Data Protection Policy

January 2023

Table of Contents

Our Data Protection Policy is produced in consideration of Article 24 General Data Protection Regulation (GDPR) as follows:

'1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 (above) shall include the implementation of ***appropriate data protection policies*** *by the controller.'*

1. Purpose & Scope

1.1 Purpose

1.1.1 Our Data Protection Policy (DPP) underpins our commitment as an organisation to produce the most ethical, effective and accurate facial recognition technology on the global market whilst safeguarding the rights of data subjects. We recognise that the manner by which personal data is processed by the technology we produce, and by those who operate it has implications for the human rights of citizens across the world wherever it may be used, including, but also beyond the right to privacy. Our ethical values drive our corporate mission. They are published on our open source web site and can be accessed at the following link; https://www.corsight.ai/trust-center/

1.1.2 Our Mission as a responsible organisation is to produce AI as a force for good to the benefit of the world which our algorithms help to shape, and in a manner which delivers security and respect for the human rights of citizens everywhere..

1.1.3 The publication of our DPP builds upon guidance that we produce to help safeguard the rights of data subjects. For example; our 'Privacy Manual' sets out how to operate our technology and its inherent 'Privacy Controls' in a manner which helps mitigate risk of disproportionate intrusion to others.

1.1.4 The purpose of our DPP is to provide transparency and enable responsible accountability by setting out how we manage personal data across our data processing activities. It informs as to the relevant standards, provisions and safeguards which we apply to our data processing activities wherever such processing takes place by any of the entities which comprise Corsight AI. The DPP also set out the rights of individuals who are data subjects, how those rights may be exercised and how we are held to account for compliance with our statutory responsibilities for processing personal data. We believe that publishing our DPP will help foster greater trust and confidence in others as to the integrity of our data processing activities and the technology that we produce.

1.2 Scope

1.2.1 The following key considerations are addressed within the scope of this policy;

a) An explanation as to the data privacy obligations and commitments of Corsight AI
b) Our employees' responsibilities as entities of Corsight AI and accountability for managing data privacy and security;
c) The rights of individuals who are data subjects and how they will be managed;
d) How Corsight AI addresses complaints and queries regarding data privacy and security;
e) How to contact Corsight AI regarding any matters contained within these BCRs.

1.2.2 There are many and varied data privacy laws which govern how Corsight AI processes personal data in those countries and jurisdictions in which our business entities are located, registered or otherwise operate across the globe.

1.2.3 In our view, the United Kingdom (UK) and European Union (EU) currently provide for the highest standards of data privacy laws which is the GDPR. Its provisions include statutory requirements which are applicable to the transfer of personal data outside of the UK and the European Economic Area (EEA) to entities in other countries around the world, and also transfers internally within our business wherever our entities are located around the world.

1.2.4 The transfer of personal data is only allowable in the context of the GDPR where appropriate safeguards have been established which are at least the equivalent to those required by that particular legislation, and where the mechanisms which are to be used have been approved by the relevant data Supervisory Authority. The standards provided by the GDPR are therefore adopted as the high standard of consistency which applies throughout Corsight AI. All legal references to 'articles' or otherwise within this policy should be taken as referring to 'articles' of the General Data Protection Regulation unless explicitly set out as being otherwise.

1.2.5 The DPP applies to all personal data processing activities by Corsight AI and all of its entities as a data controller for our own purposes. The nature of the data concerned includes recruitment, employment, marketing, correspondence and details of individuals who engage with, or are engaged by our business.

2. Application of the Data Protection Principles

2.1 Key Data Protection Principles

2.1.1 Article 5 of the GDPR sets out the key principles which lie at the heart of the UK GDPR. They are the foundation upon which our DPP is established. They are each explained in terms of their applicability in the following paragraphs of this section. In brief, they are as follows;

1. Lawfulness, fairness & transparency;
2. Purpose limitation;
3. Data minimisation;
4. Accuracy
5. Storage limitation
6. Integrity & security
7. Accountability

2.2 Lawfulness, Fairness and Transparency (1)

2.2.1 Corsight AI processes personal data only where it is necessary pursuant to a valid lawful basis which is set out in the UK GDPR, the nature of which we record, explain to data subjects and set out in our Privacy Notice before processing activity is conducted. We will only process personal data where one of the following conditions applies;

a) The individual has given clear consent to the processing;
b) Processing is necessary for a contract which we have with the individual or because they have asked us to take specific steps before entering in to a contract;
c) The processing is necessary to comply with the law or with a legal obligation which our company is subject to;
d) The processing is necessary to protect someone's life;
e) The processing is necessary for us to perform a task in the public interest or for our official functions for which there is a clear basis in law;
f) The processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's data which overrides those legitimate interests.

