Governance and Accountability Policy

BISS

1. Introduction

1.1 Purpose

The purpose of this policy ("Policy") is to establish - within the British International School of Stavanger, which consists of four different institutions (BISS Preschool, BISS Gausel, BISS Sentrum, BISS Foundation, hereinafter "BISS") – the governance structure of BISS, describing the roles, responsibilities, objectives, risks, documents, and operational controls put in place to implement the accountability principle introduced by European and National Legislation.
To ensure the highest degree of organization and control, the Policy was written following the high-level structure of the ISO standards (so-called Annex SL), trying to also include the ISO standards on the protection of information and personal data (e.g., ISO27001 and ISO27701).

1.2 Entry into force

All Authorized Persons working for BISS are required to be familiar with the contents of this document as of the Effective Date.

1.3 Reference regulations

- GDPR;
- Opinions, guidelines and recommendations of the Supervisory Authorities.

2. Context of the organization

2.1 BISS and its context

To understand BISS and its context in relation to the Processing of Personal Data, it is necessary to analyse:

- how BISS decide and assume decisions in relation to the Processing of Personal Data;
- the power of influence exercised by BISS Foundation in relation to the other relevant BISS entities.

Considering the context described above, the achievement of BISS's data objectives may be affected by:

- External factors:
  - Rules, regulations, international standards applicable to BISS;
  - Judgments, arbitrations, administrative decisions held by the competent courts;
  - External attacks (e.g., phishing, malware) on IT systems.
  - Jurisprudence/opinions of the Supervisory Authorities and the Court of Justice of the European Union.

- Internal factors:
  - Conflicting interests within BISS;
  - Behaviour not compliant with Data Protection Compliance Framework (DPCF) procedures by BISS departments.

2.2. Needs and expectations of stakeholders

In achieving its goals, BISS must manage:

- different channels of acquisition of Personal Data (e.g., school activities, websites, events, social media, etc.);
- different types of Personal Data (e.g., Special categories of Data, Personal Data, etc.);
- different categories of Data Subjects (e.g., students, employees, third parties, etc.).

In view of the context in which BISS operates, the stakeholders who are capable to influence BISS's ability to achieve the expected results, together with their respective needs and expectations, are identified below:

- Data Subjects of which BISS are Data Controller: this category includes the BISS students, the Authorized Persons; the subjects who interact with BISS websites or participate in BISS events. Even if the needs and expectations of these Data Subjects may vary, it is reasonable to state that they all have in common the expectation of seeing their Personal Data Processed in accordance with legal and ethical principles of fairness, social responsibility and transparency.
- BISS departments and Authorized Persons: this category includes the needs of BISS departments (e.g., HR, Finance, ICT, etc.) to achieve business or strategic objectives through the widest and simplest possible exploitation of data.
- BISS's direct suppliers: this category includes all suppliers to whom BISS entrust the Processing of Personal Data. The interest of these entities is to provide the established service while minimizing their contractual liability (e.g., in case of Data breach), as well as to freely subcontract or transfer Personal Data abroad, if necessary for the performance of the service.
- Jurisdictional and administrative authorities: this category includes first and foremost the Supervisory Authority competent for BISS (the Norwegian Data Protection Authority); the administrative or judicial authorities competent for BISS (e.g., the competent Norwegian courts and the CJEU), which may have jurisdiction under the law of the Data Subject. These are the conveyers of general compliance interests that may differ from each other, as they may concern the interpretation of different laws.

2.3. Data Protection Compliance Framework (DPCF)

Depending on the context and the interests expressed by the stakeholders, BISS has created and implemented a policy on the Processing of Personal Data by means of a DPCF, with the aim of aligning with European and National Legislation and reducing the risk of non-compliance.

3. Senior management (leadership)

3.1. Senior management's commitment

By approving this Policy, BISS assures:

- that the content described in the "Policy" section below and the objectives indicated in the "Planning" section below are compatible with BISS's strategic direction;
- the integration of the DPCF policies and procedures into BISS's internal processes;
- the availability of the resources necessary for the DPCF to operate and achieve the objectives set out in the "Planning" section;
- communication within BISS about the importance of respecting the DPCF;
- to make every effort to ensure that the DPCF achieves the objectives set out in the "Planning" section;
- supporting individuals, and in particular Privacy Team, to contribute to the effectiveness of the DPCF in their respective areas of competence;
- the continuous improvement of the DPCF.

Policy

Data protection practices at BISS has been regulated by means of the DPCF, which:

- reflects the activities carried out by BISS;
- constitutes a framework for setting the objectives indicated in the "Planning" section;
- includes a commitment to comply with applicable requirements;
- includes a commitment to continuous improvement;
- is maintained as documented information (see "Documented Information" section below);
- will be available in English;

- is communicated to the so-called stakeholders (see previous paragraph "Needs and expectations of stakeholders"), as appropriate.

