THE UNIVERSITY of EDINBURGH

Assessment Details

Name Noteable Service DPIA (outwith University of Edinburgh)

Respondent James Stix,Anne Robertson

Date Completed 26/03/2021 09:13

Approver Rena Gertz

Stage Completed

Result Approved

Assessment Questions

1 Description of Activity

1.1 **Activity Name**

Response

Noteable Service DPIA for organisations outwith The University of Edinburgh

1.2 **Activity Outline**

Explain broadly the scope of the activity, particularly what the activity aims to achieve (e.g. the benefits to the University, or to data subjects etc.) and what type of data processing it involves.

To do so, you should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows – where you are getting the data from, where it will be stored and where it could be transferred to. You should also say how many individuals are likely to be affected by the project.

e.g. Data will be collected via online forms

↓

Data will be stored encrypted on departmental drives

↓

Pseudonymised dataset will be provided to Department X along with report

Response

Noteable is a cloud-based service that provides access to Jupyter notebooks via a web browser. Users access Noteable through their existing single sign on authentication mechanism. We collect, store and use the following categories of personal data: Username as it appears within the users' organisational single sign on system. We capture user information to provide users with access to a personal Noteable storage area and to provide relevant course materials such as released assignments. If an organisation requests, we will also capture user first name and surname.

1.3 **Why is the processing necessary?**

Why is it necessary to process the data you have described in the Activity Outline?

Response

We capture user information to provide users with access to a personal Noteable storage area and to provide relevant course materials such as released assignments. If an organisation requests, we will also capture user first name and surname to make assignment class listings more meaningful to teachers.

1.4 **How will the activity help you achieve your objective(s)?**

Describe how what you plan to do will help you achieve your purpose -describe how you ensure that the personal data is proportionate to the objective. Is there a less intrusive way of achieving your aim?

Response

Noteable supports the teaching of coding. The capture of personal data ensures a user has a personal space to carry out their coding. It also ensures a teacher can mark their individual work.

1.5 **List of Stakeholders - Activity or Proposal Stakeholders**

This should cover all individuals or groups involved in the activity, the so-called activity or proposal stakeholders. Examples are School/College/Department planning to use the activity; project officers; IS, if involved; or external organisations such as software providers. At this stage you want to have as broad a list of groups as possible - these are the people with the knowledge you need who will help you answer the questions in this DPIA.

*Note: This list does **NOT** include data subjects affected by the proposal/activity.*

Response

James Stix, Noteable Service Owner, EDINA
Bert Robberechts, Noteable Service Operations Manager, EDINA
Anne Robertson, Head of Services, EDINA
Keith Copeland, Head of Services, EDINA

1.6 **List of data subjects affected by the activity**

For example: staff members, students, members of the public

Response

Users of Noteable including staff and students at UK Higher Education institutions and teachers and pupils at Scottish secondary schools.

1.7 **Other examples**

Conduct a search for similar activities undertaken by either another part of the University or an outside organisation. This may save you time by learning from a DPIA done for a similar activity, or you might learn how that activity identified and mitigated risks, thus helping you with your own DPIA.

Response

The University of Edinburgh's Noteable service

2 Compliance with Privacy Laws

2.1 **Compliance Check**

Data Protection legislation is relevant to any DPIA, and this section forms the data protection compliance check which should always be carried out. The Data Protection Officer will be able to advise you on the relevance of other privacy laws.

2.2 **What type of personal data are you processing?**

For guidance on what personal data is, consult the ***definitions.***

Response

Any other personal data

Justification

None

2.6 **List the personal data you are going to process?**

For guidance on what personal data is, consult the ***definitions*****.**

Response

Authentication system usernames
Individuals' first names and surnames

2.7 **Which of the legal bases in Article 6 (1) will provide a lawful basis for the processing?**

Which of the legal bases in Article 6 (1) will provide a lawful basis for the processing? Consult the document ***Guidance – how to determine the legal basis for processing personal data***

Response

Contract

Justification

EDINA are offering organisations a comprehensive cloud computational notebook service for the purposes of teaching and learning delivered upon an organisations' own authentication system. A comprehensive computational notebook service provides all users with their own personal notebook server and workspace to save notebooks. To this end, EDINA must maintain persistent identify of users across sessions.

2.8 **Are you processing a special category of personal data?**

Click all those that apply or, if you are not processing a special category, click 'No'.

Response

No

Justification

None

2.10 **How are individuals being made aware of how their personal data will be used?**

Check if what you intend to do is already covered in one of the University privacy notices, a list of which can be found ***here****. If not, you will need to either ask for it to be included in the relevant privacy notice(s) or create a bespoke privacy notice. Templates for bespoke notices can be found* ***here.***

Response

Bespoke privacy notice to be created

2.11 **Does the activity involve the use of existing personal data for new purposes?**

Response

No

Justification

Personal data used for authentication and user experience only.

