DATA PROTECTION AUTHORITY (JERSEY) LAW 2018

PUBLIC STATEMENT

Data Controller: Planning and Building Control

1. The Data Protection Authority for the Bailiwick of Jersey (the "**Authority**") has determined that the Planning and Building Control Department, Government of Jersey (the "**Controller**") has contravened Art.8(1)(f) of the Data Protection (Jersey) Law 2018 (the "**DPJL 2018**") in that it failed to comply with the integrity and confidentiality principle and ensure that it had appropriate technological and organisational measures in place to ensure the security of the data it processes resulting in the public disclosure of sensitive health information of a vulnerable minor.

2. Following investigation, the Authority has determined that the Controller was responsible for two separate breaches relating to information that had been provided to it as part of the appeals process under the Planning and Building (Jersey) Law 2002.

3. The first breach of significant gravity related to insufficient redaction being applied to information that had been uploaded to the Controller's online registry of planning applications (the "**Registry**"). The redactions were insufficient to prevent piecing together of information so as to allow identification of a vulnerable minor and allude to the fact that the published information related to certain highly sensitive health information.

4. The second breach was of even greater gravity, relating to the disclosure of extremely sensitive special category data (health information) about a vulnerable minor. This information was published in error and the Department has accepted that the relevant document should not have entered the public domain nor been uploaded to the Registry.

5. Special category data (including health data) are afforded higher levels of protection in the DPJL 2018, reflecting the harm and distress that can result from a breach. The Authority is clear that where organisations do not take their legal responsibilities to protect such data seriously or where they are negligent as to their responsibilities, consideration will be given to the appropriate sanction (including the issuing of a fine, where available). Had the Authority not been prevented by law from imposing a fine due to the Controller being a Public Authority, the Authority would have considered a fine in these circumstances.

6. In this case, the Authority has identified the following mitigating factors including:

    a. The Controller maintained open and candid correspondence with the Authority whilst enquiries took place and made early admissions.

b. Complete cooperation by the Controller's staff including acting immediately upon contact by the Authority to remove offending material from the Registry;
c. Updated advice and support has been provided by the Controller for employees handling personal data;
d. The Controller has updated relevant systems.

7. However, the Authority also took into account certain aggravating factors, including:

a. That the Controller showed insufficient appreciation of the significance of some of the problems arising from the processing of personal data which were the subject of the investigation and tended to minimise the significant effect the processing had on a vulnerable minor;
b. That whilst the Controller cooperated with the Authority and removed the data relating to Breach 1 at the Authority's request, it was subsequently uploaded again on two further occasions whilst still containing insufficient redaction.

8. Given the formal breach determination, the Authority must consider whether it is appropriate to impose a formal sanction and, if so, decide what is the appropriate sanction in these particular circumstances. In other circumstances the Authority would have considered the imposition of a significant fine in a case of this gravity. However the Authority Law sets out that the Authority cannot issue administrative fines against public authorities and so the only sanctions available for consideration are the issuing of a formal reprimand and/or the making of certain orders designed to bring processing in-line with the DPJL 2018.

9. Accordingly, by written notice to the Controller the Authority has imposed a formal reprimand and made a number of orders pursuant to 25(3) of the Authority Law regarding the updating of its systems and policies, education for staff and providing notification to the affected data subject.

Legal Framework

10. This is a public statement made by the Authority pursuant to Art.14 of the Authority Law following an Investigation by the Authority and following receipt of a complaint regarding the Controller's processing of certain personal data. Individuals can make a formal complaint under Art.19 of the Authority Law if they think that a controller has contravened the DPJL 2018 and it involves or affects their rights.

11. The Authority may investigate a complaint and once an investigation has been completed, Art.23 of the Authority Law requires the Authority to make a Proposed Determination as to whether a data controller has contravened the DPJL 2018.

12. If the Authority determines that there has been a contravention, it must then go on to consider what sanction should be imposed against the data controller, if any.

13. 25 of the Authority Law sets out the various sanctions that are available to the Authority following a Proposed Determination and, having considered all relevant facts (including representations made by the Controller), the Authority has considered that this matter is most appropriately disposed of by way of a formal reprimand and the imposition of an order that affected data subjects must be notified of the breaches of system integrity for which the Controller was responsible. (Administrative fines may not be levied against public authorities and so this form of sanction was not available in this particular case.)

14. 32 of the Authority Law allows an affected party a right of appeal to the Royal Court of Jersey. Any such appeal must be made within 28 days.

    19 October 2020