DPCF is composed of:

- Policy on Governance and Accountability (this Policy);
- Records of Processing and Internal Security Measures;
- Processor Security Assessment Checklist;
- Privacy notices (i.e., for employees; for students; for websites);
- Data Protection Impact Assessment (DPIA) Template;
- Legitimate Interest Assessment (LIA) Template;
- Policy on Data Retention;
- Procedure for Data Subjects requests;
- Procedure on Data Breach Management;
- Data Processing Agreement template;
- Policy on IT tools;
- Glossary and Acronyms.

The DPCF documents listed above may evolve in number and form depending on regulatory developments and BISS Processing.

3.4 Roles, responsibilities and decision-making in BISS

BISS ensures that roles, responsibilities and decision-making powers are assigned to ensure implementation of the DPCF in the following ways.

3.4.1 Delegate

Each school board is the main decision-making centre that determines the overall purposes to be achieved and means of Processing through which they are to be achieved. The expression of will, with respect to the purposes and means of Processing, takes place through its competent body (the BISS School Board) as well as, where appointed, through its legal representatives who have specific power of attorney to represent it both substantively and procedurally.

In particular, as BISS - and their privacy activities are concerned decided to entrust the respective Managers/Principals of BISS Foundation and BISS Preschool, BISS Gausel and BISS Sentrum - ("Delegate") with all responsibilities attributed by the European and National Legislation to the Data Controller (each one competent and accountable for the relevant belonging entity), with the power to implement, in full operational autonomy and with broad decision-making powers, including with regard to assets, the measures and actions necessary to best fulfil all the responsibilities and obligations laid down by that law in relation to the above Processing and data; with appropriate organization and means and with the relevant BISS's entity representation, where necessary, towards third parties and towards the Supervisory Authority and with particular reference to the collection, security, communication and particular dissemination of the aforementioned data and respect for the rights of all "Data Subjects" in relation to the Processing in question and with the right to use, if deemed necessary, external parties who, upon acceptance, will in turn be required to make a declaration of conformity of the measures adopted; delegating therefore to the aforementioned legal representative all the tasks for the full discharge of the responsibilities entrusted.

Operationally speaking, within the DPCF, the Delegate's powers and responsibilities include the following activities:

a) Designate the Authorized Persons, including the System Administrators, who will operate on behalf of the relevant BISS belonging entity and in accordance with its instructions; provide them with the necessary instructions, also by means of training, so that they operate in compliance with the European and National Legislation and in accordance with the opinions/decisions of the competent Supervisory Authorities.

b) Drafting, approving and keeping up to date the Records of Processing Activities and Risk analysis with the support of the Privacy Team.
c) Prepare, approve and disclose the Privacy notices relating to the Processing of Personal Data in the manner provided for by European and National Legislation.
d) Ensure the collection of evidence of Consent within the Privacy notices as provided for in the DPCF and in the European and National Legislation.
e) Draft and approve the results of DPIAs and LIAs after consultation with the Privacy Team, if needed.
f) After consultation with the Privacy Team, indicate and confirm the retention times and/or criteria for Personal Data within the Policy on Data Retention, ensuring that the relevant BISS entity will ensure compliance in this regard.
g) Prepare and acknowledge requests from Data Subjects through the Procedure for Data Subjects requests.
h) Select Data Processors/Data Controllers/Joint Controllers who, by virtue of their experience, capacity and reliability, provide suitable guarantees of full compliance with the European and National Legislation, including the security profile, and enter into data agreements with them in the manner provided for by the DPCF.
i) Adopt, check and keep up to date: i) BISS's Internal Security Measures; ii) the organizational and technical measures required from Data Processors/Joint Controllers when dealing with the relevant BISS entity and iii) the Policy on IT Tools, so as to minimize, through the adoption of suitable and preventive security measures, Data Breaches.
j) Negotiate, agree, sign, renew, terminate and modify agreements dealing with the Processing of Personal Data, as well as confer and revoke professional appointments in relation to the above.
k) Attend and make determinations within its purview during Data Breach Assessment Unit ("DBAU") and Data Breach Management Unit ("DBMU") - especially for such data breaches whose severity is High/Very High - meetings provided for in the Procedure on Data Breach Management.
l) Inform the Privacy Team with respect to any changes in the Processing, including replacements of Data Processors; and inform the Privacy Team with respect to appeals, complaints, requests for prior consultation, opinions or otherwise.
m) Program and perform, in agreement and collaboration with the Privacy Team, internal audits (i.e., for the relevant BISS areas/departments) and second party audits (i.e., audits for third party suppliers appointed as Data Processors) required as a form of accountability by the European and National Legislation, as well as those required by certifications and/or codes of conduct in view of the continuous improvement of the DPCF.
n) Carry out whatever is necessary to correct any non-compliance detected within the relevant BISS entity, keep the DPCF updated with a view to continuous improvement.
o) Participate in the inspections of the Supervisory Authority according to the Procedure on the cooperation with the Supervisory Authority.
p) To represent the relevant BISS belonging entity before the competent Supervisory Authorities and in disputes, both tions.
q) Identify the Authorized Persons who, by virtue of their experience, capacity and reliability, provide an adequate guarantee of full compliance with the European and National Legislation, including the security profile, assigning them the role of Management and delegating to them all the necessary or appropriate powers of the Delegate to ensure compliance with the pro tempore regulations in force and the DPCF.
r) As far as not expressly mentioned, to fully implement the European and National Legislation; to adopt any decision and implement any initiative necessary to ensure, and be able to demonstrate, the conformity of the Processing carried out by BISS.
s) In case of irreconcilability between two or more Managements, whenever a privacy topic impacts on two or more departments, adopt a binding decision.

