Data Protection Impact Assessment (DPIA)

Slido - for interactive events

Document Name	Data Protection Impact Assessment – **Slido**
Author/Owner (name and job title)	Suzanne Forshaw - Lead Communications officer
Department/Team	Corporate Communications
Document Status	Draft
Version Number	0.1
Release Date	
Approver (if applicable)	
Review Date	
Distribution	Internal

Guidance for completing this DPIA template

- If you're unsure whether you need to complete a DPIA, use the Screening assessment - do I need to do a DPIA? first to help you decide.

- ***Must*** and ***should*** are used throughout the guidance notes in this template to help you understand which things are a legislative requirement and ***must*** be done versus things that the ICO considers ***should*** be done as best practice to comply effectively with the law.

- You ***must*** complete this DPIA template if your screening assessment indicates a DPIA is required.
- You ***should*** aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you won't be able to continue with your plans without changing them, or at all.
- We recommend that you fill out each section of this template in order, as each subsequent section builds upon the last. You will not be able to complete later sections correctly if you skip ahead. You ***should*** read the guidance notes throughout this template to help you with each section.
- If you are struggling with completing this template the Information Management and Compliance Service is available to provide advice and support. Please keep in mind their service standards if you require help.

1. Process/system overview

1.1 Ownership

Project Title:	Slido
Project Manager:	Suzanne Forshaw
Information Asset Owner:	Exec Director of Communications and Public Affairs - Angela Balakrishnan
Controller(s):	ICO & Slido (see section 1.3. for more information)
Data processor(s):	Slido (see section 1.3. for more information)

1.2 Describe your new service or process

Guidance notes:

- Provide a brief summary of the service or process you want to implement. Include any relevant background information and your key aims/objectives.

The communications department are seeking to procure an online audience interaction platform for external and internal events. Slido - Audience Interaction Made Easy

Slido is a cloud-based service that facilitates real-time communication at events. Slido will allow us to engage participants with live polls, Q&A, quizzes and word clouds — whether the event is in person, online or in-between.

As most of our events are digital this tool will enable us to have more dynamic interaction with our audience, who are primarily people working in data protection on the front line in organisations and in government.

Slido can be used at both our own events and external speaking engagements attended by any senior members of the ICO.

Initially the request for using Slido came from senior leaders within the ICO.

A senior leader in the ICO has requested a tool which will provide him with assisted technology support during internal events, meaning he can use the Q&A function independently. He will also use the added features like creating word clouds and quizzes to make internal staff briefing more interactive.

A senior leader within the ICO has requested a tool that they can use to include delegates in a conversation directly with them via for Polls and Q&A when they are at speaking engagements external to the ICO – not hosted on our platforms. We often support our leaders on social media channels in the same way but with Slido we can target an audience who are specifically engaged in the event but using the ink / hashtag to allow them to enter our Slido page related to the discussion.

Also as outlined in the ICO25 plan we talk about 'increasing access' in our stakeholder engagements.

- create, host and moderate a forum for organisations to discuss and debate compliance questions and standards online, bringing together experts; and
- bring together businesses and organisations to learn and share with us and each other through our Data Protection Practitioners' Conference and other stakeholder engagement events. We will

increase access and reduce costs by holding them virtually where our objectives are best met this way.

1.3 Personal data inventory

Guidance notes:

- We ***must*** have a clear understanding of the personal data being processed. This is **essential** for identifying and managing risks.
- Use the table below to list each category of personal data being processing. Use a new row for each data category. You can add as many rows to the table as you need.
- Categories of data may not be obvious to you from the outset e.g. tracking data (IP or location) or data collated via cookies and you need to take the time to fully understand the extent of the personal data you will process.
- Your data subjects are the individuals the personal data relates to. For example, these could be members of the public, ICO employees, our contractors etc.
- Recipients will be anyone who the data is shared with.
- UK GDPR restricts transfers of personal data outside of the UK so any overseas transfers ***must*** be identified.
- Personal data should be kept for no longer than is necessary. You ***must*** identify a retention period for the personal data you intend to process.

