Admin Report - Annex

Breach Report - North Somerset data breach 20/9/2019

Over view of what happened:

- 71 annual benefit statements (ABS's) containing Name, Address, Employer, email address, partnership status, Pensionable pay and Final Salary Pay information with projected Pension calculations were posted out containing a partially incorrect address.
- The postcode and the main body of the address is correct, but first line and postcode will not match.
- 15 ABS's have been returned via Royal Mail to APF. A total of 56 are unaccounted for although no pension members or members of the public have contacted APF about receiving an incorrectly addressed letter.

How did the breach occur?

North Somerset Council's (NSC) i-Connect data extract for the period April 2019 was uploaded by APF on 7/6/19. Employers normally load their own data directly in to Altair using i-Connect, however APF were still loading NSC's data files as part of the implementation process of on-boarding a new employer to i-Connect (they went live in February 2019). The address error occurred in the April file provided to the fund by NSC. NSC had applied a manual filter to the data extract to populate address line 2. This was a mandatory field in the IC extract (but not in NSC's payroll system i-trent). The filter was not used correctly and caused a data error and incorrectly updated the 1st line of the address for 71 members. The data for North Somerset's Annual Benefit Statements was extracted on 22/07/19 while the addresses were still incorrect. The addresses were subsequently corrected on the May data extract that was loaded on 23/7/19.

The breach was discovered following the return of a higher than normal amount of ABS's which lead to an internal investigation. On 20th September 2019 APF reported this as a GDPR breach to Information Governance and after further investigation it was reported to the ICO on 27 September 2019.

Action by APF following the breach

As a result of the beach APF have carried out a review of the way data is loaded on to the Altair database by employers and the checks and controls the fund has in place to monitor data. These checks and process have now been deemed inadequate and allowing employers to load data directly on to Altair without a high level of checks and fund approval is too high risk. Therefore, wef 4th October 2019 APF have decided to take the loading of all employer i-Connect data in-house and have changed the way the data is internally controlled, checked and monitored. New data tools have been created to compare the data and review it for possible errors. A new sign off process is in place that requires the employer to declare the data is accurate plus an internal sign off process within APF before the data is loaded to confirm all checks have been carried out.

Other actions now in place:

- Review meeting with North Somerset and Liberata (payroll) to discuss the data error and how they create their data file
- Meeting with Financial Systems to review current controls and monitoring
- GDPR training for APF Administration on 27 November 2019
- All staff to re take APF online training and evaluation before 27 November 2019

Response from ICO

On 13 November 2019 the ICO responded to the data breach to confirm not further action is required based on the action we have already implemented. Other recommendations were made as follows:

- Communicate amongst staff the importance of data security and reiterate the significance of being robust regarding their use, dissemination and storage of personal data;
- Review the content of your data protection training and also the frequency of your refresher training to ensure that sufficient practical guidance is given to staff in how to comply with the GDPR and the DPA 2018. Also consider your methods of control, delivery and monitoring of such training and of ensuring staff who deal with personal data complete this. This training should also be tailored to specific roles. The ICO recommends, as good practice, that refresher training is carried out annually. However, the ICO also recognises that some organisations may be restricted by available resources but would recommend that, in such cases, refresher training does not exceed two years;

All recommendations from the ICO have been implemented.

Claire Newbery 18/11/19