SAAS Student Awards Agency Scotland

Funding your future

Guidance on Individual Rights

Protect the Student, Protect SAAS, Protect Yourself.

Last updated May 2018
Next review: November 2018

Version 1.0

Contents

1. Introduction

One of the aims of the new data protection legislation is to give individuals (whether students, contractors or members of staff) more control over the way in which organisations process their personal data, this has led to the granting of new rights for individuals, as well as enhancing and improving rights that existed previously.

This guidance is based on information currently provided on the UK Information Commissioners website.[1] The purpose of this guidance is to help internal and external stakeholders familiarise themselves with individual's rights under the Data Protection Act, 2018 (the Act) and to help understand how SAAS will respond to individuals wishing to exercise any of these rights.

It is important to recognise that requests may be made by any current or former students, third parties whose data SAAS has collected (e.g. benefactors, dependants), current or former employees. Requests may not follow a clear or standard format where data subjects clearly set out which right they are requesting to be exercised. For example they may simply say 'I want to know what SAAS is using my data for' or 'I want to see all the emails about me that SAAS hold'.

2. Who should read this guidance

This guidance is for all employees working for SAAS (including all full-time and part-time permanent members of staff, consultants, contractors and fixed term workers and Agency staff) and individuals whose personal data SAAS processes.

3. Right to be Informed

The Act gives individuals (data subjects) the right to obtain:

1. Confirmation that data is being processed;
2. Access to their personal data;
3. Information about the purpose of the processing;
4. Information about the categories of data being processed;
5. Information about the categories of recipients with whom data is shared;
6. Information about how long data is held (or criteria used to determine how long data is held);

[1] www.ico.org.uk/

7. Information about rights to erasure, to rectification, to restriction of processing and to object to processing;
8. Information on how to complain; and,
9. Information about any automated processing that has as an impact on your rights.

Most of this information is provided in the SAAS Privacy Statement which can be found on the Data Protection section of the SAAS website[2].

SAAS is committed to being open and transparent about how we process personal information. The SAAS Privacy Statement has undergone a number of changes in recent years. We welcome constructive feedback to continually improve how we engage and provide information to our customers.

SAAS sends a separate Privacy Statement to benefactors and adult dependants within 30 calendar days of a student submitting an application form.

4. Subject Access Requests

SAAS must provide individuals (data subjects) with:

- confirmation their data is being processed
- access to their personal data; and
- other supplementary information, including verification of the lawful basis for processing.

This information must be provided in a commonly used electronic form, unless otherwise specified by the data subject.

SAAS have a procedure to deal with requests for access to information - known as Subject Access Requests (SARs).

Information about SARs can be found in the subject_access_request_form.pdf. Where SAAS receives any request that cannot be dealt with as 'business as usual' the requester should be directed to the 'How to Request Personal Information' section of the Privacy Statement.

If requests for personal information come in via SAAS email and SAAS Accounts or social media channels they should be forwarded to the SAAS Data Protection Mailbox: **SAASDataProtection@gov.scot**

SAAS' Information Management Team will handle the response to requests for personal information from individuals which are outside the 'business as usual'

[2] **http://www.saas.gov.uk/privacy_data_protection_index.htm**

requests for information. Examples of 'business as usual' requests include requests for copies of documents where individuals have passed security questions e.g. copies of award notices, copies of previous applications.

Examples of Subject Access Request IMT respond to include where individuals have asked for all the personal information that SAAS hold about them, copies of call recordings, requests for personal information which isn't the requesters.

SAAS will respond to a request promptly and in any event within 30 calendar days at the latest following:

- Receipt of the request; or
- Receipt of any information we may ask to be provided to enable us to comply with the request.

SAAS will provide an acknowledgement of a Subject Access Request within **three** working days of receipt of a valid request.

To enable requests to be dealt with quickly all request must be sent to the Information Management Team as soon as possible. Any written request received via a SAAS mailbox, SAAS Account, fax or via social media channels must be considered a valid request.

Making a request is free of charge, however SAAS may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies".

All staff have access to Subject Access Request Guidance for Staff which provides practical examples to identify SARs.