Guidance Link: What is personal data? | ICO

Category of data	Data subjects	Recipients	Overseas transfers	Retention period
ICO as Controller				
Participant content data in Enterprise plans (optional): Questions, poll answers, ideas, chats – content shared by participants and related to a Non anonymous individual	ICO staff / external event participants	Slido	Yes If yes, list the countries the data will be transferred to: Ireland Germany	< 1 year (please specify time period below) If selecting other, please specify the length of time personal data will be retained: 3 months
ICO and Slido as separate controllers				
Organiser profile data: Name, email address, role, company	ICO staff	Slido	Yes If yes, list the countries the data will be transferred to: Ireland Germany	Other (please specify time period below) If selecting other, please specify the length of time personal data will be retained:

				Retained until account termination
Contact data of representatives involved in the procurement, legal, IT & security and audit processes: Name, email address, role, company	ICO staff	Slido	Yes If yes, list the countries the data will be transferred to: Ireland Germany	Other (please specify time period below) If selecting other, please specify the length of time personal data will be retained: Slido will keep this information for 6 years
Other organiser data (optional): video & voice. This may include e.g. support, user experience research calls, testimonials, feedback	ICO staff	Slido	Yes If yes, list the countries the data will be transferred to: Ireland Germany	Other (please specify time period below) If selecting other, please specify the length of time personal data will be retained: Until deletion requested

Purchase data (optional): E.g.; invoices. Slido do not collect payment card information - this is collected directly by the payment gateway	ICO staff	Slido	Yes If yes, list the countries the data will be transferred to: Ireland Germany	6 years (by both ICO and Slido) If selecting other, please specify the length of time personal data will be retained:
Slido as controller				
User technical data: Most of this data is not personal data, but some may be in some circumstances. E.g.: - Device data (e.g. hardware model, operating system version, unique device identifiers), - Log data (e.g. details about your connection such as IP address, date, time, edge-location, sslprotocol, ssl-cipher or time-taken to serve you requested site, device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL) - Location	ICO staff / external event participants	Slido	Yes If yes, list the countries the data will be transferred to: Ireland Germany	< 1 year (please specify time period below) If selecting other, please specify the length of time personal data will be retained: 180 days after collection

information - (IP address) - Unique application numbers - Browser local storage and application data caches				
Cookies and other trackers: Essential cookies, Analytical and advertising cookies are optional. For more information about cookies, please see our Cookie Policy	ICO staff / external event participants	Slido	Yes If yes, list the countries the data will be transferred to: Ireland Germany	Other (please specify time period below) If selecting other, please specify the length of time personal data will be retained: Depends on cookie type, more detail in Cookie Policy
Support data (optional): E.g. on web forms, chat, email, demo, contact us, newsletter, webinars, masterclasses, feedback, user research etc. Usually name, email, company, queries, rarely voice, pictures and video	ICO staff	Slido	Yes If yes, list the countries the data will be transferred to: Ireland Germany	6 years If selecting other, please specify the length of time personal data will be retained: Slido will keep this information for 6 years

In response to the DPIA forum questions about why both the ICO and Slido are controllers Slido have responded:

Slido identified ourselves and our customers as independent controllers with respect to the "other organiser data" and "purchase data" for legal clarity and transparency. By stating that we and our customer are independent controllers, we are acknowledging that each party independently determines how the "other organiser data" and "purchase data" are collected, used, and disclosed.

For example regarding the purchase data: As an independent controller, you have a distinct role and responsibility in determining the purposes and means of processing the purchase data. This data may include information such as payment details, invoices and order history.

By designating you as an independent controller for purchase data, we recognize that you have your own legal obligations and responsibilities in handling this data. This designation ensures that you have autonomy and control over the processing activities related to the purchase data, such as managing orders and payments.

1.4 Lawful basis for processing

Guidance notes:

- To process personal data, you ***must*** have a lawful basis. Select a lawful basis for processing the personal data in your inventory from the drop-down lists below.

Guidance Links: Lawful basis for processing & Lawful basis interactive guidance tool

First, select a lawful basis from Article 6 of the UK GDPR.

Article 6(1)(f) - legitimate interests

If more than one lawful basis applies to your processing, please list any additional basis here:

Guidance notes:

- If your personal data inventory includes any ***special category data,*** you ***must*** identify an additional condition for processing from Article 9 of the UK GDPR.