2.2.2 We provide individuals with information to explain how their data is processed in accordance with law to ensure fair and lawful processing. The information is set out in our Privacy Notice which is made accessible to everyone by being displayed upon our public facing internet site. It is provided in clear and easily understandable language.

2.2.3 In addition, all email correspondence conducted by our employees contains a clear and easily readable notice which fairly and transparently sets out our data privacy obligations and directs recipients to our privacy notice by means of a clearly highlighted hyper-link.

2.2.4 We understand the importance of individuals having the right to know how we process personal data and to verify that such processing is lawful. The information which we therefore provide to data subjects in respect of our processing also includes the following;

a) The name and address of the relevant data controller together with their contact details;
b) The contact details of the Data Protection Officer;
c) The legal basis upon which we rely for the processing of data and the purpose for which we are processing it;

2.3 Purpose Limitation (2)

2.3.1 Under the terms of the UK GDPR purpose limitation is a requirement that personal data be collected for specified, explicit, and legitimate purposes, and not be processed further in a manner incompatible with those purposes (Article 5(1)(b).

2.3.2 The entities of Corsight AI only collect personal data for those specific and legitimate purposes which explicitly set out in our Privacy Notice. We process the personal data of data subjects fairly for those purposes and we ensure that personal data is accurate, up to date and not otherwise processed in any way which may not be compatible with those purposes.

2.4 Data Minimisation, Accuracy & Storage (3 &4)

2.4.1 Our business entities take all reasonable steps so as to ensure that your personal data is;

a) Accurate and up to date with regards the purposes for which it has been collected;

b) Adequate, not excessive and relevant in relation to the purposes for which it has been collected;
c) Not maintained in an identifiable form for longer than is necessary for the purposes for which it has been collected;
d) Only retained for purposes and periods permitted by applicable data protection law;

2.5 Integrity and Security (5)

2.5.1 Corsight AI applies appropriate administrative, procedural and technical means to protect the integrity and security of the personal data that we process from unlawful and inappropriate, intentional or accidental, access, alteration, disclosure, destruction or loss. This applies whether the personal data is stored, transferred or otherwise processed by us.

2.5.2 Personal data is retained securely and confidentially and access to it is limited by our procedures to only those who may legitimately need to have access to it in accordance with law and in connection with the business of Corsight AI. Our systems employ state of the art security. They are "*secure by default"* and "*secure by design"* which means that our security approaches are systemic and that systems which consume, process, store and share data have high levels of security embedded within them. We are proud to hold Cyber Essentials and UK Secure by Default (Fortify) which demonstrates this commitment.

2.5.3 The measures which we apply to the security of personal data takes into account the sensitivity of the information, the risk, context, scope and impact upon data subject rights. These may include the following measures where it is considered to be a legitimate and appropriate undertaking;

a) Encryption
b) Pseudonymisation
c) Safeguards which ensure the confidentiality, integrity, availability and resilience of our systems and services;
d) Safeguards for our business continuity which ensure our ability to restore the security, availability and access to personal data in the event of a physical or technical incident; Procedures for testing and evaluating the effectiveness of our security measures, whether physical, human or technical.

2.5.4 Our Data Protection Officer (DPO) is notified whenever a Corsight AI business entity suspects or identifies that a breach of data security has taken place. The full facts are investigated and reported to the DPO who then considers the necessary action to take including determining whether the known facts require the ICO to be notified.

2.6 Accountability of Corsight AI Entities

2.6.1 Our business entities are accountable for ensuring that they act responsibly and in accordance with our DPP. They are responsible and accountable for meeting our standards regarding the maintaining of auditable records of processing activities including data transfer activities, the nature and categories of data processed, the recipients and contact details of persons receiving the data, security measures applied, adhering to data storage/retention periods, implementing data protection measures, identifying and reporting risks of non-compliance and data breaches internally.

