Guidelines for the processing of personal data by the Assumption Foundation

March, 2019

TABLE OF CONTENT

1. Introduction

The purpose of this document is to determine the guidelines for processing personal data by the Assumption Foundation (hereafter known as ”AF”).

Personal data means any information which (i) can identify a natural person, or (ii) that relates to a natural person. Examples of personal data:

- name
- address
- social security number
- gender
- email address
- phone number
- date of birth
- age
- income
- bank account
- health information
- religious belief

The list is not exhaustive.

In general, according to Danish law and EU law, any electronic processing of personal data must be done in accordance with good data processing practices.

This means, among other things, that:

- any collection and processing of personal data must be for a purpose; and
- personal data that is processed must be relevant and sufficient, and must not exceed what is required for the purposes for which the information is gathered.

It is important to note that the term ”processing” covers any form of electronic handling of personal data. Examples of processing includes: Collection, registration, systematization, storing, use, disclosure and deletion.

All board members and any employees in AF are obliged to comply with the guidelines for electronic processing of personal data described in this document.

2. Applicants for scholarships from AF

2.1 In General

Information about the applicants’ names, email addresses and phone numbers may only be stored in case processing systems..

Information about applicants may be sensitive information, as it will be information on religious matters and health information.

Therefore, particular care must be taken to treat such information legally and safely.

2.2 Application procedure

In connection with an application procedure, AF will receive personal information from applicants. AF is entitled to use such information in connection with the application procedure.

However, only relevant AF personal may have access to information about applicants.

If AF receives sensitive information from an applicant, consent must be obtained for its processing. Examples of sensitive information:

- race or ethnic origin
- political, religious or philosophical conviction
- healt information
- sexual orientation
- information on criminal matters

2.3 The distribution is effected

Once a scholarship is awarded, the AF may immediately record and process non-sensitive information about the applicant, to the extent that AF is required to use the information in the performance of the scholarship, the treatments is objective and the treatment is done in a secure and confidential manner.

The disclosure of information to independent third parties may only take place if the applicant has given express written consent.

However, disclosure of information on name, address, social security number to SKAT (the Treasury Department) can be done, to the extent that AF is legally required to do so.

With regard to sensitive information (see definition in section 2.2), it is the starting point that no electronic processing / storage is allowed.

However, processing / storage of sensitive information will be permitted if:

- The applicant has given express written consent; or
- The processing / storing is for a special purpose, for example:
  - If necessary to comply with the provisions of a law or regulation (e.g. reporting to the Treasury Department),
  - Criminal matters relating to a case on the applicant's possible fraud, or
  - In connection with a trial that involves the applicant.

2.4 After distribution

When the distribution of the scholarship has taken place, it is the starting point that the information that AF no longer has any legitimate need to keep must be deleted.

What "legitimate need" is must be determined according to an individual assessment. Examples of cases where one has a legitimate need:

- As long as there are disputes / lawsuits involving the applicant; or
- If AF considers that there is a not insignificant risk that a dispute / trial involving the applicant may arise.

Since there is a general limitation period of three (3) years, it will only be justified in special cases (or if a trial continues) to save the data for more than three years.

Information included in AF's bookkeeping must, of course, not be deleted before deletion is permitted under the Accounting Act (i.e. five (5) years after the end of the financial year in which distribution took place).

2.5 Retention of information regarding the applicants

Information about the applicants is kept in the usual case processing system on an external server at the host provider, however, so that they can only be accessed by the employee or employees who deal with distributions. A Data Processing Agreement is entered into with the host provider.

2.6 Security requirements regarding the administration of distributions

Employees or board members who handle information about applicants must have instruction and training on what to do with the information and how to protect the information.

Personal information on paper – e.g. in folders and binders – must be kept locked when not in use.

When documents (papers, index cards etc.) with personal information are to be thrown out, shredding or other action must be taken to avoid unauthorized acces to the information.

Passwords must be used to access personal computers and other electronic equipment. Only those who need access must receive a password.

The people who have passwords, must not share it with others or leave it out for others to see.

Personal data must not be stored on other portable media, e.g. on a flashdrive unless the information is protected by encryption and password.

Computers connected to the internet must have an updated firewall and virus control installed.

AF must use secure mail if the correspondence with applicants or others contains sensitive or confidential information.

In connection with the repair or service of computer equipment containing personal data and when data equipment is to be sold or discarded, appropriate measures must be taken so that information cannot come to the knowledge of any unauthorized person.

When using an external administrator to handle personal data, a written data processing agreement must be prepared.

3. Records of personal data processing activities

According to the EU Personal Data Ordinance, Art. 30, AF currently keeps a record of processing activites in the following areas:

- Distribution for AF's purpose

AF regularly assesses whether there is a need to keep records in other areas.

The records must be kept in electronic form.

The record are kept by AF's board.

4. The right to insight

Any person that AF has collected information from, has the right to gain insight into what information about the person AF has. In the event of a request for access, AF shall inform the person:

- What information is being processed,
- The purpose of the processing,
- Who will have access to the information collected, and
- Where the information comes from.

If a person approaches AF and requests insight, the request must be answered within four weeks. If this is not possible, the person requesting insight must be informed of the reason for this within the four weeks mentioned, and when the final answer can be expected.

In the case of extensive requests, it may be possible to charge a small fee.

Information that contains trade secrets or which cannot be disclosed for other specific reasons may, as the case may be, be exempted from the right to insight.

5. Data Protection Advisor

AF has not appointed a data protection advisor since AF core activities do not involve (i) regular and systematic monitoring or large scale registered persons, or (ii) large scale processing of personal information.

6. Breach of data security

6.1 In general

If it has been found that there has been a breach of data security, whereby unauthorized persons may have gained access to AF's personal data, the chairman of the board must be informed immediately.

6.2 Reporting to the Data Inspectorate

In the event of a breach of data security, where unauthorized persons have gained access to AF's personal data, the Data Inspectorate (www.datatilsynet.dk) must be notified as soon as possible (and no later than 72 hours after the fact). The notification must at least:

(i) Describe the nature of the breach of personal data security, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

(ii) Provide the name and contact details of the AF contact with which additional information may be obtained;

(iii) Describe the likely consequences of the breach of personal data security;

(iv) Described the measures taken or proposed by the controller to address the breach of personal data security, including, where appropriate, measures to limit its potential adverse effects.

AF must document any breach of personal data security, including the facts of the breach of personal data security, its effects and the remedial actions taken. .

6.3 Reporting to registered persons

In the event of a breach of data security where unauthorized persons have gained access to AF's personal data, AF shall promptly notify the persons whose information has been compromised.

The notification must describe the character of the breach of personal data security and must at least:

(i) Provide the name and contact information of the AF contact with which additional information may be obtained;

(ii) Describe the likely consequences of the breach of personal data security;

(iii) Describe the measures taken or proposed by the controller to address the breach of personal data security, including, where appropriate, measures to limit its potential adverse effects.

Approved at the board meeting of March 26, 2019

BOARD OF DIRECTORS

Annelise Bruus, Chairman	Claus Nybro Bonde, Vice chairman
Johnny Roj-Larsen	