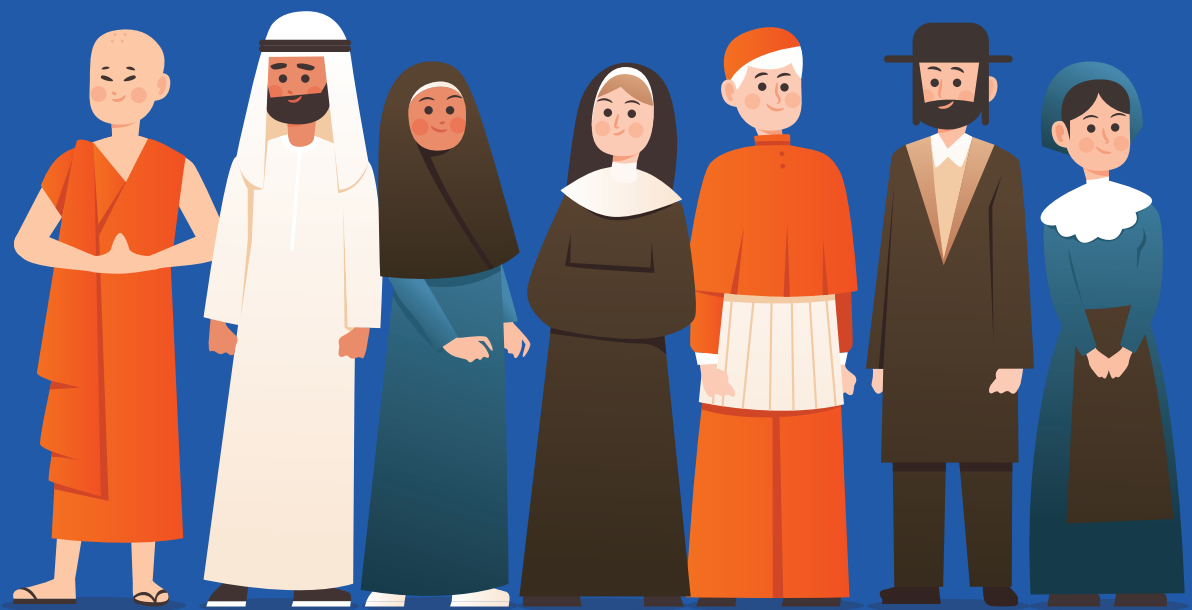


Places of Worship Re-Opening Guidance



kazient

PRIVACY EXPERTS

www.kazient.co.uk

On 9 July 2020, the government updated its guidance for the safe use of places of worship during the pandemic. It is important that places of worship follow the guidelines to avoid any enforcement action and negative publicity when re-opening.

One significant aspect of the guidance includes collecting personal details for the NHS Test and Trace Service.

“Any place of worship that collects personal data must ensure they are processing personal data in a way that is compliant with the General Data Protection Regulation (GDPR).”

Key Points

For consent to be valid it needs to be freely given, specific, informed and unambiguous.

The consent should be communicated by a clear affirmative action.

You must meet the additional conditions for consent such as keeping a clear record and make sure it can be withdrawn easily at any time.

For more information & Support

For further information and assistance about collecting and processing personal data compliantly for your place of worship contact **The Amanah Project by Kazient Privacy Experts:**

hello@kazient.co.uk [0330 022 9009](tel:03300229009)

What is the NHS Test and Trace service?

The government has launched an NHS Test and Trace service to manage the risk of the virus re-emerging.

The service:

- Provides testing for anyone who has symptoms of coronavirus to find out if they have the virus
- Gets in touch with anyone who has had a positive test result to help them share information about any close recent contacts they've had

- Alerts those contacts, where necessary and notifies them when they need to self-isolate to help stop the spread of the virus

In line with other government guidance for other venues including in the retail and hospitality sector, you should assist this service by keeping an **accurate temporary record of visitors for 21 days**. This should be done in a way that is manageable for your place of worship, and assist NHS Test and Trace with requests for that data if needed for

contact tracing and the investigation of local outbreaks.

