

Data Protection Policy

Aims of this Policy

Retinalyze System A/S needs to keep certain information on its users customers to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organization.

This policy covers employed staff, and users.

Definitions

In line with the Data Protection Act 1998 principles, Retinalyze System A/S will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA)

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.

Stewardship: Those collecting personal data have a duty of care to protect this data throughout the data life span.

Type of information processed

Retinalyze System A/S processes the following personal information: Images of the retina

Groups of people within the organisation who will process personal information are:
Employed staff and users

Responsibilities

The Data Controller is responsible for:

- Understanding and communicating obligations under the Act
- Identifying potential problem areas or risks
- Producing clear and effective procedures
- Notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes

All employees and users who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy will result in termination of the contract with the employee or user.

Policy Implementation

To meet our responsibilities staff will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.

Queries about handling personal information will be dealt with swiftly and politely.

Gathering and checking information

Before personal information is collected, we will consider if the information is relevant and needed.

We will inform people whose information is gathered about the following:

- Which information is collected
- Their rights

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

Data Security

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- All communication between the users and servers will be encrypted
- Physical access to servers will only be allowed by essential maintenance personal

Any unauthorised disclosure of personal data to a third party by an employee may result in termination.

Subject Access Requests

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to info@retinalyze.com

The following information will be required before access is granted:

- Full name
- Name of place where the image was taken

We may also require proof of identity before access is granted. The following forms of ID will be required:

- Passport
- Drivers license
- ID card

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request.

Review

This policy will be reviewed at intervals of 3 years to ensure it remains up to date and compliant with the law.