Guidance link: Special category data

Next, if applicable, select an additional condition for processing from Article 9 of the UK GDPR:

N/A - no special category data being processed

If you have selected conditions (b), (h), (i) or (j) above, you also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018. Please select from the following:

N/A - no special category data being processed

If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of the conditions set out in Part 2 of Schedule 1 of the DPA 2018. Please select from the following:

N/A - no public interest processing

Guidance notes:

- If you are processing **criminal offence data,** you ***must*** meet one of the 28 conditions for processing criminal offence data set out in paragraphs 1 to 37 Schedule 1 of the DPA 2018.

Guidance Link: Criminal offence data

Finally, if applicable select an additional condition for processing any criminal offence data:

N/A - no criminal offence data being processed

1.5 Necessity and proportionality

Guidance note:

- You ***must*** assess whether your plans to process personal data are both necessary and proportionate to you achieving your purpose. You should explain why this is the case below.
- You ***must*** take steps to minimise the personal data you process; processing only what is adequate, relevant and necessary.
- You ***should*** think about any personal data you can remove without affecting your objective.
- You ***should*** consider if there's any opportunity to anonymise or pseudonymise the data you're using.

We hope to use Slido to increase the interactive element of internal and external events.

We currently use MS Teams meetings and Live events as the main platform for all external events for up to 500 attendees. And as the main platfrom for internal events.

MS live events is the larger of the two platforms allowing up to 10,000 participant however does not offer the use of polls, word cloud or quizzes.

Teams meetings offers the use of Polls – which has been quite effective but we are not able to pre submit the poll questions meaning additional resources is require at each events to create each poll, in real time. We can only use team chat within a Team meeting which is not accessible to all.

The Slido platform can offer a fully accessible, dynamic Q&A platform where we can moderate the Questions, utilise Polls and quizzes to enhance a webinar / conference topic.

Additionally the request for using Slido has come from senior leaders within the ICO.

As per section 1
A senior leader within the ICO has requested a tool which will provide him with assisted technology support during internal events, meaning he can use the Q&A function independently. He will also use the added features like creating word clouds and quizzes to make internal staff briefing more interactive.

A senior leader within the ICO has requested a tool that they can use to include delegates in a conversation directly with them via for Polls and Q&A when they are at speaking engagements external to the ICO – not hosted on our platforms. We often support our leaders on social media channels in the same way but with Slido we can target an audience who are specifically engaged in the event but using the ink / hashtag to allow them to enter our Slido page related to the discussion.

The information gathered on Slido, in order for someone to take pat in a conversation with the ICO is minimal. Participants don't need to create a user profile; they can stay anonymous and take part in in polls, q&a.

Each Slido event has a unique event code (and QR code, URL link), which is generated at the time of creation. For any delegtes to join they will need to be sent this information in advance of the event. This means we will only invite registered to attend an event since we already have their data.

Slido events **can be** protected by an additional passcode or unique login pin code. The need for this additional features will be determined by the team who are running the content and will be assessed on the level of security needed. If an event is set up with a pin code to access the event, it will be sent to them in advance.

Any of the above options does not impact the outcome.

1.6 Consulting with stakeholders

Guidance notes:

- You ***should*** consult with relevant stakeholders both internally (for example Cyber Security, Legal Services, IT etc.) and externally to help you identify any risks to your data subjects.
- Briefly outline who you will be consulting with to inform your DPIA.

- Where appropriate you ***should*** seek the views of your data subjects, or their representatives, on your intended processing. Where this isn't possible, you should explain why below.

We have completed a SRA and filed with with Info. Sec colleagues. The response was as follows:

Thank you for sending over that Supplier Risk Assessment. I have been through their documentation and mostly everything seems in order so with it being a low-risk supplier we are saying "met with exceptions" with no further action required on their part for the supplier assessment.
From [redacted].

We have contacted collegues in procurement for the purpose of payment for this services, and due to the relatively low cost under the threashild of £5k per year collegues have advised that we simply need to complet the New supplier request form.

We plan to consult with legal services with regards the contractual terms and conditions, we have already been sent the contact from Slido.

