DATA PROTECTION POLICY

1. BACKGROUND, PURPOSE AND SCOPE

Background

1.1 All HKA employees, temporary staff, consultants, contractors and third parties have a duty to protect HKA data that they create, store, process or transfer.

1.2 The UK Data Protection Act 1998 [6] and French Data Protection Act [7] will be superseded by the EU General Data Protection Regulation [8] (GDPR) on 25th May 2018. At a minimum, HKA must ensure data protection standards within the company meet these regulations. The following document sets out the requirements for HKA employees, third parties and other stakeholders, to fulfil these regulatory obligations.

Purpose

1.3 The purpose of this document is to specify and communicate to all personnel the HKA policy on data protection. In particular:

- To ensure data protection good practice across the organisation;
- To ensure compliance with GDPR [8] and other applicable legislation and regulation related to personal data.

1.4 This document outlines internal policy in respect of data handling, but this policy is subject to all the laws, rules and regulations that HKA is governed by. In the event this policy allows employees of HKA to exercise discretion, such discretion must be exercised within the confines of HKA statutory obligations and must not contravene any of its legal, accounting or other regulatory requirements.

Scope

1.5 This policy applies to all HKA personnel irrespective of status, including temporary staff, contractors, consultants, and third parties.

2. STATEMENT OF POLICY

1.1 It is the policy of HKA to ensure that all data shall be protected in proportion to the sensitivity of the data, and in line with all legal and regulatory requirements.

3. REQUIREMENTS

General Requirements

1.2 All data created, stored, processed and transferred by personnel shall have a classification in accordance with the HKA Data Classification Policy [2].

1.3 Following its classification, all data shall be handled with respect to the HKA Data Handling Policy [3].

Personal Data

1.4 Personal data shall be protected by the implementation of appropriate technical and organisational measures and integration of necessary safeguards, taking into account:

- The state of the art;
- The cost of implementation;
- The nature, scope, context and purposes of processing the data; and
- The risks to rights and freedoms of persons posed by the processing.

1.5 Appropriate technical and organisational measures shall be implemented for ensuring that, by default, personal data:

- Personal data collection is limited to that which are necessary for each specific purpose of the processing;
- Personal data processing is limited to that which are necessary for each specific purpose of the processing;
- Personal data access is limited to that which are necessary for each specific purpose of the processing;
- The storage period of all personal data is limited to that which are necessary for each specific purpose of the processing.

1.6 All personnel shall ensure that data protection advice is sought where needed in all issues which relate to the protection of personal data in a properly and in a timely manner.

Data Protection Officer

1.7 HKA shall have a designated Data Protection Officer (DPO) at all times.

1.8 All personnel shall support the DPO in performing his/her tasks, these tasks shall be carried out without influence on or consequence to the DPO and without any conflict of interest.

1.9 The DPO shall be designated on the basis of (amongst other capabilities) professional qualities and expert knowledge of data protection law and practices.

1.10 HKA shall publish the contact details of the DPO and communicate them to the relevant data protection supervisory authority (The Information Commissioner's Office in the UK and Commission Nationale de l'Informatique et des Libertés – CNIL in France).

1.11 The DPO shall have at least the following tasks:

- To inform and advise HKA and its employees who carry out processing of their obligations pursuant to GDPR [8] and other data protection provisions;
- To monitor compliance with GDPR [8], other data protection provisions and HKA policies in relation to the protection of personal data;
- To provide advice where requested as regards the data protection impact assessment and monitor its performance;
- To cooperate with the supervisory authorities;
- To act as the contact point for the supervisory authorities on issues relating to personal data processing.

4. ROLES AND RESPONSIBILITIES

1.12 All personnel are responsible for the records they create, use and store.

1.13 Managers are directly responsible for implementing this policy within their functional areas, and for adherence by their staff.

1.14 The Data Protection Officer has direct responsibility for maintaining this policy and providing advice on implementation.

APPENDIX A - DEFINITIONS

1. ‘Personal data’ 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;

2. ‘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;

3. ‘Restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

4. ‘Profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

5. ‘Pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

6. ‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

7. ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

8. ‘Recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

9. ‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.