APUC Ltd
DATA PROTECTION POLICY
April 2018

Title	APUC Data Protection Policy		
Document number	GDPR POL001	**Document status**	Approved

Owner	Kerry Simpson
Approver(s)	Angus Warren

Version	Version history	Version date
0.1	Initial Version Approved	April 2018

Contents

1. Introduction

APUC (Advanced Procurement for Universities and Colleges) Limited is the procurement centre of expertise for Scotland's Universities and Colleges. It is wholly owned by its member HE and FE institutions and therefore acts as a subsidiary of them, as a shared service.

In undertaking the business of APUC, we create, gather, store and process data on a variety of data subjects such as staff, customers/suppliers and member institutions.

Some of the data we create/collect and process will be individual's "personal and/or sensitive data", i.e. data concerning a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health or sexual life.

The processing of personal data is governed by the General Data Protection Regulation 2016/679 (GDPR) and relevant UK Data Protection legislation. APUC is committed to protecting privacy and complying with this regulation with data protection being an important part of APUC's overall information security arrangements. All information must be handled safely and securely according to agreed policy.

As APUC processes 'personal data' of staff, customers/suppliers and member institutions, it is registered with the Information Commissioner's Office (ICO) as a Data Controller under GDPR. This means it decides how personal data is processed and for what purposes. APUC currently processes personal data strictly in accordance with Data Protection legislation and this will continue to be the case in relation to the GDPR.

The GDPR applies to all data relating to, and descriptive of, living individuals defined in the Regulations as 'personal data'. Individuals are referred to as 'data subjects'.

As our recording and use of data continues to increase, it is more important than ever that every member of APUC staff understands the law that exists in relation to data protection and staff responsibilities in ensuring that data is secured and protected in line with the law.

The GDPR places obligations on APUC and the way it handles personal data. In turn the staff have responsibilities to ensure personal data is processed fairly, lawfully and securely. This means that personal data should only be processed if we have a valid condition of processing (a legitimate interest; a legal obligation; performance of a contract; or your consent to process your data) and we have provided information to the individuals concerned about how and why we are processing their information (i.e. a privacy notice). There are restrictions on what we are allowed to do with personal data such as passing personal information on to third parties, transferring information outside the EU or using it for direct marketing.

APUC is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

2. Purpose of Policy

This policy sets out the responsibilities of APUC and its staff to comply fully with data protection legislation. It is accompanied by a list and links to other, associated policies which provide information and guidance on different aspects of data protection and data security. This policy and its associated procedures form the framework from which staff should operate to ensure compliance with data protection legislation.

3. Scope

The policy applies to all staff, customers/suppliers and APUC member institutions and all items of personal data that are created, collected, stored and/or processed through any activity of APUC.

4. Associated Documentation

The following associated documentation should be consulted in conjunction with the Data Protection Policy as appropriate. (add links to all)

- APUC Governance Manual
- Privacy Notices
- Document Management and Retention Policy
- Records of Processing Activities
- Information Security Policy (Cyber Essentials + version in development)
- Subject Access Request Procedure
- Data Impact Assessment Procedure
- Data Breach Procedure
- Acceptable Use Policy
- And other relevant internal policies

5. Policy

5.1. Data Protection Principles

APUC is required to adhere to the six principles of data protection as laid down in the GDPR, which means that information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The six principles are:

- Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes ('purpose limitation')
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation')
- Personal data shall be accurate and where necessary kept up to date ('accuracy')
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose ('storage limitation')
- Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Compliance with the GDPR and adhering to these principles is the responsibility of all members of APUC. Any deliberate breach of this policy may lead to disciplinary action being taken, access to APUC facilities being withdrawn, or even criminal prosecution.

5.2. Personal Information Covered by GDPR

'Personal data' means information about individuals, and any information from which they can be identified - either by reference to an identifier (for example names, location data or online identifier (IP address)) or from factors specific to their physical, cultural or social identity.

GDPR also refers separately to 'special categories' of personal data which includes particularly sensitive personal information such as health details, racial or ethnic origin or religious beliefs. (see GDPR Article 9). The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see GDPR Article 10).

5.3. Data Processing Covered by GDPR

The definition of 'processing data' includes obtaining/collecting, recording, holding, storing, organising, adapting, aligning, copying, transferring, combining, blocking, erasing and destroying the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.

APUC, as data controller, remains responsible for the control of personal data it collects even if that data is later passed onto another organisation or is stored on systems or devices owned by other organisations or individuals (including devices personally owned by members of staff).

