Data Protection Policy

Document Ref No	DP-01
Version No	V1.0
Last review date	15/08/2022
Approved by	Harry Mongini
Next review	15/08/2023

Table of Contents

1. Introduction

Faces Consent Limited (Faces) is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of Faces Employees and Third Parties in relation to the collection, destruction, disclosure, retention, transfer and use of any Personal Data.

Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process it. Non-compliance may expose Faces to complaints, regulatory action, loss of revenue, fines and/or reputational damage.

Faces expects all Employees and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanctions.

2. Purpose, scope and users

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

This policy has been designed to establish a baseline standard for the processing and protection of Personal Data. Should national law impose a requirement, which is stricter than imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to.

3. Definitions

Consent – Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

Data Controller – A 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.

Data Processors – A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.

Data Protection – The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.

Data Protection Authority – The independent Public Authority responsible for monitoring the application of the relevant Data Protection regulation set forth in national law.

Data Subject – The identified or Identifiable Natural Person to which the data refers. Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Employee – An individual who works part-time or full-time for Faces under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.

Personal Data – Any information (including opinions and intentions) which relates to a Data Subject.

Personal Data Breach – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

Process – Any operation or set of operations performed on Personal Data or on sets of Personal Data. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Restricted Transfer - A transfer which is covered by Chapter V of the UK GDPR.

Special Categories of Data – Personal data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Third Country – Any country outside of the EEA (European Economic Area) not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

Third Party – An external organisation with which Faces conducts business and is also authorised to process the Personal Data.

Profiling – Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to a Data Subject. To analyse or predict certain aspects concerning their performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

4. Governance

4.1. Data Protection Officer

Under the General Data Protection Regulation, an organisation **must** appoint a DPO if:

- They are a public authority or body (except for courts acting in their judicial capacity);
- Their core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- Their core activities consist of large-scale processing of special categories of data or data relating to criminal convictions and offences.

At this moment in time Faces does not fall into any of the above categories and therefore are not required, by law, to appoint a Data Protection Officer. This will be reviewed annually.

4.2. Policy Dissemination & Enforcement

Faces must ensure that all Employees, Directors and Consultants responsible for the Processing of Personal Data are aware of and comply with the contents of this policy.

In addition, Faces will ensure that all Third Parties engaged to Process Personal Data on their behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data.

4.3. Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

4.3.1. Data Protection Impact Assessments

Faces must ensure that a Data Protection Impact Assessment (DPIA) is conducted for all new and/or revised systems or processes for which it has responsibility. Where applicable, Faces will assess the impact of any new technology uses on the security of Personal Data.

4.3.2. High Risk to the Data Subject

Where the data protection impact assessment indicates that the processing would result in a high risk to the rights and freedoms of the Data Subject and where suitable organisational and technical measures are not implemented, Faces may be required to inform the relevant Data Protection Authority.

4.4. Compliance Monitoring

To confirm that an adequate level of compliance is being achieved in relation to this policy, Faces will carry out an annual Data Protection compliance audit. Each audit will, as a minimum, assess:

- Compliance with Policy in relation to the protection of Personal Data, including:
  - The assignment of responsibilities.
  - Raising awareness.
  - Training of Employees.
- The effectiveness of Data Protection related operational practices, including:
  - Data Subject rights.
  - Personal Data transfers.
  - Personal Data incident management.
  - Personal Data complaints handling.
- The level of understanding of Data Protection policies and Privacy Notices.
- The currency of Data Protection policies and Privacy Notices.
- The accuracy of Personal Data being stored.
- The conformity of Data Processor activities.
- The adequacy of procedures for redressing poor compliance and Personal Data Breaches.

Any deficiencies identified will be logged in the Corrective Actions Log and reported to and monitored by the Faces Board of Directors.

5. Data Protection Principles

The General Data Protection Regulation sets out seven key principles which lie at the heart of the regulations.

5.1. Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to data subjects. This means, Faces must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

5.2. Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means Faces must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

5.3. Principle 3: Data Minimisation

Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are Processed. This means Dilgram must not store any Personal Data beyond what is strictly required.