.

4. Support

4.1. Resources

Through the Delegates, BISS determines and provides the resources necessary for the establishment, implementation, maintenance and continuous improvement of the DPCF.
In accordance with European and National Legislation, the Privacy Team is entitled to request to the Delegates for the allocation of resources (economic, organizational) for the proper performance of its activities.

4.2. Awareness

BISS ensures knowledge and awareness of European and National Legislation, the DPCF and the roles and responsibilities provided therein through training organized by privacy consultant and/or external e-learning platforms and through making the DPCF available to Authorized Persons in ways deemed appropriate.
The Managements and/or the Privacy Team may propose awareness courses for Authorized Persons.

4.3. Communication

All communications pertaining to the DPCF shall be made available to Authorized Persons in an appropriate manner.

4.4. Documented information

All DPCF documents shall be retained and made available in appropriate ways as documented information.
Each DPCF document is identified with at least a title and the date it came into force. For policies, procedures and guidelines: the author, approving party and any changes from previous versions are also indicated.

4.5. Approval of related DPCF documents

BISS has set up different ways of approving DPCF documents:

- Ordinary. The Privacy Team sends the document to the directly affected Management for approval and shares it for information/consultation with the indirectly affected Managements. This includes, for example, the approval of a privacy notice that directly or indirectly involves the Managements of the Marketing departments.
- Extraordinary. It is applied in cases where the document drawn up by the Privacy Team has an impact on BISS as a whole or in cases of disagreement between Managements or between Managements and the Privacy Team. In these cases, the document is approved directly by the Delegate of the relevant BISS entity involved. For example, this method includes the final approval of the Record of Processing Activities or the results of some DPIAs/LIAs not entirely shared by the Managements.

In all cases, documents pertaining to the DPCF are transmitted in pdf format to the Delegate for alignment and approval and shared during the Privacy Committee. The Privacy Team then provides summary minutes of the decisions taken during these meetings so that documented information can be created.
The maintenance/review of the DPCF is carried out by the Privacy Team.

5. Performance evaluation

The evaluation of the performance of the DPCF and therefore the execution of operational controls is carried out as follows.

5.1. For controls on compliance with the DPCF

Since these controls are based on reports from Authorized Persons, their Managements or detected during the normal course of the Privacy Team's functions, it can be confirmed that this is a permanent control, therefore performed throughout the entire year.
In the presence of omissive/commissive behaviours by the persons in charge and responsible for implementing the DPCF, the Privacy Team shall draw up a "Privacy Teams Note" to the Delegate and the relevant Management to report the misalignment.

5.2. For controls on Processing

These controls are carried out on a six-monthly or annual basis depending on when the Supervisory Authority has issued its inspection plan. The practices of the inspection plans and the jurisprudence of the Supervisory Authority and the national and European courts are included in this time frame.

5.3. For controls on outsourced activities

When appointed with an *ad hoc* mandate, the privacy consultant or any other entity performs a second-party postal audit (i.e., BISS audits of third-party supplier acting ad Data Processors) following the ISO19011 methodology.
The outcome of the audit is set out in an "Audit Report", submitted for information to the Management, who entrusted that Data Processor, to the Privacy Team, and to the Delegate for approval of any actions suggested by the results.

6. Improvement

6.1 Non-conformities and corrective actions

The Privacy Team Notes and Audit Reports address actions to be solved, opportunities for improvement, priorities, and suggested timelines for implementation.
Following and according to the priorities established by the Delegate with the approval, the Management – supported by the Privacy Team - proceeds as the operational arm of BISS to follow up on the approved actions.

6.2. Continuous improvement

Through the Privacy Team, BISS verifies annually the status of the DPCF, the needs of the stakeholders and the performance of the DPCF to ensure its continuous improvement according to the Deming cycle methodology "Plan - Do - Check - Act".

Title	Policy on Governance and Accountability			
Date	Version	Changes	Owner	Approved by
June 2024	1.0		BISS Schools/Preschool	BISS Managment