I cannot seek the input of data subjects as they will be participants of events that are not yet finalised. We will provide Slido as an optional addition to the events therefore participants can choose to take part or not.

2. Personal data lifecycle

Guidance Note:

- You ***must*** provide a systematic description of your processing from the point that personal data is first collected through to its disposal.
- This ***must*** include the source of the data, how it is obtained, what technology is used to process it, who has access to it, where it is stored and how and when it is disposed of.
- If your plans involve the use of any new technology, for example a new piece of software, you ***must*** explain how this technology works and outline any 'privacy friendly' features that are available.
- If helpful you can use the headings provided below to help you construct your lifecycle. You can include a flow diagram if this helps your explanation.

Data source and collection:

Some personal data will be provided by Slido users (ICO staff with user accounts to access the platfrom) and event participants, and some data will be collected automatically (e.g. user technical data, browser data.)

An ICO Staff account holder will create the unique event page within the Slido website – requiring only a title for the event. Each Slido event has a unique event code (and QR code, URL link), so for a person to join an event, they need to know these - which will be sent to anyone who is registered to attend the event. Slido events can also be protected by an additional passcode or secure login as needed.

Only ICO staff connected with the event will have log in details to the Slido site and therefore changes or passwords will be set by ICO staff, and an access link will be distributed to event attendees in the joining instructions. Attendees do not need to have a Slido account to access the service. They will access the event by a unique link and once within the site they can take part in interactions relating to the events – like Q&A or Poll and quizzes. Participants don't need to create a user profile; they can stay anonymous and take part in in polls, q&a.

Slido will be an optional part of any event – meaning that attendees are not obliged to take part in the interactive element of our events.

Event data (e.g. poll and Q&A responses, word clouds) created as part of each event will be retained and anaylsed by Comms to gauge the success of the event.

Slido offers the account holder the options to export event data. I am not sure if we will need to since I have not yet used the platfroom and therefore I don't know what the reporting system is like. . If in the event any data is exported it will be saved in excel and held in a teams folder for up to 3 months. The teams folder will be access controlled to only the popele involved in the event.

Technology used for the processing:

Automatic data collection tools, such as cookies, embedded web links, and web beacons are used to collect IP addresses, MAC addresses, clickstream behaviour and telemetry. The purpose of this is set out in their Privacy Policy:

'These tools help make your visit to our website and Solutions easier, more efficient, and personalized. We also use the information to improve our website and Solutions and provide greater service and value, to better understand your potential interest in our Solutions, and to provide you with more relevant ads and other content.'

Users can opt out of the use of analytics and advertising cookies.

Storage location:

The personal data will be help in Slido's servers, located in Ireland and Germany

Access controls:

There are 3 licenses provided in the Enterprise package, Comms will manage 1 for external events, Internal comms will manage 1 for internal events and it is not yet decided who will manage the 3rd one yet.

The Senior comms officer for Events and Conferences will be the overarching account holder and will manage the Slido account and change / appoint new users, and make an annual review of the account and license holders to identify leavers as required.

Slido maintains a formal access control policy and employs a centralized access management system to control Slido staff access to Customer Data and to support the secure creation, amendment and deletion of user accounts.

Slido regularly reviews the access rights to ensure that all user accounts and user accounts privileges are allocated on a need-to-know basis. Upon a change in scope of employment or termination of employment, access rights are removed or modified asappropriate.

Access to highly sensitive systems such as data centres is controlled by secure log-on procedures including MFA or VPN technology.

Data sharing:

A list of Slido's subprocessors is listed in the 'Subprocessors' section of Slido's Privacy Policy

Disposal:

The ICO will retain events data (e.g. poll and Q&A responses, numbers of participants, etc) for 3 months , after which it will be manually deleted from Slido.

3. Key UK GDPR principles and requirements

Guidance notes:

- Answering the questions in this section will help you comply with essential data protection requirements.
- You may identify specific actions that are needed and you should add these to your list of DPIA outcomes in section 6.0.

3.1 Purpose & Transparency

Guidance notes:

- In most cases you will need to communicate essential information about your data processing to your data subjects. A privacy notice is the most common way of doing this.
- You ***must*** review the existing privacy notice on the ICO website. If your data processing involves the personal data of ICO staff, review our Staff Privacy Notice on IRIS.
- You need to decide if our existing privacy notices sufficiently cover your plans. If not, you ***must*** get them updated or you ***must*** provide your data subjects with a separate, bespoke privacy notice.

