CA 41/2022

AISBL Association de parents des élèves de l'Ecole européenne de Bruxelles III

Privacy Governance Policy

Version: 1.0

Document control

Title	Privacy Governance Policy
Department	IT
Type Document	Policy / Procedure
Document Owner	Data Protection Manager, APEEE Director and APEEE President
Author	EY Law for APEEE in relation to version 1.0
Approved by	Management of APEEE
Date and version	14 June 2022, version 1.0
Effective date	_____2022
Date next review	_____2023
Related documents	• Privacy Policy Employees • Register of Processing Activities • Privacy Policy Website • Cookie Policy Website • Template Data Processing Agreement

Errors and omissions

When you as a reader of this document would spot mistakes or omissions, you are kindly invited to reach out to the author in writing and provide him with a description of the finding as well as the specific location in this document that would require to be updated.

Confidentiality

This document can include sensitive and/or confidential information related to the Association de parents des élèves de l'Ecole européenne de Bruxelles III. Each person that gets access to this document must take the appropriate measures to prevent either intentional or unintentional disclosure of information to an unauthorized individual.

Table of Contents

1 Introduction

Association de parents des élèves de l'Ecole européenne de Bruxelles III (hereafter referred to as "**APEEE**", "**we**", "**us**", "**our**") values the right to privacy. This policy describes how APEEE personal data must be collected, handled and stored to meet APEEE's data protection standards — and to comply with the Applicable Legislation. It sets out the principles to be applied to the processing of personal data, including relating to APEEE's current, past, and prospective employees, members, non-members (e.g. teachers, parents, pupils,…), APEEE's suppliers, sub-contractors, and other third parties.

This policy establishes a foundation for the privacy of all personal data which is processed by APEEE. This policy applies in conjunction with other policies and procedures, established by APEEE. Furthermore, this policy sets out internal standards and should not be construed as establishing contractual or legal rights for any persons.

This policy is intended to ensure compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("**Applicable Legislation**").

This policy specifically applies to any personal data we process about an identified or identifiable natural person ("**data subjects**"). For APEEE this concerns amongst others its members, non-members (e.g. teachers, parents, pupils,…), APEEE's suppliers, APEEE's business contacts, employees and other people the organisation has a relationship with.

This policy refers to the processing of personal data in hard copy (i.e. paper) form, held in physical files or in an electronic form (including electronic mail and documents created using word processing or spreadsheet software etc.).

2 APEEE as controller of personal data

Under the Applicable Legislation, the controller is the one who determines the purposes ('*why are we processing data*') and the means of the processing of personal data ('*how are we processing data*'). It does not matter whether that person is a natural or a legal person, a public or private body, a non-profit organization, or has a commercial purpose.

A controller can decide to process personal data internally if the capacity and/or means are available or can outsource the processing to a so-called external processor. A processor is the one who processes personal data on behalf of the controller. Again, it does not matter whether

that person is a natural or a legal person, a public or private body, a non-profit organization, or has a commercial purpose.

In most cases APEEE will act as controller for the personal data that it processes. It should be taken into account that it is not always easy to determine whether APEEE or the third party to whom APEEE makes the personal data available is a controller or a processor. In some cases, it may even be that APEEE and/or the third party in one and the same contractual relationship may be both controller and processor at the same time. Such evaluation should be left to the data protection manager.

3 Definitions

The Applicable Legislation contains key terms (or definitions) which we need to understand when processing personal data. Without being exhaustive we have listed some of the key definitions below:

data subject	see above under clause 1.
controller	see above under clause 2.
personal data	means any information relating to an identified or identifiable natural person; one who can be identified, directly or indirectly, by reference to an identifier such as name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation , use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
processor	see above under clause 2.
sensitive personal data	means personal data that relates to race or ethnic origin, political opinion, religion or philosophical beliefs, sexual orientation or gender identity, trade union membership and activities, genetic or biometric data, health or sex life, administrative sanctions, judgements, criminal or suspected offenses, convictions or related security measures.

4 Processing principles

APEEE processes personal data in line with Applicable Legislation and in accordance with the following data protection principles. The type of personal data you may process depends on the reason you are processing it for and what you want to do with it.

