GDPR for Charities

How to conduct a DPIA

Shamal Faily

Small charities face bankruptcy for not complying with GDPR, but put clients at risk if they do

May 21, 2018 11.53am BST

The way charities use and hold data on behalf of their clients and donors creates problems under GDPR. Tashatuvango/Shutterstock

You will no doubt have received the emails yourself: don't forget to opt in, click here to stay in touch, we don't want to lose you. The General Data Protection Regulation, or GDPR, comes into force on May 25, and organisations and businesses large and small are racing to ensure the way they collect, store and use the personal data of their customers and clients meets the new, higher standards of this new European Union privacy law.

Compliance with GDPR can be costly, requiring organisations to analyse the way they work, the data they use, how it is handled and secured. Documenting how personal data is held and processed is tedious and time consuming, as is developing procedures for dealing with

Author

Shamal Faily
Senior Lecturer in Systems Security Engineering, Bournemouth University

Disclosure statement

Shamal Faily does not work for, consult, own shares in or receive funding from any company or organisation that would benefit from this article, and has disclosed no relevant affiliations beyond their academic appointment.

Partners

Bournemouth University

Bournemouth University provides funding as a member of The Conversation UK.

The Conversation UK receives funding from Hefce, Hefcw, SAGE, SFC, RCUK, The Nuffield Foundation, The Ogden Trust, The Royal Society, The Wellcome Trust, Esmée Fairbairn Foundation and The Alliance for Useful Evidence, as well as sixty five university members.

View the full list

Photo by rawpixel on Unsplash

Data protection impact assessments

Click here for information about consulting the ICO about your data protection impact assessment.

At a glance

- A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.
- You must do a DPIA for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing. You can use our screening checklists to help you decide when to do a DPIA.
- It is also good practice to do a DPIA for any other major project which requires the processing of personal data.
- Your DPIA must:
  - describe the nature, scope, context and purposes of the processing;
  - assess necessity, proportionality and compliance measures;
  - identify and assess risks to individuals; and
  - identify any additional measures to mitigate those risks.
- To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- You should consult your data protection officer (if you have one) and, where appropriate, individuals and relevant experts. Any processors may also need to assist you.
- If you identify a high risk that you cannot mitigate, you must consult the ICO before starting the processing.
- The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, we may issue a formal warning not to process the data, or ban the processing altogether.

Checklists

DPIA awareness checklist

□ We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.

□ Our existing policies, processes and procedures include references to DPIA requirements.

Agenda

0930	Basics of GDPR & Overview of DPIA Data Wheel
1000	DPIA Data Wheel: worked example
1030	Practical session [with coffee break]
1200	Review of DPIA results
1230	Lunch
1330	StreetScene perspective of DPIA Data Wheel
1345	Finding Security & Privacy Risks
1430	Panel: How GDPR affects charities and what this means in practice
1530	Coffee
1600	Next steps