Test and Protect Guidance for the Hospitality Industry

This guidance is for hospitality businesses in Scotland, and is a tool to support visitor data gathering where the nature of the premises means there may be an increased risk of transmission of COVID-19 due to a higher degree of interaction between unknown individuals. It sets out how to collect individual contact details in a safe, secure and legally compliant manner, to assist NHS Scotland in responding to outbreaks of COVID-19.

The regulations that create the mandatory requirements that this guidance covers come into effect from 14 August 2020. From these dates, hospitality businesses serving food or drink to customers who remain on the premises while engaging with the business, must gather minimal contact details from customers to support NHS Scotland's Test and Protect service, and share these details with public health officers for the purposes of contact tracing when requested.

What is Test and Protect

Test and Protect was launched across Scotland on 28 May and aims to prevent the spread of coronavirus in the community by:

- identifying cases of coronavirus through testing
- tracing the people who may have become infected by spending time in close contact with them
- supporting those close contacts to self-isolate, so that if they have the disease they are less likely transmit it to others

The gathering of contact information from customers, staff and visitors by hospitality businesses, in a secure and safe manner, will assist NHS Scotland's Test and Protect service to identify any clusters of cases, contact those who may have been exposed to the virus, and request them to take appropriate steps to prevent potential onward spread.

Mandatory Requirements

In order to support NHS Scotland's Test and Protect service, it is mandatory for all hospitality businesses – such as pubs, restaurants and cafes – to gather, record and retain minimal contact information from non-takeaway customers, visitors and staff.

Where customers are attending as a small household group, the contact details for one member of each household – a 'lead member' – will be sufficient alongside the number of people attending from each household. If a business offers a mixture of a sit-in and takeaway service, contact information only needs to be collected for customers who are dining in.

Businesses should:

- Explain why you are asking for contact information and encourage customers, visitors and staff to provide it.
- Collect, store, manage and dispose of information in line with GDPR requirements which may include registering with the Information Commissioner's Office.
- Display a notice on your premises and on your website explaining that dine in customers will be required to supply this information.

The following guidance sets out more detailed information on how to do this.

How Do I Register with the Information Commissioner's Office?

In order to gather and store customer information securely, businesses may need to be registered with the Information Commissioner's Office (ICO). This will be the case if you are using an electronic system to gather and store data.

If your business is already a data controller, you should already be registered with the ICO. A data controller can be any organisation or sole trader who processes personal information such as CCTV, staff or customer details.

However, if you are using an electronic system to store customer data and not already a data controller, or have not already registered as one, you may need to register with the ICO. If you are unsure whether you need to register, please contact the ICO via their helpline on 0303 123 1113, or visit www.ico.org.uk.

The cost of the data protection fee depends on the size and turnover of the business, but for most businesses it will cost £40 or £60. The form will take around 15 minutes to complete. Access the data protection form. The ICO has published its own detailed guidance on collecting customer and visitor details for contact tracing.

What is a Privacy Notice?

It will be important to ensure that data is collected and handled in line with data protection laws. As part of this, the Scottish Government has published a template privacy notice alongside this guidance, setting out the terms of how data should be gathered, stored, used and disposed of. The privacy notice is how your business will demonstrate compliance with Article 13 of the General Data Protection Regulation (GDPR) that sets out what information needs to be provided when data are collected from the data subject (visitors to the premises).

The privacy notice can be viewed online and should also be downloaded and made available in each establishment, and online if your premises has a website, so that customers providing details are informed as to what will happen with their data.
The privacy notice sets out the purpose for which the data is being collected, what data is being collected, the lawful basis for doing so, how long the data will be retained, what rights customers have over this data and how to complain to the establishment and the ICO if there is a concern. Customers or visitors phoning to make a booking in your premises must be made aware of the requirement to collect their contact details in support of Test and Protect.

As a controller, each business will be using the GDPR lawful basis under Article 6(1) (c) 'Legal Obligation'. Where an individual is not willing to provide their data, premises are advised to refuse service, or a booking.

Read the privacy notice.
Read more information on GDPR and how to access GDPR training.

Secure Collection, Storage and Disposal of Data

What Information Do I Need to Collect?

The following information should be collected by the venue, where possible:

Staff

- the names of staff who work at the premises
- a contact phone number for each member of staff
- the dates and times that staff are at work

For larger establishments, and where possible, it is also helpful to keep a record of what areas staff work in, e.g. what tables/sections they serve.

Customers and Visitors

- the name of each customer, or when customers are attending as a small household group, the contact details for one member of that group – a 'lead member'
- a contact phone number for each customer, or for the 'lead member' of a small household group
- date of visit and arrival and, where possible, departure time

For larger establishments, and where possible, it is also helpful to record table numbers or sections where customers were seated.

