Abstract from Information Commissioner's website

This section provides advice for organisations and small businesses that are asked by government to collect and retain customer and visitor information, for a limited time period, for the purposes of a COVID-19 contact tracing scheme.

This guidance is designed for those who have limited experience of collecting and retaining personal data for business purposes.

Are we allowed under data protection law to collect personal data from our customers as part of a contact tracing scheme?

Yes. Data protection law does not prevent you from collecting personal data that people provide voluntarily as long as it is lawful, fair and that you tell your customers and visitors what you are doing. We have more information on what we mean by lawful here.

You must still consider the principles of data protection law. That means you must make sure the information you collect is adequate, relevant and limited to what you need. It must be accurate and not used for anything else. You should also keep it secure, so you minimise the risk of accidentally losing or destroying it.

What do we need to tell people when we collect their data for the contact tracing scheme?

You must be clear, open and honest with people about why you are collecting their data, who you will be sharing it with and how long you will keep it. You must not collect and process personal data in a way that is misleading, detrimental or outside of what people would reasonably expect. In this case, the collection of customer data is for a contact tracing scheme (such as NHS Test and Trace in England), so you need to make this clear to people.

Collecting customer contact details may already be standard practice for your organisation, but the purpose of collecting this particular information is wider than managing bookings or similar tasks, and there are greater implications should an outbreak occur. You need to explain this to people.

You must consider appropriate methods of communicating this message (including children and young people). For example, you could provide information over the phone, you could put signs up on site, direct people to further information online, or simply tell them when they arrive.

How do I make sure my collection and sharing of data is lawful?

Firstly, you should check government guidelines for information about whether your business is encouraged to collect customer contact information for these purposes. This may vary between England, Scotland, Wales and Northern Ireland. The guidance should indicate whether it is necessary for your industry to collect customer logs.

If government is asking to collect this data, there are gateways known as lawful bases that allow you to do so under data protection law.

- Legitimate interests. This is likely to be the most applicable lawful basis if you are a private organisation. This basis recognises that collecting the data is likely to be in the interests of the individual, the organisation, and the public health efforts to tackle COVID-19, as long as individuals' rights are protected and data protection principles are followed.
- Public task. This is likely to be the most applicable lawful basis if you are a public authority. It allows you to identify a task, function or power with a clear basis in law – such as your legal responsibilities around public health – which requires you to process this data.
- Consent. Most organisations will not need to rely on consent. But there are some notable exceptions which are covered here. You should not use consent as your lawful basis unless it is truly voluntary to provide personal data.

Should I use consent as my lawful basis?

Most private sector and public authorities should not need to rely on consent. Where you do collect consent, you must give people genuine choice about whether they provide their data. You should not use consent as your lawful basis unless it is truly voluntary to provide personal data.

Consent is recommended when the information you are collecting could reveal something sensitive about the person involved. In law, this is called special category data and it means you need to treat it particularly carefully. It includes health information, racial or ethnic origin, sex life or sexual orientation, political opinions, religious or philosophical beliefs, or trade union membership.

In the context of contact tracing, we recommend using consent if you are logging details in places of worship, for example. You should also use consent if you provide a service to small groups or on a one-to one basis, like tailoring or sports massage. That's because the information you may be asked to share for contact tracing purposes may only apply to one or two people – rather than a roomful – making it more likely that you'd make assumptions about your customer's health.

There are particular rules around consent and, if you need to rely on it, we recommend you follow our guidance. In practice, this might be asking people to fill out a specific consent form, for example.

Under data protection law, it is especially important that consent is freely given, meaning that people should be able to refuse or withdraw their consent without facing negative consequences, such as being denied access to your service.

How much personal data should we collect for a contact tracing scheme?

You should only collect the personal information that is needed to help with contact tracing. Government is likely to have specified the exact information you should collect, and you must not collect any more for this purpose.

The information should be limited to staff, customer and visitor contact details and time and date of arrival and departure, for example.

In England, the government has requested that organisations collect only the lead party member's name, telephone number, and date and time of arrival and departure.

The guidance for Scotland can be found here. The guidance for Wales and Northern Ireland is currently in development and we will update this page as soon as it is published.

How long can we keep personal data collected in accordance with government guidance?

Only for as long as it's needed.

Guidance on how long that will be is provided by the public health authorities in whichever part of the country you live in. In England, for example, it is 21 days. Once that period is up you must dispose of the information securely. That means shredding paper records or permanently deleting digital files, for example.

The only reason you should keep the data for longer, is if you would usually do so in line with other sector specific guidelines.

How do we make sure that the personal data we collect is accurate?

