JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

PUBLIC STATEMENT

PUBLIC STATEMENT

JERSEY OFFICE OF THE INFORMATION COMMISSIONER

Data Controller: Jersey Financial Services Commission (JFSC)
Registration No: 17955

1. This is a public statement made by the Authority pursuant to Art.14 of the DPAJL 2018 following an Inquiry by the Authority.

2. Following the Inquiry which commenced on 19 April 2024 pursuant to Art.20 of the Data Protection Authority (Jersey) Law 2018 (**DPAJL 2018**), the Jersey Data Protection Authority (the **Authority**) has determined that the JFSC has contravened Art. 8(1)(f), Articles 15(1)(a) and (b) of the Data Protection (Jersey) Law 2018 (the **DPJL 2018**).

3. JFSC was issued with a formal Reprimand.

Background

4. In January 2024 JFSC's Data Protection Officer contacted the Authority to advise that the JFSC had suffered a personal data breach involving its Companies Registry portal, due to a critical flaw in third party provided software, which was implemented in 2021.

5. The submission confirmed that a vulnerability in the software allowed an unregistered user to access data, specifically names and addresses, that should not be publicly accessible. It also verified that the issue had been identified and permanently resolved.

6. Art.20(6) of the DPJL 2018 states organisations must notify individuals if a personal data breach is likely to result in a high risk to their rights and freedoms. After undertaking analysis of the incident and confirming the names and addresses of 66,806 individuals had been accessed inappropriately, the JFSC released a public statement on 7 March 2024 to inform affected individuals. In addition, the JFSC wrote directly to 2,477 individuals who they assessed to be in a higher risk category.

7. The JFSC's Public Statement confirmed that they had engaged the services of independent forensic experts to carry out an investigation to establish the root cause of the breach.

8. A comprehensive report detailing the findings of the independent experts was provided to the Authority in September 2024. The report concluded the breach could be attributed to the failures in information security arrangements, initial development testing, ongoing testing and the monitoring of the portal.

9. In November 2024, the JFSC provided the Authority with its response to the independent report. It detailed their approach to how each observation of the report was to be addressed and included actions already taken, mitigations already put in place and improvements to processes that were ongoing or due for completion.

PUBLIC STATEMENT

10. One key improvement was the introduction of a procedure for regular reporting on the Registry portal. This process supports ongoing performance monitoring, helps identify any weaknesses, and provides oversight of usage patterns to reduce the risk of similar issues occurring in the future.

The contraventions of the DPJL 2018

11. The Authority found that the Jersey Financial Services Commission contravened the DPJL 2018 as follows:

12. FINDING 1: Breach of Art.8(1)(f) of the DPJL 2018

Art.(8)(1)(f) of the DPJL states: *"a controller must ensure that the processing of personal data in relation to which the controller is the controller complies with the data protection principles, namely that data are processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures"* ("integrity and confidentiality").

Due to a programming vulnerability within the Registry Portal, unauthorised third parties gained access to the personal data (names and addresses) of 66,806 data subjects.

There was insufficient follow up and testing of security measures which led to the vulnerability not being discovered until after the data breach had occurred.

Accordingly, the Authority found the controller failed to provide appropriate technical and organisational measures resulting in the unauthorised access to personal data and is therefore in contravention of Art.8(1)(f) of the DPJL 2018.

PUBLIC STATEMENT

13. FINDING 2: Breach of Arts.15(1)(a) and (b) of the DPJL 2018

Arts.15(1)(a) and (b) of the DPJL 2018 state: *"A controller must, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures that are designed to – implement the data protection principles in an effective manner; and integrate the necessary safeguards into the processing to meet the requirements of this Law and protect the rights of data subjects".*

The consideration of security by the JFSC was not as extensively documented as would be expected in the initial design and implementation of a new processing activity on the scale of the Registry implementation. The Authority's investigation confirmed that opportunities designed to discover the software flaw existed during the initial testing period, but they were either missed or rated as low risk.

Monitoring was included in the requirements provided for the initial project, but investigations revealed there were inadequacies in ongoing monitoring activity. Log monitoring applications did exist in the JFSC, however, the incompatibility of systems resulted in a lack of oversight. If closer monitoring had taken place, it is likely to have highlighted the unauthorised data extraction and reduced the substantial period that the personal data was at risk.

Accordingly, the Authority makes a finding that the controller failed to implement appropriate technical and organisational measures that are designed to – implement the data protection principles in an effective manner and integrate the necessary safeguards of the processing in order to meet the requirements of the Law and protect the rights of data subjects. Therefore, the controller is in contravention of Arts.(15)(1)(a) and (b) of the DPJL 2018.

