Data Privacy Protection Policy Statement

Introduction

Hong Kong Aid Services CIC takes its responsibilities with regard to the management of the requirements of the General Data Protection Regulation (GDPR) very seriously. This policy sets out how we manage those responsibilities.

Hong Kong Aid obtains, uses, stores and otherwise processes personal data relating to potential, current, former clients, contractors, website users and contacts, collectively referred to in this policy as data subjects. When processing personal data, we are obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation (data protection law).

This data privacy protection statement explains how and what personal data we collect from you through this survey. We collect your data through conducting surveys etc. in accordance with Article 4 Clause 7 of the EU General Data Protection Regulation (GDPR).

The data processed by us are deleted or their processing is limited in accordance with Articles 17 and 18 of the GDPR. Unless explicitly stated otherwise in this data privacy statement, the data stored by us are deleted as soon as it is no longer required for its intended purpose and no legal obligations to retain data prevent its deletion. Limitations are imposed on the processing of the data which has been not deleted because it is required for other legally allowed purposes. In other words, such data is blocked and not accessible for processing for any other purpose.

Data protection policy purposes

This policy therefore seeks to ensure that we:

1. are clear about how personal data must be processed and the University's expectations for all those who process personal data on its behalf;

2. comply with the data protection law and with good practice;

3. protect the organization's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights

4. protect the organization from risks of personal data breaches and other breaches of data protection law.

Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff and others processing personal data on the organisation's behalf must read it. A failure to comply with this policy may result in disciplinary action.

All internal management staff should implement appropriate practices, processes, controls and training to ensure that compliance.

The secretariat is responsible for overseeing this policy.

Our Data Protection Officer can be reached through admin@hkaid.uk at any time.

Personal data protection principles

When you process personal data, you should be guided by the following principles, which are set out in the GDPR. The organisation is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below:

Those principles require personal data to be:

1. processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency).

2. collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose limitation).

3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data minimisation).

4. accurate and where necessary kept up to date (Accuracy).

5. not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (Storage limitation).

6. processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality).

Data Subjects' Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

1. where the legal basis of our processing is Consent, to withdraw that Consent at any time;

2. to ask for access to the personal data that we hold (see below);

3. to prevent our use of the personal data for direct marketing purposes

4. to object to our processing of personal data in limited circumstances

5. to ask us to erase personal data without delay:

a. if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

b. if the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data;

c. if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;

d. if the data subject has objected to our processing for direct marketing purposes;

e. if the processing is unlawful.

6. to ask us to rectify inaccurate data or to complete incomplete data;

7. to restrict processing in specific circumstances e.g. where there is a complaint about accuracy;

8. to ask us for a copy of the safeguards under which personal data is transferred outside of the EU;

9. the right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with the University; it is based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards;

10. to prevent processing that is likely to cause damage or distress to the data subject or anyone else;

11. to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

12. to make a complaint to complaint and handling team; and

13. in limited circumstances, receive or ask for their personal data to be transferred to a third party (e.g. another organisation to which a client is transferring) in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed

Requests (including for data subject access – see below) must be complied with, usually within one month of receipt. You must immediately forward any Data Subject Access Request you receive to the Information Compliance Team at admin@hkaid.uk. A charge can be made for dealing with requests relating to these rights only if the request is excessive or burdensome.

Accountability

The organisation must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The organisation is responsible for, and must be able to demonstrate compliance with, the data protection principles.

We must therefore apply adequate resources and controls to ensure and to document GDPR compliance including:

1. appointing a suitably qualified staff;

2. implementing Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects;

3. integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches;

4. training staff on compliance with Data Protection Law and keeping a record accordingly; and

5. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

University responsibilities

As the Data Controller, we are responsible for establishing policies and procedures in order to comply with data protection law.

Staff responsibilities

Staff members who process personal data about clients or any other individual must comply with the requirements of this policy. Staff members must ensure that:

(a) all personal data is kept securely;

(b) no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;

(c) personal data is kept in accordance with the organisation's retention schedule;

(d) any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Information Compliance team;

(e) any data protection breaches are swiftly brought to the attention of the Information Compliance team and the data protection staff and that they support the Complaint handling team in resolving breaches;

(f) where there is uncertainty around a data protection matter advice is sought from the Information Compliance team and the data protection staff.

Where members of staff are responsible for supervising students doing work which involves the processing of personal information (for example in research projects), they must ensure that those students are aware of the Data Protection principles.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Information Compliance team or the secretariat.

Data Subjects' responsibilities

Data subjects are responsible for:

(a) familiarising themselves with the Privacy Notice provided when their data has been collected by us;

(b) ensuring that their personal data provided to us is accurate and up to date.

