Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Data Protection Act 1998
Undertaking follow-up

Student Loans Company
ICO Reference: ENF0462460 & ENF0467127

On 22 October 2014 the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Student Loans Company (SLC) in relation to the undertaking it signed on 24 April 2014.

The objective of the follow-up is to provide the ICO with a level of assurance that the agreed undertaking requirements have been appropriately implemented. We believe that appropriate implementation of the undertaking requirements will mitigate the identified risks and support compliance with the Data Protection Act 1998 (the DPA).

The follow-up assessment consisted of a desk based review of the documentary evidence SLC supplied to demonstrate the action it had taken in respect of the undertaking requirements. This included:

- An Internal Audit briefing note dated 24 April 2014.
- Internal Audit key controls questionnaire documentation and collated responses of the Assurance Framework section of the January 2014 exercise.
- A sample report detailing QA team results, covering January to August 2014.
- Documentation relating to data protection training, including:
    - The relevant information from the data protection eLearning module that staff are required to complete;
    - A template performance development plan listing mandatory compliance training; and
    - A compliance training report produced July 2014.
- A sample of team bulletins covering DPA issues.
- Systems logs showing changes to databases to aid in reducing/eliminating data protection errors.

The review demonstrated that SLC has taken appropriate steps and put plans in place to address the requirements of the undertaking and to mitigate the risks highlighted.

In particular SLC confirmed that it has taken the following steps:

- A review has been carried out by SLC's Internal Audit department in 2014 to provide assurance of the effectiveness of the procedures concerning the handling of correspondence containing sensitive personal data. This review focused on the team identified as the source of the reported data breaches.
- A process for 'real-time' quality assurance testing on a sample of data being processing has been established and continues to be monitored.
- The annual review of the SLC Data Protection Policy and Guideline has recently been carried out with a revised Policy being approved by the Company Secretary on 03 October 2014. The updated SLC Data Protection Policy and Guideline will be communicated to all staff by 31 October 2014.
- An existing bi-annual questionnaire used by Internal Audit to monitor staff awareness has been amended to include a specific question relating to staff awareness of the corporate Data Protection Policy and Guideline. Staff awareness will be assessed upon receipt of responses to the September 2014 questionnaire.
- Compliance statistics dated 15 July 2014 show that 89% of staff had completed the annual, mandatory, SLC Data Protection eLearning module.
- Workshops have been held to reiterate the impact of DPA breaches and responsibility of the individual to get it right first time.
- System based solutions have been established to provide further assurance that staff are using the correct contact email addresses and to help mitigate the risk of inaccurate contact details being used.
- Processes have been updated to include a DPA checklist to be updated each time certain sensitive personal data is to be sent externally. Further address checking procedures have also been built into the QA process.
- 100% DPA Quality Checks are being completed for an agreed period of time on all staff who have been involved in an actual, or potential, information security breach.
- All instances of DPA breaches, potential breaches and failure to report breaches are recorded against QA results as of 1st September 2014. This information is also recorded centrally and on the individuals' personnel file.

Whilst the ICO has determined that SLC has taken appropriate remedial steps in response to the undertaking we will continue to monitor issues of unauthorised disclosure occurring at SLC.

Date Issued: 30 October 2014

The matters arising in this report are only those that came to our attention during the course of the follow up and are not necessarily a comprehensive statement of all the areas requiring improvement.
The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rests with the management of Student Loans Company.
We take all reasonable care to ensure that our Undertaking follow up report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.