

Privacy protocol MosaLira

Contents

Introduction	2
Article 1: definitions	3
Article 2: scope and objective of the protocol	3
Article 3: aim of personal data processing	3
Article 4a: processing of pupil data	4
Article 4b: processing of staff data	4
Article 5: the management of personal data (processing)	4
Article 6: provision of data	4
Article 7: access to personal data	5
Article 8: security and secrecy	5
Article 9: obligation to provide information	5
Article 10: rights of person/people concerned	5
Article 11: record retention period	6
Article 12: former pupils and / former staff members	6
Article 13: complaints	6
Article 14: effective date and official title	6
<i>Appendix</i>	
Notes to articles	7
Overview of MosaLira schools	11

Introduction

On 19 November 2003, the “*Protection of pupil, participant and student data at schools and institutes*” covenant was signed by the education sector and the Minister of Education, Culture and Science. The covenant was the result of a request from the Lower House during the discussion of the Education Number Act to place more emphasis on the protection of personal data of participants in education in view of the fact that a personal number (the social security number) is now being added to the administration (See *Uitleg 29/30 • 22 • 10 December 2003*).

In the covenant, administrators and management have agreed to draw up model regulations per education sector which can be used as a guideline by a school or institute on how to use pupil data present at the school or institute (article 4 of the covenant).

Several administration and management organisations in primary and secondary education, i.e. *Besturenraad, Bond KBO* and *Bond KBVO*, VBS, VGS and VOS/ABB, have drawn up this joint privacy protocol model. The model has been submitted for assessment to the Data Protection Board.

For general information about personal data processing, the Personal Data Protection Act (Wbp) and privacy issues, we refer you to the following websites:

www.justitie.nl (guide for processors of personal data, text of the Personal Data Protection Act, Exemption Decree text)

also via:

www.cbpweb.nl

www.overheid.nl

Guidelines relating to the protection of staff data were added to the model regulations. The protocol therefore applies to both pupil and staff data.

Article 1 Definitions

The following definitions are used in this protocol:

- a. Pupil: person attending primary education, as referred to in the Primary Education Act (WPO), Secondary Education Act (WVO) and the Expertise Centres Act (WEC);
- b. Staff: personnel employed by MosaLira, *Stichting voor leren, onderwijs en opvoeding* (hereinafter: MosaLira);
- c. Personal data: all data relating to an identified or identifiable natural person ;
- d. Personal data processing: all actions related to personal data, including collecting, recording, ordering, filing, updating, editing, requesting, consulting, using, provision through forwarding, distributing or any other way in which data is made available, compiling, linking, as well as screening, deleting or destroying data;
- e. Personal number: the social security number, referred to in article 2 (3j) of the State Taxes Act (AWR) or the education number issued by the *Informatie Beheer Groep* (Information Management Group);
- f. Administration code: single code used for efficient personal data processing;
- g. File: any structured body of personal data, whether or not this data is centralised or distributed in a functional or geographical way, which is accessible according to certain criteria and which relates to different people;
- h. Responsible party: the natural person, legal person or any other person or administrative body that, alone or together with others, establishes the aim and the means of processing personal data, in this case the competent authority of MosaLira;
- i. Administrator: the person reporting to the responsible party who is charged with processing personal data and with filing, deleting and providing data;
- j. Processor: the person who processes data based on an agreement with the responsible party, without being subjected to his direct authority;
- k. User: the person referred to in article 7 who is entitled to know certain data in a personal data registration system;
- l. The person concerned: the person to whom personal data relates;
- m. Third party: anyone who is not the person concerned, the responsible party, the processor or the person/people who is/are authorised under the authority of the responsible party or the processor to process personal data;
- n. Recipient: the person to whom the personal data is provided;
- o. Competent authority: the board of MosaLira;
- p. Data Protection Board: the board referred to in article 51 of the Personal Data Protection Act;
- q. Permission from person concerned: all freely given, specific and informed indication of intention with which the person concerned accepts the processing of the personal data relating to him/her;
- r. WBP: Personal Data Protection Act, Bulletin of Acts and Decrees 2000, 302;
- s. Exemption Decree Personal Data Protection Act: decree of 7 May 2001, (Bulletin of Acts and Decrees 2001, 250), specifying personal data which are exempt from the provisions of article 27 of the Personal Data Protection Act.

