Data Protection Policy V3.3

Document Control

Document Information

Document Title	Data Protection Policy
Version	V3.3
Publication Date	25/05/2018
Status	Approved
Review Date	13 January 2027

Revision History

Version	Date	Author/Reviewer	Details
V3.0	20/12/18	Qamar Sheikh	Reviewed
V3.0	06/01/20	Joe Holmes	Reviewed
V3.1	17/12/20	Qamar Sheikh	Reviewed Updated EU GDPR to UK GDPR
V3.1	06/01/21	Qamar Sheikh	Reviewed
V3.1	06/01/22	Qamar Sheikh	Reviewed
V3.2	24/01/23	Qamar Sheikh	Reviewed
V3.3	16/01/24	Qamar Sheikh	Reviewed /minor updates
V3.3	08/01/25	Qamar Sheikh	Reviewed
V3.3	09/06/25	Jo Hudson	Reviewed/updated formatting
V3.3	14/01/26	Qamar Sheikh	Reviewed

Classification

PROTECT - OFFICIAL

Legal Notice

Contents

1. Introduction 4
2. Scope 4
3. Definition of Key Terms 5
4. Responsibilities 6
5. Notification Requirements of UK GDPR 7
6. Principles of General Data Protection Regulations 7
7. Conditions for the Processing of Personal Data 8
8. Conditions for the Processing of Sensitive or Special Category Data 8
9. Rights of the Data Subject 9
10. Compliance 11
11. Point of Contact 11

1. Introduction

Data Protection is concerned with respecting the rights of individuals (data subjects) when processing their personal information. This is achieved by being open and honest with Data Subjects about the use of information about them and by following good data handling procedures. In consequence, **Data Protection is a task in which everyone has a part to play.**

The Data Protection Officer is available to assist in this task. However, they need the active help and support of all those involved.

This Policy:

- defines the Data Protection Policy for VISAV Limited in relation to the Data Protection Act 2018 (DPA) and UK General Data Protection Regulation (UK GDPR)
- explains the roles of those involved in Data Protection
- offers help and guidance to assist in the discharge of responsibilities in relation to Data Protection

The aim of this Policy is to ensure that VISAV Ltd fully complies with the requirements of UK GDPR and the DPA by identifying the procedures, duties and responsibilities to be carried out.

2. Scope

All staff have responsibilities under the UK Law to ensure that their activities comply with the Data Protection Policy.

For personal data collected by VISAV,

- Line managers have the responsibility for the type of Personal Data they collect and how they use this data
- Staff have the responsibility for not disclosing Personal Data outside VISAV's procedures, or against the lawful processing requirements of the DPA or UK GDPR

VISAV is required by the DPA to notify the Information Commissioner's Office (ICO) of the use it makes of personal data. Any member of staff who knowingly or recklessly uses, shares or transfers personal information other than as disclosed to the ICO could be prosecuted, unless there is a legal justification for example under 'whistle-blowing' legislation. The ICO has the power to issue a monetary penalty notice requiring organisations to pay up to £18 Million or 4% of gross annual turnover (whichever is higher) for serious breaches of the DPA and UK GDPR.

This policy determines the way such personal data shall be processed. Where there is any doubt as to the purpose of way personal data should be processed, the Data Protection Officer will provide guidance and can be contacted via email at mike@visav.co.uk

3. Definition of Key Terms

Data Subject

Any individual whose personal data is process by the organisation.

Personal Data

Any information that can directly or indirectly identify a Data Subject such as a name, identification number, location, an online identifier (e.g., an IP address) or specific physical, physiological, genetic, mental, economic, cultural or social identity data that can be collated into identifiable information.

The Regulations apply to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This is wider than the current definition and will include chronologically ordered sets of manual records containing personal data.

"Pseudonymisation" of data means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be identified. Personal data that has been pseudonymised, e.g., key-coded, now falls within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to an individual.

Sensitive Data or Special Category Personal Data

Sensitive data is defined as information that, if misused, could potentially lead to discrimination or harm, examples include:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data and biometric data for uniquely identifying a natural person
- Data concerning mental or physical health
- Data concerning a natural person's sex life or sexual orientation.

Criminal offence data is also considered sensitive, and is covered under UK GDPR Article 10, and must be under the control of official authority.

Data Processing

Processing of personal information or data means obtaining, recording, organising, disclosing or holding the information or data. This could include:

- organisation, adaptation or alteration of the information or data (e.g., creating categories or lists with the data that is gathered)
- retrieval, consultation or use of the information or data (e.g., profiling data subjects, sending emails)
- disclosure of the information or data by transmission or otherwise making available (e.g., sharing data with third parties); or
- alignment, combination, blocking, erasure, or destruction of the information or data.

Relevant Filing System

Any set of information relating to individuals to the extent that the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to an individual is readily accessible.

Reference should be made to the Data Protection Act 2018 for a complete list of definitions and terms.

