INTERNATIONAL SCHOOL OF STAVANGER

LEARNING WELL-BEING COMMUNITY

# Data Protection Impact Assessment

## KnowBe4

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.** |
| KnowBe4 KMSAT is B2B SaaS (Software-as-a-Service) company that provides its Customers a variety of services. The services that will be included in this document are:<br><br>KMSAT Console - a simulated phishing and security awareness and compliance training platform |

This platform is essential to ensure that ISS employees are properly trained to detect social engineering, phishing and other attacks, as well as how to appropriately handle and protect sensitive data.

## 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?**

Data and information that's provided to KnowBe4 are Name, Email address, Title, Security, Strictly Necessary Cookie Information, IP addresses, Web browser Information, Third Party Integration Data. Source of data is OneLogin IAM provisioned to KnowBe4 using SAML 2.0.

**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?**

Data collected is used for Phishing Campaign Results and Metrics, Security Awareness Training Results, Risk Score, Training and Coaching Information. Collections happen upon completion of training/phishing campaigns. KnowBe4 does not request nor does it provide appropriate fields for submitting special categories of data for any of its tools. Any special categories of data that may be received would be incidental and can be deleted upon request. KnowBe4 operates both US and EU instances. Customers may choose where data is stored during the course of the services. Our data is stored within EU.

**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)?**

Data is processed only for staff as part of their ongoing security training. No children or vulnerable groups are involved.

**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?**

Access to the accounts will be controlled by the school. KnowBe4 protects user data by using appropriate security measures, including encryption, and by disclosing the information only to third parties that are capable of and contractually obligated to maintain its confidentiality and security.

**Do they include children or other vulnerable groups?**

No children or vulnerable groups are involved.

**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:** KnowBe4 maintains a security program designed to protect the security, privacy, confidentiality and integrity of users personal information against risks such as unauthorised access or use, or unintended or inappropriate disclosure.

---

**ISSUE:** Unauthorised access to KnowBe4 through a breach of IDP

**RISK:** ISS owned account is breached

**MITIGATING ACTION**: The only information stored on KnowBe4 will be a user's email address, name and training progress and contains no special category data. The risk of sensitive data loss in this situation is deemed as minimal.

---

**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 KnowBe4 services is encrypted. KnowBe4 have also enabled HTTPS for all of its services, so that the school data is encrypted when travelling from a school device to KnowBe4.

---

**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 KnowBe4 administrative consoles and services functionality to help access, rectify,
restrict the processing of, or delete any data. This functionality will help the school fulfil its obligations to respond to
requests from data subjects when exercising their rights under the GDPR

| **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?** |
|---|
| Processing is done to provide staff with security training, data handling training and simulated phishing testing. |

| **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, DPO and Director if necessary. |

| **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:<br><br>Article 6, Paragraph 1:<br><br>(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;<br>(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<br>Reduced<br>Accepted | Low<br>Medium<br>High | Yes/No |
| Data Transfer | Secure network, end to end encryption | Reduced | Medium | Yes |
| Asset protection & resilience | Data Centre in EU, Certified, | Reduced | Medium | Yes |

| | | | | |
|---|---|---|---|---|
| | Penetration Testing and Audit. | | | |
| 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 | Reduced | Low | Yes |
| Data Retention | Implementing school data retention periods in the cloud<br><br>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<br>risk, consult the ICO before going<br>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 |