Article 2 Scope and objective of the protocol

- 2.1 This protocol applies to all personal data relating to a pupil and/or member of staff which is processed by or on behalf of MosaLira.
- 2.2 This protocol is intended:
 - a. to protect the privacy of pupils and staff who are subject to the data processing against misuse of that data and against processing incorrect data;
 - b. to prevent personal data being processed for a purpose other than the purpose for which it was collected;
 - c. to guarantee the rights of pupils and staff.

Article 3 Aim of personal data processing

Data processing is only performed pursuant to article 19 of the Exemption Decree for:

- a. the organisation or provision of education, guidance of pupils and staff, or provision of study advice;
- b. provision of teaching resources or making them available;
- c. calculating, recording and collecting registration money, school and teaching fees and contributions or payments for teaching resources and extra curricula, including payments to third parties;
- d. dealing with disputes and performing audits;
- e. implementing or applying a statutory regulation.

Article 4 a Processing of pupil data

No other personal data relating to a pupil is processed than:

- a. name, first names, initials, title, gender, date of birth, address, postcode, town, telephone number, etc. for data relating to communication as well as bank and giro account of the person concerned;
- b. personal number;

- c. nationality and place of birth;
- d. data which is essential with regard to the health or wellbeing of the pupil;
- e. data regarding the pupil's religion, insofar as essential for his/her education;
- f. data regarding the nature and progress of the education, as well as the study results achieved;
- g. data aimed at the organisation of the education and the distribution or availability of learning resources;
- h. data aimed at calculating, recording and collecting registration fees, school and teaching fees and contributions or payment for learning resources and extra curricula activities;
- i. data as referred to under a of the parents, guardians or carers of pupils;
- j. other data than that referred to under a to i requiring processing as a result of or in compliance with the application of a statutory regulation;
- k. an administration code for processing data under a to j.

Article 4 b Processing of staff data

No other personal data of a staff member may be processed than:

- a. name, first names, initials, title, gender, date of birth, address, postcode, town, telephone number, etc. for data relating to communication as well as bank and giro account of the person concerned;
- b. the personal number (social security number);
- c. nationality and place of birth;
- d. data aimed at calculating, recording and paying salary.
- e. data regarding the nature and progress of work, including performance and assessment interviews;
- f. any study results achieved;
- g. other data than that referred to under a to i requiring processing as a result of or in compliance with the application of a statutory regulation.

Article 5 The management of personal data (processing)

Personal data is collected by name. The collection of personal data forms the dossier.

Article 6 Provision of data

Personal data is only issued to:

- a. anyone, including third parties, who is responsible for managing or processing personal data of pupils and / or staff who are necessarily involved;
- b. others, in cases referred to in article 8 a, c and d, or article 9 (consistent use), third section of the Personal Data Protection Act;
- c. others, in cases referred to in article 8 under e and f, of the Personal Data Protection Act, insofar as this concerns data referred to in article 4 of this protocol, and after the person concerned has been informed of the intention to do so and after this person has been given reasonable opportunity to exercise his/her right as referred to in article 40 or 41 of the Personal Data Protection Act.

Article 7 Access to personal data

7.1 Regardless of any statutory provisions, only the following people have access to personal data:

- a. those people, including third parties, who are responsible for or who manage the activities related to the processing of the data or who are necessarily involved in this;
- b. others, in cases referred to in article 8 under a, c and d, and article 9 (3) of the Personal Data Protection Act.

7.2 The school provides a system which states the period in which the people mentioned under a can access a dossier.

Article 8 Security and secrecy

8.1

The responsible party ensures suitable technical and organisational measures are in place to prevent loss or illegal processing of personal data. Taking into account the level of technology and the costs of implementation, these measures guarantee an appropriate security level, in view of the risks involved in data processing and the nature of the data to be protected. The measures are also aimed at unnecessary collection and further processing of personal data.

8.2

If the personal data is processed electronically, the administrator will give the various officials as referred to in article 7 access to certain parts of the personal data or to all personal data according to the requirements of their work through a coding and password security system.

8.3

Anyone involved in implementing this protocol and who has access to personal data which he/she knows or can reasonably expect to know is confidential and whose position does not oblige him/her to maintain secrecy pursuant to a statutory requirement must observe secrecy. This does not apply if he/she is legally obliged to publish information or if his/her task in implementing this protocol involves publishing the information.

Article 9 Obligation to provide Information

9.1

The responsible party notifies the person concerned about the personal data being processed, the purpose of the data processing and to whom the data is being given.

9.2

The responsible party notifies the person concerned about the processing of his/her personal data prior to collecting the personal data or, if the data comes from third parties, prior to processing.