Q1. How will you provide your data subjects with information about your data processing?

An update is required to our existing privacy notice/s. This required action has been added to the DPIA outcomes (see section 6.0).

Guidance notes:

- If you identified consent as your lawful basis for processing in section 1.4 you ***must*** maintain appropriate records of the data subjects consent.

Guidance Link: Consent

Q2. Are you satisfied you're maintaining appropriate records of data subjects' consent?

N/A - no processing based on data subjects consent

Guidance notes:

- If you identified legitimate interests as your lawful basis for processing in section 1.4 you ***should*** complete a Legitimate Interests Assessment (LIA). A template LIA is available here.

Guidance Link: How do we apply legitimate interests in practice?

Q3. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

Yes

If applicable, please provide a link to your completed assessment.

https://indigoffice.sharepoint.com/:w:/s/TGrp_CorporateCommunications_CorporateAffairsandGovernance/EcbT43_aYGJPtmjVQza7gxYBA1V5zI0qoq9aQqHEeTJ_Dg?e=b8NnRI

3.2 Accuracy

Guidance notes:

- All reasonable steps should be taken to ensure personal data is kept accurate and up to date. Steps ***must*** be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

Q4. Are you satisfied the personal data you're processing is accurate?

Yes

Q5. How will you ensure the personal data remains accurate for the duration of your processing?

Polls, quiz answers, etc will be captured during the event and will therefore be an accurate representation of what the participants have answered in real time.

Guests have the choice to cerate their own profile and with therefore input their own data.

3.3 Minimisation, Retention & Deletion

Guidance notes:

- You should only collect and hold the minimum amount of personal data you need to fulfil your purpose. Data should be retained for no longer than is needed for that purpose and then deleted without delay.

Q6. Have you done everything you can to minimise the personal data you're processing?

Yes

Q7. How will you ensure the personal data are deleted at the end of the retention period?

Comms department and the individual users for the account holder Slido will create a process and calendar reminders in the months following an event to ensure proper deleteion of event data. It can be built into our event planning checklist along with other post event activities – like gathering feedback and follow up with attendees.

In the first instance data gathered is minimal, once we have conducted general analytics in terms of number of attendees and level of interaction we no longer need to keep it.

Q8. Will you need to update the ICO retention and disposal schedule?

Yes

3.4 Security: Confidentiality, integrity and availability

Guidance notes:

- Personal data ***must*** be processed in a way that ensures it is appropriately secure and protected from unauthorised access, accidental loss, destruction or damage.
- You ***must*** make sure access to the personal data is limited to the appropriate people and ensure you're confident the processing system being used is secure.

Guidance link: Security

Q9. Where will the personal data be stored and what measures will you put in place to maintain confidentiality, integrity and availability?

According to the Slido privacy policy all data is sorted in the EU – in Ireland and Germany.

We would expect to be notified in advance of any changes.

Slido's Security Appendix outlines their security procedures.

Q10. Have you confirmed there are appropriate access controls to keep the personal data secure?

Yes

Q11. Has the cyber security team completed a security assessment of your plans?

Yes

Q12. If yes what was the outcome of their assessment?

I have completed a SRA and filed with with Info. Sec colleagues. The response was as follows:

Thank you for sending over that Supplier Risk Assessment. I have been through their documentation and mostly everything seems in order so with it being a low-risk supplier we are saying "met with exceptions" with no further action required on their part for the supplier assessment.
From [redacted].

Q13. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

The main user assicoated with the Slido account will be Senior Communications offierce, Suzanne Forshaw. If we are able to purchase the Enterprise package we have an additional two accounts. When we have identified who they are. I will include other users to the training session and create a process document with clear instructions on how to use the platfrom.

3.5 Accountability and governance

Guidance notes:

- The accountability principle makes us responsible for demonstrating our compliance with the UK GDPR. We do this by clearly assigning responsibilities for compliance tasks, and by maintaining relevant records relating to our processing activities and decision making.
- Your Information Asset Owner is the risk owner for any residual risk associated with your data processing and ***must*** sign off this DPIA.

