Data Protection Impact Assessment (DPIA)
IG Form

A DPIA:-

a. Is a process that assists organisations in identifying and minimising the data protection/privacy risks of new projects or policies.

b. Involves working with internal and external stakeholders to identify and reduce privacy risks.

c. Will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

d. Benefits organisations by producing better policies and systems and improving the relationship between organisations and individuals.

e. Is an integral part of taking a privacy by design approach

When completing this form please refer to the Guidance at the end of this document.

Name of information asset/ processing.	Data Processors:- • Use of new CRM provider; and • Two new mechanisms by which financial donations/payments to Young Epilepsy will be managed.

1. Identify the need for a DPIA

Please explain in the box below:-

- ✓ What processing will be undertaken
- ✓ What the project aims to achieve and its purpose
- ✓ The necessity and proportionality of the processing in relation to its purpose
- ✓ The benefits of the project (to the organisation, individuals and others)

✓ Why the need for a DPIA was identified You may at this stage wish to add relevant documents, such as a project proposal

Processing:-	Donor/Supporter contact details etc.
Aims:-	To improve fundraising donations and supporter engagement
Necessity: -	Only the minimum amount of information necessary is being kept, used etc. (please refer to IG Compliance Analysis).
Benefits:-	Organisation – income improvement Donors/Supporters – consistency and relevance of communications
Need for DPIA:-	Use of new data processors

2. Describe the information flows

Please describe in the box below:-

- ✓ The information flows:-
  - ~ What information is used
  - ~ What it is used for
  - ~ Who it has been obtained from
  - ~ Who it will be disclosed to
  - ~ Who will have access to it
- ✓ The collection, use and deletion of personal data
- ✓ How many people are likely to be affected by the project

You may at this stage wish to refer to a flow diagram or other way of explaining data flows

Information used:- Used for:-	Names, contact details, history of contact, donation & engagement history. Also relationship to epilepsy (if provided) Tto optimise supporter/donor engagement with Young Epilepsy and record engagement with donors/supporters

	To record contact details and a record of engagement and/or donations with supporters/donors, with a view to developing relationships via email and other communication channels.
Obtained from:-	Directly from donors/supporters
Disclosed to:-	Data Processors
Access:-	Young Epilepsy staff and Data Processors
Collection etc.:-	Data will be collected, used and deleted in accordance with Young Epilepsy policy
Individuals:-	Approx. 15k supporters/donors

3. Identify the privacy and related risks

In the table below please identify the key privacy risks and the associated compliance and corporate risks (add extra rows as needed). Larger-scale PIAs might record this information on a more formal risk register.

Some will be risks to individuals – for example damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy.

Some risks will be to the organisation - for example damage to reputation, or the financial costs or a data breach.

Legal compliance risks include the DPA, PECR, and the Human Rights Act.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Inadequate disclosure controls	Information being shared inappropriately	Sanctions, fines and reputational damage. Loss of supporters	Non-compliance with the GDPR, DPA 2018 and Privacy & Electronic Communications Regulations (PECR).
Information being used for different purposes without people's knowledge (if the context in which information is	Information being used without consent or inappropriately	Sanctions, fines and reputational damage. Loss of supporters	Non-compliance with the GDPR, DPA 2018 and PECR.

used or disclosed changes over time).			
Security risks Inappropriate security measures used to protect the data.	Unauthorised disclosure of personal data	Sanctions, fines and reputational damage. Loss of supporters	Non-compliance with the GDPR, DPA 2018 and PECR.
Security risks If information is collected and stored unnecessarily, or is not properly managed so that duplicate records are created.	Unauthorised disclosure of personal data	Sanctions, fines and reputational damage. Loss of supporters	Non-compliance with the GDPR, DPA 2018 and PECR.
Login Access Control	Unauthorised exposure of personal data	Sanctions, fines and reputational damage. Loss of supporters	Non-compliance with the GDPR, DPA 2018 and PECR.

4. Identify privacy solutions

In the box below explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy.

Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective.

Result - is the risk eliminated, reduced, or accepted?

Evaluation - is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Risk	Solution	Result	Evaluation
Inadequate disclosure controls	By Data Processors Fundraising & Comms project leads:-	Risk reduced to acceptable level	Impact on individuals justifiable

	• Undertake due diligence by to ensure adequate disclosure controls • Ensure adequate disclosure controls are a contractual requirement <u>By Young Epilepsy staff</u> • Forms part of policies, procedures, staff training, departmental induction and line management (standard part of staff appraisal).		
Information being used for different purposes without people's knowledge (if the context in which information is used or disclosed changes over time).	<u>By Data Processors</u> Fundraising & Comms project leads:- • Undertake due diligence by to ensure suitable controls are in place to ensure this does not happen • Ensure this is a contractual requirement <u>By Young Epilepsy staff</u> • Forms part of policies, procedures, staff training, departmental induction and line management (standard part of staff appraisal).	Risk reduced to acceptable level	Impact on individuals justifiable
Security risks Inappropriate security measures used to protect the data.	<u>By Data Processors</u> Fundraising & Comms project leads:- • Undertake due diligence by to ensure appropriate security measures are used. • Ensure this is a contractual requirement <u>By Young Epilepsy staff</u>	Risk reduced to acceptable level	Impact on individuals justifiable

	• Forms part of policies, procedures, staff training, departmental induction and line management (standard part of staff appraisal).		
Security risks If information is collected and stored unnecessarily, or is not properly managed so that duplicate records are created.	<u>By Data Processors</u> Fundraising & Comms project leads:- • Undertake due diligence by to ensure appropriate collection and storage measures are used. • Ensure this is a contractual requirement <u>By Young Epilepsy staff</u> • Forms part of policies, procedures, staff training, departmental induction and line management (standard part of staff appraisal).	Risk reduced to acceptable level	Impact on individuals justifiable
Use of data processor	<u>Fundraising & Comms project leads</u>:- • Select data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf • Undertake due diligence to ensure GDPR, DPA 2018 and PECR standards are applied by Data Processors. • Ensure this is a contractual requirement • Ensure contract includes the minimum contractual terms for a data processor, as recommended by the ICO	Risk reduced to acceptable level	Impact on individuals justifiable
Login Access Controls	<u>By Data Processors</u>		

	• Set Session times and Authentication requirements to agreed levels • Ensure log out if unattended <u>Fundraising & Comms project leads</u> • Ensure Password Paradigm is understood • Make two factor authentication devices are available <u>By Young Epilepsy staff</u> • Ensure log in security when working away from campus • Comply with password policy		

5. Sign off and record the DPIA outcomes

Make sure that the privacy risks have been signed-off by a member of the Exec team. This can be done as part of the wider project approval.

A PIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.

Publishing a PIA report will improve transparency and accountability, and lets individuals learn more about how your project affects them.

Risk	Approved solution	Approved by who?
Inadequate disclosure controls	See above	✓ Data Protection Officer ✓ IT Lead ✓ Fundraising & Comms project leads
Information being used for different purposes without people's knowledge (if the	See above	

context in which information is used or disclosed changes over time).		✓ Director of Fundraising & External Engagement
Security risks Inappropriate security measures used to protect the data.	See above	
Security risks If information is collected and stored unnecessarily, or is not properly managed so that duplicate records are created.	See above	
Use of data processor	See above	
Login Access Control	See above	

6. Integrate the PIA outcomes into the project plan

In the box below please identify who is

- ✓ Responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork
- ✓ Responsible for implementing the solutions that have been approved
- ✓ The contact for any privacy concerns that may arise in the future
- ✓ Responsible for monitoring that these actions are undertaken

It may be necessary to return to the PIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.

Action to be taken	Date for completion of actions	Responsibility for the actions
Due diligence on the data processors	Completed 21/12/19 prior to use of data processor.	✓ Fundraising & External Engagement project leads
Contractual terms to include use of :- • Adequate disclosure controls	Completed 21/12/19 prior to use of data processor.	✓ Fundraising & External Engagement project leads

• Requirement that information will only be used for Young Epilepsy's specified purposes • Appropriate security measures • Appropriate collection and storage measures • GDPR, DPA 2018 and PECR standards • Minimum contractual terms for a data processor, as recommended by the ICO		
Establish policies, procedures, staff training, departmental inductions and line management processes (to become standard part of staff appraisal).	Completed 21/12/19 prior to use of data processor.	✓ Fundraising & External Engagement project leads
Name of contact for future DPIA concerns (please detail below)		
Director of Fundraising & External Engagement		