Articulacy Data Protection Impact Assessment (Google Classroom)

Introduction

Cloud computing is a method for delivering information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server at the school. Articulacy operates a cloud based system. As such Articulacy must consider the privacy implications of such a system.

The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action. Articulacy recognises that moving to a cloud service provider has a number of implications. Articulacy recognises the need to have a good overview of its data information flow.

The Data Protection Impact Assessment looks at the wider context of privacy considering Data Protection Law and the Human Rights Act. It considers the need for a cloud based system and the impact it may have on individual privacy.

Articulacy needs to know where the data is stored, how it can be transferred and what access possibilities there are to its data. The location of the cloud is important to determine applicable law. Articulacy will need to satisfy its responsibilities in determining whether the security measures the cloud provider has taken are sufficient, and that the rights of the data subject under the GDPR is satisfied.

Articulacy aims to undertake this Data Protection Impact Assessment on an annual basis

The Projects

Future Me and Articulate Your Way to HE will be administered to schools remotely using Google Classroom as the online platform which is accessible by both teacher and students.
Through Google classroom Articulacy will create, distribute and evaluate assignments in a paperless way.

In this setting access to Google Classroom is via RM Unify which in this instance is a Single Sign On. This means to access the Google Classroom environment schools log into RMUnify, select GSuite and land on the users GSuite page.

By opting for a cloud-based solution Articulacy aim to achieve the following:

- Scalability
- Reliability
- Resilience
- Support of mobile access to data securely
- Update of documents in real time
- Good working practice i.e. secure access to any personal files

Google Classroom has the ability to link with Google Drive, Google Docs, Sheets and Slides, and Gmail together to help achieve a paperless system. Articulacy can invite students to classrooms through the ICT infrastructure, through a private code that can then be added in the student's user interface or automatically imported from a school domain.

Each class created with Google Classroom creates a separate folder in the respective user's Google Drive, where the student can submit work to be graded by a teacher. Assignments can be stored and graded on Google's suite of productivity applications that allow collaboration between the teacher and the student or student to student. Instead of sharing documents that reside on the student's Google Drive with the teacher, files are hosted on the student's Drive and then submitted for grading. Teachers may choose a file that can then be treated as a template so that every student can edit their own copy and then turn back in for a grade instead of allowing all students to view, copy, or edit the same document. Students can also choose to attach additional documents from their Drive to the assignment. Google Classroom supports many different grading schemes.

- Teachers have the option to attach files to the assignment which students can view, edit, or get an individual copy
- Students can create files and then attach them to the assignment if a copy of a file wasn't created by the teacher.
- Teachers have the option to monitor the progress of each student on the assignment where they can make comments and edit.
- Turned in assignments can be graded by the teacher and returned with comments to allow the student to revise the assignment and turn back in.
- Once graded, assignments can only be edited by the teacher unless the teacher turns the assignment back in.

The information is held securely with regular data backed up. The network is only accessible through dedicated password linked to the school. Cloud based systems enable Articulacy to upload documents, photos, videos, and other files to a website to share with others or to act as a backup copy. These files can then be accessed from any location or any type of device (laptop, mobile phone, tablet, etc). The cloud service provider cannot do anything with Articulacy's data unless they have been instructed by Articulacy. Articulacy's Privacy Notice will be updated especially with reference to the storing of pupil and workforce data in the cloud.

Data Processing

Data will be collected and securely stored in line with the Articulacy GDPR policy. The policy seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject.

For Future Me and Articulate Your Way to HE, Articulacy require a minimum amount of personal data i.e.

- Student name
- Student school
- Student school email address
- Assignments including video assignments
- Evaluations
- Student CVs (work and school history only, no personal information)

Data that will NOT be collected:

- Home address
- Telephone number
- DOB
- SEND information
- Criminal records
- School records
- Ethnicity
- Any other information that could be categorised as sensitive

This data will be provided by the client/school and retained securely until the end of the project (minimum 1 week to maximum 4 weeks) when it will be deleted from the Articulacy systems.

Articulacy routinely shares student evaluations with the lead teacher on the project, the school and the project funders.