You must always respect all of the following data protection principles when processing personal data:

- you must process personal data in a lawful, fair and transparent manner (**lawfulness, fairness and transparency**);
    - processing personal data in a *lawful* manner means you must have a legal basis for processing personal data for which we refer to clause 5 below;
    - processing personal data in a *transparent* manner means you must always inform the data subjects of whom you are processing data of what you are doing and why. Any communication on this must be simple, clear and accessible;
    - processing personal data in a *fair* manner means that we do not deceive or mislead data subjects when processing their personal data, we consider how the processing may affect these individuals and we only process personal data in a way the data subject could reasonably expect and explain why if that would not be the case;
- you must process personal data for a specific purpose and you must indicate the purpose(s) to the data subjects prior to collecting their personal data. Subsequent changes to the purpose(s) are only possible to a limited extent and will, in general, require consent (**purpose limitation**);
- you must only process personal data that is necessary, adequate and relevant to achieve the purpose(s) for which such data are being processed. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or pseudonymised data will be used (**data minimization**);
- you must always ensure that the personal data processed is accurate and up-to-date, having regard to the purposes for which it is processed. Inaccurate or incomplete data will/should be deleted, corrected, supplemented or updated (**accuracy**);
- you must ensure that the personal data will not be kept for longer than is necessary for the purpose(s) for which personal data is processed. Data that is no longer needed after the expiration of the defined retention period will be deleted (**storage limitation**);
- you must ensure that personal data will be processed in a manner that ensures appropriate security of data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical organizational measures (**integrity and confidentiality**).

Compliance with the above principles must be documented. Pursuant to the Applicable Legislation each processing activity must be recorded in a dedicated register of processing activities for this we refer to clause 12 below.

Although this may be obvious in light of the above data protection principles, APEEE would like to emphasize that:

- personal data collected for one purpose cannot be further processed for (an)other purpose(s) that is(are) not compatible with the original purpose of collection;
- personal data cannot be collected in advance and stored for potential future purposes.

Failure to comply with these principles may leave APEEE open to fines and other sanctions, so if you have any question in relating to the above, please reach out to the data protection manager: privacy@apeeeb3.be.

5 Lawfulness: legal basis for processing personal data

APEEE must be transparent about the legal basis for the processing of personal data. Processing of personal data is only lawful if and to the extent at least one of the following applies:

- we have obtained **consent** from the individual to process his/her personal data for one or more specific purposes;
- the processing is *necessary* for the **performance of a contract** to which the individual is party or to take steps at the request of the individual prior to entering into a contract;
- the processing is *necessary* for compliance with a **legal obligation** to which the APEEE is subject;
- the processing is *necessary* to protect the **vital interests** of the individual or of another natural person;
- the processing is *necessary* for the performance of a **task carried out in the public interest**;
- the processing is *necessary* for the purposes of the **legitimate interests** pursued by the APEEE or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual which require protection of personal data, in particular where the data subject is a child.

In light of the above legal bases, APEEE would like to emphasize that

- only the above 6 possible legal bases exist and the word 'necessary' is placed in italics as it is to be interpreted and applied restrictively;
- it is important to identify correctly the legal basis for each processing purpose. It is not sufficient to select multiple possible legal bases for the processing purposes;
- we can in principle not simply change our legal basis during the processing activity (save for the case in which such change would be due to the introduction of a legal obligation upon APEEE to process personal data). Thus for instance, if consent is withdrawn we cannot continue to process personal data because we believe APEEE still has a legitimate interest to process the personal data.

Below, we have set out the main legal bases which apply when APEEE processes personal data of current, past, and prospective employees, members, non-member (parents, teachers, pupils), suppliers, sub-contractors, and other third parties:

- the processing is necessary for the **performance of a contract** (e.g. employment contract, a contract for membership with a parent, a contract with a supplier,…);
- the processing is necessary under a **legal obligation** to which APEEE is subject (e.g. social and employment legislation to which APEEE is subject, the requirement to obtain *l'extrait de casier judiciaire modèle 2* as we are working in a school environment);
- the processing is necessary to satisfy the **legitimate interests** of APEEE;
- APEEE has obtained the **consent** from the individual (e.g. during the registration process of the pupils at EEBIII, parents given their consent to the EEBIII for the latter to transfer the parents' contact details to the APEEE so that the APEEE can send an invitation to them to become a member of APEEE; from the members for contact tracing purposes, from the non-members to receives marketing communication by APEEE).