Q14. Is your Information Asset Owner aware of your plans?

Yes

Q15. Will you need to update our article 30 record of processing activities?

Yes

Q16. If you are using a data processor, have you agreed, or will you be agreeing, a written contract with them?

Yes

3.6 Individual Rights

Guidance Note:

- UK GDPR provides a number of rights to data subjects when their personal data is being processed.
- As some rights are not absolute, and only apply in limited circumstances, we may have grounds to refuse a specific request from an individual data subject. But you ***must*** be sure your new service or process can facilitate the exercise of these rights and it should be technically feasible for us to action a request if required.

Guidance Link: Individual rights

Q17. Is there a means of providing the data subjects with access to the personal data being processed?

Yes

Q18. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes

Q19. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes

Q20. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes

Q21. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes

Q22. Can we erase the personal data on receipt of a request from the data subject?

Yes

4. Risk assessment

Guidance Note:

- You ***must*** use the table below to identify and assess risks to individuals. You can add as many rows to the table as you need.
- **Remember:** Our risk appetite towards Information Governance and Organisational Controls and Compliance is **Minimalist** (see our Risk Management Policy and Appetite Statement for more information).
- You ***must*** identify measures to reduce the level of risk where possible.
- In the risk description column, you can select from common risks to individuals in the drop-down list provided. Alternatively, you can enter your own risk descriptions if preferred.
- **The drop-down list is not exhaustive**, and you must identify and assess risks within the context of your planned processing.
- Mitigation measures can be existing, i.e. they're already in place and reduce the risk without any further action being needed. Or they're expected i.e. these are additional measures you intend to take before the data processing begins in order to further reduce risk.
- Use the risk scoring criteria in Appendix 1 to score your risks. You ***must*** score both the impact (I) and probability (P). The expected risk score total is the result of I multiplied by P.
- When considering probability, you should score based on all your mitigation measures having been implemented in order to get an *expected* risk score.

Risk description	Response to Risk	Risk Mitigation	Expected Risk Score		
			Impact	Probability	Total
Example: *Access controls are not implemented correctly, and*	Choose an item.	*Existing mitigation: We have checked that the system we intend to procure allows us*	3	1	3 - low

personal data is accessible to an unauthorised party.			*to set access permissions for different users.* *Expected mitigation: We will appoint and train a system administrator who will be responsible for implementing access controls and monitoring access. The system administrator will also audit the system periodically to review access permissions.*			
1.	**Access controls are not implemented correctly and personal data is accessible to an unauthorised third party**	Treat: this risk is being reduced by management action such as implementing controls or tackling the cause	Existing mitigation: Slido maintains a formal access control policy and employs a centralized access management system to control Slido staff access to Customer Data and to support the secure creation, amendment and deletion of user accounts. Slido regularly reviews the access rights to ensure that all user accounts and user accounts privileges are allocated on a need-to-know basis. Upon a change in scope of employment or	**3**	**1**	**3 - low**

			termination of employment, access rights are removed or modified asappropriate. Access to highly sensitive systems such as data centres is controlled by secure log-on procedures including MFA or VPN technology. Expected mitigation: ICO staff will receive training with regards how to set up and manage the slido pages for each specific event. Each event page will be created with a unique password and link to join - they will only be sent to people who are registered to attend the event. There will be an annual review of account holders to identify and remove any leavers. Some events may also be protected by a pin code that delegtes will require in order access the event space.			

2.	**Personal data is retained for longer than is necessary by us**	Treat: this risk is being reduced by management action such as implementing controls or tackling the cause	Existing mitigation: Expected mitigation: Comms will set calendar reminders in line with the event dates to ensure that anything held on the account is deleted appropriately after 3 months .	**2**	**2**	**4- low**
3.	**Security controls are inadequate for protecting personal data resulting in a loss of confidentiality, integrity or availability.**	Treat: this risk is being reduced by management action such as implementing controls or tackling the cause	Existing mitigation: Slido platform has been assesed by collegues in Cyber security and it was identified as low risk. Expected mitigation: Each event page will be created with a unique password and link to join - they will only be sent to people who are registered to attend the event.	**3**	**2**	**6 - medium**
4.	**Our processing of personal data isn't transparent to the data subjects**	Treat: this risk is being reduced by management action such as implementing	Existing mitigation: Expected mitigation: The privacy notices will be updated to mention what	**1**	**1**	**1 - low**