Article 10 Rights of the person/people concerned: access, correction, objection

10.1

Everyone is entitled to access their personal data. A charge may be made for requests to see data.

10.2

A request to see personal data should be submitted to the responsible party. He/she will respond in writing within four weeks of receiving this request.

10.3

If the person concerned proves to the responsible party that certain data is incorrect or incomplete, is not required for the declared purpose or is in conflict with this protocol, the responsible party will correct, update or delete the data within four weeks of receiving proof from the person concerned regarding the incorrectness or incompleteness of the data. In this case, any charges imposed will be refunded.

10.4

If the responsible party doubts the identity of the applicant, he will request the applicant to provide further data in writing regarding his/her identity or to submit valid proof of identification at his/her earliest convenience. As a result of this request, the term will be extended until the required proof has been supplied.

10.5

If the personal data is processed on the basis that this is a. essential for the satisfactory implementation by the responsible party of a task governed by public law, or b. essential for a legitimate interest of the responsible party or a third party, the person concerned may submit a written objection against the processing of the data, based on his special personal circumstances. The responsible party should assess whether this objection is justified within four weeks of receiving the objection. If so, the processing of personal data should be terminated immediately.

10.6

If the personal data is being processed for direct marketing purposes, the person concerned may also submit a written objection against the data processing. If the person concerned applies this right, the processing of personal data for this purpose must be terminated immediately.

Article 11 Record retention period

11.1

The pupil's personal data will be deleted within two years at the latest of completing his/her studies, unless the personal data is necessary to fulfil a statutory obligation.

11.2

The personal data relating to staff is deleted at the end of the calendar year following the year in which employment was terminated, unless statutory provisions require the data (or some of it) to be kept for longer in an automated registration system. This data will never be kept for longer than statutorily required.

Article 12 Former pupils and / former staff members

12.1

The responsible party may decide to process data from former pupils.

12.2

This data is only processed to: a. maintain contact with former pupils; b. send information to former pupils; c. calculate, record and collect contributions and donations, including payments to third parties, as well as other internal management activities; d. deal with disputes and conduct audits.

12.3

No other personal data is processed than: a. name, first names, initials, title, gender, date of birth, address, postcode, town, telephone number, etc. necessary for communication, as well as the bank account number of the person

concerned; b. data relating to the nature of the study and the period in which the pupil attended the school; c. data used to calculate, record and collect contributions and donations. d. an administration code which contains no other information than referred to under a to c.

12.4

The personal data is only issued to: a. those, including third parties, who are charged with or manage activities referred to in section 2 or who are necessarily involved; b. others, in the cases referred to in article 8, under a, c and d, and article 9 (3) of the Personal Data Protection Act.

12.5

The personal data is deleted at the request of the person concerned or on his/her death.

Article 13 Complaints

13.1

If the person concerned feels that the institution has not complied with the provisions of this protocol, he/she should contact the responsible party.

13.2

If the complaint does not produce an acceptable result for the person concerned, he can contact the Data Protection Board at PO Box 93374, 2509 AJ Den Haag (The Hague), fax +31 (0)70-3811301 or e-mail mail@cbpweb.nl.

Article 14 Effective date and official title

This protocol can be referred to as a privacy protocol regarding the processing of pupil and staff data and takes effect on

Notes to the articles

Article 1 Definitions

Most of the definitions are directly taken from the Dutch Personal Data Protection Act.

Personal data processing

The question is whether someone can actually exercise any real power or influence, possibly through a computer system, over the data: someone must be able to use the data. If someone cannot exercise power or influence over the personal data, this processing is not covered by the Personal Data Protection Act.

Responsible party

The responsible party is the competent authority; in primary and secondary education, this is usually the school board.

Personal number

The limited use of the personal number is elaborated further in the sector education Acts.

Processor

This could be an external organisation such as an APS (application service provider), education agency or a firm of accountants.

If it is decided to delegate data processing activities to a processor, a relationship with the processor will be entered into. The Personal Data Protection Act stipulates requirements regarding the choice of a processor and how the relationship with that processor is established;

- The chosen processor must offer sufficient guarantees with regard to technical and organisational security;
- A contract with the processor must be signed, or a regulation imposed which creates enforceable obligations;
- In the contract (or other provision), the responsible party must stipulate that the processor only processes personal data on behalf of the responsible party;
- It must be stipulated that the processor complies with the security obligations imposed on the responsible party pursuant to the Personal Data Protection Act and finally
- The responsible party must actually monitor compliance with these security obligations. The right to do so will also be incorporated in the contract (or other provision).

article 14 of the Personal Data Protection Act stipulates that the sections relating to the protection of personal data and the security measures are recorded in writing.

