FONASBA GDPR COMPLIANCE

LONDON, April 2018

DATA BREACH POLICY

BACKGROUND

With the exception of that held on its employees (which is not held on FONASBA's network) the personal data FONASBA holds on individuals is minimal and only collected, processed and retained as required for its legitimate business interests. (See FONASBA's data collection and processing policies). FONASBA recognises however, that breaches of personal data can occur and that a coherent and structured course of action must be in place should such a breach take place.

The undernoted policy sets out the detection, investigation and reporting actions to be taken following the discovery of a breach of the personal data FONASBA collects, processes or retains.

IDENTIFICATION OF A DATA BREACH

FONASBA subscribes to the definition used by the UK Information Commissioner (ICO) to the effect that: "A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed".

NOTIFICATION OF A DATA BREACH BY EXTERNAL PROCESSORS

Where data is processed by a FONASBA member, for example in the case of registrations for the FONASBA Agent Diploma or in relation to a FONASBA event, or by any other third party, any data breach must be notified to the FONASBA General Manager (generalmanager@fonasba.com), immediately the breach is noted. The notification must include: details of the nature of the personal data that has been lost, destroyed, corrupted or disclosed, the individuals concerned, when the breach took place and, if possible, information as to how the breach has occurred. The FONASBA member or third party will then take the steps outlined in the paragraph "ACTION IN THE EVENT OF A BREACH" to minimise the chances of the breach recurring.

NOTIFICATION OF A DATA BREACH BY A DATA SUBJECT

Any individual whose data is collected or processed by FONASBA and who believes their data has been breached as a result of it being processed by FONASBA, is requested to notify the General Manager immediately they are aware of the suspected breach. Upon receipt of the notification, FONASBA will then take action to ascertain if a breach has indeed occurred as a result of its own actions and if so proceed as detailed in the following paragraph.

ACTION IN THE EVENT OF A BREACH

Should a breach occur, FONASBA, its member of a third party will immediately take steps to identify the breach and the reasons for it, ascertain the likely impact on the individuals concerned and communicate it to them. FONASBA will also notify the ICO within 72 hours. Action will also be taken to ensure that the chances of such a breach recurring are minimised. This may involve implementing additional IT security measures, modifying data collection, processing and retention policies and procedures or any other action that may be appropriate and proportional to the scale of the breach and the information involved.

JCW/London, April 2018.