2.7 Onward Data/International Transfers

2.7.1 Personal data is transferred between our business entities both inside and outside of the jurisdictions covered by the GDPR in a manner which ensures a consistency of security and legitimacy in accordance with applicable data protection law and as set out within this policy.

2.7.2 We do not generally transfer personal data to third parties for processing. In the event that such a transfer becomes necessary and justifiable within the terms of the GDPR, those third parties are not bound by this policy. We therefore require in such circumstances a written agreement with those third parties which ensure that the personal data which they receive from us and process is protected by adequacy of law and safeguards which protect the privacy of data subjects to a standard which is consistent with the GDPR and in any event in compliance with our obligations which arise in such circumstances from Article 46 UK GDPR.

2.8 Processing of Special Category Data

2.8.1 Corsight AI processes 'special category data' as part of its business. Article 9 GDPR describes special category data as being personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2.8.2 The nature of the special category data processed by our business is the creation of a 'biometric mask' which is established by our algorithms where they identify and network the features of a human face which is placed within the focus of the system. The resulting biometric mask is unique to any given individual. Once a 'biometric mask' has been established of any person, that person can be later identified by our algorithms by comparing the biometric mask it has scanned against others stored within its database.

2.8.3 The GDPR is very clear that the processing of special category data is generally prohibited unless one of several proscribed factors apply to the processing activity. We ensure that our processing activities are based upon the following lawful grounds;

> *'The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provides that the prohibition ……. may not be lifted by the data subject;*

2.8.4 We process special category data in the three following circumstances:

a) Training the FR algorithms. - We ethically source images of humans from a broad and balanced representative diaspora and use those for our algorithms to learn how to recognise a human face and in a manner which mitigates risk of inaccuracy and bias.
b) Testing the FR algorithms. We rigorously test our algorithms by using the images we obtained and those of our own personnel so as to ensure that the algorithms perform to high levels of accuracy and consistency. We also undertake testing processes to identify potential areas of risk, understand how they may occur and take restorative action to mitigate or remove any risk identified.
c) Demonstrating the performance of our FR algorithms. - Our facial recognition technology is ethically produced and the nature of our business is such that we regularly are called upon to demonstrate its performance. Examples of such actions include submitting our technology to independent and accredited testing bodies, providing demonstrations at exhibitions, conferences, to clients and potential clients and other third parties who may

be acting as a procurement agency rather than an end user. We readily acknowledge and will readily meet our responsibilities to make the capabilities of our technology available to the ICO, other statutory regulators and judicial scrutineers where such access is reasonably required.

2.8.5 We have completed a Data Protection Impact Assessment (DPIA) in respect of the above processing activities which is kept under review and amended when necessary by the DPO who ensures that it remains up to date and relevant. The DPIA is made available on our publicly facing web site so that individuals may consider its content.

2.9 Explicit Consent

2.9.1 We obtain the explicit consent of those whose special category data we process where this is a requirement within the law.. We ensure that explicit consent, where it is given, involves a specific, informed and unambiguous indication of the individual's wishes. Information is provided to data subjects as to what the data will be used for, their rights are explained to them and an explanation provided that they do not have to consent and where they do so they may withdraw their consent at any time. In such circumstances the processing of their special category data will stop, any data obtained will be deleted and the circumstances will be reported to the DPO who may decide upon any further action necessary.

2.9.2 Information is provided in clear and easily understood terms and language.

2.9.3 We do not process the personal data or any special category data of children as part of our processing activities.

3. The Rights of Data Subjects and the Means of Exercise.

3.1 Data Subject Rights

3.1.1 Data subjects have the following rights which are enforceable by law, a relevant GDPR supervisory authority and the courts, wherever their personal data is processed by any Corsight AI entity;

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

3.2 The Right to be Informed

3.2.1 Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. We will provide privacy information to individuals at the time we collect their personal data from them. Where we obtain personal data from other sources, we will provide individuals with privacy information within a reasonable period of obtaining the data. We will not provide this information if an

individual already has the information or if it would involve a disproportionate effort to provide it to them. The information we provide to people will be concise, transparent, intelligible, easily accessible, and it will be provided in clear and plain language. We regularly review, and where necessary, update our privacy information and will bring any new uses of an individual's personal data to their attention before we start the processing.