2.12 **Can you confirm that data collection procedures are adequate, relevant and not excessive, i.e. that you are not collecting more information than necessary?**

Response

Yes

Justification

Personal data used for authentication and user experience only.

2.13 **How will the personal data be checked for accuracy?**

Response

Personal data will be provided by the customer's own authentication system via an agreed system specification.

2.14 **How long will the personal data be retained for?**

Response

As agreed with customer as per their own data retention policy generally one year post degree /award completion.

2.15 **What technical and organisational security measures will be in place to prevent any unauthorised or unlawful processing of the personal data?**

Response

Only EDINA technical engineers have access to Noteable infrastructure. EDINA technical engineers undertake mandatory information security training. Noteable infrastructure is managed by UofE network engineers to consistent standard as with all university infrastructure.

2.16 **Has the personal data been evaluated to determine whether its processing could cause unwarranted damage or distress to data subjects?**

Response

Not Applicable

Justification

None

2.17 **Do you use a data processor?**

Response

No

Justification

None

2.21 **Will you be transferring personal data to a country outside of the European Union or the European Economic Area (EEA)?**

Countries in the EU
Countries in the EEA

Response

No

Justification

None

2.25 **If the data will be anonymised, is it likely that a 'motivated intruder' will be interested in attempting re-identification by linking the data with other information available to them?**

*For guidance on 'motivated intruders', please see**here.***

Response

Not Applicable

Justification

None

2.26 **If a subject access request (SAR) is received for personal data included in the activity, how easy is it to comply? Is the data easily accessible elsewhere?**

Consider whether if the University receives a subject access request you easily find and extract the relevant personal data, or if the 'golden copy' is held elsewhere. Guidance on how to answer SARs can be found here.

Response

Only username first name surname as supplied by the customer are used.

2.27 **Are you able to comply with requests for erasure or restriction of processing? Can you apply an exemption?**

*For help with deciding whether an exemption applies, consult chapter 11 of the Data Protection Handbook, which can be found **here**.*

Response

We can comply

Justification
If a customer requests the manual deletion of a user account outside of the agreed data retention cycle, that can be carried out manually be EDINA technical colleagues.

2.28 **Are provisions in place in case a data protection breach occurs as part of the activity?**
*Ensure that you are familiar with the University data protection breach reporting procedure, available on the website **here**.*

Response
Yes

2.29 **From the Data Protection compliance check in this section we have concluded:**
Have you satisfied all the requirements asked for above?

Response
We have concluded that processing is data protection compliant.

Justification
Only username first name surname as supplied by the customer are used for the purposes of authentication and user experience.

3 Screening

3.1 **Screening**
The answers to the following questions will determine whether you need to continue to the next stage. If you have answered all screening questions with 'no', then you can stop here - you will not need to carry out a full DPIA.

3.2 **Will there be new or additional information technologies that have the potential for privacy intrusion?**
This could involve external suppliers of software having access to personal data.

Response
No

Justification
Noteable is hosted on university infrastructure. Only EDINA software engineers and university ISG ITI staff have access to this infrastructure.

3.3 **Will the activity involve the collection of new identifiable or potentially identifiable information about individuals?**

Response
No

Justification
Noteable integrates with an organisations' existing authentication mechanism for the purposes of consistently identifying a user only.

3.4 **Will the activity compel individuals to provide information about themselves, i.e. where they will have little awareness or choice?**

Response
No

Justification
Noteable provides a coding environment, the only personal data requested is for authentication purposes.

3.5 **Identification methods - Will there be new or substantially changed identity authentication requirements that may be intrusive or onerous, such as new log in requirements?**

Response
No

Justification
Noteable uses an organisations' existing authentication system.

3.6 **Will any other organisations outside the University have access to the personal data?**

Response
No

Justification
Noteable is fully delivered by The University of Edinburgh on university infrastructure.

3.7 **Will there be new or significant changes to the handling of special categories of personal data or data that would be considered sensitive by the data subjects?**

Response
No

Justification
Personal data are used for authentication and assignment management only.

3.8 **Are you using information about individuals for a purpose it is not currently used for or in a new way?**

Response
No

Justification
Personal data are used for authentication and assignment management only.

3.10 **Will there be new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?**

Response
No

Justification
Personal data are used for authentication and assignment management only.

3.11 **Will there be new or changed ways of data collection that may be considered intrusive?**
Examples are:

- *CCTV cameras in a coffee lounge*
- *fingerprint authentication to enter the library*
- *non-anonymous surveys into teaching quality*

Response
No

Justification
Personal data are used for authentication and assignment management only.

3.12 **Will there be changes to data quality assurance or processes and standards?**

Response
No

Justification
Personal data are used for authentication and assignment management only.

3.13 **Are there any concerns about new or changed data security arrangements?**

Response
No

Justification
Personal data are used for authentication and assignment management only.