Third Party Consent

An individual may authorise third party representatives to act on their behalf when requesting personal information. This could be a family member, legal representative or student advisor. In such cases, SAAS must be satisfied that the representative is entitled to make a legitimate request on behalf of the individual. We will accept the following evidence as proof of authorisation:

- Letter of Authority;
- Official Form e.g. mandate form;
- Correspondence; or,
- SAAS Third Party Consent Form.

A third party consent form can be found on our website[3]. This form must be scanned and submitted using the document uploader, or posted directly to SAAS, so that it

[3] **http://www.saas.gov.uk/contact.htm**

can be attached to the student record as proof of consent. A new consent form is required for each academic session.

Third party consent forms must be attached to the student record and checked each time a third party representative contacts SAAS.

The third party consent form allows the representative to have access to all personal and sensitive personal information held by the student and authority to act on behalf of the student regarding any matters relating to the relationship between the student and SAAS, unless stated otherwise. Other forms of proof of authority may only provide authority to have access to specific information for a specified purpose. Always check with the Information Manager if you are unsure.

If the student no longer wishes a third party to act on their behalf, then they can with draw their consent at any time. This can be done by contacting SAAS by email and asking for the consent to be withdrawn. SAAS will delete the consent form and make a note on the student record to record when consent was withdrawn.

5. Right to Rectification

Individuals have the right to have personal information amended if it is inaccurate or incomplete.

SAAS have processes in place for updating changes to personal information such as change of name or updating an address, for dealing with requirements for change of courses, and changes in financial or personal circumstances[4]. Staff must follow them when actioning such requests.

Individuals can find information on how to update their information on the SAAS website under **update my details**.

If a request cannot be dealt with using standard processes that we already have in place, then the request must be forwarded to the Information Management Team as soon as possible.

Requests for rectification can be made in writing or verbally to SAAS and will be responded to within 30 calendar days. The response time can be extended by two months where a request is complex.

If SAAS do not change inaccurate or incomplete data, SAAS will provide an explanation why no action is being taken. An individual will also be provided with information on seeking an internal review of the decision, information about how to complain to the Information Commissioners Office and the right to apply to the Court of Session.

[4] **http://www.saas.gov.uk/update_my_details.htm**

If personal data has been disclosed to third parties, SAAS will inform them of the rectification where possible and will inform the individuals about the third parties who have been given the information, where appropriate.

SAAS share personal information with the Student Loans Company and Higher Education Institutions in relation to student loan applications and student attendance data, reports are transferred on a regular basis and any updated information is transferred to the relevant organisation.

6. Right to erasure

An individual can request the deletion or removal of personal data where there is no compelling reason for the information to be held or further processed.

The right to erasure does not provide an absolute 'right to be forgotten'.

The Right to Erasure applies in the following circumstances:

- Where data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- Where the processing is based on consent, and the individual has now withdrawn their consent;
- Where an individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- The data was unlawfully processed; or,
- The personal data has be erased in order to comply with a legal obligation.

The Act sets out circumstance when SAAS does not need to comply with a request for erasure where personal data is processed:

- To comply with a legal obligation
- For the performance of a public interest task or of official authority;
- For archiving purposes in the public interest, scientific research historical research or statistical purposes; or,
- In the exercise or defence of legal claims

This right is unlikely to apply where processing remains necessary in relation to the purpose for which they were collected.

For example SAAS is obliged by legislation governing student support in Scotland to retain personal information that identifies individuals as well as a record of eligibility for funding, type of funding and amount of funding each student has received, to appropriately manage public funds and to ensure all students only receive the funding they are entitled to. It is highly unlikely that the right to erasure could be used

to erase these records, but individuals might be able to exercise it in relation to specific processing.

SAAS has a retention and disposal policy which sets out how long information is held before it is archived or destroyed. Where specific retention periods have not been identified it provides specific dates for review.

If SAAS do not deleted information by the dates specified in our retention schedule then this would be an example of when an individual might want to exercise this right.

7. Right to restriction of processing

When this right is exercised we are permitted to store the personal data but not further process it. Restricted information about the individual is retained to ensure that the restriction is respected in the future.

