DATA PROTECTION AUTHORITY (JERSEY) LAW 2018

PUBLIC STATEMENT

Data Controller: Children's Service

1. The Data Protection Authority for the Bailiwick of Jersey (the "**Authority**") has determined that the Children's Services Department, Government of Jersey (the "**Controller**") has contravened Art.8(1)(f) and Art.20(1) of the Data Protection (Jersey) Law 2018 (the "**DPJL 2018**") in that on two occasions it failed to comply with the integrity and confidentiality principle and ensure that they had appropriate technological and organisational measures in place to ensure the security of the data it processes ("**Contraventions 1**" and "**Contravention 2**"), and also that it failed to notify the Authority of a personal data breach in the requisite timeframe ("**Contravention 3**") (together, the "**Contraventions**").

2. Following an Inquiry commenced in November 2020 pursuant to Art.21 of the Data Protection Authority (Jersey) Law 2018 (the "**Authority Law**"), the Authority has determined that the Controller was responsible for the relevant Contraventions, as follows:

   a. Contravention 1: This incident occurred during a Child Protection Conference meeting that was being conducted using Star Leaf (an online video conferencing software). Parties to the meeting included representatives from the States of Jersey Police, the child's Head Teacher, a Social Worker and the parents of the child involved. Certain family members were present with the Social Worker in a room at Liberty House while certain other family members dialled in to the conference from home. Several parties to the call had difficulties with accessing sound during the meeting (they could hear the call but could not be heard) including the Social Worker. The Social Worker left the room on a few occasions to attempt to resolve the sound issues, leaving certain family members unattended in the room but still joined to the call. Part of the Child Protection Meeting was intended to discuss certain sensitive matters in the absence of the child's family members. Unfortunately, certain family members remained connected to the call when they should not have been and, accordingly, certain sensitive information was discussed and therefore disclosed to certain attendees that they should not have been party to. Following the call, that information was disclosed to unconnected third parties and the information was also published on a social media site (albeit in anonymised format). It was the responsibility of the Controller to ensure that the meeting was properly managed and that certain participants were only on the call for the parts relevant to them and excluded/disconnected for other parts.

The meeting took place on the 13th of November 2020, the breach was detected when it occurred at 17:18 hrs.

b. Contravention 2: A complaint regarding the Child Protection Meeting was made by the Paternal family to the Controller. Details of this complaint was disclosed to an unintended recipient via email on the 14th of November 2020 (CAS-02847).

This breach occurred on the 14th of November 2020 at 08:55 and was detected on 15th of November 2020 at 08:57 hrs.

c. Contravention 3: Contravention 1 ought to have been reported to the Authority by 17:18 hrs on 16th November 2020 but was not reported until 20:12 hrs on 19th November 2020 and Contravention 2 ought technically to have been reported to the Authority by 08:57 hrs on 19th November 2020, but was not reported until 09:28 on 19th November 2020.

The Controller advised that there was a delay in reporting Contraventions 1 and 2 due to their focussing on dealing with child protection and safeguarding concerns and this resulted in a delay in communication of matters to the DPO.

3. What does the law say?

   a. Contravention 1 and 2: Art.8(1)(f) of the DPJL 2018 sets out that a controller must ensure that personal data is processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures. Both Contraventions 1 and 2 fall within the definition of "personal data breach", which is defined in Art.1 of the DPJL 2018 as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed".

b. Contravention 3: Art.20(1) of the DPJL 2018 sets out the requirements in respect of notification of a personal data breach to the Authority. In the case of a personal data breach, the controller must, without undue delay and where feasible, not later than 72 hours after having become aware of it, notify the personal data breach in writing to the Authority in the manner required by the Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

4. Special category data (including criminal intelligence) 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, 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 likely considered imposing a fine in these circumstances.

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

In respect of the Contraventions generally:

a. The Controller maintained open and candid correspondence with the Authority whilst enquiries took place and made early admissions, and liaised directly with the affected parties;

b. Complete cooperation by the Controller's staff with the Authority's inquiry.

In respect of Contravention 1

c. It took appropriate remedial steps once alerted to the breach, including.
i. A thorough investigation into the incidents.
ii. Identifying areas for improvement including; bespoke data protection training providing scenario situations and steps to deal with such situations be developed and rolled out across the Children's Service.
iii. Making series of recommendations to develop and implement a training programme for new technology.
iv. Managers to provide one-to-one or group meetings detailing the need to remove distribution email addresses; ensure work devices are the only devices used to send work emails and information; and the process for breach reporting.

v. Children's Service to develop and provide data flows for their services outlining processes for consistency, expectation, and transparency.
vi. New procedures for disclosing personal data on conference calls or other forms of technology that do not allow visibility of all the recipients.
d. The Controller has also updated processes for using Star Leaf (an online video conferencing software) and provided refresher training to relevant staff.

In respect of Contravention 2

e i A change of process has been introduced where only authorised mobile phones will be used to send personal or sensitive information.
ii Introduction of a policy to encrypt all personal and sensitive information before sending it via email, even internally.

In respect of Contravention 3

f i Staff have been reminded of the importance of reporting a breach to the JOIC within 72 hours of it being detected.

6. There are no aggravating factors.

7. Considering the above factors, the Authority has, by written notice to the Controller, imposed a formal reprimand and made a number of orders pursuant to Art.25(3) of the Authority Law regarding updating of its internal processes regarding the use of Star Leaf platform and appropriate education

for staff.

Legal Framework

8. This is a public statement made by the Authority pursuant to Art.14 of the Authority Law following an Inquiry by the Authority and following receipt of a Self-Reported Data Breach Report ("**SRDB**") received from the Controller regarding their processing of certain personal data.

9. The Authority may carry out an Inquiry following a SRDB and once an Inquiry has been completed, Art.24 of the Authority Law requires the Authority to make a Determination as to whether a Controller has contravened the DPJL 2018.

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

11. Art. 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. Administrative fines may not be levied against public authorities.

12. Art. 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.