Data Protection Impact Assessment

Kognity

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.

The International School of Stavanger (ISS) operates a cloud based system. As such ISS 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. ISS recognises that moving to a cloud service provider has a number of implications. ISS 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 taking into account 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. The school needs to know where the data is stored, how it can be transferred and what
access possibilities the school has to its data. The location of the cloud is important to determine applicable law. The school 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 by the school.

A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce or eliminate the risks.
5. Sign off the outcomes of the DPIA.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Kognity is an online teaching and learning platform with interactive content for IB DP, Cambridge IGCSE and High School Science students. At ISS Kognity is used by grade 11 and 12 students (IBDP curriculum).

Students access their accounts via Google sign-in. Personal student data collected by Kognity includes full names, email addresses and graduation years.

There is also the option to add assignments to Google Classroom directly from Kognity where the appropriate section of the textbook is posted to the corresponding assignment, which gives Kognity access to a user's Google Classroom.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The Kognity Privacy Notice provides the legitimate basis for its data collection.

How will you collect, use, store and delete data?

ISS staff members designated as Kognity account administrators create subjects, allocate students to the subjects, and, when necessary, delete student accounts.

Personal data is stored only for as long as it is needed to fulfil the purpose it was collected for. In addition, Kognity could be required to keep personal data longer to fulfil legal obligations - in that case the data will not be processed for any other purpose. Personal data of users who haven't interacted with the platform in the past twelve months is anonymised or deleted. ISS staff who function as Kognity administrators can delete student accounts if necessary.

Kognity integrates with Google Classroom to allow staff to allocate sections of a textbook to an Assignment posted to Google Classroom.

What is the source of the data?

User information is collected through the application process then extracted from the ISS management information system (iSAMS) and uploaded to Kognity. In addition to this fields from OneLogin as the primary ISS IDP are used during the authentication process.

Will you be sharing data with anyone?

ISS routinely shares student information with relevant staff within the school, schools that the student attends after leaving, the Kommune, the Health Services, Learning Support Services, OneLogin and various third party Information Services applications that are used for educational purposes.. This information is recorded in the ISS document controller

template.

What types of processing identified as likely high risk are involved?

Transferring 'special category' data from the school to the cloud. Storage of personal and 'special category data in the Cloud. However, in terms of using Kognity, no special category data will be used.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

What is the nature of the data?

Student data collected by Kognity relates to personal identifiers needed for the establishment of personal accounts (full name and email address). Login is provided through Google. Kognity also keeps a record of the students graduating year and what courses they are assigned to enable the distribution of textbooks according to the specific course requirements of a student.

Special Category data?

No special category data is collected by Kognity.

How much data is collected and used and how often?

Personal data is collected when accounts are set up for students and used for login purposes.

How long will you keep the data for?

ISS can delete student accounts if necessary. Kognity anonymizes or deletes personal data for users who have not used the platform over a period of twelve months. Accounts are deleted from Kognity when a student graduates from ISS.

Scope of data obtained?

User personal data is used for analytics purposes, in order to manage and improve the Kognity platform. Similarly graduation dates and course information are used to manage which textbooks should be distributed to which students.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

What is the nature of your relationship with the individuals?

ISS collects and processes personal data relating to its pupils to ensure the school provides education to its students delivering the ISS and IBDP Curriculum.
Through the GDPR statement, ISS is committed to being transparent about how it collects and uses data and to meeting its data protection obligation.

How much control will they have?

Kognity encrypts all data at rest by Advanced Encryption Standard (AES) 256 bits, and all data communication to the platform by the Transport Layer Security (TLS) protocol (TLS 1.2 and TLS 1.3).

Kognity users have the right to information about what personal data is processed and why, and access to such data that is stored by the platform. Other rights include the right to have erroneous data corrected, the right to have the data deleted.

Do they include children or other vulnerable groups?

Kognity does retain data about children, but does not include special category data and only includes information necessary for authentication of the service and distribution of appropriate digital textbooks.

Are there prior concerns over this type of processing or security flaws?
How is the information stored? Does the cloud provider store the information in an encrypted format? What is the method of file transfer? How secure is the network and what security measures are in place?

ISS recognises that moving from a manual system to an electronic system which holds sensitive personal data in the cloud raises a number of General Data Protection Regulations issues as follows:

ISSUE: Unauthorised access by third party

RISK: There is a risk of unauthorised access to information by third parties

MITIGATING ACTION: Kognity follows industry-recognized standards such as the National Institute of Standards and Technology's (NIST) Cybersecurity Framework and the International Organization for Standardization's (ISO) Information technology - Security techniques - Information security management systems - Requirements ISO/IEC 27001:2017.

ISSUE: Unauthorised access to Kognity through a breach of IDP

RISK: ISS owned account is breached

MITIGATING ACTION: The only information stored on Kognity will be uploaded by specific users of the system and contains no special category data.

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. Google have also enabled HTTPS for all of its GSuite services, so that the school data is encrypted when travelling from a school device to Google and also while in transit between Google data centres.

ISSUE: Subject Access Requests

RISK: The school must be able to retrieve the data in a structured format to provide 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
All Google employees are required to sign a confidentiality agreement and complete mandatory confidentiality and privacy training, 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: Unauthorised access to a Google service

RISK: Staff or Student Google Account becomes compromised as a result of a Kognity breach

MITIGATING ACTION: Google accounts are controlled centrally by our IdP. Ensure that 3rd party service only has access to functions of Google required for operation of that service. Revoke all other permissions. Ensure swift action when isolating a compromised account or service from our IDP.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
Benefits: • Scalability • Reliability • Resilience • Delivery at a potentially lower cost • Supports mobile access to data securely • Update of documents in real time • Good working practice, i.e. secure access to sensitive files Kognity is an essential service for providing access to course materials and textbooks for IBDP students.

Step 3: Consultation Process
Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
Seek the opinion and / or consent of the Board of Governors, parents where necessary, DPO and Director.

Step 4: Assess necessity and proportionality
Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
The lawful basis for processing personal data is contained in the school's Privacy Notice (Users). The Legitimate basis includes the following: Article 6, Paragraph 1: (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law.

The cloud based solution will enable the school to uphold the rights of the data subject?

The right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and the right not to be subject to automated decision-making

The school will continue to be compliant with its Data Protection Policy.

Step 5: Identify and assess risks			
Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Data transfer; data could be compromised	Possible	Severe	Medium
Asset protection and resilience	Possible	Significant	Medium
Data Breaches	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Data Retention	Probable	Significant	Medium

Step 6: Identify measures to reduce risk				
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated Reduced Accepted	Low Medium High	Yes/No
Data Transfer	Secure network, end to end encryption	Reduced	Medium	Yes
Asset protection & resilience	Data Centre in EU, Certified, Penetration Testing and Audit.	Reduced	Medium	Yes
Data Breaches	Appropriate Training. Audit externally shared documents. Email restrictions.	Reduced	Low	Yes

Subject Access Request	Technical capability to satisfy rights of data subject	Reduced	Low	Yes
Upholding rights of data subject	Technical capability to satisfy data subject access request Implementing school data retention periods in the cloud	Reduced	Low	Yes
Data Retention	Retention periods set in accordance with the ISS data controller template	Reduced	Low	Yes

Step 7: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:	IT Director	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA