JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WHAT TO EXPECT FROM A JOIC AUDIT

JULY 2024 • V2 • WWW.JERSEYOIC.ORG

CONTENTS

3 Overview

6 What to expect

- Virtual audit
- Full audit

9 Audit follow up

10 Frequently Asked Questions

OVERVIEW

1. The Jersey Data Protection Authority (the **Authority**) is responsible for enforcing and promoting compliance with the Data Protection (Jersey) Law 2018 (the **DPJL 2018**). These functions (and other day-to-day tasks) are carried out by the Information Commissioner (the **Commissioner**) and their staff, under the banner of the Jersey Office of the Information Commissioner (**JOIC**).

2. Sched 1 para 7 of the Data Protection Authority (Jersey) Law 2018 (the DPAJL 2018) gives the JOIC the power to either conduct data protection audits of any part of the operations of the controller or processor itself, or to require the controller/processor to appoint a person (approved by us) to conduct a data protection audit on any part of the operations of the controller/processor and report to us on those findings. These provisions not only give us the power to carry out compulsory audits but also consensual audits pursuant to our powers under Art.11(1)(e) of the DPAJL 2018 i.e. as part of our general function "*to promote the awareness of controllers and processors of their obligations under [the DPAJL 2018] and the [DPJL 2018].*"

3. The aims of our audit process are to assess a controller/processor's policies and procedures and the level of compliance with the DPJL 2018, to highlight any areas of potential risk, and set a timeframe for any necessary remedial work.

4. We see auditing as a constructive process with real benefits for data controllers and we aim to establish a participative approach whether the audit is conducted on a compulsory or consensual basis.

5. We conduct two forms of compliance audit and these can be done on a compulsory (using our enforcement powers) or consensual (by agreement) basis (see para. 10 below for further information):
    a. Compliance Audit (Virtual): these are part of our rolling audit programme, consisting of specific, thematic reviews aimed at particular sectors of Jersey business. These are generally compulsory audits carried out pursuant to Sched 1 para 7 of the DPAJL 2018 and are carried out by way of an online survey and follow-up; and
    b. Compliance Audit (Full): these are part of our more targeted programme and may be conducted on a compulsory or consensual basis. These will tend to include a Virtual audit as part of the initial stages of the audit programme, followed up by an on-site visit which usually includes 1-2-1 meetings and focus groups with key members of staff, including the Board of the controller/processor.

6. All audits are carried out by members of our Compliance and Enforcement Team and are one of our tools used to ensure that organisations involved in the processing of personal data are complying with local data protection law.

7. Where appropriate, we will publish the lessons learned from any audit we carry out. This will usually set out the scope of the audit carried out, areas of good and bad practice identified and what is expected by the JOIC in terms of overall good practice.

Why audit?

8. There are many benefits to our audit process, which include:
    a. Assessing the controller/processor's data protection policies and procedures for compliance with the DPJL 2018;
    b. Engaging with the controller/processor's staff to understand the level of understanding of and engagement with data protection issues;
    c. Helping to embed and promote a healthy data protection culture within the auditee's organisation, empowering employees to actively contribute to the entity's data protection responsibilities and ensuring that data protection matters are managed effectively at all levels of the organisation from board level down;
    d. Gaining an independent review and evaluation of data protection policies and practices, including identifying risks and providing targeted recommendations.

What will the audit look like?

9. The focus of our audits are to identify whether an organisation has policies and procedures in place to manage the processing of personal data and, if so, whether those policies and procedures are actually being followed.

10. We will usually assess the organisation's policies, procedures, systems, records and activities in order to:
    - Understand what policies and procedures are in place and check whether they are appropriate;
    - Check that any policies and procedures that are in place are being actively implemented and followed;
    - Test the adequacy of any controls that are in place;
    - Detect any breaches or potential breaches in compliance; and
    - Recommend/require any areas for improvement.