		controls or tackling the cause	personal data is being processed and why. This privacy notice will be linked to before each event.			
5.	**Excessive personal data is communicated by participants during an event and then retained afterwards by the ICO**	Terminate: this risk will be avoided by doing something else, changing the service, or withdrawing from the activity	Existing mitigation: Expected mitigation: Our intention is to use the moderation feature on Slido so that any submission in the Q&A containing personal data are not published in the public forum, and any such information can be deleted immediately after the event.	**2**	**1**	**2 - low**
4.	**Data is transferred overseas to a country without equivalent data protection laws**	Treat: this risk is being reduced by management action such as implementing controls or tackling the cause	Existing mitigation: Slido have appropriate transfer mechanisms in place. See Privacy Data Sheet for details.	**2**	**1**	**3 - low**

5. Consult the DPO

Guidance Note:

- Once you have completed all of the sections above you ***must*** submit your DPIA for consideration by the DPIA Forum who will provide you with recommendations on behalf of our Data Protection Officer (DPO). The process to follow is here.
- Any recommendations from the DPOs team will be recorded below and your DPIA will then be returned to you. You ***must*** then record your response to each recommendation, and then proceed with completing the rest of this template.

	Recommendation	Date and project stage	Project Team Response
1.	**There was uncertainly in the Forum about whether 1 month would be long enough to retain the event data and perform all necessary analysis. If not then this could potentially lead to us retaining data for longer than is required. The recommendation would be to change the retention period to 3 months.**		**Accept** If rejecting explain why:
2.	**For 'other organiser data' and 'purchase data' listed in 1.3. Slido have said in their Privacy Data Sheet that the ICO and Slido are both controllers of this information. It is not clear why this is the case. Please can you**		**Accept** If rejecting explain why:

	obtain clarification from Slido on what data this is and why the ICO and Slido are both considered controllers?		
3.	**In section 1.5 you have said:** **'Each Slido event has a unique event code (and QR code, URL link), so for a person to join an event, they need to know these in advance – this mean we can target specific group and people are registered to attend an event since we already have their data.** **Slido events can be protected by an additional passcode or unique login pin code.'** **Please could you provide more detail on if/when you will use the additional passcode or pin code? Will this be used in all events, certain events or not at all? If you are using the additional passcode then this should be added as a mitigation to Risk 1 as this will reduce the risk of unauthorised access.**		**Accept** If rejecting explain why:
4.	**In Slido's Security Standards it says 'Slido provides Customer Data export capabilities. Organisers are able to export**		**I am not sure yet if we will need to expoert the data – since I am unfamiliar with the tools for reviewing the data withinthe slido platfrom. I have added a line about this in Section 2.**

	questions as well as polls with complete results via Admin interface.' **Will you be exporting the data from Slido? If so you will need to update the DPIA to mention where this will be stored and how long you are going to retain the export for.**		
5.	**In section 4 please add an additional risk of data being transferred overseas without adequate protection (you can find this option in the drop down menu).** **The reason for this is that, whilst Slido are storing data in the EU only, they have said in their Privacy Data Sheet that they will be transferring data overseas.** **In the mitigations section of this risk, you can say that Slido have appropriate transfer mechanisms in place and link to the above Privacy Data Sheet for further information.**		**Added this in the correct section.**

6. Integrate the DPIA outcomes back into your plans

Guidance Note:

- Completing sections 1 to 5 of your DPIA will have helped you identify a number of key actions that you now ***must*** take to meet UK GDPR requirements and minimise risks to your data subjects. For example, you may now need to draft a privacy notice for your data subjects; or you could have risk mitigations that you need to go and implement.
- You ***should*** also consider whether any additional actions are required as a result of any recommendations you received from the DPOs team.
- Use the table below to list the actions you need to take and track your progress with implementation. Most actions will typically need to be completed ***before*** you can start your processing.