Articulacy recognises that moving to a cloud-based solution raises a number of General Data Protection Regulations issues as follows:

ISSUE: The cloud-based solution will be storing personal data including sensitive information
RISK: There is a risk of uncontrolled distribution of information to third parties
MITIGATING ACTION: Google data centres are built with custom-designed servers, running Google's own operating system for security and performance. Google has 700+ security engineers that work around the clock to spot threats early and respond quickly. Google's data centres use custom hardware running a custom hardened operating system and file system. Each of these systems has been optimized for security and performance. Google controls the entire hardware stack and is able to quickly respond to threats or weaknesses that may emerge. Google is the first

major cloud provider to enable Perfect Forward Secrecy, which encrypts content as it moves between Google servers and those of other companies Google encrypts Gmail, Attachment, and Drive data while in transit. This ensures that messages are safe not only when they move between the school and Google's servers, but also as they move between Google's data centres.

ISSUE: Transfer of data between Articulacy and the cloud
RISK: Risk of compromise and unlawful access when personal data is transferred
MITIGATING ACTION: Data is encrypted at several levels. Google forces HTTPS (Hypertext Transfer Protocol Secure) for all transmissions between users and GSuite. DPIA Google Classroom 20200505 v1.2 8 8 services and uses Perfect Forward Secrecy (PFS) for all its services. Google also encrypts message transmissions with other mail servers using 256-bit Transport Layer Security (TLS) and utilizes 2048 RSA encryption keys for the validation and key exchange phases. This protects message communications when client users send and receive emails with external parties also using TLS PFS requires that the private keys for a connection are not kept in persistent storage. Anyone who breaks a single key can no longer decrypt months' worth of connections; in fact, not even the server operator is able to retroactively decrypt HTTPS sessions.

ISSUE: Security of data whilst hosted in the cloud
RISK: Risk of compromise and unlawful access when personal data is at rest
MITIGATING ACTION: Customer data that is uploaded or created in GSuite services is encrypted at rest. Google have also enabled HTTPS for all of its GSuite services, including Google Classroom, so that the school data is encrypted when traveling from a school device to Google and also while in transit between Google data centres. All Google employees are required to sign a confidentiality agreement and complete mandatory confidentiality and privacy trainings, as well as a Code of Conduct training. Google's Code of Conduct specifically addresses responsibilities and expected behaviour with respect to the protection of information

ISSUE: Use of third-party sub processors
RISK: Non-compliance with the requirements under GDPR
MITIGATING ACTION: Google Group companies directly conduct the majority of data processing activities required to provide the GSuite and Google Cloud Platform services. However, Google do engage some third-party processors to assist in supporting these services. Each data processor goes through a rigorous selection process to ensure it has the required technical expertise and can deliver the appropriate level of security and privacy. Google make information available about Google group sub processors supporting GSuite and Google Cloud Platform services, as well as third-party sub processors involved in those services, and Google include commitments relating to sub processors in current and updated data processing agreements

ISSUE: Understanding the cloud-based solution chosen where data processing/storage premises are shared?
RISK: The potential of information leakage
MITIGATING ACTION: School data is protected as if it were on its own server. Unauthorized parties cannot access school data. Other customers cannot access school data, and the school cannot access theirs. All user accounts are protected by Google's secure architecture that ensures that one user cannot see another user's data DPIA Google Classroom 20200505 v1.2 9 9 .

ISSUE: Cloud solution and the geographical location of where the data is stored
RISK: Within the EU, the physical location of the cloud is a decisive factor to determine which privacy rules apply. However, in other areas other regulations may apply which may not be Data Protection Law compliant
MITIGATING ACTION: Google Cloud Platform (GCP) allows customers to choose to store their data in Europe, North America, or Asia. If applicable Articulacy would specify this location when they configure their application to ensure compliance under GDPR Google's certification under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks includes GSuite and Google Cloud Platform. Google have also gained confirmation of compliance from European Data Protection Authorities for its model contract clauses, affirming that Google's current contractual commitments for GSuite and Google Cloud Platform fully meet the requirements under GDPR in terms of transfers of personal data from the EU to the rest of the world.

ISSUE: Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
RISK: GDPR non-compliance
MITIGATING ACTION: Google provides capabilities and contractual commitments created to meet data protection recommendations provided by the Article 29 Working Party. Google offers to sign EU Model Contract Clauses and a Data Processing Amendment for GSuite and Data Processing Amendments for Google Cloud Platform. GDPR restricts the movement of data from the EU to non-EU countries that do not meet the EU's "adequacy" standard for privacy protection. Processing personal data strictly within the EU is a means of compliance with this regulation.

