/Data Protection Impact Assessment (DPIA) Template

DMA
Data & Marketing Association

Why are Data Protection Impact Assessments (DPIA's) important?

A DPIA ensures you are taking a privacy-first approach to your direct marketing activities. It allows you to systematically identify and mitigate any risks to the rights and freedoms of those whose personal data is being processed for this purpose.

A DPIA gives you a great opportunity to demonstrate your commitment to the principles of UK General Data Protection Regulation (UK GDPR) and is key to your accountability.

When do I need to complete a DPIA?

A DPIA is only required when the activity involves the processing of personal data. The UK GDPR says that you **must** (by law) complete a DPIA **before** undertaking any activity that is likely to result in a "high risk" to individuals.

There are 3 types of high-risk activities that **automatically** require a DPIA under UK GDPR:

1. Extensive profiling with significant effects

What constitutes a "significant effect" isn't defined in the UK GDPR, but one example includes being automatically refused credit by a bank.

2. Large Scale use of sensitive (i.e. special category) data

The UK GDPR doesn't provide a specific definition of what constitutes "large scale;" however, the ICO has provided some guidance on what you'll need to consider when determining if you're meeting the "large scale" threshold, including:

1. the number of data subjects involved in the processing
2. the volume and variety of the data
3. how long you'll be processing the data
4. the geographical extent of the processing
5. Public monitoring.

3. High-risk activities

UK GDPR also requires the ICO to publish a list of activities that are likely to be considered high-risk to individuals and therefore likely to require a DPIA. Of this list, the high-risk activities that are most likely to apply in a direct marketing context are:

1. Innovative technology – including Artificial Intelligence*
2. Large scale profiling
3. Data Matching
4. Invisible processing
5. Tracking
6. Targeting children or vulnerable adults

Below is an example of a direct marketing activity that is likely to result in high risk to individuals and why it would require DPIA:

Activity	Potential "High-risk" criteria as per UK GDPR	Why is this considered "high-risk?"
Gathering of public social media data for generating profiles	• Innovative technology • Large scale profiling • Data Matching • Invisible processing • Large scale use of sensitive data	Likely to exceed reasonable expectations of individuals Individuals unaware of the processing, impacting their ability to exercise their rights and control over how their personal data is used
Adtech (e.g., Real Time Bidding)	• Invisible processing • Tracking • Data matching • Large scale profiling • Large scale used of sensitive data • Innovative technologies	

For more information about activities that require a DPIA, please consult the ICO Guidance.

While the above provides clarity on when you're required by law to complete a DPIA, it's also important to bear in mind it's good practice to complete a DPIA before undertaking any direct marketing activity that involves processing personal data.

Artificial Intelligence and DPIA's

In most cases, using AI to process personal data will meet the "high-risk" criteria above and will therefore trigger the requirement to conduct a DPIA.
AI poses unique challenges and risks to both organisations and individuals. This means there are data protection and privacy considerations, specific to AI, that must be factored into a DPIA, such as (but not limited to):

- Harms to individuals, including resulting from bias
- Transparency and explainability of AI.
- Human oversight and involvement.

Further information on how to complete a DPIA for AI can be found in the ICO's guidance.

What are the DPIA basics we need to have in place?

Organisations must clearly understand the circumstances under which a DPIA must be completed and understand the importance of factoring in the process early in the planning stage of a campaign. This should be reflected in all your relevant policies, processes and procedures.

You should also have a well-established DPIA approval process in place and staff should be trained in how to complete one.

The following direct marketing-specific DPIA template from the DMA is designed to help you ensure that you're covering all the necessary bases.

If you have any questions or would like support with this DPIA, please contact legaladvice@dma.org.uk.

Author's note: Template contents in black text *are the explanatory notes designed to support you to complete each section in your own words.*

You can find the DPIA template on the next page.

Campaign/Product Name:	Date:
Name & Job Title of the respondent:	

1. Overview and Purpose of the activity

Here, you need to outline the details of the direct marketing activity you're wanting to undertake, the purpose of processing, and why it requires a DPIA (i.e., how does it meet the "high-risk" processing criteria?).

It would be helpful to also provide information about the strategic objectives you believe the direct marketing activity will help your organisation to fulfil and provide links to more detailed proposals/plans where appropriate.

This will give you the opportunity to demonstrate that the data processing activities you want to undertake are necessary from an organisational strategy point of view.

2. What is the nature, scope and context of the data you want to process?

In each answer below you will demonstrate how the personal data to be processed will be necessary and proportionate to the purpose identified above.

2.1. What personal data will you be processing as part of this activity?

(delete as appropriate)

E.g.,
Full name
Date of Birth
Gender
Postal Address
Email Address
Telephone Number
Online Identifiers (e.g. IP address, Cookie ID, Device ID, social media handle, customer login details)

2.2. Will you be processing any "special category" data as part of this activity?

If YES select the categories of special category data that will be processed below:

Race or ethnic origin
Political opinions
Religious or Philosophical beliefs
Trade Union membership
Genetic and biometric data
Health status
Sex life or sexual orientation

When collecting and processing special category data you **must** have a lawful basis under Article 6 **and** a condition under Article 9 of UK GDPR. Consent under Article 6 and Explicit Consent under Article 9 are most likely appropriate in a direct marketing context. Please see the ICO guidance for further details.