APEEE would like to emphasize that:

- When we rely on **consent** as a legal basis for what we are doing when processing personal data, such consent must be informed and explicit. APEEE must at all times be able to prove that it has obtained the consent of data subjects prior to processing their personal data, so consent cannot be assumed we need to obtain the data subject's consent in writing. Note that data subjects can withdraw their consent at all times. Although a withdrawal shall not affect the lawfulness of the processing activity prior to its withdrawal, we must stop the processing activity as soon as possible once received. Please always consult with the data protection manager if you believe **consent** is the legal basis;
- When we rely on **legitimate interest** as a legal basis for what we are doing when processing personal data, such interest needs to be clearly specified. We cannot be vague about these interests and they need to be balanced against the interests or fundamental rights and freedoms of data subjects. Consequently an assessment will need to be performed and documented. Please always consult with the data protection manager if you believe **legitimate interest** is the legal basis;
- When we process sensitive personal data, this processing activity is subject to additional restrictions and conditions. With a few exceptions, sensitive personal data (e.g. Health data during the Covid-19 pandemic) may only be processed with the explicit consent of the data subject. Please always consult with the data protection manager for identifying the appropriate legal basis in the Applicable Legislation.

6 Sharing personal data with third party recipients

Personal data may need to be disclosed to other appropriate persons who have a need to know (so-called 'third party recipients').

APEEE is entitled to disclose personal data only to third party recipients ensuring an adequate level of data protection. In all cases, access and transfer of personal data must be restricted to individuals who have a need to know.

For APEEE such third party recipients can be for instance class representatives, volunteers for certain APEEE services (canteen, transport,…), recruitment agencies APEEE relies on for hiring new staff members, insurance companies and social security agencies to whom APEEE must provide certain personal data of employees, legal advisors and auditors of the APEEE, government authorities and instances if APEEE is obliged to do so by law or judicial process, accounting company, translators, etc..

In the beginning of each school year, APEEE collects the data of all class representatives, elected in accordance with Article 7 of the APEEE Statutes. In order to ensure that the data of class representative is shared appropriately and for the right purposes, APEEE has created the role of GDPR coordinator for each Language Section. For this function, Language Sections should preferably designate one of the four Language Section representatives (as defined in Article 12 of the APEEE Statutes), unless decided otherwise.

APEEE can transmit the data of class representatives of each Language Section only to the appointed GDPR coordinator of the respective Section, with the clear understanding that those will be used for communication purposes within the Sections, organisation of Section meetings, purposes related to the Education Councils or any other activity that derives directly from the APEEE Statutes for a period of one school year. The GDPR coordinator remains liable for any inappropriate use or mismanagement of the data of class representatives, once transmitted to him/her by the APEEE. The APEEE has a list of all service providers - with indication of whether these services providers are processor of the APEEE or not - which is to be updated as needed.

Third party recipients should process personal data shared with them by APEEE only for agreed purposes and where possible should protect personal data by applying measures substantially similar to those in this policy. If you have any questions on whether you may share personal data of APEEE's current, past, and prospective employees, members, non-members, etc. please reach out to the data protection manager.

If such third party recipient acts as a processor of APEEE (see above clause 2) for the processing of personal data, the APEEE must enter into a data processing agreement with that party. Please refer to the data protection manager for this as APEEE has an agreed template for this.

7 Cross-border transfer of personal data

If personal data is being transferred from the European Economic Area to a country outside of it which does not offer adequate protection of personal data, appropriate safeguards must be put into place to protect personal data to the standards under the Applicable Legislation and those set our herein. APEEE remains responsible for the personal data transferred and should

take the necessary measures to protect the processing thereof (through for example Standard Contractual Clauses).

In light of the above, APEEE would like to emphasize that in principle APEEE does not transfer personal data of current, past, and prospective employees, members, non-members, suppliers, etc. to recipients in countries outside of the European Economic Area. If you have any questions on this, please reach out to the data protection manager.

8 Data retention

Personal data must be kept no longer than necessary for the purposes for which the data was collected. The Applicable Legislation does not determine for how long APEEE can keep personal data; **it is up to the APEEE to determine the exact retention period**. This retention period will depend on the purpose for which we collect and process personal data. In addition, there are laws and regulations that apply to certain types of personal data and which set minimum or maximum periods for retention of personal data.

In light of the above, APEEE would like to emphasize that for each processing activity the specified data retention period is indicated in the register of processing activities and the relevant privacy policy. Unless otherwise provided in the ROPA, personal data are maintained by the APEEE for seven calendar years to comply with external auditing requirements. For any new processing activity being developed within APEEE the responsible employee for this activity will need to determine in advance for how long APEEE can keep the related personal data processed. If need be the data protection manager should be consulted to see if there are any laws and regulations imposing minimum or maximum periods for retention of personal data. Subsequently, the retention period should be completed in the register of processing activities.

Finally, once the retention period for a certain processing activity is reached personal data is/will be irreversibly deleted (or alternatively anonymized) as soon as reasonably possible and no later than necessary in relation to the purpose for which it was originally collected/processed.