Person concerned

In the Personal Data Protection Act, the person whose data is processed is called “the person concerned”. He or she also has various special rights pursuant to the Personal Data Protection Act, such as the right to know and correct the data and the right to lodge an objection against the processing of his/her personal data.

If the person concerned is a minor and is under the age of sixteen, or has been placed under a guardian or counsellor, permission from his/her legal representative is required instead of from the person concerned.

The person concerned or his/her legal representative may withdraw permission at any time.

Data Protection Board (CBP)

As an independent organisation and pursuant to the Personal Data Protection Act, the Data Protection Board ensures that personal data is used carefully and securely and that the privacy of citizens also remains guaranteed in the future. If an organisation does not observe its legal obligations, the Board can take measures. The most important of these is the imposition of an administrative order. This means that the Board can force the perpetrator to undo the violation. The board can thereby impose a penalty. It can also impose a fine, for example when personal data processing is not reported, reported incorrectly or too late.

Exemption Decree

The Exemption Decree (Vb) lists the data which is exempted from processing. In particular article 19 of the Exemption Decree may apply to data processing performed by educational institutes with respect to their pupils. It is only possible to appeal to one of the articles of the Exemption Decree if the requirements of the Exemption Decree are met, not only at the start of the data processing but also later. It is therefore a good idea to check whether these requirements are met, if you wish to process more or different data, for example, or want to switch from one registration system to another. It is therefore impossible to state unreservedly that schools are exempt from the notification requirement.

Incidentally, the Exemption Decree only provides for exemption from the notification requirement. For the rest, the Personal Data Protection Act normally applies.

Article 3 Aim of personal data processing

Organisations may only collect and use personal data for a clearly defined goal. That goal must be defined in advance, i.e. before they start collecting the data. They may not collect more data than is strictly necessary for that goal, nor too little data as this could result in incomplete information. However organisations may process personal data for several goals at the same time. These goals must be well defined in advance. They may only use the data if this is in accordance with the original goal.

An example: the data which a school has incorporated in its pupil database may be used to chart the number of pupils who successfully complete their studies. However, the school may not sell this personal data to a company in such a form that the company can create a profile of the pupil, based on which the pupil can be personally approached. In this case, the aim for which the data is collected is not compatible with the way in which it is later used.

Article 4 Processing personal data

This article further defines what data may be registered within the framework of the goal of registration. In principle, the personal number can be defined as an administration code. However, the use of the personal number is subject to strict statutory regulations. The personal number may not be used as an administration code for the institute's own registration system. It may not therefore be used in lists containing pupil data for a range of purposes, such as organising classes/groups.

Article 5 The management of personal data (processing)

All data relating to a pupil which is covered by this protocol constitute the dossier of the pupil in question. The data can therefore be distributed over several separate or joint registration procedures.

Article 6 Provision of data

Providing personal data involves any way in which personal data is published or made available, in any form. This may be verbally, in writing or digitally. It also includes accessing data, for example on CD-Rom. Provision of data is also referred to if someone looks over someone else's shoulder.

Personal Data Protection Act, articles 8 and 9:

Article 8

Personal data may only be processed if:

- a. *the person concerned has given his/her unequivocal permission for the processing;*
- b. *the data processing is essential for the execution of a contract to which the person concerned is a party, or for taking pre-contractual measures relating to a request by the person concerned and which are necessary for finalising a contract;*
- c. *data processing is essential for compliance with a statutory obligation to which the responsible party is subject;*
- d. *data processing is essential to safeguard a vital interest of the person concerned;*
- e. *data processing is essential for the satisfactory fulfilment of a task related to public law by the relevant administrative body or the administrative body to which the data is sent, or*
- f. *the data processing is essential to promote the justifiable interest of the responsible party or of a third party to whom the data is provided, unless the interests of the fundamental rights and freedom of the person concerned, in particular the right to protection of personal life, prevails.*