In the context of contact tracing, all you need to do is record the information the customer or visitor provides you in an accurate way. If you believe that the information is wrong or out of date, you can ask the customer or visitor for clarification.

We appreciate that some people may provide false information. However, as long as you accurately record the information provided, you are likely to meet your requirements in terms of accuracy under data protection law.

As the collection of this data is voluntary, identity checks would be disproportionate in the vast majority of circumstances. You should not undertake identity checks, or other more intrusive means of gathering data, unless you would normally do so (such as for age verification at licenced premises).

What data protection rights do people have in relation to the data we collect about them for a contact tracing scheme?

When you hold their personal data, people have rights under data protection law. These rights include:

- the right of access to the personal data you hold on them – for example their contact details, or details of their booking with you;
- the right to ask for any factually inaccurate data to be corrected;
- the right to object to the processing of their data; and
- the right to ask for their data to be erased.

A full list of rights is here. These rights can be exercised verbally or in writing. You need to ensure that you have measures in place, and can recognise any requests for the information to be erased or amended, for example. More information is available in our guidance.

What do we need to do about security?

You are responsible for ensuring that the personal data you hold is kept securely. That includes making sure it's physically safe, in the case of paper records, or digitally safe, in the case of electronic records. You may need both. You must also have rules and staff training in place to make sure information isn't lost, stolen or destroyed.

These measures will vary depending on how you hold this information, including whether it is collected manually or electronically. We understand that electronic collection measures are recommended by government in England, and you will need to ensure you have adequate cyber security in place. Again, you should involve some form of staff training so that employees understand their responsibilities when handling personal data.

Basic measures include:

- Make sure your staff understand what they should and shouldn't do with customer information. You should ensure that your staff are aware that it is a criminal offence under the Data Protection Act to obtain or disclose customer information without your organisation's consent.
- Do not use an open access sign-in book where customer details are visible to everyone.
- Keep any paper records in a safe place, with measures to prevent malicious access (eg locked doors, safes, CCTV).
- Consider which members of staff need access to the logs and limit access to those staff.
- Do not store customer logs in an accessible, unsecured file.
- Check your approach to cyber security – the ICO has published online guidance and the National Cyber Security Centre's Cyber Essentials scheme is a good place to start.
- When deleting or disposing of logs, do so in a way that is not at risk of unintended access (eg shredding paper documents as opposed to disposing them in public refuse bins, and ensuring permanent deletion of electronic files).

Who can we share the customer data we collect with?

You should only share the information when it is requested by a legitimate public health authority.

If you are contacted by a contact tracing scheme, and you are asked to provide details of individuals, you should ensure that the caller is genuine. You should be cautious that fraudsters or scammers could seek to obtain information from you by pretending to be a contact tracing agency.

Government guidelines will provide an explanation of what contact tracers will and won't do. Once you are satisfied that you can share the customer data with the contact tracer, make sure that you are able to securely share this information.

In a very narrow range of circumstances, it may be appropriate to share this information with other parties. For example, the information may be required by the police if they need it for a criminal investigation. In this case, an appropriate exemption would need to be identified.

Can we use the personal data we have collected for a contact tracing scheme for marketing or other business purposes?

No. Data protection law states that personal data which has been collected for a specific purpose should not be used for other reasons which conflict with the original purpose. This includes direct marketing or advertising, profiling your customer base or analysing demographics. This would be considered as a misuse of the information.

There are even more specific rules around electronic marketing.

If we become aware of someone who has tested positive for COVID-19, should we report them to a contact tracing scheme?

No. Contact tracing personnel have the responsibility for following up cases of COVID-19 following a positive test result. They will make the appropriate assessments and contact the people affected themselves.

If you are aware of a case of COVID-19, you should not seek to contact the people who have visited your premises yourself. You should only share the details you have collected with the contact tracing scheme in a secure way and only if requested. Contact tracing personnel will undertake an individual assessment and, if necessary, contact you to provide public health support and guidance, but this will be dependent on the specific circumstances.

You can advise staff of any precautions they may need to take. If there is more than one case of COVID-19 on your premises, you should contact your local health protection team to report the suspected outbreak.

How should my staff handle personal data that we collect for the purposes of contact tracing?

If you are collecting customers' personal data for contact tracing, you need to make sure you have procedures in place to handle it securely and safely. You must make sure your staff understand what they should and shouldn't do with customer information and you must make sure they put it into practice. For example, customer logs should only be available to those who need them. They should not be used to make personal contact with customers or for direct marketing or anything else other than contact tracing.

Not handling personal data properly means businesses and staff risk breaching the Data Protection Act with severe consequences for both.