Sanction

14. The Authority considered all of the information provided to it by the JFSC when considering whether it is appropriate to impose any sanction and has paid particular regard to the following:

a. The software configuration flaw existed from implementation of the Registry in 2021 until it was discovered in early 2024.

b. The software configuration flaw allowed unauthorised access by third parties to personal information, that needed no specialist knowledge to gain access. The information could be extracted both manually and electronically, however, it was noted that a higher degree of technical knowledge was needed in order to do this by using automated software.

PUBLIC STATEMENT

c. The lack of appropriate security arrangements (failure to identify and address the configuration flaw) led to inappropriate access to the names and addresses of 66,806 individuals.

d. The investigation did not reveal any evidence that the personal information extracted had been used to the detriment of individuals affected and the Authority has not (to date) been made aware that the affected individuals have been impacted.

e. No complaints have been received by the Authority from individuals affected by the breach.

f. The JFSC co-operated fully with the Authority's Inquiry and has answered all the investigatory questions posed and provided requested documentation in a timely manner.

g. The JFSC made full and frank admissions as to the shortcomings in various areas that led to system vulnerability and although they maintained the design flaw was attributed to supplier provided software the JFSC accepted full responsibility for the issue.

h. The Authority noted that the JFSC introduced mitigations and improvements to processes without the need to be directed by the Authority.

i. Having reviewed all of the documentation, evidence and answers to the questions, the Authority is satisfied that there is little risk to individuals regarding a reoccurrence of these vulnerabilities in system security.

15. Considering the above factors, the Authority issued a formal reprimand pursuant to Art.25(3) of the DPAJL 2018 but due to the proactive approach and remedial actions taken by the JFSC, the Authority did not need to issue any formal orders to remedy the matter.

16. Having considered all the relevant facts, the Authority concluded that the nature of the breach would have warranted initiating the relevant process to assess the imposition of an administrative fine. However, as public authorities are not subject to such fines under the current framework, no further consideration was given to this by the Authority.

17. Under the provisions of the DPAJL 2018, enforcement action taken against organisations cannot be published unless the Authority considers the disclosure is in the public interest. The Authority determined the threshold was met in this case.

18. The Inquiry proved to be complex with the need for careful consideration of information provided, to evidence the mitigations put in place to check if the organisation had taken steps to fix the problem. An Inquiry must follow strict legal processes under the DPAJL 2018. This includes giving

time for responses and appeals, which can add to the length of time required for a satisfactory conclusion.

Lessons Learned

19. Organisations that are proactive and work openly with the Authority can expect this to be considered when deciding what level of action is appropriate. Cooperation can lead to reduced penalties, faster resolution, and a more constructive outcome. It also shows a commitment to accountability which can help rebuild trust with those affected.

20. The DPJL 2018 states organisations must build data protection into their processes by **design and default**. This means that you must think about data protection from the very beginning of any project. As an organisation, you are responsible for complying with these requirements and it applies to everything you do with personal data.

21. **By design**: This means that you think about data protection issues from the design phase of any system, service, product or process through to implementation, operation and regular review. This includes when you amend, update or terminate the system or process. Examples include:

    - Developing new IT systems, services, products and processes that involve processing personal information.
    - Developing organisational policies, processes and strategies that have privacy implications.
    - Embarking on data sharing initiatives; or
    - Using existing personal information for a new purpose.

22. **By default**: This means that you adopt a 'privacy first' approach with any default settings of systems, applications or processes. For example, you only collect/use as much information as is necessary for your specific purpose (you don't get more than you need).

23. If you use a product, piece of software, or another organisation to help you (e.g. an external IT provider, outsourced payroll, accountancy or HR) you need to make sure that those things/organisations comply with data protection requirements. You are ultimately responsible, for the products, software, and organisations you choose.

24. A tool to help with this is a Data Protection Impact Assessment (**DPIA**). It is a checklist or process you follow to look at what risks your data use might create and how to reduce them. It helps you identify problems

before they happen and show that you've thought things through properly. It's a way to check if your project (e.g. the piece of software you want to use) could impact on someone's privacy rights and supports you in making sure that you have built data protection into your processes right from the start.

25. For new projects, DPIAs are a vital part of data protection by design. They build in data protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented. DPIAs help organisations meet their legal obligations by:

    - Demonstrating transparency
    - Embedding privacy into project planning
    - Identifying problems at an early stage
    - Preventing data breaches and misuse
    - Supporting informed decision making

26. A DPIA is not a one-off exercise to file away. It is a 'living' process to help you manage and review the risks of the processing and the measures you've put in place on an ongoing basis. You need to keep it under regular review and reassess if anything changes.

More Information

More information about how we regulate and enforce the DPJL 2018 can be found in our Regulatory Action and Enforcement Policy here.