Article 9

1. *Personal data is not further processed in a way which is incompatible with the purposes for which they have been acquired.*
2. *When assessing whether processing is incompatible as referred to in (1), the responsible party must take into account:*
 - a. *the relationship between the goal of the processing and the goal for which the data was acquired;*
 - b. *the nature of the relevant data;*
 - c. *the consequences of the processing for the person concerned;*
 - d. *the way in which the data was acquired and*
 - e. *the degree to which the person concerned is provided with suitable guarantees.*
3. *Further processing of the data for historic, statistical or scientific purposes is not considered as incompatible if the responsible party has taken the necessary measures to ensure that the further processing is only performed for these specific purposes.*
4. *No personal data is processed where there is an obligation to observe secrecy by virtue of office, profession or statutory regulation.*

Article 7 Access to personal data

Transparency guarantees privacy. There must be clarity with regard to who has access to the personal data. Generally, those with access to the data are the staff at the school or institute reporting to the responsible party. This is repeated in this article. Section 2 specifically refers to these staff members and the creation of a registration system of designated users.

Having access to personal data means being able to see personal data without you being able to exercise any power of influence on the personal data.

Paragraph 1 refers to the Personal Data Protection Act to indicate who else could have access to the data. It indicates that there are other situations than those defined in the Personal Data Protection Act when others could have access to the data. This is difficult to incorporate in a protocol. The Personal Data Protection Act outlines a number of situations, such as police departments involved in tracing criminal offences and Area Health Authorities which are permitted to request participants' records in the case of an epidemic. The Personal Data Protection Act offers this possibility. Paragraph 1 refers to this situation.

Article 8 Security and secrecy

Data processors must also focus on the security of privacy-sensitive information. They are obliged to keep this data secret from unauthorised persons and people who have nothing to do with the data. More information about the security of personal data can be found on the website of the Data Protection Board.

The competent authority should sign a secrecy agreement with those who are not in a hierarchical relationship with the competent authority (processor). Article 14 of the Personal Data Protection Act requires that the sections which refer to the protection of personal data and to security measures are recorded in writing (see also the notes to article 1 i with regard to the processor).

Article 9 Obligation to provide Information

All organisations which use personal data have an obligation to provide information. This means that they must inform the people to whom this data relates about what they plan to do with their data. The school or institute should notify the person concerned *on its own initiative* with respect to what personal data it has and why. This is an important instrument in the Personal Data Protection Act for making data flows transparent.

The school or institute can publish this by listing the data processing on the website and/or in the school prospectus and by referring to the website and/or school prospectus on forms requesting data. It is recommended that this information to the person concerned also explicitly includes his/her rights (right of access, correction and complaint; described in articles 10 and 13 of this protocol) and to refer to the procedure agreements (to whom and how a complaint can be submitted) on the website and/or in the school prospectus.

The duty to provide information applies when the data is collected on a form or through the internet, for example. This duty also applies when the data is acquired through third parties, unless the supplier of the data has already informed the person concerned or unless the duty to provide information leads to disproportionate work for the processor, for example if it is very time consuming to trace the address of the person concerned and advertising gives insufficient guarantee.

The person concerned does not need to be informed if their data is recorded or distributed pursuant to a statutory obligation.

The provision of information to the person concerned must always include:

- Who you are (i.e. who is the responsible party); and
- For what goal or purposes you are collecting and processing the data.

However, this is not always enough. You must provide further information if such is required with respect to the person concerned in order to guarantee adequate and careful processing. You will therefore have to decide whether to provide more or less detailed information about the processing to the person concerned as a precaution. You should thereby take into account (1) the nature of the data, (2) the circumstances under which you acquired them and (3) the use you wish to make of them. The more sensitive the data for the person concerned, the more reason there is to inform the person concerned in more detail about your data processing.

Article 10 Rights of person/people concerned: access, correction, objection

Everyone is permitted to enquire, at reasonable intervals, whether and if so what personal data the competent authority, the school, processes with regard to them. If the person concerned makes excessive requests to the competent authority, the school, the latter is not required to respond.

A request for access (but this also applies to requests for correction, for example) must be replied to within four weeks. The reply must be provided in writing, unless the significance for the person concerned requires another form being chosen, for example a verbal response. If the reply is sent by e-mail, this is also deemed to be a written response.

The reply must be sent in an understandable form:

- A complete overview of the data of the person concerned processed by the competent authority, the school;
- A description of the goal or purposes of the data processing;
- The categories of data to which the processing relates;
- The recipients or categories of recipients;
- All available information about the origin of the data.

The charge covering the costs of the message as referred to in article 10.1 is €0.23 per page to a maximum of €4.50 per message.

In deviation from the above, the responsible party may charge a reasonable sum to a maximum of €22.50 if:

- the copy consists of more than a hundred pages, or
- the message consists of a copy of data processing which is difficult to access on account of its nature.