3.3 The Right to Access

3.3.1 Data subjects have the right to access and receive a copy of their personal data, and other supplementary information that we hold about them (more commonly referred to as a subject access request or 'SAR'). Individuals can make SARs verbally or in writing or via a third party. We will perform a reasonable search of the requested information for which we will not charge a fee. Information will be disclosed to you securely in a manner which is clear, concise and intelligible. Ordinarily we will respond without delay and within one month of receipt of the request. We may extend the time limit by a further two months if the request is complex or if we receive a number of requests from the individual, in which case we will inform you of the extended time frame. We may refuse to provide the information if an exemption or restriction applies, or if the request is manifestly unfounded or excessive.

3.4 The Right to Rectification

3.4.1 Data subjects have the right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. Individuals can make a request for rectification verbally or in writing and we will respond to requests within one month of having received your request. If we require further time we will inform you of this together with the reasons. We may refuse a request which is manifestly unfounded or excessive in our view.

3.5 The Right to Erasure

3.5.1 The right for individuals to have personal data erased is commonly referred to as being 'the right to be forgotten.' You may request erasure of your personal data where the personal data is no longer necessary for the purpose which we originally collected or processed it for; we are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent; we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing; we are processing the personal data for direct marketing purposes and the individual objects to that processing; we have processed the personal data unlawfully; or we have to do it to comply with a legal obligation.

3.5.2 The right to erasure does not apply if processing by us is necessary to exercise the right of freedom of expression and information; to comply with a legal obligation; for the performance of a task carried out in the public interest or in the exercise of official authority; for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or for the establishment, exercise or defence of legal claims.

3.5.3 Where we are required by law to process individuals' personal data, then the right to erasure will not apply.

3.6 The Right to Restrict Processing

3.6.1 Individuals have the right to request the restriction or suppression of their personal data so as to limit the way that we use their data. This is an alternative to requesting the erasure of their data and applies in circumstances where the individual contests the accuracy of their personal data and we are verifying the accuracy of the data; the data has been unlawfully processed and the individual opposes erasure and requests restriction instead; we no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim; or the individual has objected to us processing their data under Article 21(1), and you are considering whether our legitimate grounds override those of the individual.

3.6.2 We may refuse any request which is manifestly unfounded or excessive.

3.7 The Right to Data Portability

3.7.1 The right to data portability means that data subjects have the right to receive personal data, (but only the personal data which they have provided to us), in a structured, commonly used and machine readable format. This right includes a right to request that we transmit your personal data directly to another controller. This right only applies where our lawful basis (Article 6) for processing this information is one of 'consent' or otherwise for the performance of a contract; and we are carrying out the processing by automated (not paper hard copy) means. We may not agree with a request where we believe that to do so would adversely affect the rights and freedoms of others. In such circumstances we will justify to you in writing why these reasons are legitimate.

3.8 The Right to Object

3.8.1 Individuals have the right to object to the processing of their personal data at any time to stop or prevent us from processing in relation to all of the personal data we hold about them, to certain information or to a particular purpose we are processing the data for. The right to object only applies in certain circumstances such as where our processing is for direct marketing purposes; a task carried out in the public interest; the exercise of official authority vested in us; our legitimate interests (or those of a third party). If we are processing data for scientific or statistical purposes, the right to object is more limited. Individuals must give specific reasons why they are objecting to the processing of their data. We may refuse to comply with any request where we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims. We may also refuse to comply with a request if it is manifestly unfounded or excessive.

3.9 Rights Related to Automated Decision Making Including Profiling

3.9.1 Corsight AI will ensure that you are not subject to decisions based solely on automated processing of your personal data, including profiling which produces legal effects or similar significant effects, unless the processing is necessary for entering into or performing a contract between you and Corsight AI; is authorised by a law to which Corsight AI is subject and which also lays down suitable measures to safeguard your rights and freedoms and legitimate interests; or is based on your explicit consent to such processing. Where such circumstances arise, we will give individuals specific information about the processing; take steps to prevent errors, bias and discrimination; and give individuals rights to challenge and request a review of the decision.

