Guidelines for processing of personal data at Rygaards School

21 January, 2019

TABLE OF CONTENTS

1. Introduction

The purpose of this document is to determine guidelines for the processing of personal data at Rygaards School (hereafter listed as ”Rygaards”).

By personal data we mean any type of data that, (i) can identify a physical person, or (ii) that concern a physical person. Examples of personal data:

- Name
- Nationality and mother tongue
- Contact information for parents, including address and phone number
- Year group
- Grades
- Biometric data, including photos
- Deposit information
- Leaving certificate
- Result of admissions test
- Health information
- Possible medication consumtion
- Possible allergies
- Possible reports from previous schools
- CPR number
- Gender
- Picture ID (passport or driving license)
- Birth date
- Age
- Income
- Bank account
- Religious conviction (Catholic or not)
- Criminal record/Child record
- Job title
- Salary and pensions
- Results of personality tests
- Courses, skills profile and employee performance record
- Vacation time and other absences
- Tax information of staff
- Information of relevance to wage withholding

The list is not comprehensive.

In general, according to Danish and EU legislation, the processing of personal data should be done in accordance with good computing practice.

This involves, among other things, that:

- Any gathering and processing of personal data must be done for professional purposes; and
- The personal data that is processed must be relevant and sufficient, and not extend beyond the scope of the purpose they were gathered for.

It is important to take notice that the concept of processing covers any form of electronic handling of personal data. Examples of processing include: Gathering, registration, systematization, storage, use, disclosure and erasure.

All members of the board and the staff of Rygaards School are required to comply with the guidelines for processing of personal data laid out in this document.

2. Staff

2.1 Before hiring – recruitment procedure

In connection with the recruitment procedure, Rygaards School will receive personal data from the applicants. Rygaards is justified in using this data in connection with the recruitment procedure.

However, only the relevant members of staff will be granted access to data concerning possible applicants.

If you wish to obtain a reference from an applicant, the applicant must give his or her explicit, written consent to it (optionally through email).

If Rygaards finds it necessary to gather sensitive information, such as health information, the applicant must give his or her explicit, written consent.

If an external recruitment agency is used, it is Rygaards' responsibility to ensure that the agency complies with the law, as the agency acts on behalf of Rygaards. In such cases, Rygaards must enter into a data processing agreement with the agency.

If Rygaards receives sensitive information from an applicant, further electronic processing can only be done after the applicant has given written consent. Examples of sensitive information includes:

- race or ethnic origin
- political, religious or philosophical conviction
- union membership
- health information
- sexual conviction
- criminal record
- Biometrick data, including photo

If these types of information are received in paper form, they may not be transferred to digital form. If they are received electronically, they must be saved in the format they are received in (for example in an email, if received as an email), but they must not be transferred to a different format for electronic data processing, for example to a spread sheet or a different data base.

Once the recruitment procedure is concluded, the information may be stored for 3 years after refusal for documentation purposes, to show that the employment is done on the correct legal basis.

If Rygaards wishes to save an application for use with any subsequent appointments, Rygaards must submit a written (email) inquiry to the applicant and obtain his or her explicit consent to save the application.

2.2 During employment

Once the terms of employment have been established, Rygaards may continue to register and process non-sensitive information about the employee, to the extent that the information is necessary to employment, the processing is done objectively and in a way that is safe and confidential. This does not require consent.

If Rygaards wishes to put a photo of the employee on the school's website, that requires written consent.

Transmission of information on name, address, social security number, bank account and tax information is made to the school's payroll system with UV data, which handles salary calculation, payroll etc. A written data processing agreement has been entered into between Rygaards and UV-data.

As a rule, the electronic processing and storage of sensitive information (see definition in section 2.1) is not allowed. Processing and storing sensitive information will only be allowed when:

(i) The employee gives express, written consent; or

(ii) If the processing/storage is done for a special purpose, such as:

a. If it is necessary in order to comply with the law (for example health information in connection with sickness benefits),

b. Health information in connection with a case of work injury,

c. Criminal matters in connection with a case of employee embezzlement or other crime, or

d. In connection with a trial that involves the employee, or

e. As long as it is necessary for a legal claim to be enforced, defended or determined

If the employee informs Rygaards about sensitive information (see definition under section 2.1) during an employee development interview, the employee must sign the minutes of the interview and at the same time give consent to the information being kept for continued development of the employee.

Copy of pay check for union delegate

If the union delegate requests a copy of pay checks for a salary check or salary negotiations, these can be provided in an anonymous version.

If the pay check is to be handed out in a non-anonymous version, the employee must consent to that.