This type of personal data is particularly sensitive and therefore warrants greater protections under data protection law. In section 4 and 5 below, you need to identify the risks is processing this special category data and how mitigate these.

If No, please move to Question 2.3.

2.3. What's the scope of the data processing activities you're planning to undertake?

Here, you need to outline:

a)The amount of data you'll be collecting and processing e.g. the approximate number of individuals involved or impacted by the activity
b)Whether the activity will involve profiling or AI of any kind and what, if any, the subsequent impact will be on data subjects
c) How long you're planning to use the data and how long you'll be keeping it
d) What geographical area the activity covers, if known

It will be helpful for you to outline/include/link to a data mapping exercise for the activity in question. This is a a graphical depiction (like a flow chart) of the end-to-end journey of personal data, from collection to deletion. This will help you identify at what stage risks may arise, as per Section 4.

2.4 What's the context of the data processing activities you're planning to undertake?

Here, you need to outline:

a)Whether the activity will involve processing the data of people who are new to your organisation or your existing customer base. Explain the nature of your relationship with these individuals

b)Does the processing involve or affect children and vulnerable groups

c) the GDPR legal basis you're planning to rely on for the direct marketing activity. The two most relied on for direct marketing purposes are Consent and Legitimate Interests.

If you're relying on Consent, you should signpost the consent statement in the DPIA that you're either a) planning to serve to data subjects or b) the consent statement that would have been served to your existing customer base when first collected their details.

If you're relying on Legitimate Interests, you must indicate whether you've completed a Legitimate Interests Assessment and provide a link to the in the DPIA. You can find our LIA template here.

d) the level of control that data subjects will have over the data you're processing. Can they exercise their rights, for example to object? What are them/what have you told them about how you'll use their information?

e) whether the activity is new or novel in any way

f) whether there are any general concerns from consumers about what you're planning to do.

3. Will data be shared with and processed by any third parties?

If "Yes," you must specifically name any third parties involved in the direct marketing activity along with details of:

a)The nature of the relationship with each third party e.g joint/independent data controller, data processor etc
b)How data will be transferred
c)Agreed retention periods
d)Measures you'll take to make sure your data processors are GDPR-compliant
e)How any information rights from data subjects will be managed
f)Confirmation of the written agreement you have in place with the third party e.g. a Data Processing Agreement or a Data Sharing Agreement

If "No," go to Question 4.

4. Risks

Here, you need to outline the data protection-related risks you've identified with the direct marketing activity. RAG rate each risk based on the a) the likelihood of harm happening to individuals and b) the potential severity of that harm.

Risk	Likelihood of Harm to individuals	Severity of Harm to individuals	Overall RAG Rating
Outline the risk (e.g. is it at the point of data collection, profiling, online tracking?) and the nature of that risk (e.g. is it compliance, reputational or individual impact?) Are there any AI-specific risks? (See supporting information below). Number each risk so you can easily reference each of them in the next section.	Remote, Possible or Probable (delete as appropriate)	Minimal, Significant or Severe (delete as appropriate)	Red, Amber, Green (colour code for ease of reference).

5. Mitigations

Outline what measures you plan to take to reduce the risks you've identified under Section 4.

Risk	What will you do to reduce the risk?	Overall effect on Risk once mitigations have been put in place	Revised RAG rating	Mitigation Approved?
#1:(list appropriate) #2 #3	This includes technical and organisational measures in place to protect the security of personal data	Eliminated, Reduced or Accepted (delete as appropriate)	Red, Amber, Green (colour code and delete as appropriate)	Yes/No (delete as appropriate)

6. Approvals and sign offs

Here, you need to clearly record whether the DPIA has been approved; you'll need to outline what residual risks have been approved and who's approved them and whether you've sought external advice as part of the DPIA process.

Actions	Yes/No/N/A	Approved by/Date Approved	Notes
DPIA Approved			Take any outstanding actions and incorporate them back into your project plan.

Remaining Risks Approved			If there are any remaining high risks being accepted, speak to the ICO before proceeding.

Summary of external advice if applicable: Here, you should outline what advice you've received from any external sources you've consulted as part of completing the DPIA e.g. a Data Protection Officer, the ICO or the DMA.

External advice accepted or rejected by:	

Rationale for rejecting external advice, if applicable: Here, you should summarise the reasons why it's been decided to reject advice provided by an external source. You'll need to demonstrate how your approach is still compliant despite it differing from the advice provided.

This DPIA will be kept under review by:	

Appendices

Supporting information

a. As members of the DMA, you must conduct your direct marketing activities in accordance with the DMA Code: https://dma.org.uk/the-dma-code

b. Further information can be found on the ICO website:

Direct Marketing Guidance and resources: https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/

DPIAs detailed guidance: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/

AI Risk toolkit: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/