11. We do not usually cover the processing operations of the whole organisation and will usually focus on certain areas.
    - In a consensual audit, the areas will be discussed and agreed with the organisation in advance of the audit taking place, but the areas proposed will usually have been identified by us as a result of the organisation's own concerns and/or our own intelligence (including following a formal investigation or inquiry).
    - In a compulsory audit, the areas will be similarly defined but may also be designed to take into account any data protections issues or risks which affect specific sectors or organisations more widely.

How do we plan our audit programme?

12. For our compulsory audit programmes (both Virtual and Full) we adopt a risk based, proportionate and targeted approach.

13. When deciding which organisations to audit, we will consider matters like emerging patterns/trends in terms of complaints and self-reported data breaches e.g., does our intelligence suggest that there are particular sectors/industries struggling in certain areas of data protection, or are there high numbers of SRDBs relating to similar types of breaches? We will also take into account open source information like media reports and any other information we believe shows that it is appropriate for us to carry out an audit.

14. The scope of the audit will then be developed in light of the identified risks/trends and will focus on those areas.

15. Similarly, where we are conducting a consensual audit, the terms of reference will be agreed focusing on key risk areas for the organisation, which will be identified in accordance with the following criteria:
    - The organisation's compliance history in terms of SRDBs, complaints and formal investigations and inquiries, as applicable;
    - Any other interactions between the organisation and the JOIC that may suggest deficiencies in terms of understanding and/or compliance with data protection matters (including following submission of a Data Protection Impact Assessment (**DPIA**) for consultation);
    - Open source information e.g. media stories suggesting data protection issues involving the organisation;
    - Information received from other regulators/law enforcement agencies (either pursuant to any MoUs or otherwise, local, national and/or international);
    - Information published by the organisation and in the public domain which demonstrates potential misunderstanding of the requirements and/or highlight any other issues in terms of that organisation's compliance with the requirements of the DPJL 2018;
    - Any previous audit activity conducted with the organisation;
    - Any issues in terms of registration (including non-payment/late payment);
    - The type of processing activity carried out by the organisation (in terms of categories and number of data subjects, type and volume of data) and the likely risks and impact for relevant data subjects in terms of non-compliance by the organisation in question;
    - Any other relevant information, including that received from whistle-blowers.

WHAT TO EXPECT

Virtual Audit

16. Although we may carry out Virtual audits on a random basis, we generally carry them out against certain sectors as a whole, according to risk. When deciding which organisations will form part of our Virtual audit plan for the year we consider matters such as:
    a. The categories of data they process (e.g. special category data such as health data or criminal records information)
    b. The number of complaints we have received about organisations operating in a particular sector in the preceding year
    c. Whether there is regular sharing of data between/with other organisations
    d. The length of time that has elapsed between any previous audits
    e. The overall sectoral compliance on previous audits

How do we carry out our Virtual audits?

17. Before we start a Virtual audit, we write to the organisations in the relevant sector advising them that we will be carrying out a Virtual audit and setting out the timetable for provision of information via our online survey platform. Where the sector has a representative or other regulatory body (e.g. the Jersey Care Commission, or the Jersey Charity Commissioner) we will ordinarily advise them that we are going to be auditing the organisations they are also involved in regulating/representing. We may hold a preliminary information session for organisations and their representative, talking through the audit process and what is required and to answer any questions.

18. Virtual audits are conducted via our online survey platform and organisations will usually be asked a series of questions about their data protection compliance and may also be asked to upload certain documents by which they can demonstrate compliance with certain provisions of the DPJL 2018 e.g. their privacy notice, retention schedule, breach log, copies of any internal policies etc.

19. Once the survey has been completed and the documents received, our audit team will review the information provided and they may have further questions for you. They may make comments, have suggestions or require you to do further work to ensure that the organisation is operating in compliance with the DPJL 2018.

20. If we have significant concerns regarding the responses provided by the organisation and consider that there are issues that cannot be remedied as part of the Virtual Audit and/or there are other concerns suggestive of a broader compliance issue, we may decide to initiate a formal Inquiry under Art.21 of the DPAJL 2018.