9 Security

Appropriate technical, physical and organizational measures that are reasonably designed to protect personal information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, and against other unlawful forms of processing must be applied to the processing of personal data. Access to personal data is restricted to authorized recipients on a need-to know basis. In addition, the maintenance of a comprehensive information security program that is proportionate to the risks associated with the processing should be in place. Security programs should be continuously adapted to mitigate operational risks and to protect personal information, taking into account industry-accepted practices.

10 Data subjects rights

Data subjects have various rights under the Applicable Legislation which APEEE must be able to respect and honour, some of which are absolute rights and others should only be honored under certain conditions.

APEEE does not have a separate procedure for handling data subject rights' requests; the below procedure sets out in brief which rights data subjects has and how we should handle a request made by a data subject.

10.1 Which rights do data subjects have?

APEEE would like to emphasize that besides the below listed rights, all data subjects have the right to be informed about the processing of their personal data. Under the Applicable Legislation APEEE must inform data subjects about who we are, which personal data we use and for what purpose(s), the legal basis for processing the data, for how long we are keeping the data, who else might receive the data and whether the data will be transferred outside the European Economic Area, all of the data subjects rights including the right to lodge a complaint with a data protection authority.

This is a basic right of all data subjects. Data subjects do not have to exercise this right in order to be informed; APEEE must inform all data subjects of whom it processes personal data at the time of collection. APEEE provides information on its processing activities via multiple ways, e.g. the privacy policy on the website(s), the cookie policy on the website(s), the employee privacy policy available via internal distribution to staff, etc. It is important that these documents correctly state what we do and why, and that they are kept up-to-date. If you notice any errors or omissions in these policies please inform the data protection manager.

Data subjects also have the following rights:

(i) **right of access**, which provides data subjects with the right to obtain confirmation as to whether or not the APEEE is processing personal data about them and, if so, obtain access to this personal data and information regarding the processing (e.g purpose(s), which data, recipients, etc.);

(ii) **right to rectification**, which provides data subjects with the right to request correction or completion of incorrect or incomplete personal data without undue delay, and have recipients to whom personal data were provided informed of the rectification;

(iii) **right to erasure**, which provides data subjects with the right to request deletion of the personal data APEEE processes about them without undue delay. APEEE is not always obliged to honour such a request for instance when the personal data is still needed to comply with a legal obligation, or for the exercise or defence of legal claims;

(iv) **right to restrict**, which provides data subjects with the right to request APEEE to freeze the use by us of their personal data, without deleting it. In case of such a request the processing by APEEE is limited to mere storage;

(v) **right to object**, which provides data subjects with the right to oppose the processing by APEEE of their personal data. APEEE shall no longer process the data unless we can show compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the exercise or defence of legal claims;
Data subjects can at all times object to the use by APEEE of their personal data for **direct marketing purposes**. When in doubt on whether APEEE is using personal data for direct marketing purposes, please consult the register of processing activities;

(vi) **right to withdraw consent,** which provides data subjects with the right to withdraw their consent at all times in case APEEE was processing personal data based on the consent of this data subject. This is not the case when the data subject is bound by an existing contract for the provision of services. Such withdrawal shall not affect the lawfulness of the processing activity carried out prior to its withdrawal provided such consent was validly obtained;

(vii) **right to data portability**, which provides data subjects to request a transfer, copy or forward of their personal data in an easily accessible form from one data controller to another. APEEE must honour this request if we are processing personal based upon the consent of the data subject, or upon an agreement we have with the data subject.

10.2 What process must be followed in case a data subject right is exercised?

10.2.1 Identification of the request

All employees of APEEE should be aware that when a data subject exercises one or more of his/her rights (or has any questions relating to his/her personal data), the data subject can do so in any way whatsoever.

Such request will not always enter the organization of APEEE in a clear and structured manner, i.e. data subjects do not have to explicitly state which right they are exercising, nor do they have to refer to the Applicable Legislation. It is therefore key that all of us are able to recognize a request from a data subject.

Sometimes a request will be directed at the data protection manager via the dedicated email address mentioned in all of our privacy policies [privacy@apeeeb3.be], yet the data subject can also address his/her request directly to any employee of APEEE (e.g. because this person was his/her last point of contact, etc.).

Should you receive an oral request from a data subject (e.g. over the phone), you shall explain to the data subject in a friendly and clear way how and to whom a request can be made in writing.

If you receive a request directly from the data subject, you should forward this to the data protection manager without delay. The data protection manager shall take appropriate action to communicate directly with the data subject who made the request, e.g. by sending a friendly email acknowledging receipt of the request and that appropriate follow-up shall be given.