5.4. Principle 4: Accuracy

Personal Data shall be accurate, and kept up to date where possible. This means Faces must have in place processes for identifying and addressing out-of-date, incorrect, and redundant Personal Data.

5.5. Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means Faces must delete or anonymize any Personal Data as soon as it is no longer needed.

5.6. Principle 6: Integrity & Confidentiality

Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction, or damage. Faces must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

5.7. Principle 7: Accountability

The Data Controller shall be responsible for and be able to demonstrate compliance. This means Faces must demonstrate that the six Data Protection Principles (outlined above) are complied with for all Personal Data for which it is responsible.

6. Data Collection

6.1. Data Sources

Faces will obtain Personal Data only by lawful and fair means, where appropriate, with the knowledge and Consent of the individual concerned. Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances to protect the vital interests of the Data Subject or another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

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

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

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

6.2. Data Subject Consent

Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, Faces must obtain such Consent. Systems should be established for obtaining and documenting Data Subject Consent for the collection, Processing, and/or transfer of their Personal Data. The system must include provisions for:

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

Please note that the Consent described above is required in addition to medical consent. These must not be treated the same.

6.3. Data Subject Notification

Faces will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data.

When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

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

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

6.4. External Privacy Notices

Each external website or application provided by Faces will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law. All Privacy and Cookie Notices must be approved prior to publication on any Faces external website or application.

7. Data Use

Faces uses Personal Data for the following purposes:

- The general running and business administration of Faces.
- To provide services to Faces Practitioners and Patients.
- The ongoing administration and management of customer services.

The use of Personal Data should always be considered from the perspective of the Data Subject and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a Data Subject's expectations that their details will be used by Faces to respond to a request for information about the products and services on offer. However, it will not be within their reasonable expectations that Faces would then provide their details to Third Parties for marketing purposes.

Personal Data will be Processed in accordance with all applicable laws and applicable contractual obligations. Faces will not Process Personal Data unless at least one of the following legal requirements are met:

- **Consent** - The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- **Contract** - Processing is necessary for the performance of a contract to which the Data Subject is party to or in order to take steps at the request of the Data Subject prior to entering into a contract.
- **Legal Obligation** - Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- **Vital Interests** - Processing is necessary to protect the vital interests of the Data Subject or of another natural person.
- **Public Task** - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- **Legitimate Interests** - Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected.

In any circumstance where Consent has not been gained for the specific Processing in question, Faces will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

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

7.1. Special Categories of Data

Faces will only Process Special Categories of Data (also known as sensitive data) where one of the following conditions apply:

- The Data Subject has given explicit consent.
- The Processing is specifically authorised or required by law.
- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.
- The Processing relates to Personal Data which has already been made public by the Data Subject.
- The Processing is necessary for the establishment, exercise or defence of legal claims.
- The Processing is necessary for reasons of public interest in the area of public health.
- The Processing is necessary for archiving purposes in the public interest.

7.2. Data Quality

Faces will adopt all necessary measures to ensure that the Personal Data it collects and Processes, is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by Faces to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading, or outdated, even if the Data Subject does not request rectification.

- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.
- Restriction, rather than deletion of Personal Data, insofar as:
    - a law prohibits erasure.
    - erasure would impair legitimate interests of the Data Subject.
    - the Data Subject disputes that their Personal Data is correct, and it cannot be clearly ascertained whether their information is correct or incorrect.

7.3. Profiling & Automated Decision-Making

Faces will only engage in Profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the Data Subject or where it is authorised by law.

Where Faces utilises Profiling and automated decision-making, this will be disclosed to the relevant Data Subjects. In such cases the Data Subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.
- Object to the automated decision-making being carried out.

Faces must also ensure that all Profiling and automated decision-making relating to a Data Subject is based on accurate data.

8. Data Retention

To ensure fair Processing, Personal Data will not be retained for longer than is necessary in relation to the purposes for which the data was originally collected, or for which it was further Processed. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

*****INSERT DATA RETENTION TABLE HERE ONCE ROPA IS COMPLETE*****

9. Data Protection

Faces will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the

physical or natural environment. The minimum set of security measures to be adopted is provided in the Faces Information Security Policies.