Full Audit

21. We will hold an initial meeting with representatives from the organisation to discuss the audit process and the proposed focus areas for the audit. We will follow that up with a draft letter of engagement setting out the proposed scope of the audit, explaining the audit process and advising of our proposed timetable. The organisation will be invited to respond to us with any comments on the letter of engagement, and confirm the proposed timescales. Once finalised, the letter of engagement will be formally issued to the organisation and the audit process will commence.

22. Before any on-site visits take place, the organisation will be asked to provide some initial background information (usually by way of questionnaire) and there may be some follow up questions from our office, depending on the information provided.

23. We will also review any relevant policies and procedures the organisation has in place and this may include:
    a. Privacy policies
    b. Retention schedules
    c. Records of processing activities
    d. DPIAs
    e. Breach log
    f. Any other policies/procedures relating to data protection matters such as subject access and breach reporting policies
    g. Staff training (including copy training materials, training schedules, staff attendance records).

24. We will usually want to have 1:2:1 meetings with key staff (such as the CEO, data protection officer) and conduct focus groups with certain relevant groups of staff. We aim to create as little disruption as possible and whilst some of these sessions may be conducted remotely, as appropriate, we generally prefer to conduct these sessions "in person" and we will keep notes of these meetings and store them in accordance with our JOIC retention schedule which can be found at **www.jerseyoic.org/retention-schedule/**

On the day

25. The audit programme, including the duration of our visit, will have been set out well in advance and a timetable will already have been agreed with the organisation.

26. The day will usually start with an initial meeting with the organisation's representative/senior leadership team to remind them of the timetable and the audit process.

27. We will then carry out any 1:2:1 interviews and focus groups in accordance with the agreed timetable.

28. Once the 1:2:1s and/or focus groups have concluded, we will hold a closing meeting on the final day with the organisation's representative/senior leadership team to provide an initial indication of what has been uncovered as part of the audit process, including any immediate areas of concern that require urgent attention. We will also remind the organisation about our proposed timeframe for the provision of any report and any follow up activity.

The Audit Report

29. We will produce a report of our findings in line with our agreed timetable. This will initially be provided to the organisation in draft and will include:
    a. Our findings in terms of each scope area and a proposed assurance rating for each area;
    b. Details of areas of non-compliance and recommended/required remedial action (including proposed timeframe);
    c. An overall assurance rating.

30. The organisation will be invited to reject, accept or partially accept our findings and to complete an action plan setting out how our recommendations/requirements will be implemented, the timeframe for their implementation and by whom.

31. When we have received the organisation's response to the draft, those responses will be considered and the final report issued.

Assurance Ratings

32. Each area of scope we audit will be rated as per the below table:

COLOUR RATING AND AUDIT CONCLUSION	EXPLANATION	RECOMMENDATION PRIORITY
VERY LIMITED ASSURANCE	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.	High priority
LIMITED ASSURANCE	There is a limited level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPJL 2018.	Medium priority
REASONABLE ASSURANCE	There is a reasonable level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPJL 2018.	Low priority
HIGH ASSURANCE	There is a high level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with the DPJL 2018.	Minor points only are likely to be raised

AUDIT FOLLOW UP

33. We will be in touch at an agreed point to review the progress of any follow-up activities and ensure that the recommendations/requirements are being implemented in accordance with the agreed timeframe set out in the final report.

34. If the actions have not been addressed or are not being progressed in accordance with the agreed timetable, we will discuss these matters with you to understand why those matters have not been progressed. Serious areas of non-conformity may result in our initiating formal enforcement activity, including by way of an Inquiry.

35. We will provide a follow up report to the organisation, but this will not be published. We may update anything previously published on our website to say that an audit has been successfully concluded.

FAQS

How long will the audit take?

Virtual audits are designed to be completed online. The questionnaire should take only a short amount of time to complete and it will be easy for you to upload the documents we have asked for. Once we have reviewed your submission, you might have further work to do but we will give you a clear timeframe in which to carry out the work and report back to us.

