OUR GENERAL DATA PROTECTION POLICY

AIESEC Singapore

Data Protection Policy

Last Updated: 3.12.2018

1. Introduction

1.1. General Statement

We are required to process relevant personal data regarding members/employees, volunteers, applicants, alumni and customers as part of our operations: thus, we shall take all reasonable steps to do so in accordance with this policy. It is important that personal data is processed lawfully and appropriately, in accordance with the requirements of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and abiding by the appropriate local/national laws regarding privacy.

*Personal data* is any information relating to an identified or identifiable individual, such as members/employees, volunteers, applicants, alumni, customers and anyone else with whom we do business. Personal data is an important and valuable asset, and the way we handle this data should demonstrate respect, promote trust and avoid security incidents. In many cases, there are laws that govern how we collect, use and dispose of personal data: for these reasons, we must follow the law and the internal policies/guidelines for handling personal data.

We respect the confidentiality of personal data, in both paper and electronic form: information shall not be used/disclosed improperly and/or used by someone who is not authorised to do so. Furthermore, we are committed to protecting and respecting the privacy of our stakeholders, because we respect the trust that is being placed in us to use personal information appropriately and responsibly: therefore, we have to take our data protection duties seriously.

1.2. About this Policy

This website uses cookies and other similar technologies to provide you with a better experience, assist with navigation, analyse your use of our products and services, personalise content and marketing efforts and provide content from third parties. Third parties may follow your internet behaviour through such tracking cookies. By clicking "I accept cookies!" you agree with all cookies used by this website. You can refuse cookies via settings. In case you want to get to know more, please visit our cookie policy.

I ACCEPT COOKIES!  NO  PRIVACY POLICY
Every director, member/employee, contractor and third party – including the ones related to the local committees – working for or acting on behalf of AIESEC Singapore, including AIESEC in NTU, AIESEC in NUS, AIESEC in SIM and AIESEC in SMU must be aware of and follow this policy.

Our Data Protection Officer is responsible for ensuring compliance with the data protection requirements and with this policy ("please refer to point 5., "Data Protection Officer"). Any questions about the operation of this policy and/or any concerns that this policy is not being followed should be referred to the Data Protection Officer.

### 1.3. Main Definitions

Expressions mentioned in this policy shall have the same meaning provided by the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and the appropriate laws. For basic understanding of this policy, the main concepts are:

- **Personal data** (whether stored electronically or paper based) means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- **Special categories of personal data** is an expression which refers to sensitive categories of personal data, such as the ones regarding a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, sexual orientation or sexual life. In general, it is forbidden to process sensitive personal data; in case it is processed, conditions must be met. *Please note that data about criminal offences or convictions are another “special” category and we do not process such data.*

### 2. Data Processing Principles

Anyone processing personal data must ensure that activities respect the provisions of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), ensuring that data is:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- processed for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
- accurate and, where necessary, kept up-to-date;
- kept in a form which permits the identification of the data subject for no longer than is necessary for the purposes for which the personal data are processed.

This website uses cookies and other similar technologies to provide you with a better experience, assist with navigation, analyse your use of our products and services, personalise content and marketing efforts and provide content from third parties. Third parties may follow your internet behaviour through such tracking cookies. By clicking "I accept cookies!" you agree with all cookies used by this website. You can refuse cookies via settings. In case you want to get to know more, please visit our cookie policy.

I ACCEPT COOKIES!  NO  PRIVACY POLICY
• not kept for longer than necessary for the intended purposes;
• processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Lastly, we must be able to demonstrate compliance with all the principles mentioned above – and, of course, respect the rights of the data subjects. In this way, we must keep a register of data processing activities, which must be updated periodically and reflect/regulate the way we use personal data.

2.1. Lawfulness, Fairness and Transparency

Processing must be done fairly and without adversely affecting the rights of the individual: thus, in accordance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), we will only process personal data where it is in line with a lawful ground – which, according to the relevant provisions of the Article 6 (1) of such regulation, are:

• the data subject has given consent to the processing of his/her personal data for one or more specific purposes;
• processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
• processing is necessary for compliance with a legal obligation to which the controller is subject;
• processing is necessary in order to protect the vital interests of the data subject or of another natural person;
• processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
• processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Please note that when sensitive personal data is being processed, additional conditions must be met. Furthermore, all processing activities must be recorded in the appropriate register.

2.1.1. Consent

Whenever consent is the lawful basis for processing, it must be:

• recorded, so that we can demonstrate that the data subject has consented to the processing of his/her personal data;
If communications (including direct marketing) are sent to individuals based on their consent, the option for the individual to revoke consent must be clearly available and systems should be in place to ensure such revocation is reflected effectively.

