GDPR

SMARTASSESSOR
Next Generation E-Portfolio Software

General Data Protection Regulations Requirements Summary

Increased Territorial Scope (extra-territorial applicability)

Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high profile court cases. GPDR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-Eu businesses processing the data of EU citizens will also have to appoint a representative in the EU.

All Smart Assessor data is hosted in UK sites, all processing completed in UK sites, no impact on SA operations
All backup data is stored within the UK.

Smart Assessors Hosting partner is Rackspace, our primary hosted site is in the London Data Centers

- **8 backbone providers**
- **SOX, HITRUST, PCI-DSS**
- **ISO 2700-1 Compliance Certifications**
- **Critical Infrastructure Rating N+2**

rackspace

Penalties

Under GDPR organizations 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. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Smart Apprentices take very seriously the protection of client data especially the security of personal data, this ethos is also extended to our partners and our suppliers.
As part of our ISO 27001 approval, all suppliers and partners are made aware of the requirement to comply with all aspects of GDPR.

Consent

The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

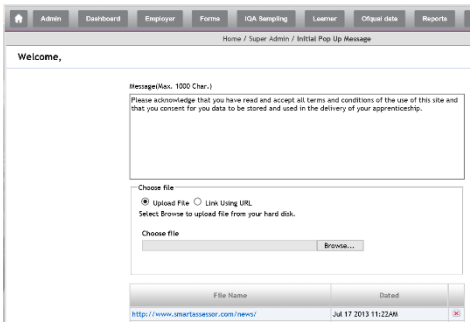
Smart Assessor deals with consent across a range of data entry options with a single solution.

1. **Data transferred from MIS system, at the point of data collection and storage consent should have already been**

GDPR

validated by the MIS system, any data which is then mirrored can be covered by this acceptance.

2. **Data transferred from MIS system where no specific consent to transfer this data or a manual data entry can be covered by the use of a initial pop up dialog which will display until acceptance of consent.**



Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Smart Assessor works with all is partners and suppliers to ensure first that all efforts are made to avoid any type of breach occurring.
In the event of a detected breach the data is analysed for potential personal information loss and an immediate notification actioned to all affected clients in line with our ISO 27001 policies.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

All data is made available to students through the system and through the college or provider.
All personal data held on the SA servers is restricted to authorised users but can be made available upon request.
All processing of data is constrained to individual client sites, no data is processed outside of the Smart Assessor application.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

All data can be archived by the college/provider this data is then excluded from any access or processing except to the originating providers.
Some data may be required to be kept for a period of time in support of audit requirements.

GDPR

Full deletion of user data is available upon request to Smart Assessor support although backup data may still be maintained for a period.

Data Portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

Smart Assessor data containers maintained within a single server environment, this data is available upon request to the data subject and can be provided in a variety of formats.

Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At it's core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - 'The controller shall implement appropriate technical and organisational measures in an effective way in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

All new development has this control as a basis for the development logic, only data required and approved for use is processed by any system.

The DPO ensures that all new development considers the design aspect of deploying these controls.

Smart Assessor has over the past 18 months enhanced significantly the security controls as part of its GDPR readiness programme and will continue to assess the need for specific data to provide the service currently available.

Data Protection Officers

Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices

May be a staff member or an external service provider

Contact details must be provided to the relevant DPA

Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge

Must report directly to the highest level of management

Must not carry out any other tasks that could results in a conflict of interest

The current CTO holds responsibility for these activities and controls. All new processing activities and data acquisitions are reviewed for appropriateness by the CTO.

The DPA reports monthly to the Senior Leadership Team each month on all aspect of Security management.