10. Individual Rights Requests

Individuals have other certain rights, not yet covered in this Policy, in respect of their own personal data: -

- **The right of access** – Data Subjects have the right to obtain confirmation that their data is being processed and to request access to that Personal data.
- **The right to rectification** – Data Subjects are entitled to have their personal data rectified if it is inaccurate or incomplete.
- **The right to erasure** – The right to erasure is also known as 'the right to be forgotten'. This enables a Data Subject to request that Faces deletes or removes their personal data where there is no compelling reason for its continued processing.
- **The right to restrict processing** – Data Subjects have the right to block or supress processing of their Personal Data where there is no compelling reason for the processing. When processing is restricted Faces will be permitted to store the Personal Data, but not further process it, and will retain just enough data about the Data Subject to ensure that the restriction is respected in future.
- **The right to data portability** – Data Subjects have the right to obtain and reuse their Personal Data for their own purposes across different services. It allows them to move, copy or transfer Personal Data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- **The right to object** – Data Subjects have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercises of official authority, direct marketing (including profiling) and processing for purposes of scientific/historical research and statistics.

If a Data Subject makes a request relating to any of the rights listed above, Faces will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing, and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject.
- The categories of Personal Data stored.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.

- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.
- The use of any automated decision-making, including Profiling.
- The right of the Data subject to:
    - object to Processing of their Personal Data.
    - lodge a complaint with the Data Protection Authority.
    - request rectification or erasure of their Personal Data.
    - request restriction of Processing of their Personal Data.

All requests received must be logged. A response to each request will be provided within 1 calendar month of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative.

If a request cannot be responded to fully within 1 calendar month, Faces must provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject, where request is excessive.
- Contact details where the Data Subject can follow up their request.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

11. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. Where the disclosure of the Personal Data is necessary for any of the following purposes:

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

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

12. Data Protection Training

All Faces Employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, Faces will provide regular Data Protection training and procedural guidance for their staff. Once training is complete, Employees may be required to complete an assessment, a minimum pass rate of 80% must be achieved. If any Employee does not achieve 80% then it may be necessary to consider any additional training requirements.

13. Data Transfers

Faces may transfer Personal Data to recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism.

Faces may only transfer Personal Data where one of the transfer scenarios listed below applies:

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

13.1. Transfers to Third Parties

Faces will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, Faces will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, Faces will enter into an appropriate agreement with the Data Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

Where the Third Party is deemed to be a Data Processor, Faces will enter into an adequate Data Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with Faces instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

Where Faces is outsourcing services to a Third Party (including Cloud Computing services), they will identify whether the Third Party will Process Personal Data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data. In either case, it will make sure to include adequate provisions in the agreement for such Processing and Third Country transfers.

Faces shall conduct regular due diligence of Processing of Personal Data performed by Third Parties, especially in respect of technical and organisational measures they have in place. Any deficiencies identified will be logged in the Corrective Actions Log and reported to and monitored by the Faces Board of Directors.

13.2. Transfers to Third Countries

In March 2022 further requirements regarding International Data Transfers were issued under Section 119A of the Data Protection Act 2018. To ensure compliance with the amendment to the Act, Faces have adopted the ICOs International Data Transfer Agreement (IDTA) and the International data transfer addendum templates.

In order to provide appropriate safeguards an IDTA must be completed to Faces making a Restricted Transfer. Any Restricted Transfers agreed prior to 21st of September must undergo an IDTA no later than the 21st of March 2024 in line with the ICO transitional provisions.

14. Complaints Handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Subject will be informed of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the Data Subject and Faces, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

15. Breach Reporting

Any suspected breach of Personal Data must be logged and investigated to confirm whether a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the relevant authorised procedure must be followed based on the criticality and quantity of the Personal Data involved. For severe Personal Data Breaches, the Faces Board of Directors will initiate and chair an emergency response team to coordinate and manage the Personal Data Breach response.

16. Document management

This policy shall be available to all Faces Employees and any Third Parties where required. The policy must be reviewed and, if necessary, updated at least once a year. Notice of significant revisions shall be provided to Faces Employees via email.

17. Version History

Summary of Change	Date of Change	Author	Version No
First Draft	15/08/2022	1T Compliance	1