“When collecting the names and contact details of people attending your place of worship, you should ask for their consent. This is because of the potentially sensitive nature of the data collected in these circumstances, which is protected by law.”

You should make clear that giving contact details is optional and is not a condition of attending your place of worship.

Obtaining Valid Consent

Did you know that for you to be able to rely on consent as your lawful basis for processing personal data the consent you obtain must be valid?

The GDPR has strict requirements that must be met for any consent you obtain to be valid. Consent means giving people genuine choice and control over how you use their personal data.

Here are some key elements you must get right for any consent you obtain to be valid:

1. The consent must be freely given

If the individual has no real choice, consent isn't freely given and it will be invalid.

This means people must be able to refuse consent without detriment and must be able to withdraw consent easily at any time. It also means consent should be unbundled from other terms and conditions wherever possible.

For example:

If a mosque requires visitors to consent to their details being collected prior to being allowed entry, the mosque is making consent a condition of the visit. But collecting the data isn't necessary for access, so consent in this case isn't freely given and would not be valid.

The mosque could ask visitors to consent to collecting their personal data which may be shared with the NHS Test and Trace service, but it must allow them a free choice to opt-in or out.

The consent must be freely given without any detriment to the individual if they choose not to give consent.

2. The consent must be specific

You must clearly explain to people what they are consenting to in a way they can easily understand.

The request for consent needs to be prominent, concise, separate from other terms and conditions, and in plain language.

If the request for consent is vague, sweeping or difficult to understand, then it will be invalid. In particular, language likely to confuse – for example, the use of double negatives or inconsistent language – will invalidate consent.

3. The consent should be informed

This means you need to identify your organisation, and also name any third parties who will be relying on the consent.

You must specifically cover all processing activities. A consent request must specifically cover all purposes for which you seek consent

Separate consent will be needed for different processing operations – so you need to give granular options to consent separately to separate purposes. For example; If you want to use that personal data to send fundraising messages (unless this would be unduly disruptive or confusing).

You should include details of how to withdraw consent too. It must be as easy to withdraw consent as it was to give in the first place.

4. The consent must be indicated by a clear affirmative action

This requires more than just a confirmation that they've read terms and conditions – there must be a clear signal that they agree. If there is any room for doubt, the consent won't be valid.

A clear affirmative action means someone must take deliberate and specific action to opt-in or agree to the processing such as an opt-in box.

For example, other affirmative opt-in methods might include signing a consent statement or oral confirmation.

The key point is that all consent must be opt-in consent, – a positive action or indication – there's no such thing as 'opt-out consent'. So no pre-ticked boxes!

Failure to opt-out isn't consent as it doesn't involve a clear affirmative act. You can't rely on silence, inactivity, default settings, pre-ticked boxes or your general terms and conditions.

It must be clear that the individual deliberately and actively chose to consent.

The GDPR also sets out further 'conditions' for consent, with specific provisions on keeping records to demonstrate consent – you need to record when the consent was obtained and how it was obtained.

Further guidance on collecting visitor details for Test and Trace, including issues around consent, is provided by the Information Commissioner's Office.

The personal data collected through this scheme can only be used for the NHS Test and Trace service. For guidance on how to use the database for other purposes (e.g. sending marketing information) in compliance with GDPR, contact The Amanah Project by Kazient Privacy Experts.

Checklist

- We have a clear and accessible Privacy Notice
- Our staff and volunteers have received GDPR training
- We have an appropriate process for safe collection, storage and deletion of personal data
- The consent we obtain satisfies all the conditions to be valid

If you require any help with the above [please contact us](#).



 **kazient**
PRIVACY EXPERTS



Kazient Limited is incorporated and registered in England and Wales under registered number 09324798. Registered office: The Minster Building, Great Tower Street, Great Tower Street. This document is intended for guidance only.

www.kazient.co.uk