10.2.2 Validation of the request

Prior to granting or denying a request, the request should be validated by the data protection manager on a number of different aspects. Depending on the outcome of these validation checks, this process either continues, is put on hold or aborted.

- Check if in writing

  All requests received must be in writing. If the request was not in writing, the data protection manager must request the data subject to submit a written request.

- Validate identity of the requestor

  There is a risk that unauthorized third parties might attempt to exercise a data subject's rights. APEEE must use all reasonable measures to verify the identity of the data subject making the request to avoid providing data to unauthorized third parties. If we provide data to unauthorized third parties this could result in a data breach (see clause 11 below) and leave APEEE open for sanctions.

  If the data protection manager has reasonable doubts as to the identity of the data subject, he/she puts the request on hold and requests the data subject to provide additional information necessary to confirm his/her identity.

  If we cannot fully identify the data subject we need to inform the data subject accordingly and provide information on which type of information we would need to allow identification by us. This cannot be a way for us to process more data than we already have so we should look at APEEE identifiers which would allow for identification (e.g. employee number, membership number or digital identification details such as log-in credentials of a member,…. **We should not ask to be provided with a copy of the ID card or passport of an individual** as this could result in the APEEE processing more personal data than we should of an individual and this also poses a security risk for the individual if stolen for instance.

  As soon as the necessary information to confirm the identity of the data subject is provided, the request is re-initiated.

  Under the Applicable Legislation APEEE should not comply with a request if it is not in a position to identify the data subject. If a request is aborted for this reason, APEEE should inform the data subject of this. This should remain exceptional and our efforts performed in identifying the data subject should be recorded (see clause 10.2.6 below).

- Check if manifestly unfounded or excessive

Where a request is manifestly unfounded or excessive, in particular because of their repetitive character, the data protection manager must consider to either:

a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
b) refuse to act on the request.

As APEEE bears the burden of demonstrating the manifestly unfounded or excessive character of the request, the data protection manager must record such cases thoroughly (see clause 10.2.6 below), and seek approval of the APEEE management.

In the event that it is decided to charge a fee, the data protection manager informs the data subject of the fee and the payment instructions. The request is put on hold until the fee is paid.

10.2.3 Collection of information on the request

Once the data subject/requester has been identified, the data protection manager collects the required information to reply to the request. For this the data protection manager can rely on the information included in APEEE's register of processing activities, the assistance of the department and/or APEEE employee involved in the relevant processing activity, the advice of an outside counsel if this should be necessary, etc..

During this information collection process, the data protection manager should **keep track of the timing** given the deadline within which APEEE must respond to a request. Swift and efficient cooperation of each involved APEEE employee is greatly appreciated.

Where needed, IT is consulted to support this activity (e.g. extraction based on database queries). Where data is processed by a processor on behalf of APEEE, we should reach out to this processor to collect the information from them.

10.2.4 Validation of the information on the request

The data protection manager reviews the collected information to check on the following:

- are there any indications that the collection was incomplete?;
- can APEEE rely on an exemption for the specific request?;
- are there any personal data of other data subjects included in the data collected which requires APEEE to take preliminary measures (e.g. wiping out names, etc.) before sharing this with the requesting data subject?;
- does the collected information indicate a situation where APEEE may not be in compliance with the Applicable Legislation?;
- does the requestor already have access to (part of) the date, e.g. via myAPEEE site?.

10.2.5 Responding to a request

The data protection manager prepares an answer in writing to the data subject regarding his/her request based on the above performed actions. If any data was omitted from the

response due to exceptions this is mentioned to the data subject. If the request concerned the exercise of “right of access”, the required copies of the personal data are sent together with the response.

Under the Applicable Legislation APEEE must respond to each request as soon as possible and in any case within one month of receipt of the request. Throughout the handling period of the request we should inform the data subject on actions taken if need be, e.g. to confirm receipt of the request, to confirm the identity of the requestor, etc. If not all data can be provided within the expected deadline, the data protection manager already provides the data that is available and identifies the (potentially) missing data with a confirmation that it will be sent later (where possible a time estimate is provided).

10.2.6 Recording of the request

Each request made shall be recorded in a dedicated record (this can be for instance in the form of an excel sheet or word document). For each request at least the following information should be recorded:

- the date of receipt of the request;
- the type of request (see clause 10.1 above);
- the means of validation of the identity of the data subject making the request;
- the date of reply; and
- a brief description of the reply made, indicating in general whether the submitted request was lawful or denied (and on which ground).