3.9.2 We implement suitable measures to safeguard your rights and freedoms and legitimate interests, particularly the right to obtain human intervention, to express your point of view and to contest the decision. These methods are regularly tested by our entities to ensure that they remain fair, effective and unbiased. As well as restricting the circumstances in which we carry out solely automated individual decision-making we will provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual; use appropriate mathematical or statistical procedures; ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it; correct inaccuracies and minimise the risk of errors; and secure personal data in a way that is proportionate to the risk.

3.10 Means of Exercise

3.10.1 Individuals may exercise any or all of their rights as described in the preceding paragraphs simply by contacting our DPO by email and setting out the nature of their request.

3.10.2 We will respond to all requests made by individuals within one calendar month of a request having been received by Corsight AI. Where we require more time to respond fully to a request for example due to complexities associated with providing it, we will notify you of this eventuality and provide our reasoning for requiring further time within the above timeframe of one calendar month.

3.10.3 In any event, recognising that exceptional circumstances may exist in some cases, we will strive in so far as is reasonably practicable to ensure that all requests will be completed within a maximum time frame of three calendar months regardless of complexity and will provide you with a realistic alternative date.

3.10.4 Where we determine that we will not take any action to meet a request this will only be where an exemption is provided for by law and applies to the request made. In this eventuality we will inform you about our reasons for not taking action; your right to make a complaint to the ICO; and your right to seek a judicial remedy.

3.10.5 We will also provide information where we request a reasonable fee or need additional information from the person exercising their rights or any other source. Individuals may also have the right to make a complaint to a supervisory authority and also the right to seek judicial remedy at any time.

4. How Information is Provided

4.1 Providing Information

4.1.1 Corsight AI maintain a public facing web site which contains a broad range of information in respect of our ethical credentials and also our human rights centric mission to produce facial recognition technology as a force for good to the benefit of societies whilst protecting human rights of citizens. https://www.corsight.ai/trust-center/

4.1.2 This DPP is published openly and available on the public facing web site of Corsight AI

4.2 Information Collected Regarding Data Subjects

4.3.2 We shall provide to data subjects all information required of us by law within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

4.3.3 Where Corsight AI intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information unless;

a) the data subject already has the information;
b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89 (1). In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

5. The Role & Tasks of Designated Data Protection Officer

5.1 Key Functions

5.1.1 In accordance with Article 37(c) Corsight AI has appointed a DPO because the core activities of the data controller may consist of the processing on a large scale of special categories of data as described at Article 9.

5.1.2 The role of the DPO includes the following functions;

a) Monitor and audit compliance of Corsight AI entities with the terms of these BCRs and applicable data protection legislation;
b) Direct, assist, inform, assign responsibilities, train and advise Corsight AI entities as to their obligations under the terms of these BCRs and applicable data protection legislation;
c) Keep the content of this policy under review, ensuring that they remain effective and fit for the purposes for which they were established, making amendments or changes where necessary in consultation with the ICO supervisory authority;
d) Being a single point of contact between Corsight AI and the ICO and other regulatory supervisory authorities;
e) To cooperate with the ICO and other regulatory supervisory authorities.

5.1.3 The DPO is appointed to the role by the executive board on the basis of professional qualities including expert knowledge of data protection law and practices, and the ability to fulfil the above referred undertakings.

5.1.4 The DPO is supported in his/her role by the Chief Executive and the board of Corsight AI and company lawyers. The role has a network of data, privacy and surveillance specialists to add value to the role.

6. Complaint Procedures and Verification of Compliance

6.1 Complaint Procedures

6.1.1 Where any person wishes to submit a complaint or exercise their rights as set out in the UK GDPR or otherwise in relation to this policy, they may do so by making contact with our DPO.

6.1.2 Our DPO will respond to all requests made by individuals within one calendar month of a complaint or verification of compliance having been received by Corsight AI. Where we require more time to respond fully to a request for example due to complexities associated with providing it, we will notify you of this eventuality and provide our reasoning for requiring further time within the above timeframe of one calendar month. In any event, recognising that exceptional circumstances may exist in some cases, we will strive in so far as is reasonably practicable to ensure that all requests will be completed within a maximum time frame of three calendar months regardless of complexity and will provide you with a realistic alternative date.