ISSUE: Implementing data retention effectively in the cloud
RISK: GDPR non-compliance
MITIGATING ACTION: Google provide tools to make it easy for Articulacy to take its data without penalty or additional cost imposed by Google. Administrators can export customer data in standard formats at any time during the term of any agreement entered into by the school and Google. Google Cloud Platform customers can extract their data using industry standard tools, for which there may be charges.

ISSUE: Responding to a data breach
RISK: GDPR non-compliance
MITIGATING ACTION: GSuite and Google Cloud Platform provide contractual commitments around incident notification for many years. Google will continue to DPIA Google Classroom 20200505 v1.2 10 10 promptly inform schools/organisations of incidents involving its data in line with the data incident terms in Google's current agreements and the updated terms that apply when the GDPR came into force. Google's security practices are verified and certified by third-party auditors. Google has achieved ISO 27001 certification, which means that an independent auditor has examined the controls present in its data centres, infrastructure, and operation. Amongst these practices, employees are subject to background investigations based on their level of access. Any employee access is governed by a policy of "least privilege access," which means that access is only granted to the information and resources that are necessary for the execution of the assigned task.

ISSUE: Subject Access Requests
RISK: The school must be able to retrieve the data in a structured format to provide the information to the data subject
MITIGATING ACTION: Data controllers can use the GSuite and Google Cloud Platform administrative consoles and services functionality to help access, rectify, restrict the processing of, or delete any data that they and their users put into Google systems. This functionality will help the school fulfil its obligations to respond to requests from data subjects when exercising their rights under the GDPR.

ISSUE: Data Ownership
RISK: GDPR non-compliance
MITIGATING ACTION: Articulacy as data controller retains ownership of the data. Google Classroom is the data processor.

ISSUE: Cloud Architecture
RISK: Articulacy needs to familiarise itself with the underlying technologies the cloud provider uses and the implications these technologies have on security safeguards and protection of the personal data stored in the cloud
MITIGATING ACTION: Google's application and network architecture is designed for maximum reliability and uptime. Data is distributed across Google's servers and data centres. If a machine—or even an entire data centre—fails, school/organisation data will still be accessible. Google owns and operates data centres around the world to keep the DPIA Google Classroom 20200505 v1.2 11 11 services the school uses running 24 hours a day, 7 days a week. Google's application and network architecture is designed for maximum reliability and uptime. Google's computing platform assumes ongoing hardware failure, and it uses robust software failover to withstand disruption. All Google systems are inherently redundant by design, and each subsystem is not dependent on any particular physical or logical server for ongoing operation. Data is replicated multiple times across Google's clustered active servers so that, in the case of a machine failure, data will still be accessible through another system. Google also replicate data to secondary data centres to ensure protection from data centre failures.

ISSUE: Security of Privacy
RISK: GDPR non-compliance
MITIGATING ACTION: Google is subject to independent verification of its security, privacy, and compliance controls. In order to provide this, Google undergo several independent third-party audits on a regular basis. For each one, an independent auditor examines Google's data centres, infrastructure, and operations. ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. Google has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centres that make up its shared Common Infrastructure as well as for GSuite and Google Cloud Platform. ISO 27017: is an international standard of practice for information security controls based on ISO/IEC 27002, specifically for Cloud Services. Google has been certified compliant with ISO 27017 for GSuite and Google Cloud Platform ISO 27018: is an international standard of practice for protection of

personally identifiable information (PII) in Public Cloud Services. Google has been certified compliant with ISO 27018 for GSuite and Google Cloud Platform. The American Institute of Certified Public Accountants (AICPA) SOC 2 (Service Organization Controls) and SOC 3 audit framework defines Trust Principles and criteria for security, availability, processing integrity, and confidentiality. Google DPIA Google Classroom 20200505 v1.2 12 12 has both SOC 2 and SOC 3 reports for Google Cloud Platform and GSuite. This means that independent auditors have examined the controls protecting the data in Google's systems (including logical security, privacy, and data centre security), and assured that these controls are in place and operating effectively:

- The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;
- Details of the legitimate interests being pursued by the Company;
- An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- An assessment of the risks posed to individual data subjects; and
- Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

Risk

Data could be compromised	Low
Data breaches	Low
Subject Access request	Possible
Data transfer	Reduced
Data Retention	Low

Implementation of Policy

This Policy shall be deemed effective as of 10.06.2020. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Signed on behalf of Articulacy	
Print name here	Leanne Fennell
Date reviewed	31st August 2020