11 Personal data breach

APEEE does not have a separate procedure for handling data breaches; the below procedure sets out in brief how we should handle personal data breach incidents.

11.1 What is a personal data breach?

A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed. See Annex 2 for examples of personal data breaches and who to notify.

11.2 What process must be followed in case of a potential personal data breach?

11.2.1 Identify and report a potential incident involving personal data

Any employee of APEEE who has identified a potential personal data breach (e.g. stolen or lost device with personal data on it, receipt of an email from a member reporting suspicious e-mail activity from APEEE, etc.) should report this without undue delay to the data protection manager.

The attached form in Annex 3 can be used for this. This is a very short form which requires you to complete some basic information concerning the potential data breach. Once completed you should send it via email to the data protection manager. APEEE would like to emphasize that it wants to create a positive attitude towards data protection and welcomes any report of an incident. Data protection manager will explore the facts and report to the APEEE Director and the Board President. No disciplinary actions shall be taken if a report is made of an incident which afterwards does not appear to be a personal data breach. Any report is in the interest of APEEE and can be used for training purposes and sharing lessons learned.

11.2.2 Investigate potential personal data breach

Note that after first being informed of a potential personal data breach, the data protection manager may undertake a short period of investigation in order to establish what the impact is and whether or not personal data was involved. The initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a personal data breach has taken place and the possible consequences for the data subject. A more detailed investigation can follow.

11.2.3 Record potential personal data breach

The data protection manager reports the incident and all relevant information concerning the incident in a dedicated record, e.g. the facts relating to the Personal Data Breach (what took place, which data was affected), the root cause(s), its effects and consequences, and the remedial action taken. If need be, the data protection manager can perform interviews with anyone within APEEE to gather the required information.

11.2.4 Evaluate severity and escalate the incident

The data protection manager further consults with relevant APEEE staff to assess the type and amount of personal data at risk, the extent of the incident, the persons affected by the incident and the risk of harm to data subjects and APEEE

A necessary component of this response involves assessing the likely risk to data subjects that may result in order to determine whether the requirement for notification has been triggered, as well as the action(s) needed to address the personal data breach.

To evaluate the risks, the data protection manager evaluates the following:

1. What Personal Data is involved

- What type of personal data is involved?
- Is sensitive personal data involved? How sensitive is the information? Generally, the more sensitive the information, the higher the risk of harm. Some personal data is more sensitive than others (e.g., health information, social security numbers, and financial account numbers such as credit or debit card information). A combination of personal data is more sensitive than a single piece of information. However, sensitivity alone is not the only criteria in assessing risk, as foreseeable harm to data subjects is also important.

- How many data subjects are affected? Assessing the number of data subjects affected will help you gauge the severity of the problem and will be relevant in deciding whether or not to notify local privacy authorities.
- With lost data, what protections were in place to protect the information at the time of the breach (for example, encryption)? If the information was coded or encrypted, how easy is it to decode the information?
- Can the personal data be used by third parties for fraudulent or otherwise harmful purposes?

2. Cause and extent of the Personal Data Breach

- How did the personal data breach occur?
- Was the personal data breach inadvertent or intentional?
- Is there a risk of further exposure of the personal data?
- Was the personal data adequately encrypted?
- If the personal data was stolen, can it be determined whether the personal data was the target of the theft or not?
- Can the personal data be recovered?
- What steps have already been taken to mitigate harm?

3. Who is affected by the Personal Data Breach?

- Who is affected by the incident (employees, contractors, public, clients, service providers, other)?
- Does the risk affect data subjects in multiple EU countries?

4. Determine Risk of Harm to Data Subject

- If the personal data has been stolen, what is the potential risk of misuse?
- What harm to the data subject could result from the personal data breach? Examples include: security risk (i.e., physical safety), identity theft, financial loss, loss of business or employment opportunities, humiliation, damage to reputation or relationship.ps.

It is important to document these findings as it may be necessary to communicate them to the data subject affected by the personal data breach.

A personal data breach may potentially result in complaints, reputational damage, fines and litigations, etc. Therefore, and depending on the severity, the necessary escalations may need to be initiated. As a minimum, the data protection manager must escalate the incident recorded under item 11.2.3 and its severity to the APEEE Director and the Board President, so that they can evaluate and decide whether or not the incident must be notified as a personal data breach. Each incident needs to be considered on a case-by-case basis to determine whether a personal data breach notification is needed.

11.2.5 Decide if Personal Data Breach notification is needed

The APEEE Director and the Board President must evaluate the information provided to it in order to determine whether or not the incident must be notified as a personal data breach.