If a customer does not have a telephone number, businesses may give customers the option to provide:

- a postal address
- an email address

How Should I Collect this Data?

Contact details will need to be collected by premises for each customer or visitor, or for a 'lead household member' of each household, upon their arrival, or prior to their arrival where booking in advance allows. If only the contact details of the 'lead household member' are recorded, it must include a note of how many other people not separately recorded visited as part of that household.

Many businesses that take bookings already have systems for recording their customers – including restaurants and hotels – which can serve as the source of the information above. This could include taking bookings online or over the phone.

If not collected in advance, this information should be collected at the point that customers enter the premises. Customers will need to be informed of the need to provide information upon their arrival and the purposes for which it will be used. The resources published alongside this guidance include a poster that can be put up in an establishment to alert customers to this need, and copies of the template privacy notice which should be displayed to inform customers of how their information will be used and protected. There may also be instances where it is necessary to also explain to visitors the content of the privacy notice, e.g. where bookings are taken over the phone.

Information should be recorded digitally if possible, but a paper record is acceptable too. Writing customer details in a book or register and destroying these when the retention period is over is acceptable so long as the register is **kept out of public sight** and **stored securely**. Similarly,

digital records must be securely deleted at the end of the 21 day retention period. Staff need to be identified and appropriately trained for this.

To minimise the risk of virus transmission, and any likelihood of other individuals having access to personal data during this process, any written information must be noted/recorded by a designated member of staff and not by each individual customer/group.

The ability to record departure times where possible, as well as arrival time (including staff shift times) is important to reduce the potential number of customers or staff needing to be contacted (and potentially asked to self-isolate) by NHS Scotland's Test and Protect service, although it is acknowledged that in certain circumstances this may be more difficult.

What Should I Do If Someone Does Not Wish to Share Their Details?

There is no legal requirement that individuals must provide their data for NHS Test and Protect purposes. However, if the individual still does not want to share their details then premises should refuse to offer the service requested. Employers should make clear to their employees the approach that they wish them to take in these circumstances.

What are Right of Access?

It is within the rights of individuals to request to access the data held on them, or to request that it is corrected. In those circumstances, businesses should comply with such requests.

How Do I Store Data Securely?

Once customer details have been gathered, the business will be the data controller, and the data must not be shared with individuals or organisations other than public health officers. All customer data should be stored securely and in accordance with the requirements of the GDPR. Records should be held for at least 21 days from the date of each separate visit of a staff member or customer.

Following this, subject to any other lawful obligation to retain it, the data will normally no longer be required to be held by the business and must be disposed of securely.

If data is shared with public health officers on the basis of individuals being identified as at risk of being close contacts by the Test and Protect service, public health officers including NHS Scotland may need to retain the data for longer than the 21 day period and will hold the data in line with NHS information governance processes. NHS Scotland may also need to share information with other local and statutory delivery partners as part of responding and containing the virus, such as Local Authority Environmental Health Departments. In enforcing this regulation, it is also possible that Environmental Health Departments may request to see an establishment's data, collected for these purposes, only to ensure compliance with the regulation, and not to process the data in any other way.

How Should I Dispose of Data?

Subject to the information above, after 21 days data should be disposed of securely.

If you are using a paper register then pages can be removed daily after the 21-day retention period is over and destroyed through secure shredding or other destructive process. Where IT systems are used, establishments will need to ensure that data provided for Test and Protect is deleted and not retained beyond the stated period. The data should not become part of a wider marketing or other resource otherwise used in contravention of the GDPR.

When Should Information be Shared?

If cases of COVID-19 detected that have a link to a business, NHS Scotland may contact the business by phone to request staff and customers' details to allow contact tracing to take place. The NHS Test and Protect service has a number of mechanisms in place to reassure people contact tracers are legitimate, including call back options, visible numbers, and specific location and date information.

Establishments must share the information of staff and customers with NHS Scotland as soon as possible, but in any event within 24 hours if asked to do so.

Contact tracers will NEVER:

- ask you to dial a premium rate number to speak to them
- ask you to make any form of payment, including a charitable donation
- ask for any details about your medical history that are unrelated to COVID-19
- ask for any details about your bank account
- ask for your social media identities or login details, or those of your contacts
- ask you for passwords or PINs, or ask you to set up any passwords or PINs on the phone
- ask you to purchase a product or attempt to sell you anything
- ask you to download any software to your device or ask you to hand over control of your PC, smartphone or tablet

Establishments should not share this information with anyone else other than NHS Scotland.

Contact

Central Enquiry Unit
Email: ceu@gov.scot
Phone: 0300 244 4000
Post:
The Scottish Government
St Andrews House
Regent Road
Edinburgh
EH1 3DG