Data Protection Policy - GDPR

Scope

This document lays out the procedures and principles of data protection that will be followed by all employees at Prodeo LTD.

All employees will have completed the Prodeo GDPR Training Session and the Employee of Prodeo LTD – GDPR Compliance Document (Appendix A).

Key Definitions:

GDPR: General Data Protection Regulation

Controller: A controller determines the purposes and means of processing personal data.

Processor: A processor is responsible for processing personal data on behalf of a controller.

Personal Data: The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Prodeo LTD: Processor

As defined above, Prodeo LTD (Trading as SMID) acts as a processor of data on behalf of controllers *(Education establishments, namely secondary schools).*

As a processor of personal data we are required under the GDPR to provide information on the following key data protection areas:
Lawful basis for processing
Data Types Stored
Data Storage - Security
Data Subject Access
Data Breach procedures
Data Retention
Data Protection Officer

Lawful Basis for Processing

GDPR requires that a processor must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing:

REF: *Information Commissioner*

1 Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

2 Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

3 Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

4 Vital interests: the processing is necessary to protect someone's life.

5 Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

6 Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Prodeo LTD is processing the data on behalf of an education establishment, with which we have an annual contract in order to provide access to our cloud based software. Therefore SMID meets the lawful obligation point 2 which states the processing is necessary for a contract you have with the individual. It is important that the school as a controller of the data has the necessary consent in place when obtaining certain data from students who attend the school.

Data Types Stored

Prodeo LTD requires the following personal data as a minimum to use the SMID cloud software:

Code - *This can be decided by the school, commonly admission number but may be UPN or candidate number*
Forename Surname
Classes - The classes a student is currently studying
Report Grades - assigned within school or from final exams
KS2 Results

Optional Data (Required for full functionality):

Pupil Groups - A school can choose which data to include as pupil groups common examples are Free School Meals (FSM), Pupil Premium (PP) and Prior Ability Grouping.
Attitude To Learning Scores - Scores assigned within school to categorise students behaviour. **Attendance - %** Attendance Scores may be added to the system to monitor attendance patterns.

Data Storage and Security

Prodeo LTD trading as SMID will not supply any of your data to any third party and will only use the data you provide to support your school.

Prodeo Limited is registered with the Information Commissioner's Office (ZA138870) in accordance with the Data Protection Act of 2018 and the code of practice issued by the regulators of England, Wales and Northern Ireland.

The personal data stored within the SMID Report & Dashboard includes Names, School Selected Pupil Groups e.g. Pupil Premium, Grades, Gender, Attendance. The data will only be used within the context of the SMID Dashboard and Report and will only be used to identify the progress made by students from any school that is a member. When accessing the SMID Dashboard you will be using a Secure Hyper Text Transfer Protocol (HTTPS) along with Secure Sockets Layer (SSL) Protection. This provides encrypted access to our servers protecting you from others accessing the data. All data is hosted using Amazon S3 Servers, which are secure and encrypted.

Security information from host website, Heroku

Data Centres
Heroku's physical infrastructure is hosted and managed within Amazon's secure data centres and utilize the Amazon
Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure
compliance with industry standards. Amazon's data centre operations have been accredited under:

ISO 27001
SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
PCI Level 1
FISMA Moderate
Sarbanes - Oxley (SOX)

Physical Security

Heroku utilizes ISO 27001 and FISMA certified data centres managed by Amazon located in Ireland (EU- West - 1) Amazon has many years of experience in designing, constructing, and operating large- scale data centres. This experience has been applied to the AWS platform and infrastructure. AWS data centres are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection.

Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data centre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Amazon only provides data centre access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centres by Amazon employees is logged and audited routinely.

Data Subject Access

Under the right of subject access, an individual is entitled to request a copy of the personal data held about them.

Valid Subject Access Request:
For a subject access request to be valid, it should be made in writing. In order for a subject access request to be made successfully we will require proof of a persons identify and legitimacy to make the request. Should any request be made our data protection officer will contact the designated data controller at the relevant establishment to fully confirm the legitimacy of a request. We will then move forward in providing the data in an appropriate format.

For example in the unlikely event of a parent or a pupil contacting Prodeo LTD directly with a subject access request. We would clearly inform them that we would be contacting the school data protection officer in order to verify the request and all communication would come through the school.

We do not expect the above scenario to be a common occurrence but should it arise the school data protection officer will always be our first point of contact.

Request Procedure / Format
Under GDPR legislation an organisation is not allowed to require an individual to complete a subject access request in a certain format. Therefore Prodeo LTD does not require an individual to complete a specific form to make the request. It is recommended that any request should be sent by email to *support@smidreport.com* so that we can deal with your request as quickly as possible. Should a subject access request be made to another member of staff or in a different format such as a written letter all staff are fully aware of GDPR procedures and will take any request and pass them on to the data protection office.

Response Format
Prodeo LTD will meet the GDPR requirements that state the information provided to the individual is in an intelligible form. Any response made by Prodeo LTD will be sure to include a glossary of terms should any technical information be included that may not be understood by the average person.

Subject Access Request Cost
The GDPR legislation states companies can charge up to £10 for a subject access request. However, Prodeo LTD will not require any charge for any request made.