Note that if the personal data breach is likely to result in a risk to the rights and freedoms of data subjects, a notification to the data protection authority is required. of course, in case APEEE is the processor, the third party data controller will need to be notified.

Furthermore, if the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, an additional notification to the data subjects will be required.

Such notification is to be made without undue delay and, where feasible, not later than 72 hours after having become aware of the personal data breach. Where the notification to the supervisory authority is not made within 72 hours, the APEEE must include the reasons for the delay in the notification.

In the event that a notification is needed, to the supervisory authority, the data subject, or the third party controller, the data protection manager prepares the different communications related to the personal data breach notification. To ensure that the required information is communicated please consult the content of articles 33 and 34 of the GDPR.

12 Register of processing activities

Pursuant to its obligations under the Applicable Legislation, APEEE has established a dedicated register of processing activities in which all activities of the APEEE which involve processing of personal data are recorded.

This register contains the minimum information as required under the Applicable Legislation, e.g. the identification of the purpose(s) of the processing activity, description of the individuals whose data are being processed, identification of the retention period, etc. This register is available to all APEEE employees via email.

When new activities are being developed within APEEE, and such activity involves processing of personal data, the responsible department or employee for this activity must reach out to the data protection manager to ensure this register is updated accordingly. The same applies when changes to existing activities of the APEEE, which involve processing of personal data are being considered.

13 Training and awareness

The existence of this policy and other written policies and procedures concerning data protection is not enough to ensure APEEE acts in compliance with the Applicable Legislation. It is important to continually sharpen awareness so that employees become more knowledgeable about the risks involved. Safe and responsible behavior is encouraged.

For this reason, APEEE will take reasonable and appropriate steps to inform its employees on the content of this policy and to provide appropriate training on the requirements of this policy. Such reasonable steps can include, amongst other things, sending regular communication on

this policy via email or other means (e.g. posters,…), sending regular communication to employee matters on information security matters (e.g. staying alert for phishing, importance of recognizing phishing from spam, etc.), as needed setting up a meeting with all employees of APEEE to discuss also this policy, the importance of compliance and possibly share lessons learned from past compliant and/or non-compliant behavior, etc.

Furthermore, all newly hired employees of APEEE will receive information on this policy from the data protection manager within one month of the start of their employment.

In addition, APEEE will ensure that all employees receive at a given time a dedicated training on data protection and all related policies, procedures and documents within APEEE. The data protection manager and other key employees in relation to data protection, such as the APEEE Director, can follow dedicated trainings on data protection matters to the extent these are relevant for the tasks performed within the APEEE.

14 Roles and responsibilities

Compliance with this policy is a responsibility of everyone within APEEE. Each department within APEEE is responsible for processing personal data in compliance with this policy and as such all APEEE employees must familiarize himself/herself with this policy.

In this respect it is essential that roles and responsibilities are clearly defined:

Data protection manager	APEEE has appointed a data protection manager (also acting as an IT manager) who will manage and control APEEE's compliance with the Applicable Legislation for all of its activities that involve processing of personal data. Note that APEEE is not required to appoint a data protection officer. Tasks of the data protection manager include the following: • handling of data protection questions from APEEE employees and APEEE management; • reviewing and updating, where necessary, all data protection policies, procedures and other related data protection documents (such as the register of processing activities,..) at least once a year. To do this he/she can rely on the assistance of all APEEE departments and employees; • dealing with requests from data subjects about APEEE's processing of their personal data; • acting as point of contact for the data protection authorities; • ensuring that personal data are irreversibly deleted or anonymized pursuant to this policy and other relevant data protection policies, procedures and documents;

	• ensuring that in the event of a breach or irregularity, the required information concerning this breach or irregularity is documented and if need be the required notifications are sent to the relevant data protection authorities and data subjects whose personal data is at risk; • reporting to APEEE Director and Board President directly on data protection responsibilities, risks and issues on an annual basis.
APEEE management	The management of APEEE is also responsible for compliance with this policy and other relevant data protection policies and procedures within APEEE. Every data protection policy, procedure or other relevant data protection document is reviewed and approved by the management. More importantly the management of APEEE is ultimately accountable for compliance with the Applicable Legislation and therefor it also relies on the cooperation of each employee within APEEE.
APEEE employees	Each employee within APEEE is responsible for the personal data processed by it in compliance with this policy. For this you can always rely on the assistance of your APEEE Director and of course the data protection manager. To help each employee in this task APEEE has included some practical guidelines in Annex 1 to this policy.
External service provider	To provide training and awareness on data protection matters to APEEE employees in lieu of the data protection manager.

