JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

CONTACT TRACING PERSONAL INFORMATION

Checklist

FEB 2021 • V3 • WWW.JERSEYOIC.ORG

INTRODUCTION

The Government of Jersey now requires organisations whose activities have the potential for people to be within 2 metres of each other for longer than 15 minutes, to ask for contact information from patrons, for the purposes of supporting its contact-tracing efforts.

While many organisations already collect similar information for other purposes, in complying with this requirement, organisations will be collecting the personal information of patrons for a different purpose and may collect more than they are currently collecting. In assisting with the Government of Jersey's contact-tracing efforts, organisations must remember to comply with the Data Protection (Jersey) Law 2018 (the Law).

Organisations that have concerns or questions about how to collect and store personal data under the Law, or individuals who have questions about what is happening to their personal information and how to exercise their individual rights under the Law, should contact the JOIC team via **enquiries@jerseyoic.org** or by calling the JOIC office on 01534 716530.

The purpose of this checklist is to help organisations to navigate their legal responsibilities when collecting personal data in these circumstances to support the contact-tracing effort.

The Law covers all personal data, which is any data relating to a data subject (so, any information relating to a living, identifiable individual).

The Law requires organisations to process personal data lawfully, fairly and in a transparent manner. This means that patrons should know exactly what information organisations are collecting as part of the contact-tracing scheme and to whom the information will be disclosed and how it will be protected.

CHECKLIST

☐ **REGISTRATION**

Has your organisation **registered** with the Jersey Office of the Information Commissioner? This is a requirement under the Law to allow any organisation to process personal data in the course of their organisational/charitable activities.

☐ **CONDITIONS FOR PROCESSING**

Whenever your organisation collects, stores, or uses personal data in any way, it needs to have a specific reason for this collection, as set out in **Schedule 2** of the Data Protection (Jersey) Law 2018.

The Law requires that your organisation has a **'lawful basis'** upon which to process (so to collect and potentially share) any additional information it collects to assist with the Government of Jersey's contact-tracing scheme. If Government requires your organisation to ask all people attending your premises if they are willing to provide their information for contact-tracing purposes, the lawful basis for processing personal data that allows your organisation to do so is likely to be one of the following:

☐ **Legitimate interests**
This is likely to be the most applicable condition if you are a private organisation. This condition 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.

☐ **Consent**
Organisations will not need to rely on consent, where the legitimate interest principle applies, except in certain circumstances. This would include where the information you are collecting is **Special Category Data** which is information that could reveal something sensitive about the person involved. It includes racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as data concerning health, data concerning a natural person's sex life or sexual orientation; or data relating to a natural person's criminal record or alleged criminal activity.

☐ If your organisation chooses to rely on consent as its lawful basis:

- Can your organisation demonstrate that the data subjects granted their consent freely and in an informed manner?
- How will your organisation record that the data subject has consented?
- What will your organisation do if the data subject exercises their legal right to withdraw their **consent?**
- Has your organisation ensured that all staff are aware that they cannot deny entry to your premises to patrons that refuse to grant their consent?

(Please note that it is unlikely that the legal basis for processing for the purposes of sharing the data with Government as part of the contact-tracing programme will be the same as the legal basis your organisation uses for collecting customer data for normal business purposes, e.g. Marketing or booking a table at a restaurant).

The Government requires organisations to collect only the following data for contact-tracing purposes:

- Full Name.
- Mobile contact number.
- Date and time of arrival.
- Area where seated.

- [ ] Can your organisation demonstrate and justify its 'lawful basis' for collecting personal data?
- [ ] Can your organisation demonstrate it has considered retention and security of contact-tracing information?
- [ ] How is your organisation keeping the personal data collected for contact-tracing secure?
    - » What is the format it is being held in?
    - » Who has access to it?
- [ ] Your organisation is only permitted to collect personal data which is relevant for the purpose it is using it. This means your organisation should not gather more than is needed in the hope it could be used for a different purpose such as marketing.
- [ ] The Law stipulates organisations must not keep any personal data for longer than is necessary for the purposes for which it has been collected. The Government guidance on this is 21 days for the purposes of the contact-tracing programme, after which the information should be destroyed.
    - » How will your organisation dispose of/delete the data? (remember the organisation is obliged to do so securely)
- [ ] With whom, when and how will your organisation be sharing the information? Does your organisation know what it will be doing with it? Is this detailed in your organisation's **privacy policy?**
- [ ] Consider putting together an information sheet to provide to patrons if they ask why your organisation is collecting their data. Alternatively, your organisation may choose to make available a mini privacy policy covering collection of contact-tracing data and/or has your organisation updated its usual privacy policy?

LOOKING AFTER PATRON INFORMATION

Your organisation may already be collecting data for other purposes, such as table reservations, for example. As the information being collected for the contact-tracing initiative is a different purpose, your organisation should treat this information separately. Similarly, it is important that the data collected for contact-tracing purposes is not used for any other purpose than to provide it to the Government upon request. Your organisation should not, for example, ask customers if they will also consent to the data being provided to be used for marketing communications.

Your organisation is responsible for ensuring that it stores the personal data securely. This applies both to paper records and electronic data. Your organisation must also have rules and staff training in place to prevent the loss, theft or inappropriate destruction of the data. These measures will vary depending on how your organisation holds this information.

- [ ] Staff members must know what they should and should not do with the patron information they are collecting. Your organisation needs to ensure its staff understand that the data is confidential and that they can use it only for the purposes of contact-tracing. It is a breach of the Law to misuse personal data.
- [ ] Your organisation should keep the patron information it collects, on paper or electronically, only for a **maximum of 21 days**. After this period expires, your organisation must destroy it securely. It may be advisable to assign an appropriate member of staff to destroy expired records on a daily basis.
- [ ] The data collected must be kept securely and should not be accessible to anyone who does not have a reason associated with contact-tracing to see it. Basic measures include:
    - » Do not use an open sign-in book where patron details are visible to everyone – each patron should complete a separate form or provide their details in a manner that would not allow others to see them.
    - » Keep any paper records in a safe place, with measures to prevent malicious access (e.g. locked doors, safes, CCTV).
    - » Consider which members of staff need access to the records and limit access to those staff.
    - » Do not store contact-tracing records in an accessible, unsecured file.
    - » Where using an electronic solution, check your organisation's approach to cyber security and do due diligence on the supplier.
- [ ] When deleting or disposing of the records, do so securely (e.g. shredding paper documents as opposed to disposing them in public refuse bins, and ensuring permanent deletion of electronic files).

MORE INFORMATION

Organisations that have concerns or questions about how to collect and store personal data under the Law, or individuals who have questions about what is happening to their personal information and how to exercise their individual rights under the Law, should contact the JOIC team via **enquiries@jerseyoic.org** or by calling the JOIC office on 01534 716530.

Jersey Office of the Information Commissioner
2nd Floor
5 Castle Street
St Helier
Jersey JE2 3BT

Telephone number: +44 (0) 1534 716530
Email: enquiries@jerseyoic.org