Data Breach Policy

A data breach occurs when personal information is lost or subject to unauthorised access.

Definition of personal data breach:
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.

Data Breach Response Team:
The Data Breach Response Team has been set up to deal with any form of data breach which can occur.

ICO provides examples of data breaches which range from an email being sent to the incorrect individual through to stolen data from a breach of the database. Prodeo LTD takes data protection extremely seriously encrypting all data at rest, however if a breach were to occur Prodeo LTD will contact all schools with the following information:

- The name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

When a data breach occurs Prodeo LTD will establish whether the breach needs to be reported to ICO. This is only the case if there is likely to be a risk to people's rights and freedoms.

Prodeo LTD will record any breaches that occur even if they don't need to be reported to ICO.

Data Retention
Any school that terminates their contract with SMID will have all data removed from SMID's live database within 1 week of the end of the subscription.

Data will still exist within backups for 3 months after the end of the subscription after which it will be destroyed.

Data can be removed immediately from our database if a school instructs us to carry out this process in a written request. However, the data will remain in our backups for 3 months after which it will be destroyed.

INDEMNITY

Data Processor shall indemnify and keep indemnified and defend at its expense Data Controller against all costs, claims, damages or expenses incurred by the Data Controller or for which the Data Controller may become liable due to any failure by the Data Processor or its employees or agents to comply with the obligations under this Data Processor Agreement.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The ICO recommends that you carry out a DPIA if you plan to use processors that are likely to result in 'a high risk to individuals'. If you wish to carry out a DPIA before starting or during your contract with SMID we will fully support you with this process.

Please find further information on conducting a DPIA here (ICO Website)

AUDIT SUPPORT

As with the DPIA if as a controller you wish to carry out a data audit, we will support you with this process. We can provide you with detailed information on the data processed by Prodeo LTD specifically for your establishment.

SSO Policy

This section of the policy pertains to the Single Sign-On (SSO) feature provided by Prodeo LTD. We understand the importance of data privacy and are committed to ensuring that our SSO processes are transparent, secure, and compliant with the General Data Protection Regulation (GDPR).

Purpose of Data Collection

The primary purpose of collecting and processing data via SSO is to simplify the user authentication process, offering users a seamless and secure method to access our platform using their existing credentials from a trusted third-party identity provider.

Data We Collect

During the SSO process, we may collect the following information, this will already be within the SMID Platform as the access is controlled by admin users setting up account:

- Email address

How We Collect Data

The data is collected automatically when a user chooses to sign in using the SSO option. The exact data points are fetched from the third-party identity provider after receiving the user's consent.

Data Storage and Security

All data collected via the SSO process is stored securely on our servers, which employ advanced encryption and security measures to prevent unauthorized access.

Third-party Identity Providers

We partner with trusted third-party identity providers to offer the SSO feature. We ensure that these providers are GDPR compliant and handle user data with utmost security and confidentiality.

User Rights

Users have the right to:
Request access to the data collected via the SSO process.
Request rectification of their data if they find any inaccuracies.
Withdraw consent and request the deletion of their data.
Raise concerns or complaints regarding the data processing activities related to SSO.

Data Retention
We retain the data collected via SSO only for as long as the user's account remains active on our platform. Upon account deletion, all associated data, including that fetched via SSO, is permanently deleted from our servers.

Data Protection Officer

Stephen Howse 27 Bennethorpe Doncaster DN2 6AA

Appendix A: Employee of Prodeo LTD – GDPR Compliance Documentation – May 2018

This document is to notify that all staff have received training and fully understand the GDPR on data processing within Prodeo LTD.

Training Process

All staff that are employed by Prodeo LTD must complete the Prodeo GDPR Training session. This provides staff with a detailed overview of the data protection procedures carried out whilst data processing occurs. It also provides all employees with the opportunity to raise any queries they may have regarding GDPR and its impact on Prodeo.

I fully understand and agree to abide by the following statements:

- Prodeo LTD processes personal data on the SMID Online platform
- All data is stored in an encrypted format on the Amazon AWS (European based) platform.
- Any data processing that is carried out to support schools must be removed from any local machines after it has been completed.
- No personal data relevant to SMID will be stored on a local machine beyond the time it is being processed.
- Data will not be sent to schools by email as this is not a secure method of transferring personal information.
- If a school sends data by email, this must be transferred to Amazon AWS to the encrypted folders and then removed from the email account.
- All passwords that allow access to the super admin section of the SMID platform must be secure. This requires them to be more than 8 characters, include at least one number, one capital letter and one special character.
- Data should only be processed on work machines, NO personal laptops/devices should be used to carry out data processing.
- A school that terminates their contract with SMID will have all their data removed from the live database within 1 week. The data will continue to remain in backups for 3 months at which point it will be removed.
- I have completed the Prodeo GDPR Training Session and have had any necessary questions answered about GDPR and the impact it has on my role.
- I understand that at any point if I am unsure on any aspect of GDPR I will contact the Data Protection Officer – Stephen Howse.

Employee Confirmation

Print Full Name:_____ Date:_____

Signature: _____

Employer Confirmation

Print Full Name:_____ Date:_____

Signature: _____