2.3 After the resignation

When an employee has resigned, it is the basic policy of Rygaards that the data we no longer have a legal need to keep, must be deleted. What "legal need" is must be determined by an individual assessment. Examples of cases with a legal need include:

(i) as long as any customer or competition clause is in force;

(ii) as long as there are disputes / lawsuits, that involve the employee; or

(iii) if Rygaards considers that there is a not insignificant risk that a dispute / lawsuit involving the employee may arise.

Since there is a five-year expiration date on any pay claim, if will only be legal in special cases (or if a lawsuit is ongoing) to save data for more than five years.

Information, included in Rygaards accounting, must be deleted following the accounting law (meaning five years after the end of the financial year, of when the employee resigned).

After a resignation, the former employee's e-mail account may only stay active for 12 months; and only one or a few trusted employees may have access to the account.

Is it not necessary to delete the e-mail account – making it inactive is enough (so it is no longer possible to send e-mails to or from the account).

2.4 Storing of information regarding employees

Information about employees are stored in personal folders on the school's server, and are only accessible by the employees who deal with employee relations.

2.5 Safety regarding employee administration

Employees handling personal data must receive instruction and training on what they are allowed to do with that data, and how to protect it.

Hard copies of personal information – for example in folders and binders – must be kept under lock and key, when they are not in use.

When documents (papers, index cards, etc.) containing personal information are to be thrown out, shredding or other measures must be used to prevent unauthorized access to the information.

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

Those with a code, must not share it with others or leave it lying around for others to see.

Personal information must not be stored on portable media, such as flash drives or external cloud based services like Dropbox or Google Drive.

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

In connection with the repair and servicing of computer equipment containing personal data and when electronic equipment is to be sold or discarded, appropriate measures must be taken so that personal information is not shared with unauthorized people.

When using an external data processer to process information, a written data processing agreement must be compiled.

3. Students and their parents

3.1 In general

Information about students' and parents' names, addresses and e-mail addresses must be stored in a case management system.

Applicant information can be of a private nature, since there is information about religious convictions as well as health information. Therefore, particular care must be taken to treat such information legally and safely when processing it.

Rygaards has established a secure e-mail account for receiving sensitive information.

3.2 Application procedure

In connection with the application procedure, Rygaards will receive personal information about parents and possible students. Rygaards is justified in processing such information in connection with the application procedure.

Only relevant people at Rygaards must have access to information about parents and possible students, however.

In situations where Rygaards receives sensitive information from parents and possible students, further electronic data processing must not be done without explicit, written consent. Examples of sensitive information includes:

- Nationality and mother tongue
- Religious conviction (Catholic or not)
- Health information
- Sexual relations
- Criminal record
- Biometric data, including photo

It is permissible to use situation photos on the school's Facebook page and on parent intra without gathering consent. Use of portrait photos requires consent, however.

When the application procedure is concluded, all the information gathered about applicants who did not achieve admission to the Rygaards, will be kept for 3 years from the date of notification of rejection, since it is necessary documentation to prove that the rejection was justified.

3.3 Acceptance and ongoing administration

When a student has been accepted to Rygaards, Rygaards is justified in registering and processing non-sensitive information about the student and their parents, to the extent that the information is necessary to fulfill the agreement on school fees, and processed objectively and safely in a confidential manner

Regular personal data is transferred to a number of collaborators. The school ensures that all information is stored and processed according to good computing practice and has processor agreements with all collaborators.

Transferring information about name, address and CPR number to the Ministry of Education may occur, as Rygaards is legally obligated to do so.

With regards to sensitive information (see definition in section 3.2) it is policy not to process or store this information electronically. Processing / storing of sensitive information is allowed if:

- The student's parents have given express, written consent; or
- Processing / storing is done for a special purpose, for example:
  - If it is necessary to follow the law (for example reporting to the Ministry of Education),
  - Criminal matters relating to a case, or
  - In connection with a lawsuit that involves the student and/or their parents, or
  - As long as it is necessary for a legal claim to be enforceable, defended or determined

A status report of consent for each student will be done on a yearly basis.

Rygaards keeps a list of students who are not wanted at the school, such as previous students who have been expelled or deemed unfit to be accepted at Rygaards.

3.4 After the expiry of the agreement

Student information that Rygaards is no longer legally required to keep, must be deleted once a student leaves the school.

What is "legally required" must be determined after an individual assessment. Examples that would constitute legal requirement:

- For as long as Rygaards is under legal obligation in order to comply with the provisions of a law (for example reporting to the Ministry of Education),
- For as long as disputes / law suits concerning the student or their parents are active; or
- If Rygaards considers that there is a not insignificant risk that a dispute / trial involving the applicant may arise.