Action	Date for completion	Responsibility for Action	Completed Date
To consult with legal services with regards the contractual terms and conditions.	01 August 2023	Suzanne Forshaw	Ongoing
To raise a New Supplier request form with procurement	01 August 2023	Suzanne Forshaw	Ongoing
To include any other likely users to the training session and create a process document with clear instructions on how to use the platfrom.	01 August 2023	Suzanne Forshaw	Cannot do this until we have sign off .

Create calendar reminders for manual deletions and review of organiser accounts	01 August 2023	Suzanne Forshaw	Will complete once we have a go live date.
An update is required to our existing privacy notice/s. This required action has been added to the DPIA outcomes (see section 6.0).	01 August 2023	Suzanne Forshaw/[redacted]	17/07/2023
Update retention schedule	01 August 2023	[redacted]	13/07/2023
Update the ROPA	01 August 2023	[redacted]	13/07/2023

7. Expected residual risk and sign off by the IAO

Guidance note:

- Summarise the expected residual risk below for the benefit of your IAO. This is any remaining risk ***after*** you implement all of your mitigation measures and complete all actions. It is never possible to remove all risk so this section shouldn't be omitted or blank.
- If the expected residual risk remains high (i.e. red on the traffic light scoring in the Appendix) then you ***must*** consult the ICO as the regulator by following the process used by external organisations.

I understand the risk of using Slido as an interactive tool on our events platforms to be low. I will ensure that all mitagations are in place and managed correctly for each individual event.

We may not be required to use Slido for each event however I plan to keep a tracking document to show how many particpants are actively engaged via the platfrom so we can accurately measure the success and impact of this interactive tool on our live events.

7.1 IAO sign off

Guidance Note:

- Your IAO owns the risks associated with your processing and they have final sign off on your plans. You ***must*** get your IAO to review the expected residual risk and confirm their acceptance of this risk before you proceed.
- Once your DPIA has been signed off it is complete. You should review it periodically or when there are any changes to your data processing.

IAO (name and role)	**Date of sign off**
Angela Balakrishnan, Exec Director for Communications and Public Affairs	20/7/2023

8. DPIA change history

Guidance note:

- You should track all significant changes to your DPIA by updating the table below.

Version	Date	Author	Change description

V0.1			First Draft
V0.2	06/07/2023	[redacted]	Forum met, recommendations added to section 5
V0.3	17/07/2023	[redacted]	All actions assigned to IM team completed

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability

Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (e.g. does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.

Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.

High (Red)	Within this range risks shall not be accepted, and immediate action is required to reduce, avoid or transfer the risk.

6.0 Template document control and change history (for Information Management Service use only)

Document Name	Data Protection Impact Assessment - template
Author/Owner (name and job title)	Steven Johnston, Team Manager Information Management and Compliance Service
Department/Team	Information Management and Compliance Service
Document Status (draft, published or superseded)	Published
Version Number	V3.0
Release Date	07/10/2020
Approver (if applicable)	N/A
Review Date	31/01/2024
Distribution (internal or external)	Internal

Version	Date	Author	Change description
v0.1	01/06/2020	Steven Johnston	First draft
v1.0	07/10/2020	Steven Johnston	First release
v1.1	07/01/2021	Iman Elmehdawy	Amendment to guidance note page 2.
v1.2	18/03/2021	Helen Ward	Addition of Privacy by design at the ICO (pages 2 and 3)
v1.3	24/06/2021	Steven Johnston	Section 3.0 Q13 amended. Removed request for link to security assessment.
v2.0	07/03/2022	Steven Johnston	Full document review. Simplified privacy by design explanation on page 3 and made minor format changes throughout. Guidance note for 2.0 was updated and flow headings inserted to the text box. Next review date set to 31/1/2023.
v2.1	11/05/2022	[redacted]	Amended title of section 2 from 'data flows' to 'personal data lifecycle'
v2.2	26/10/2022	Steven Johnston	Guidance notes updated throughout following feedback from Project Management Office.

V3.0	16/01/2022	Steven Johnston	Annual review. Inclusion of further guidance notes to reflect feedback received from colleagues. Introduction of drop-down lists in sections 1.3, 1.4,, 3.0 and 4.0. Addition of Q2 and Q14 in section 3.0. Removal of Appendix 2.