6.1.3 Individuals also have the right to make a complaint to a supervisory authority and the right to seek judicial remedy. More information as to these matters may be found on our Privacy Statement which you may visit online.

6.2 Verification Procedures

6.2.1 In accordance with Article 47(2)(j) we have measures in place which enable us to verify that the terms of this policy is being complied with by our entities. Those measures include;

- data protection audits;
- spot checks by the DPO;
- departmental discussions with DPO;
- internal feedback and reporting mechanisms
- monitoring reports of risk, breach, good practice and successes;
- content and quality of engagement with a relevant supervisory authority

6.2.2 The results of such verification activities are assessed by the DPO who is responsible for reporting such matters to the senior executive of the organisation and identifying/implementing restorative action where required.

6.2.3 The results of our audit activities are made available upon request to a relevant supervisory authority.

7. Making Changes to the Data Protection Policy

7.1 Reporting & Recording Procedures

7.1.2 Where the DPO identifies that there is a requirement to change any content of this policy either as a result of his/her verification or other activities or by being informed by any party, they shall make a record of the change required and the reason(s) for them being necessary.

Thereafter the DPO is responsible for establishing what the amendment should be in consultation with the senior executive and company lawyers as considered appropriate.

8. Cooperation Mechanisms with Relevant Supervisory Authorities

8.1 Point of Contact with Relevant Supervisory Authorities

8.1.1 The DPO is the point of contact between Corsight AI and relevant supervisory authorities. For the purpose of this policy a 'relevant supervisory authority' shall be taken as meaning the regulatory authority which has responsibility for regulating data protection legislation in any given jurisdiction.

8.1.2 Corsight AI will cooperate to the full extent required by the GDPR with relevant authorities. We will comply with lawful instruction, act upon advice and guidance, facilitate access for the purpose of investigation, audit or checking as to our compliance with relevant data protection legislation.

8.1.3 In the event that a relevant supervisory authority determines that a breach of applicable data protection law has occurred by a Corsight AI entity in the context of its data protection responsibilities we will cooperate fully with that supervisory authority and abide by its findings, subject to the right to exercise a reasonable defence challenge or appeal to the extent provided by law in appropriate cases.

9. Reporting Mechanisms Regarding Adverse Effect

9.1 Conflict of Laws & Adverse Effect

9.1.1 Where any entity of Corsight AI has reasonable ground to believe that a law to which it is subject in any jurisdiction in the world, either prevents, inhibits or otherwise adversely influences our ability of to meet any requirement of this DPP or our wider data protection obligations, the circumstances will be notified internally to the DPO as soon as is reasonably practicable. The DPO will consult with the senior executive and lawyers to identify the risk and make appropriate decisions.

9.2 Relationship between this policy and National Laws

9.2.1 Where any data protection legislation is applicable to an entity of Corsight AI and requires higher level of safeguards to be applied to the processing of personal data that that provided by the GDPR, then that higher level shall apply and the relevant data protection laws in that jurisdiction will take precedence.

10.The Provision of Training

10.1 General Provisions

10.1.1 All our business entities who have permanent or regular access to personal data, or are likely to do so as part of their role, are provided with appropriate awareness training in relation to their responsibilities to protecting personal data.

10.1.2 The training provision is delivered by the DPO to all of our people and at a level which is proportionate to the nature of the particular functions which they undertake, the nature and extent of their access to personal data, and the risks applicable to the inherent sensitivities of the data and the processing activities.

10.1.3 Training content includes the UK GDPR, relevant data protection legislation, human rights legislation, ethics and the details of these BCRs. Appropriate training and reference material is made available to all personnel who additionally have access to company resources and these BCRs.

10.1.4 Training provision is mandatory for all Corsight AI entities. Compliance is monitored by the DPO and any shortfalls are reported to the senior executive. The DPO is responsible for ensuring that training provision remains up to date, relevant and effective.

10.1.5 We provide awareness which is both relevant and adequate to those who operate the technology which we provide to them as end users. The nature of the training that we provide is intended to help end users to satisfy themselves as to the data protection credentials of our organisation and of our technology. In doing so it is our expectation that end users in turn will meet their own particular obligations, statutory or otherwise in respect of data protection and thereby establish their own measures and safeguards to deliver legitimacy, legality and equality wherever our technology is used by them, and for which they are responsible and liable.