An individual has the right to ask for the restriction of processing of personal data when:

- The data subject contests the accuracy of their personal data, processing should be restricted until accuracy is verified;
- When the data subject objects to processing which is being carried out for the reasons of performance of a task in the public interest, or for the legitimate interests of the data controller (SAAS), then SAAS must restrict processing whilst considering whether their legitimate interests override the rights and freedoms of the individual;
- The processing is unlawful and the data subject does not want the personal data to be deleted and requests restriction of the use instead;
- SAAS no longer needs the personal data for processing, but the data is required by the data subject for the purpose of a legal claim.

8. Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows individuals the right to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided directly to SAAS;
- where the processing is based on the individual's consent or for the performance of a contract; and

- when processing is carried out by automated means.

SAAS must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

CSV is a simple file format used to store tabular data, such as spreadsheet or database. Files in the CSV format can be imported and exported from programs that store data in tables, such as Microsoft excel. CSV stands for 'comma-separated values.

9. Right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics

SAAS must stop processing the personal data unless:

- We can demonstrate legitimate grounds for processing which outweighs the interests and rights of the individual; or
- The processing is for the establishment, exercise or defense of legal claims.

10. Rights in relation to automated decision making and profiling

This right provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

The right not to be subject to a decision applies when:

- It is based on automated processing
- It produces legal/significant effects on the individual

It does not apply if the decision:

- Is necessary for entering into a performance of a contract
- Is authorised by law
- Is based on explicit consent
- Does not have a legal/significant effect on data subjects

SAAS will inform customers about any automated decision making and profiling we carry out, what information we use to create the profiles and where we get this information from. This information would be provided in the SAAS Privacy Statement.

Where profiling or automated decision making is undertaken the individual will be given the opportunity to:

- Express their point of view;
- Obtain an explanation of the automated decision;
- Supplement the automated system with additional information;
- Have a human carry out a review of the automated decision;
- Contest the automated decision;
- Object to the automated decision-making being carried out.

A Data Protection Impact Assessments will be undertaken to consider and address privacy risks before SAAS starts any new automated decision making or profiling.

11. Responding to Requests

SAAS has 30 calendar days in which to respond to requests made under sections 3-10.

SAAS must be sure they are dealing with the data subject in relation to any requests. Where SAAS is in correspondence with the data subject and they are satisfied of the identity of the individual we may not ask for proof of identity. In most cases we will ask for a copy of some form of identification such as driving license or passport before proceeding with a request.

SAAS aims to provide an acknowledgement to all requests within three working days of receipt of a valid request.

In some cases, SAAS may extend the 30 calendar day deadline, by up to two months where the request is complex. If we need more time, we will contact the individual as soon as possible to explain why more time is required.

If SAAS upholds a request to amend, delete or restrict processing of personal information and we have disclosed that information to third parties, we will where possible inform third parties of these changes.

If SAAS is unable to comply with a request, we will provide an explanation and provide details of how an individual can make request a review to the decision. The Act does not provide a timescale for responding complaints. SAAS has decided to implement the review process used under the Freedom of Information Scotland Act, 2002. Further details can found under the complaints section of this guidance document.

12. Complaints procedure

SAAS aims to fully comply with its obligations under the Act. If an individual has any questions or concerns regarding SAAS' management of personal data, they should be directed to SAAS Data Protection Officer.

Student Awards Agency Scotland
Saughton House
Broomhouse Drive
Edinburgh
EH11 3UT

Email: **SAAS_Data_Protection_Mailbox@gov.scot**

If an individual is unhappy with the response to your data protection request, they may ask for us to carry out an internal review of the response, by writing to the address above.

The review request should explain the reason the requestor is dissatisfied with the response and it should made within 40 working days from the date when the individual received the response from SAAS. SAAS will complete the review and tell the individual the result, within 20 working days from the date when SAAS received the review request.

If an individual is still dissatisfied, they have the right to contact the Information Commissioner's Office, the independent body overseeing compliance with the Act and should be directed to the ICO website[5].

Individuals have the right in certain circumstances to seek a judgement through the courts where they are not satisfied with a decision made by SAAS. Individuals can seek a judgement via the Court of Session.

[5] **http://ico.org.uk**