5.4. Lawful Basis for Processing

In order for it to be legal and appropriate for APUC to process personal data at least one of the following conditions must be met:

- The data subject has given his or her **consent**
- The processing is required due to a **contract**
- It is necessary due to a **legal obligation**
- It is necessary to protect someone's **vital interests** (i.e. life or death situation)
- It 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.
- It is necessary for the **legitimate interests** of the controller or a third party and does not interfere with the rights and freedoms of the data subject.

All processing of personal data carried out by APUC must meet one or more of the conditions above. These conditions are detailed in the record of processing activities. In addition the processing of 'special categories' of personal data requires extra, more stringent, conditions to be met in accordance with Article 9 of the GDPR.

5.5. Right of the Individual

The GDPR gives data subjects the right to access personal information held about them by APUC. The purpose of a subject access request is to allow individuals to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary.

Individuals can request to see any information that APUC holds about them. APUC must respond to all requests for personal information and information will normally be provided free of charge. Any requests made to invoke any of the rights, as detailed below, must be dealt with promptly and in any case within one month of receiving the request.

Data subjects have a number of other rights under the GDPR. These include:

Right to object – Data subjects have the right to object to specific types of processing which includes processing for direct marketing, research or statistical purposes. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right.

Right to be forgotten (erasure) – Individuals have the right to have their data erased in certain situations such as where the data are no longer required for the purpose for which they were collected, the individual withdraws consent or the information is being processed unlawfully. Individuals can ask the controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved or the processing is unlawful.

Rights in relation to automated decision making and profiling – The right relates to automated decisions or profiling that could result in significant affects to an individual. Profiling is the processing of data to evaluate, analyse or predict behaviour or any feature of their behaviour, preferences or identity. Individuals have the right not to be subject to decisions based solely on automated processing. When profiling is used, measures must be put in place to ensure security and reliability of services. Automated decision-taking based on sensitive data can only be done with explicit consent.

Right to Rectification - The right to require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data is incomplete, an individual can require the controller to complete the data, or to record a supplementary statement.

Right to Portability – the data subject has the right to request information about them is provided in a structured, commonly used and machine readable form so it can be sent to another data controller. This only applies to personal data that is processed by automated means (not paper records); to personal data which the data subject has provided to the controller, and only when it is being processed on the basis of consent or a contract.

5.6. Privacy Notices

Under the 'fair and transparent' requirements of the first data protection principle, APUC is required to provide data subjects with a 'privacy notice' to let them know what it does with their personal data. The main privacy notices for APUC can be viewed on the Privacy and Cookies section of the APUC website.

Privacy notices are published on the APUC website and are therefore available to staff, customers/suppliers and APUC member institutions from their first point of contact with APUC. Any processing of staff, customers/suppliers and APUC member institutions data beyond the scope of the relevant privacy notice, or processing of the personal information of any other individuals will mean that a separate privacy notice will need to be provided.

5.7. Data Retention

Individual areas within APUC are responsible for ensuring the appropriate retention periods for the information they hold and manage, based on the Document Retention Policy. Retention periods will be set based on legal and regulatory requirements, sector and good practice guidance.

Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. Once information is no longer needed is should be disposed of securely. Paper records should be shredded or disposed of in confidential waste and electronic records should be permanently deleted.

If data is fully anonymised then there are no time limits on storage from a data protection point of view.

5.8. Records of Processing Activities

As a data controller, APUC is required to keep a record of its data processing activities as a summary of the processing and sharing of personal information and the retention and security measures that are in place. Amongst other things this record contains details of why the personal data is being processed, the types of individuals about which information is held, who the personal information is shared with and when personal information is transferred to countries outside the EU. Details of these records can be found in the GDPR Data Processing Log.

Staff embarking on new activities involving the use of personal data that is not covered by one of the existing records of processing activities should inform the Data Protection Officer before starting the new activity.

5.9. Children

Children (under the age of 16) are identified as *"vulnerable individuals"* and deserving of *"specific protection"*. Under GDPR the following restrictions apply to the processing of personal information relating to children:

- If relying on consent as a lawful basis for processing personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent. For children under this age, consent from whoever holds parental responsibility for the child is required - unless the online service you offer is a preventive or counselling service.
- Any information provided to a child in relation to their rights as a data subject has to be concise, transparent, intelligible and easily accessible, using clear and plain language.
- The use of child data for marketing or for profiling requires specific protection.