15 Compliance

Failure to comply with this policy can introduce significant security risks regarding the confidentiality, integrity and availability of (sensitive) information and can temporarily or permanently damage the reputation of APEEE. Failure to comply with this policy can also leave APEEE open to fines and other sanctions under the Applicable Legislation.

Any presumed or established non-compliant behavior must be reported to the [data protection manager] to determine the appropriate actions for remediation (e.g. increase trainings towards employees, share lessons learned with employees, ensure that related data protection policies and other documentation is updated, etc.).

Annex 1: Practical guidelines for APEEE employees

Any APEEE employee handling personal data must ensure that it is processed in accordance with this policy and the Applicable Legislation. The following practical guidelines apply to all employees:

- **access to personal data** should only be granted for professional purposes and on a **'need-to-know' basis** meaning personal data will only be processed and employees will only have access to personal data when appropriate and necessary for the type and scope of the task in question.
- Personal data of members, (non-member) parents, pupils, employees should not be **disclosed to unauthorized people** within APEEE and externally.
- You should only have **access to personal data** you **require to complete your** tasks. If you feel you have access to personal data you should not have available to you, please report this to the data protection manager.
- You **cannot use** personal data of APEEE data subjects for your own **private or commercial purposes**.
- **Strong passwords** must be used and should never be shared. APEEE shall never ask you to communicate your password.
- You should **keep all data secure** at all times, by taking precautions and strictly following any and all of the provisions in this policy.
- You should **not make off-system copies** of personal data. Do not copy files to a local or removable drive.
- You are required to report loss or theft of any device that contains personal data and/or has access to the APEEE.
- You are forbidden to use any kind of **cloud storage service not approved** by the IT department and/or to install or use **software not approved** by the IT department.
- When working with personal data, you should ensure that **screens of your computers are always locked** when left unattended.
- Personal data should be regularly reviewed to ensure it **is up-to-date** and, if not, update it. If this is not possible, these personal data should be irreversibly rendered anonymous; or be deleted.
- You should always **request help** from either your Director and of your IT and data protection manager, if you are unsure about any aspect of data protection.

Annex 2: Examples of personal data breaches

The following non-exhaustive examples assist in determining whether APEEE needs to notify in different personal data breach scenarios where APEEE is the controller. These examples may also help to distinguish between risk and high risk to the rights and freedoms of data subject.

Example	Notify the supervisory authority?	Notify the Data Subject?	Notes/recommendations
APEEE stored a backup of an archive of Personal Data encrypted on a CD. The CD is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist, and the unique key is not compromised, this may not be a reportable personal data breach. However, if it is later compromised, notification is required.
Personal Data of data subject are exfiltrated from a secure website managed by APEEE during a cyber-attack.	Yes, report to competent supervisory authority if there are potential consequences to data subject.	Yes, report to data subject depending on the nature of the personal data affected and if the severity of the potential consequences to data subject is high.	If the risk is not high, it is recommended for APEEE to notify the data subject, depending on the circumstances of the case.
APEEE suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes, report to the competent supervisory authority, if there are potential consequences to data subject as this is a loss of availability.	Yes, report to data subject, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to Data Subject as there would have been no permanent loss of availability or confidentiality. However, the supervisory authority may consider an investigation to assess compliance with the broader security requirements of Article 32 GDPR.
A data subject phones APEEE to report a personal data breach. The data subject has received a monthly report for someone else. APEEE undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and if it	Yes.	Only the data subject affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more data subject are affected, an update to the supervisory authority must be made and APEEE takes the additional step of notifying other data subject if there is high risk to them.

Example	Notify the supervisory authority?	Notify the Data Subject?	Notes/recommendations
is a systemic flaw so that other data subjects are or might be affected.			

Annex 3: Incident Report Form

Incident Report Form for staff of APEEE	
Date incident occurred:	
Location of incident:	
Does the breach involve personal data	Yes ☐ No ☐ If yes, please describe to the best of your ability which personal data:
Type of data breach	☐ Digital, e.g. hacking, virus, ransomware, file corruption, etc. ☐ Paper, e.g. lost or misplaced files, et. ☐ electronics, e.g. lost laptop, phone, USB device,… ☐ other, e.g. wrong information given over the phone, via e-mail by for instance sending information to wrong recipient or including e-mail addresses in CC rather than BCC
Details of incident *Please describe the facts of the incident and include details of staff involved. Although generally you should refrain from taking any actions without first consulting the data protection manager, please describe here which actions have already been taken if any.*	
Please e-mail this form to the data protection manager: privacy@apeeeb3.be	