2.2. Purpose Limitation

We may collect and process the personal data we receive directly from a data subject (for example, when he/she completes forms and/or sends information via mail, phone or email) and data we receive from other sources (including, for example, location data, business partners, payment/delivery services and others).

We will only process personal data for specific purposes or for any other purposes specifically permitted by the data protection laws. We must notify the purposes to the data subject when we first collect the data (in case data was provided directly to us) or as soon as practicable (where data was received from a third party).

2.2.1. Information to Individuals

Whenever we process personal data relating to an individual, we will inform the data subject about:

- the purpose(s) for which we intend to process that personal data, as well as the legal basis for the processing;
- where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued;
- the recipients or categories of recipients of the personal data, if any;
- the fact that we intend to transfer personal data to a country or international organisation outside the European Union/European Economic Area and the appropriate and suitable safeguards in place;
- the existence of each of the rights of the data subject and their respective explanation, paying special attention to:
  - the right to request from us ("considering that we are the "data controller") access to and rectification or erasure of personal data or restriction of processing;
  - the right to object to processing and the right to data portability.
- information about the period that the information will be stored or the criteria used to determine that period;
- the right to withdraw consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn. This right must be indicated at the moment the consent of the data subject is requested and/or in the appropriate privacy notice;
- the right to lodge a complaint with the appropriate supervisory authority;
- the right to lodge a complaint with the appropriate supervisory authority;
Data subjects shall also be able to understand how to exercise their rights: in order to comply with these points (from the details regarding information to the enforcement of the rights), we shall have in place a easily accessible privacy notice.

Regarding the deadlines for providing such information, it is important to consider the source of the personal data and remind that:

- if personal data was obtained directly from the individual, we must inform him/her about the points mentioned above at the time when data is obtained. In addition, he/she must also be provided with the following:
  - whether the provision of the personal data is a statutory or contractual requirement/obligation, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any possible consequences of failing to provide the data.
- if personal data was obtained from other sources, we must provide him/her with this information as soon as practicable, but within one month of obtaining it. The individual must also be provided with:
  - the types or categories of personal data which are to be processed;
  - the source the personal data originates from and whether it came from publicly accessible sources.

2.3. Data Minimisation

We must process data in an adequate, relevant and non-excessive manner: thus, we will only collect personal data to the extent that it is required for the specific purpose(s) notified to the data subject.

2.4. Accuracy

We will ensure that personal data we hold is accurate and kept up-to-date.

In order to comply with such principle, we will check the accuracy of any personal data at the point of collection and at regular intervals subsequently, taking all reasonable steps to destroy/correct inaccurate or out-of-date data and giving individuals the opportunity to enforce their right to rectify data concerning them.

2.5. Storage Limitation

We will not keep personal data longer than is necessary for the purpose(s) for which it was collected. We will take all reasonable steps to erase/anonymise or archive from our systems all data which is no longer required, following our internal retention policies.

This website uses cookies and other similar technologies to provide you with a better experience, assist with navigation, analyse your use of our products and services, personalise content and marketing efforts and provide content from third parties. Third parties may follow your internet behaviour through such tracking cookies. By clicking "I accept cookies!" you agree with all cookies used by this website. You can refuse cookies via settings. In case you want to get to know more, please visit our cookie policy.
We must process data in accordance with the rights of the data subjects and in a manner that ensures security, integrity and confidentiality, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

Personal data shall not be transferred to people/organisations situated in countries without adequate protection safeguards or in situations which do not meet the appropriate circumstances mentioned in the Articles 44–49 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). Please note that the individual must be informed of the transfer.

### 2.6.1. Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place technical and organisational measures to maintain the security of all personal data under our responsibility, during the whole flow. In this way, personal data will only be transferred to data processors if they agree to comply with the procedures and policies and/or if they put in place adequate measures.

Our processing activities will be guided by the concepts of confidentiality and integrity of the personal data, as specified below:

- confidentiality, applying measures which guarantee that data is protected against unauthorised or accidental use or disclosure – and, therefore, accessed only by people who are authorised to use the data and who are needed for the achievement of the purposes;
- integrity, applying measures which guarantee that data is protected against unauthorised or accidental loss, destruction or alteration and guaranteeing that it is accurate and suitable for the purpose(s).

Our security procedures include:

- secure offices and workplaces, guaranteeing that the files are stored in buildings which count on appropriate safeguards (such as locks, security systems, etc.) and on furniture which allows extra protection (e.g.: locked drawers, etc). Personal information is always considered confidential and should be kept in a secure place.