In the case of APUC processing personal data for children (i.e work experience), specific measures will be put in place, taking account of national legislation. The Data Protection Officer should be informed if any of the above activities are being contemplated.

5.10. Data Sharing

Certain conditions need to be met before personal data can be shared with a third party or before an external data processor is used to process data on behalf of APUC.

As a general rule personal data should not be passed on to third parties, particularly if it involves special categories of personal data but there are certain circumstances when it is permissible.

Any transfers of personal data must meet the data processing principles as detailed in section 5.1, in particular it must be lawful and fair to the data subjects concerned.

It must meet one of the conditions of processing as detailed in section 6.3. Legitimate reasons for transferring data would include:

- That is was a legal requirement
- It is necessary to provide services to its members

If no other conditions are met, then consent must be obtained from the individuals concerned and appropriate privacy notices provided.

APUC must be satisfied that the third party will meet all the requirements of GDPR particularly in terms of holding the information securely. Where a third party is processing personal data on behalf of APUC, a written contract must be in place and a Vendor Assurance Assessment completed in order to have assurances that GDPR requirements are being met.

Staff should consult with the Data Protection Officer if they are entering into a new contract that involves the sharing or processing of personal data.

5.11. Transfers of Personal Data Outside the EU

Personal data can only be transferred out of the European Union under certain circumstances. The GDPR lists the factors that should be considered to ensure an adequate level of protection for the data and some exemptions under which the data can be exported. At present APUC does not transfer personal data outside of the EU, however if these circumstances were to change, advise should be sought from the Data Protection Officer.

APUC will gain assurances from third parties of whether personal data is transferred out of the European Union. This should be detailed as part of the Vendor Assurance Assessment.

5.12. Data Protection Impact Assessments and Data Protection by Design

It is particularly important to consider privacy issues when considering new processing activities or setting up new procedures or systems that involve personal data. GDPR imposes a specific 'privacy by design' requirement emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought.

Staff developing new projects or processes or revising existing processes need to take data protection into account as part of this process and may need to carry out a Data Protection Impact Assessment (DPIA). The types of circumstances when this is required include:

- Processing is likely to result in a high risk to individuals' interests,
- Processing of large volumes of personal data,
- Where there is automatic processing/profiling,
- Large scale processing of special categories of personal data
- Monitoring of publicly assessable areas (i.e. CCTV)

The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks. If a new project or processing activity is being considered, the Data Protection Officer should be consulted.

5.13. Direct Marketing

Direct marketing relates to communication (regardless of media) with respect to advertising or marketing material that is directed to individuals e.g. mail shots, advertising courses. Individuals must be given the opportunity to remove themselves from lists or databases used for direct marketing purposes. APUC must cease direct marketing activity if an individual requests the marketing to stop.

Direct marketing must also comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)[2] which covers marketing via telephone, text and email.

5.14. Personal Data Breach

APUC is responsible for ensuring appropriate and proportionate security for the personal data that we hold. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. APUC makes every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions. Examples of personal data breaches include:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Hacking attack
- Unforseen circumstances such as a fire or flood
- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

In the event that there is a suspected data breach, in the first instance, this should be reported to the Data Protection Officer. The breach may need to be reported to the Information Commissioner's Office no later than 72 hours after the breach is discovered, if appropriate.

5.15. Data Protection Training

All staff of APUC will have their responsibilities for data protection and security outlined to them as part of their staff induction training and the APUC Data Protection Handbook issued to them. In addition, APUC will provide regular mandatory Data Protection training and procedural guidance for their staff.

5.16. Impact of Non-compliance

All staff of APUC are required to comply with this Data Protection Policy, its supporting guidance and the requirements specified in the GDPR. Any member of staff who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy may be subject to disciplinary action. Staff may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information without the consent of APUC i.e. for their own purposes, which are outside the legitimate purposes of APUC.

APUC could be fined for non-compliance with the GDPR. There are two tiers of fines depending on the type of infringement. Organisations in breach of GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. It is important to note that these rules apply to both controllers and processors.

6. Contact Details

In the first instance all enquiries or requests for further information or guidance relating to data protection should be addressed to the Data Protection Officer at:

Data Protection Officer
APUC Ltd
Unit 27,
Stirling Business Centre,
Wellgreen,
Stirling
FK8 2DZ

Email: dataprotection@apuc-scot.ac.uk