The normal expiration date is three years, and only in special circumstances (or if a trial is ongoing) would it be justifiable to keep the information for longer than the three years.

Information that is included in Rygaards' accounting, or which is required to be stored by the Ministry of Education in connection with State Aid, follow the guidelines for deletion in the accounting law, which is five years after the fiscal year that the accounting stems from.

3.5 Storing of information regarding parents and students

Information regarding parents and students are kept in a conventional case management system on an external server with our host provider. Though stored in such a way that it is only accessible to the employees who deal with administration. A data processing agreement has been entered into with the hosting supplier.

3.6 Security requirements regarding administration of personal data about parents and students

Employees and board members who handle information about parents and students, must receive instruction and training in what they are allowed to do with the information, and how to protect the information.

Personal information on paper – for example in binders and folders – must be kept under lock and key when not in use.

When documents (papers, index cards, etc.) containing personal information are discarded, shredding or other measures that prevent unauthorized access must be used.

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

The people who have a code, may not share it with others, or leave it lying around for others to see.

Personal information may not be stored on other portable media, such as flash drives, unless the information is encrypted or password protected.

Computers connected to the internet must have an up to date firewall and virus control.

In connection with repairs or service done on data equipment containing personal information, or when data equipment is sold or discarded, the necessary precautions must be made, to ensure personal information is not shared with unauthorized people.

When using an external data processor to handle information, a data processing agreement must be signed.

4. Mail system, parent intra and other forms of communication

In addition to administrating employees, students and parents, Rygaards also process personal information in connection with the ongoing operation of the school's activities, including especially the correspondence between teachers, parents and collaborators.

That correspondence must only occur via the school's mail system, as well as parent intra (with parents) and the mail system with the school's external collaborators.

Data processing agreements have been entered into with those data processors that assist the school in relation to this correspondence, including E-learning and Microsoft (Office 365).

The mailing system on parent intra guaranties continuous deletion of messages.

Rygaards has established a mailing policy that ensures mails are automatically deleted from inboxes after 90 days. Information that is relevant for the administration of staff or students respectively, are kept separately in the electronic folder of that employee or student.

Rygaards has established a secure mail for receiving confidential or sensitive information.

5. Records of personal data processing activities

According to article 30 or the EU Personal Data Regulation, Rygaards keeps a record of data processing activities in the following areas:

- Personal administration
- Student administration

Rygaards will determine on an ongoing basis, the need to keep records of other areas.

Records will be kept in digital form.

Records will be kept by Rygaards' Chief Financial Officer.

6. The right to be informed and the right to access

Any person that Rygaards has received and collected information about, has a right to be informed about and continuously gain insight into what information about the person that Rygaards holds and what consent has been given. In the case of request for insight, Rygaards must inform that person about:

- What information is being processed,
- What the purpose of the processing is,
- Who has access to the information, and where the information comes from.
- What consent has been given and the ability to revoke them.

If a person approaches Rygaards to request access to their information, that request must be answered within 4 weeks. If this is not possible, the person must be informed of the reason within 4 weeks mentioned, and whether the final answer can be expected.

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

Information containing trade secrets or which cannot be disclosed for other special reasons, may be exempted from the right to access, as appropriate.

7. Data protection advisor

Rygaards has not identified a data protection advisor because Rygaards core activities do not involve (i) regular and systematic surveillance of a large scale of registered people, or (ii) large scale processing of sensitive information.

8. Data security breach

8.1 In general

If an employee finds that there has been a breach of data security, whereby unauthorized persons may have gained access to Rygaards' personal data, the employee must immediately inform the chairman of the board, the principal and the Chief Financial Officer.

8.2 Reporting to the DPA

In case of a breach to data security, where unauthorized persons have gained access to Rygaards' personal data, the Chief Financial Officer must as soon as possible (and no later than within 72 hours) report the breach to the DPA (www.datatilsynet.dk). The notification must at least:

(i) Describe the character of the breach of personal data, including, if possible, categories and the approximate number of personal data records concerned,

(ii) Enter name and contact information for the contact person at Rygaards, who has further information,

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

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

Rygaards must document all breaches of personal data security, including the actual circumstances of the breach of personal data security, its effects and the remedial action taken.

8.3 Reporting to registered persons

In case of breach to data security, where unauthorized persons have gained access to Rygaaards' personal data, Rygaards must inform the people whose data has been compromised as soon as possible.

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

(i) Enter name of and contact information for the contact person at Rygaards, who can provide further information,

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

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

9. Security

9.1 Rygaards has adopted a security policy that is regularly adjusted so that data breaches in as far as possible can be avoided.