This website uses cookies and other similar technologies to provide you with a better experience, assist with navigation, analyse your use of our products and services, personalise content and marketing efforts and provide content from third parties. Third parties may follow your internet behaviour through such tracking cookies. By clicking "I accept cookies!" you agree with all cookies used by this website. You can refuse cookies via settings. In case you want to get to know more, please visit our cookie policy.
information is not shown to passers-by and that they log off from systems/platforms/devices whenever they are left unattended;

- usage of modern and secure softwares which are kept-up-to-date;
- review and update of data which is out-of-date, taking every opportunity to ensure data is up-to-date;
- storage of data in as few places as necessary, without creating unnecessary additional data sets;
- methods of disposal, such as shredding papers and/or anonymising/erasing virtual data whenever it must be destroyed;

**Our staff should also pay attention to further guidelines:**

- the only people able to access the data covered by the policy shall be those who need it for their work and for the achievement of the purpose(s) informed to the data subject;
- data shall not be shared – formally or informally – to individuals outside our organisation except where it is necessary to do so in order to facilitate an exchange experience;
- our staff should participate in the trainings/activities regarding data protection, read the appropriate materials and get to know the appropriate laws;
- members/employees shall keep all data secure, by taking sensible and reasonable precautions. Thus, it is advised that they:
  - use strong passwords in systems/platforms/devices;
  - never share passwords;
  - never disclose personal data to unauthorised individuals, either within the organisation or outside it;
  - never leave personal data unattended and/or where unauthorised people could see it;
  - use only appropriate services/platforms/systems and secure devices;
  - request help to the appropriate managers/Data Protection Officer in case they are unsure about any aspect of data protection.

### 2.6.2. Data Transfers

As a general rule, personal data may be transferred outside the European Union/European Economic Area or to an international organisation only if the country to which the personal data is transferred ensures an adequate level of protection for the rights and freedoms of data subjects.

Personal data may also be transferred based on appropriate safeguards or in case one of the derogations of the Article 49 (1) of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is met, especially:

- the data subject has given his/her explicit consent, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

This website uses cookies and other similar technologies to provide you with a better experience, assist with navigation, analyse your use of our products and services, personalise content and marketing efforts and provide content from third parties. Third parties may follow your internet behaviour through such tracking cookies. By clicking "I accept cookies!" you agree with all cookies used by this website. You can refuse cookies via settings. In case you want to get to know more, please visit our cookie policy.
• the transfer is legally required on important public interest grounds or for the establishment, exercise or
defence of legal claims.

Subject to the requirements mentioned above, personal data we hold may be processed by staff
operating outside the European Union/European Economic Area who work for us: such staff
may be engaged in, among other things, the fulfilment of contracts with the data subject, the
provision of support services, etc.

2.6.3. Disclosure of Personal Data

Personal data shall not be transferred to external individuals and/or organisations except where
it is necessary to do so in order to facilitate an exchange experience. Internally, data may be
processed by the individuals acting under the power of AIESEC Singapore.

Personal data may also be disclosed to the appropriate agencies in accordance with the law.

3. Rights of the Data Subject

Anyone processing personal data must ensure that activities respect the provisions of the
General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), guaranteeing that
the rights of the data subjects are respected, in particular:

- right to be informed, receiving proper details on how data is going to be processed ("please refer to point
  2.2.1., “Information to Individuals”);
- right to access, being able to receive a confirmation as to whether or not personal data concerning him/her
  is being processed and access any data held about him/her by the data controller, following the provisions
  of the Article 15 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679);
- right to rectification, being able to request rectification or completion of data concerning him/her;
- right to object, being able to express that he/she does not – or no longer – agree with the processing and,
  therefore, asks the data controller to stop processing activities regarding a particular situation. This right
  applies to direct marketing; thus, please note that the right to object to direct marketing is absolute and
  we must not challenge the decision of the individual, stopping such processing activities immediately;

- right to erasure, being able to request the erasure of personal data where there is no compelling reason for its
  continued processing. Please note that this right is subject to some specific circumstances, which are mentioned in the
  Articles 17 and 19 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679);

This website uses cookies and other similar technologies to provide you with a better experience, assist with navigation,
analyse your use of our products and services, personalise content and marketing efforts and provide content from third
parties. Third parties may follow your internet behaviour through such tracking cookies. By clicking "I accept cookies!" you
agree with all cookies used by this website. You can refuse cookies via settings. In case you want to get to know more, please
visit our cookie policy.
• the primary right not to be subject to activities only based on automated processing and whose decisions have legal or relevant effects on him/her;

• the secondary rights – whenever automated decision-making is carried out either because of a contract or because of the consent of the data subject – to be informed (*about the existence of automated decision-making, its logics/criteria and consequences), express his/her point of view, challenge the decision and obtain human intervention.

• right to compensation and liability, as well as the right to lodge a complaint with a supervisory authority.