4. Responsibilities

Data Controller

The role of the Data Controller is the legal entity which determines the purposes and means of processing personal data, in this case VISAV Limited. They decide how and why personal data is collected and used, acting as the ultimate decision-maker regarding data processing activities.

Data Protection Officer

The role of the Data Protection Officer is an individual appointed by the Data Controller (VISAV Limited) who determines the purposes and means of the processing of personal data. The Data Protection Officer is therefore responsible for implementing data protection policies and procedures and is responsible for overseeing this policy. Where data is shared outside of the VISAV, VISAV is the controller of the data processed relating to its employees or customers and as such will:

- Understand the risk to the rights and freedoms of the data subject associated with the data they hold
- Oversee the implementation of technical and organisational measures to manage these risks and to demonstrate processing is performed in accordance with the regulation
- Adhere to approved codes of conduct or approved certification mechanisms
- Use only processors who can demonstrate implementation of measures that will ensure adherence to the Regulation
- Ensure there is a contract in place that explicitly defines:
    - technical and organisational controls required to protect the data
    - nature and purpose of processing
    - transfer of data
    - authorised persons involved in processing of personal data
    - deletion or return of data

If employees have any questions about data protection in general, this policy or their obligations under it they should direct them to the Data Protection Officer via email mike@visav.co.uk

Data Processor

A natural or legal person or other body which processes personal data on behalf of the Data Controller.

It is unlikely that VISAV will become a data processor for personal information. If this situation was to occur it would be VISAV's responsibility to:

- implement appropriate technical and organisational measures to ensure processing meets the requirements of legislation and that of the Data Controller
- not engage other processors without explicit permission from the controller
- ensure there is a contract in place that explicitly defines nature and purpose of processing or transfer of data
- Only allow access to authorised persons involved in processing of personal data
- ensure the save deletion or return of data

5. Notification Requirements of UK GDPR

In the event of a personal data breach, the data controller must notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. If the notification is made after 72 hours, the reasons for the delay must be provided.

The controller shall document any personal data breaches, detailing the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the ICO to verify compliance with the regulations.

The notification shall at least:

- describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned
- communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained
- describe the likely consequences of the personal data breach
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

6. Principles of General Data Protection Regulations

The Data Protection Officer is responsible to ensure that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which

they are processed (‘data minimisation’)

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay (‘accuracy’)
- retained for no longer than necessary
- 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, using appropriate technical or organisational measures (‘integrity and confidentiality’).

7. Conditions for the Processing of Personal Data

When processing Personal Data, one (or more) of the following conditions must apply otherwise the processing is unlawful under the terms of the DPA and UK GDPR and therefore is not permitted.

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes
- processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract
- processing is necessary for compliance with a legal obligation to which the controller is subject
- processing is necessary in to protect the vital interests of the data subject or of another natural person
- 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 controller
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data

8. Conditions for the Processing of Sensitive or Special Category Data

Processing of 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 uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

Unless one of the following conditions is present:

- the data subject has given explicit consent to the processing of their personal data for one or more specified purposes, except where law provides that such data must be processed
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security or social protection law, such processing must provide appropriate safeguards to protect the fundamental rights and the interests of the data subject
- 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

- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside that body without the consent of the data subjects
- processing relates to personal data which is manifestly made public by the data subject
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- processing is necessary for reasons of substantial public interest, and proportionate to the aim pursued, respecting the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment and subject to the conditions and safeguards
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, providing suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes which shall be proportionate to the aim pursued, and must respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

9. Rights of the Data Subject

Right to information

The controller shall take appropriate measures to provide any information relating to processing of personal data to the data subject in a concise, transparent, intelligible and easily accessible form.

Right to access

The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing
- the categories of personal data concerned
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, to recipients outside of the European Economic Area or international organisations
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- the right to lodge a complaint with a supervisory authority

- where the personal data is not collected from the data subject, any available information as to their source
- the existence of automated decision-making, including profiling

Right to rectification

The data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

Right to be forgotten

The data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed
- the data subject withdraws consent on which the processing is based and where there is no other legal grounds for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing the personal data
- the personal data is to be erased for compliance with a legal obligation
- the personal data was collected in relation to the offer of information society services

Where the controller has made the personal data public it is obliged pursue to erase the personal data, taking account of available technology and the cost of implementation, the Controller shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure.

Right to restriction of processing

The data subject has the right to obtain from the controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims
- the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject

Right to notification

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data

subject about those recipients if the data subject requests it.

Right to portability

The data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format.

Right to object

The data subject shall have the right to object, on grounds relating to his or her situation, at any time to processing of personal data concerning him or her. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

The data subject has the right to lodge a complaint with the ICO if they feel their rights and freedoms are not being protected.

Right to appropriate decision making

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

10. Compliance

The Data Protection Officer (DPO) should be notified of any changes VISAV Ltd makes to the use of personal data. The DPO will then review and update VISAV Ltd.'s notification in light of such changes.

11. Point of Contact

If you have any questions, please contact the Data Protection Officer at mike@visav.co.uk