3.14 **Are there concerns about new or changed access or disclosure arrangements?**

Response
No

Justification
Personal data are used for authentication and assignment management only.

3.15 **Will there be new or changed data retention arrangements?**

Response
Yes

Justification
Different customers may request different data retention durations.

3.16 **Will there be changes to the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?**

Response
No

Justification
Username first name and surname used for authentication and user experience only.

3.17 **Determine whether you need to do a DPIA, or whether a privacy law compliance check is sufficient.**

If you have said 'yes' to one or more of the screening questions in 3.2to 3.16, then you need to continue on to the full DPIA - click on 'Yes'. If you have said 'no' to every question, the privacy law compliance check you have completed in section 2 is sufficient - click on 'No' and you will be able to submit the DPIA.

Response

Yes

Justification

Data retention arrangements may vary depending upon customer

4 Risk identification

4.1 **Risk identification and assessment**

*Below, you will find a list of **14 common risks**. Not all these risks are visible when you begin this section; each risk question appears as you answer the preceding question. The symbol indicating the number of outstanding questions will remain at 1 until all the risk questions have been answered.*
If any of these risks apply, choose them by answering 'yes' and providing a short description of the risk and how you would mitigate the risk.

If the risk applies – select 'Yes'. As a result you will be require to:

1. Provide a brief explanation / consequence of the risk occurring
2. Provide a brief explanation of the mitigating factors that will be undertaken to either eliminate or lower the risk
*3. In considering the defined mitigation measures, determine the likelihood of the risk occurring to be Low, Medium or High **after** mitigation.*
*4. In considering the defined mitigation measures, determine the impact on the data subjects and on the University to be Low, Medium or High **after** mitigation.*

If the risk does not apply, select 'No'

*Note: If **after mitigation** you still have **high risks**, the processing activity will have to be notified to the Information Commissioner!*

*When you have considered these 14 possible risks, there is space to describe **up to 3 additional risks** not listed in the potential risks.*

4.2 **Possibility that personal data is shared inappropriately.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

Personal data used for authentication and user experience only.

4.5 **Personal data may be used for a new and different purpose without the knowledge of the data subjects, perhaps due to a change in the context in which the data is used.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

Personal data used for authentication and user experience only.

4.8 **New surveillance methods such as CCTV, email monitoring etc. may be an unjustified intrusion on people's privacy.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

Not applicable

4.11 **Actions taken against individuals as a result of collecting information about them might be to their detriment or cause damage/distress.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

None

4.14 **People cannot use a service anonymously because identifiers might be collected and linked, if anonymity is what people were led to expect.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

Users understand for satisfactory experience they must authenticate.

4.17 **Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information if anonymity is what people were led to expect.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

Users will be staff and students at educational institutions.

4.20 **Collecting information, matching and linking identifiers or whole datasets might mean that data are no longer anonymous if anonymity is what people were led to expect.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

Personal data is used for authentication and user experience only.

4.23 **Excess information collection or information not properly managed can lead to creation of duplicate records.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

Personal data is used for authentication and user experience only.

4.26 **If a retention period is not established information might be used for longer than necessary.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

Data retention duration will be agreed with customers as part of onboarding process

4.29 **The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the University.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

Not applicable

4.32 **Public distrust about how information is used can damage the University's reputation and lead to loss of business.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

Not applicable

4.35 **Data loss causing damage or distress to individuals or damage the University's business**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
No

Justification
Not applicable

4.38 **Despite proper security, is there an increased possibility of external unlawful access to the data such as hacking?**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
No

Justification
Not applicable

4.41 **Using an external data processor or sharing with another data controller increases the risk of unlawful access to personal data.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
No

Justification
None

4.47 **Any other risk you have identified - describe below.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
No

Justification
None

4.56 **Did you identify any high risks during screening?**
From the risks identified by the activity stakeholders, you should now be in a position to assess whether a data subject consultation is appropriate.

*Click on '**Yes**' If you have identified **multiple** high risks that are not hacking related.*
You will now have to conduct a data subject consultation and feed the results into the questions in section 5.

*If there are mostly low to medium risks, you will be able to continue straight to approval by clicking '**No**' and then by clicking 'Submit' when presented with this option.*

Response
No

Justification
None

6 Review

6.1 **Set a date for the scheduled review - such as in 6 months or a year**
The purpose of a review is to ensure that the mitigation measures introduced as part of the DPIA are working effectively. It is expected that such a review, particularly in the case of major DPIAs, will be carried out as part of the wider review into the effectiveness of the activity deliverables. For smaller DPIAs, the review may be carried out as a standalone process. Either way, upon completion of the DPIA you should record how this review will be carried out, by whom, and when.

Response
22/09/2021

6.2 **Who will carry out the review?**
Name the person or team that will carry out the review at the specified date.

Response
Anne Robertson

7 Submit

7.1 ***Submit***

7.1 **Submit**

Please now click the blue 'Submit' button in the bottom right corner.