DATA PROTECTION AUTHORITY (JERSEY) LAW 2018

PUBLIC STATEMENT

Data Controller: CSS Limited

1. This is a public statement made by the Data Protection Authority for the Bailiwick of Jersey (the "**Authority**") pursuant to Art.14 of the Data Protection Authority (Jersey) Law 2018.

2. Specifically, the Authority has determined that CSS Limited (the "**CSS**") suffered from three separate breaches:
    a. Loss of availability to systems caused by the GandCrab virus (August 2018);
    b. Access to CSS systems by external third parties (November 2018); and
    c. Loss of system integrity (January - May 2019).

3. The access to CSS systems was particularly significant, as it constituted an attack from a hostile external third party and led to the CSS systems being compromised. This included a loss of information about data subjects including identity information, travel itineraries, family information and employment documentation.

4. CSS failed to respond appropriately to this unauthorised access because its staff lacked proper knowledge and understanding of the DPJL 2018 meaning that it was unable to:
    a. identify the unauthorised access as a "personal data breach" (including failure to appoint/engage the services of appropriate service providers to help it investigate the alleged breach, even after being told by its processor that it did not have the relevant knowledge or expertise to investigate);
    b. appreciate the significance of the breach or understand the potential impact the breach could have on the data subjects whose information was compromised; or
    c. realise that it needed to notify the Authority, or notify any data subjects at the relevant time and as it ought to have done in these particular circumstances.

5. Following a thorough investigation, the Authority has determined that CSS has contravened Art.8(1)(f) of the Data Protection (Jersey) Law 2018 (the "**DPJL 2018**") in that it:
    a. failed to implement appropriate technological and organisational measures in place to ensure the security of the data it processes and to prevent unauthorised access to that information, including: failure to have adequate firewalls in place, a failure to properly train staff in data protection, and a failure to exercise due diligence in the selection and monitoring of its IT provider.

b. failed to respond appropriately once it was aware of a personal data breach; and
c. failed to notify the Authority and relevant data subjects of a personal data breach.

1. The Authority took a number of factors into account when considering the appropriate way of dealing with this matter. This included the following mitigating factors in CSS's favour:
    a. Full and frank admissions made by CSS as to the nature of the breaches and how they occurred;
    b. Complete cooperation by CSS staff, including allowing access to premises on an investigation day and cooperating fully with the Authority's staff (including the Authority's external information security expert);
    c. Whilst there was some delay in CSS taking steps to mitigate the impact of the breaches (particularly the unauthorised access) it is clear that this was caused, in part, by advice provided to CSS by its then IT provider and conflicting and unclear advice as to whether CSS had been breached;
    d. Taking significant steps to update its IT systems, including replacement of its previous IT provider;
    e. Providing updated data protection training for all CSS employees (including its designated Data Protection Officer).

2. Taking into account all relevant circumstances, including the available mitigating factors, the Authority has, by final written notice to CSS dated 8 January 2020, made a number of orders pursuant to Art.25(3) of the Authority Law. These orders relate to:
    a. the updating of CSS's systems;
    b. education of its staff; and
    c. notifying certain affected data subjects.

3. CSS will also remain under supervision by the Information Commissioner until the end of May 2020 to ensure that CSS bring its processing activities within the scope of the DPJL 2018 and will be subject to a final review at the end of that period by the Authority's external information security expert.

Procedural Steps

1. Once an investigation has been completed, Art.23 of the Authority Law requires the Authority to make a determination as to whether a data controller has contravened the DPJL 2018.
2. 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.
3. As it is obliged to do, the Authority wrote to CSS with a draft determination setting out its findings and advising of the order the Authority was considering imposing. A draft Public Statement was also provided. CSS was given 28 days to make representations on the drafts.

4. 25 of the Authority Law sets out the range of sanctions that are available to the Authority following a determination and, having considered all relevant facts (including the report provided by the Authority's external information security expert and the mitigation available to CSS), the Authority has considered that this matter is most appropriately disposed of by way of various orders referred to above.
5. The Final Determination was issued to CSS on 8 January 2020. 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.

28 January 2020