For Full audits, there will be some time involved in agreeing the terms of reference and setting relevant time frames including the timetable for attending on-site and working out an interview schedule. We aim to be on-site for no longer than one week and the timings for the preparation and delivery of our report will be set out in our agreed terms of reference.

Do I need to pay for the audit?

We do have the ability to order organisations to carry out an audit using an audit provider approved by us and to pay for this but generally speaking we do not charge organisations for either Virtual or Full audits.

Can we give feedback to JOIC at the end of audit process?

Yes! We are always looking at ways to improve our services and we issue feedback questionnaires to each organisation, at the end of both the Virtual and Full audit process.

Do you publish your audit findings?

For Virtual audits, we will provide an anonymised lessons learned at the end of the audit process. This will give a broad overview of the audit focus, overall levels of compliance, and an indication of the types of follow-up work required. When we carry out our Virtual audits, we will usually be targeting a specific sector, so we think it is helpful to provide that sector with an indication of our overall findings. We will not be publishing detailed findings about an identified organisation.

For consensual Full audits, we may publish an executive summary of the audit with the agreement of the organisation. This will be a very high-level document setting out the background to the audit, areas of good practice, areas for improvement and our overall rating.

For compulsory Full audits we will publish an executive summary containing the same information as set out above.

We will not publish the detailed findings for either consensual or compulsory Full audits.

Will you keep matters confidential?

Confidentiality is at the heart of everything we do and members of the JOIC staff (including those on our audit team) are legally bound under Art.7 of the DPAJL 2018 to keep information provided to them in the course of their duties confidential.

Can the JOIC take any enforcement action following an audit?

As we've already stated, we see audits as being a positive process aimed at assessing an organisation's overall level of data protection compliance, identifying areas for improvement and working with those organisations to get things right.

However, there may be occasions where either as part of a Virtual or Full audit that we discover areas of non-compliance that give us cause for concern and in those circumstances we may consider it appropriate to take formal enforcement action (including carrying out a Inquiry under Art.21 of the DPAJL 2018).

Can we ask you for an audit?

We are always happy to speak with organisations who believe that they could benefit from a JOIC audit and discuss concerns with you. Please bear in mind, however, that we do have to ensure that our resources are appropriately applied and our audit programmes are risk based, so we may not be able to conduct an audit because of other priorities. If that is the case, we will still see whether there are other ways we can work with you to address the issues you have raised.

We want to know what our staff said to you during the audit. Will you tell us who said what?

We will not divulge to you in any directly attributable manner information provided to us by your staff. There is good reason for this; for the audit to be effective we need to understand what is actually happening within your organisation so we can really understand what is being done well, and which areas require improvement. The audit process will be most effective if those engaged in the process feel empowered and able to provide us with honest information. For that reason, we do not divulge "who said what" and where we have 1:2:1s or focus groups with certain staff groups, we will tightly control the attendees.

Do I have to comply?

In all circumstances other than a consensual audit, you must comply with our compulsory Virtual or Full audit programmes. This includes providing us with the documentation we have requested and answering the questions we ask accurately and comprehensively.

Please bear in mind that it is a criminal offence to obstruct any member of the JOIC in the conduct of their duties and it is also an offence to provide us with false information.

If we tell you that there is work you need to do to address deficiencies in your data protection practices, you must do what we tell you to do in order to put things right and if we tell you that you need to have done things by a certain date, you need to comply with that deadline.

If you do not comply with our audits, we may be left with no alternative but to consider further action in line with our **Regulatory and Enforcement Strategy** and this could include our exercising our power of seizure of processing equipment, the carrying out of a formal inquiry and, in appropriate circumstances, the issuing of an administrative fine.

What if the JOIC becomes aware of a breach or other significant data protection issue whilst on-site?

If during the audit we identify a data breach (for example, a reportable incident, that hasn't been reported to the us) or some other significant issue, we'll inform our key contact at the organisation of the finding as soon as practically possible, explain what actions need to be taken and what the next steps will be from our perspective.

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