a)** Contractual clauses between the controller (you) or processor and the controller, processor or the recipient of the personal data in the third country or international organisation? **(b)** Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights?	✓			No sharing or disclosure of data takes place without consent from the data controller.

NO	ARTICLE	RECITAL	REQUIREMENT	YES	NO	N/A	AUDITORS NOTES
9.8	45	101-107	Where relying on an Adequacy Decision by the Commission, do you regularly check notices and publications for withdrawals/changes of decisions?	✓			https://ec.europa.eu/info/law/ law-topic/data-protection/data-transfers- outside-eu/adequacy- protection-personal-data-non-eu-countries_en
9.9	46, 47	108, 109, 110	Do you ensure that where you are transferring pursuant to appropriate safeguards being in place, as referred to in 9.6; that one or more of the below is used? ● A legally binding and enforceable instrument between public authorities or bodies ● Binding corporate rules ● Standard data protection clauses adopted by the Commission ● Standard data protection clauses adopted by a Supervisory Authority and approved by the Commission ● An approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards,			✓	**Human Edge** is a data processor, data transfer only happens post consent from the data controller. Any clauses or binding agreements is the duty of the data controller. **Human Edge** ensures that required security measures like encryption are adopted while any data is being transferred.

			including as regard data subjects' rights ● An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights				
9.10	47	110	Where you rely on binding corporate rules to data transfers outside of the EU, do you ensure that they are: - ● Legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees? ● Expressly confer enforceable rights on data subjects with regards to the processing of their personal data?			✓	**Human Edge** is a data processor, data transfer only happens post consent from the data controller.
10. TRAINING & COMPETENCY							
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**
10.1	70, 39, 47		Do you educate all employees & management about the GDPR requirements and principles & the possible impact of non- compliance?	✓			Verified training records for the employees on major aspects of the GDPR. Last training has been conducted for Cross functional team members. Verified the training records for the same. Training has been conducted by an empaneled consultant.

10.2	70, 39, 47		Do you have an effective data protection training program in place?	✓			Information security training has been conducted for the CFT and other employees during induction and as a refresher training programme based on ISO/IEC 27001 & ISO 27701 standard.
10.3	70, 39, 47	136, 97	Does your data protection training program cover: - ● GDPR scope & principles? ● Measures & controls for protecting data & minimizing risks? ● Data Protection Officer Duties? ● Supervisory Authority role and scope? ● Codes of Conduct and/or Certifications? ● Privacy Impact Assessments(PIA)? ● Information Audits? ● Processing Activities & Conditions? ● Conditions for Consent & Privacy Notices? ● Data Subject Rights & subject Access Requests? ● Third Country or International Organisation Transfers ● Reporting Lines & Notifications? ● Privacy by Design (i.e. data minimization, pseudonymisation & encryption)?	✓			Training programme is developed covering the major aspects of GDPR.
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**
10.4	70, 39, 47	136, 97	Do you use assessment testing and/or 1:2:1 mentoring to assess and verify and evidence employee knowledge & understanding of the GDPR?		✓		Assessment testing programmes need to be developed for GDPR

10.5	70, 39, 47	136, 97	Do you provide employees with training evaluation forms so that training is effective and adequate?	✓			Training evaluations are done for information security training program based on ISO 27001. The evaluations are in the form of judgment by the immediate supervisor/HOD based on their on job performance/ understanding.
10.6	70, 39, 47	136, 97	Are staff with direct personal data processing duties provided with support, guidance and additional training regarding the GDPR requirements?	✓			Verified training records for the employees on major aspects of the GDPR. Last training has been conducted for Cross functional team members. Verified the training records for the same. Trainings need to be planned for GDPR covering all the employees.
10.7	70, 39, 47	136, 97	Do employees sign confidentiality agreement and/or non-disclosure forms?	✓			All employees have signed confidentiality agreement and/or non- disclosure forms
10.8	70, 39, 47	136, 97	Do you have a Training & Development Policy?	✓			There is a procedure for employees' recruitment, training and separation.
10.9	70, 39, 47	136, 97	Do employees have training records, files and annual training assessments?	✓			Training records are being maintained in the form of training attendance records
10.10	70, 39, 47	136, 97	Are employees advised of their own rights under the GDPR?	✓			Not at present, as the training on the major aspects of GDPR has only been provided to the cross functional team members
10.11	70, 39, 47	136, 97	Do you have a GDPR awareness program in place for ensuring that employees understand the new Regulation prior to it coming into effect?	✓			Not at present, as the training on the major aspects of GDPR has only been provided to the cross functional team members.

11. BREACH MANAGEMENT							
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**

11.1	34	86, 87, 88	Do you have documented data breach procedures?	✓			Information security and PII breach Incident management procedure is in place
11.2			Are all staff made aware of the reporting lines for breaches?	✓			Information security and PII breach management procedure details the reporting lines.
11.3	34	86, 87, 88	Do you maintain a data breach register and record all breaches, regardless of severity or impact?	✓			There have no breaches in the past. Provisioning is there to record all the breaches in Incident reporting form and Security Incident report.
11.4			Is the breach register reviewed by the DPO monthly to look for patterns or duplicated issues?	✓			There have no breaches in the past. Provisioning is there for lesson learnt from the incidents.
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**
11.5	34	86, 87, 88	Are all breaches investigated and corrective actions taken, regardless of the size or scope?	✓			There have no breaches in the past. Provisioning is there in the Information security and PII breach to take corrective actions.
11.6	34	86, 87, 88	Where a data breach has been assessed by the DPO and deemed likely to result in a risk to the rights and freedoms, do youreportthebreachtotheSupervisoryAuthoritywithin72 hours?			✓	There have no breaches in the past.
11.7	34	86, 87, 88	***Where notifying the Supervisory Authority ,does the report include:-*** ● A description of the nature of the personal data breach? ● The categories and approximate number of data subjects concerned?			✓	There have no breaches in the past.

			● The categories and approximate number of personal data records concerned? ● The name and contact details of the Data Protection Officer (or other POC where more information can be obtained)? ● Description of the likely consequences of the personal data breach? ● Description of the measures taken/proposed to address the personal data breach? ● Measures to mitigate any possible adverse effects?				
11.8	34	86, 87, 88	Are high risk breaches reported to the data subject and the above points covered in a clear & easy to read format?	✓			Procedures are in place. However, **Human Edge** has did not face any data breach in the past
11.9	28, 34	86, 87, 88	Where you use external processor(s),do you ensure that agreementshaveprovisionsformeetingthe72-hour notification deadline if there is a breach?	✓			Yes

TO BE COMPLETED BY THE AUDITOR

Have all questions been completed? Yes

Print Name: BQC ASSESSMENT PVT. LTD. Authorised Signatory

Date: July 07, 2023

AUDIT REPORT SUMMARY

Human Edge Advisory Services Pvt. Ltd (Human Edge) working as a Processor is found to have effectively implemented the requirements of GDPR. Required security policies and practices found to be documented and implemented.

PII being processed is non sensitive in nature and presently **Human Edge** is serving the customers in India, however the required GDPR practices as controller are available and are well adopted by **Human Edge Advisory Services Pvt. Ltd (Human Edge)**