We shall inform data subjects of their rights and we shall also make it easy for data subjects to enforce their rights, using the respective appendix according to the type of contract for information, while using the email address of the Data Protection Officer to enforce their rights. Personal data shall be easily accessible to the appropriate individuals within our organisation and, where possible, data subjects should have access to their data via a secure self-service (*please refer to point 4., "Subject Access Requests").

4. Subject Access Requests

Data subjects can send a request for information regarding if and what information we hold about them, why we hold such data, how to gain access to data, how to correct/update details, how we deal with data protection, etc. (*please refer to point 3., "Rights of the Data Subject").

Whenever a member/employee receives a request, it shall be forwarded to Alejandro Hüsser Diaz (alejandro.husser.2@aiesec.net) immediately.

Data subjects shall be informed of their right and must know that they should address their requests to the Data Protection Officer: Alejandro Hüsser Diaz, via email (alejandro.husser.2@aiesec.net).

We may take reasonable steps to verify the identity of the individual who is requesting the data: personal data shall only be sent to the individual to which it is related, so it is vital to make sure that information is only given to a person who is entitled to it. Every request sent in writing must be responded within one month – and, if the request is made electronically, data shall be provided electronically (where possible).

Please note that we may supply the data subject with a standard request form, but the
It is vital that the Article 15 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is read and followed. Besides, the guidelines below shall be useful.

### 4.1.1. Procedures upon receipt of a Subject Access Request

Whenever we are the data controller, we shall proceed with the following steps upon receiving a Subject Access Request:

- confirm whether we are the "data controller";
- verify the identity of the data subject; if necessary, request any further evidence regarding the identity of the data subject;
- verify if the access request is sufficient and if the requested information is clear; if not, request additional information;
- verify whether requests are unfounded or excessive (particularly if they are repetitive); if so, we may refuse to act on the request or charge a reasonable fee. We shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request;
- promptly acknowledge receipt of the request and inform the data subject of any costs involving its processing. Please note that, as a general rule, the request must be handled free of change;
- verify whether we process the data requested; if we do not process any data, inform the data subject accordingly;
- verify whether the data requested also involves data about other data subjects and make sure this data is filtered before the requested data is supplied to the data subject.

### 4.1.2. Procedures to respond to a Subject Access Request

Whilst responding to a subject access request, follow the guidelines below:

- make sure to respond to the request within one month after it is received:
  - if the request is particularly complex, we may extend this initial period by two months, but we must communicate to the data subject in a timely manner within the first month and explain why the extension is necessary;
  - if we do not take action on the request of the data subject, we must inform the data subject about the reasons for not taking action and of his/her rights to lodge complaints/seek judicial remedy at latest within one month of receipt of the request.
- if a request is submitted in electronic form, information should preferably be provided in a commonly used electronic format (*e.g.: text or html). It is not forbidden to send information via email, but we must ensure that the transfer is secure;
- if information is kept on paper, we can provide the data subject with a paper copy of his/her information;
- if data on the data subject is processed, make sure to include at least the following information in the response:
  - the purposes of the processing;
  - the categories of personal data concerned;
  - the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data;
where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

- the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the data has not been collected from the data subject, the source of such data;
- the existence of any automated decision-making (including profiling) and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

- provide a copy of the personal data undergoing processing. Once again, this should be provided in a commonly used electronic form if the data subject has submitted the request electronically and if he/she does not request otherwise.

- An organisation shall not provide an individual with the individual’s personal data or other information if the provision of that personal data or other information, as the case may be, could reasonably be expected to —
  (a) threaten the safety or physical or mental health of an individual other than the individual who made the request;
  (b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
  (c) reveal personal data about another individual;
  (d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or
  (e) be contrary to the national interest.

- An organisation shall not inform any individual that it has disclosed personal data to a prescribed law enforcement agency if the disclosure was made without the consent of the individual.

- If an organisation is able to provide the individual with the individual’s personal data and other information requested without the personal data or other information excluded, the organisation shall provide the individual with access to the personal data and other information without the personal data or other information excluded in the previous points.

## 5. Data Protection Officer

We have appointed Alejandro Hüsser Diaz as the Data Protection Controller (DPO) who will endeavour to ensure that all personal data is processed in compliance with this policy and with the principles of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). Appropriate national laws are also relevant to this policy.
7. **Data Breaches**

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, we shall promptly assess the risks to the rights and freedoms of individuals: if necessary, the breach shall be reported to the appropriate supervisory authority – and, if appropriate, the individuals affected by the incident shall be communicated. Please refer to our *Data Breach Management Procedure* and to the appropriate templates.

8. **Disclaimer**

This policy should be used together with other documents, which are mentioned below:

- Data Breach Management Procedure;
- Internal Retention Policies;
- Personal Data Protection Act 2012 (PDPA)

9. **Alterations to this Policy**

We reserve the right to change this policy at any time. Where appropriate, we will notify changes by email.