Request for correction

The person concerned may request that his/her data is corrected. In this case, he/she must indicate the required changes. Correction involves:

- correcting;
- supplementing;
- deleting;
- screening; or
- ensuring in any other way that the incorrect data is no longer used.

The competent authority, the school, is only obliged to correct data if it is actually incorrect, incomplete or not appropriate for the goal for which it has been collected, or if it has been processed in a way which deviates from the provisions of the Personal Data Protection Act or other Act.

The right of objection

If the person concerned can prove a justified individual interest, the responsible party must stop processing this person's data.

The responsible party may charge a reasonable sum to cover the costs of handling an objection as referred to in article 10.5, to a maximum of €4.50.

If it relates to direct marketing or charity promotion, the person concerned is not required to prove anything; he/she may lodge an objection whereby his/her justified individual interest is always upheld. The processing of his/her personal data for the purpose in question must be terminated.

Article 11 Record retention period

The Personal Data Protection Act stipulates that personal data may not be kept for any longer than is essential for the purposes for which it has been collected or is used. Based on the goal, the school determines how long the relevant data must be kept. Pupil data should be deleted within two years at the latest of the pupil finishing his/her studies, unless there is a statutory obligation to retain records for a longer term (article 19 Exemption Decree). For example, the Funding Decree (article 9 Primary Education Act and article 6 Secondary Education Act) stipulates that pupil records must be kept for at least five years after the pupil has left school.

The data of *former pupils* as referred to in article 12 of this protocol, are only deleted at the request of the person concerned (article 41 Exemption Decree).

Personal data pursuant to the *Compulsory Education Act* by the responsible party is deleted two years at the latest after the end of the compulsory education period (article 20 Exemption Decree).

If personal data is used to issue payments for costs related to pupil transport, as referred to in the Primary Education Act and the Expertise Centres Act, the personal data should be deleted within two years at the latest of the end of the school year to which the payment relates (article 21 Exemption Decree).

Data from practitioners of *individual professions in health care*, as referred to in the Individual Health Care Professions Act, regarding their patients are deleted after the end of the statutory retention period and if there is no such period, five years at the latest after the end of their treatment (article 16 Exemption Decree).

In the case of an *objection, complaints or legal procedure*, the personal data should be deleted within two years at the latest of the relevant procedure being completed, unless a longer retention period has been stipulated (article 39 Exemption Decree).

The personal data from a *register or list* are deleted two years at the latest after the related capacity has expired, the desired capacity has been acquired or the desired performance has been provided (article 40 Exemption Decree).

Document management. The data which is collected with a view to registering receipt, handling and completion of documents by the responsible party are deleted five years at the latest after the data was included (article 31 Exemption Decree).

Video camera monitoring. Monitoring to safeguard the security of people, buildings, sites, property and production processes, which are delegated to the care of the responsible party, using clearly visible video cameras is also subject to the Data Protection Act. The personal data acquired in this framework are deleted 24 hours at the latest after recordings are made, or after observed incidents have been dealt with (article 38 Exemption Decree). Other communication files are deleted at the request of the person concerned or at the latest a year after the relationship between the person concerned and the organisation of the responsible party has ended (article 42 Exemption Decree).

These periods apply unless the personal data is necessary to comply with a statutory obligation.

Article 13 Complaints

Many unnecessary objection and appeal procedures can be prevented by following a complaints procedure. Paragraph 2 refers to the possibility of requesting the Data Protection Board to mediate, pursuant to article 47 Personal Data Protection Act.

MosaLira foundation for learning and education.

The competent authority of MosaLira, legally represented by the General Director, governs the following schools:

Basisschool St. Aloysius
Basisschool Amby
Basisschool Anne Frank
Jan Baptist, school voor ZML-onderwijs (school offering education for children with severe learning difficulties)
Basisschool de Burght
Basisschool Het Mozaïek
Basisschool 't Spoor
Basisschool John F. Kennedy
Basisschool Joppenhof

Basisschool de Maasköpkes
Basisschool Markus
Basisschool Montessori
Basisschool St. Oda
De Opstap, school voor speciaal basisonderwijs (school for special primary education)
Basisschool Petrus en Paulus
Basisschool St. Pieter
Basisschool de Schans
Basisschool Scharn
De Sprong, school voor speciaal basisonderwijs (school for special primary education)
Basisschool De Letterdoes
Basisschool Wijck