Sharing Personal Data

In the absence of Consent, a legal obligation or other legal basis of processing, personal data should not generally be disclosed to third parties unrelated to the organisation (e.g. clients' parents, members of the public, private property owners).

Some bodies have a statutory power to obtain information (e.g. regulatory bodies such as the Health & Care Professions Council, the Nursing and Midwifery Council, government agencies such as the Home Office, UK Visa and Immigration and Child Support Agency). You should seek confirmation of any such power before disclosing personal data in response to a request. If you need guidance, please contact the Information Compliance team on admin@hkaid.uk.

Further, without a warrant, the police have no automatic right of access to records of personal data, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders. You should seek written assurances from the police that the relevant exemption applies. If you need guidance, please contact the secretariat at admin@hkaid.uk.

Some additional sharing of personal data for research purposes may also be permissible, subject to certain safeguards.

Changes to this policy

We reserve the right to change this policy at any time without notice to you so please check regularly to obtain the latest copy.

This policy was announced on 17 July 2021 by the Internal Management staff. It will be reviewed in a time no later than 2030.

Appendix 1 - Use of Google Analytics

(1) The website may use Google Analytics, a web analytics tool by Google LLC ("Google"). Google Analytics uses so-called "cookies", i.e. text files stored in your computer which enable us to analyse how you use our website. The information automatically collected by cookies concerning your use of this website is typically transmitted to and stored on a Google server in the United States. Google will mask some parts of your IP address and shorten it within the EU member states or within other states - parties to the Agreement on the European Economic Area. The full IP address will be transmitted to a Google server in the United States and shortened there solely in exceptional circumstances. Upon instruction from the controller (operator of this website), Google will use this information to analyse use of the website by you, to compile reports about your website activity and to provide the website operator other services concerning use of the website and of the Internet.

(2) Google will not associate the IP address transmitted from your browser through Google Analytics with any other data held by Google.

(3) You can also disable acceptance of cookies by your computer by configuring your browser settings accordingly; please note, however, that in such a case you most probably will not be able to make use of some of the functions at this website. Additionally you can prevent registration and transmission to Google as well as processing by Google of the data generated by cookies in respect of your use of this website (including your IP address) by downloading and installing the browser plugin available through this link: http://tools.google.com/dlpage/gaoptout?hl=de.

Finally, you can prevent Google from collecting and processing data relating to your use of the website by clicking this link; in this case, an opt-out cookie is stored in your browser, which means that Google does not collect any session data. Please note: If you delete your cookies, the opt-out cookie will also be deleted and you may have to activate it again.

(4) This website uses Google Analytics with the extension "_anonymizeIp()". That ensures further processing of shortened IP addresses, thus disabling their direct referencing to persons. To the extent the data collected about you can be directly referenced to you, such referencing is immediately ruled out and the personal data is deleted at once.

(5) We use Google Analytics to analyse the use of our website and to be able to improve our website on a regular basis. The collected statistics helps us improve our offer and position ourselves in a more interesting way for you as our user. For exceptional situations where personal data is transmitted to the USA, Google has submitted itself to the EU-US Privacy Shield https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI&status=Active. The legal basis allowing us the use of Google Analytics is Article 6 Paragraph 1 Section (1) Letter (f) of the GDPR.

(6) Information on the third party provider: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA, Tel: +1 650 253 0000, E-Mail: support-de@google.com. Utilisation terms and conditions: http://www.google.com/analytics/terms/de.html, Data Privacy Synopsis: http://www.google.com/intl/de/analytics/learn/privacy.html and the data privacy statement: http://www.google.de/intl/de/policies/privacy.

Appendix 2 – Data Protection Complaints Information Sheet

Under GDPR/Data Protection Act 2018, those who collect and use personal information have to follow rules of good practice for handling information. The Act also gives rights to individuals whose information they collect and use. The University of Nottingham aims to comply fully with its obligations under the Act and to ensure that the service it provides for those wishing to gain access to information is simple, efficient, and effective.

If you feel the service you received does not meet these aims or your expectations, please contact the Information Compliance Team, who will try to resolve your issues informally in the first instance: admin@hkaid.uk.

Please note that requests for a review of our response must be received within forty days of the date of that response.

If you remain dissatisfied after following these steps, you can complain to the Information Commissioner's Office (ICO). You should do this within two months of receiving the final response to your complaint. For further advice on making a complaint to the ICO, please see their website at www.ico.gov.uk

You can write to the ICO at:

Information Commissioner's Office Wycliffe House

Water Lane

WILMSLOW

SK9 5AF

Email: enquiries@ico.gsi.gov.uk

You can also call their helpline (Monday-Friday 09:00-17:00): 01625 545 745