Audit report for medical spas 2014

5. Mar 2015

The audit is part of a cooperation project of the three Baltic countries agreed on at the meeting of Baltic data protection authorities that took place in Vilnius at the start of the previous year. Estonian, Latvian and Lithuanian data protection authorities made the decision to conduct an audit on medical spas operating in all three countries with respect to the performance of requirements of information security established for the protection of personal data. The audit was based on a questionnaire made up of 42 questions drawn up jointly.

Objective of the audit

In Estonia, medical spas were audited from May to November 2014, and the objective of the audit was to inspect whether or not the companies adhere to the principles provided in the Personal Data Protection Act (hereinafter PDPA) in their activities, i.e. whether or not personal data is collected in a legal manner and for the achievement of lawful objectives, whether or not personal data is processed in accordance with the provisions of the Personal Data Protection Act (PDPA), and whether or not personal data is collected to the extent necessary for the achievement of determined objectives.

The audit mainly inspected the following five aspects: how the data was processed (on paper and/or electronically); how the access to data was organised and how the user was identified and authenticated (log in); how the retention (back-up) of data is ensured, what are the retention deadlines, incl. upon log in; whether and how the data is communicated to third persons, incl. other authorities; and how the data is destroyed (deleted) both in case of paper and digital data media.

The audit was carried out by Boris Põldre (member of the Estonian Information Systems Audit Association), Data Security Expert at the Estonian Data Protection Inspectorate (hereinafter EDPI), and Supervisory Senior Inspectors Raavo Palu and Kuldar Võsa. In the course of the audit, the auditors inspected access to information technological environment, logging in to the environment and respective documentation (manuals, regulations and medical certificates) of 12 medical spas situated in Estonia. Among others, they interviewed key persons, monitored work processes and conducted relevant inspection procedures.

Results

Audit was conducted in Kalev Spa, Viiking Spa Hotel, Tervis Medical Spa, Tervise Paradiis Spa Hotel & Water Park, Estonia Medical Spa & Hotel, Tallinn Viimsi Spa, Fra Mare Thalasso Spa, Spa Hotel Laine, Narva-Jõesuu Spa & Sanatorium, Toila Spa Hotel, Pühajärve Spa & Holiday Resort and Health Center & Hotel Wasa.

According to the auditors, all 12 medical spas adhered to the principle of legality in their activity and have appointed a person responsible for the protection of personal data pursuant to subsection 30 (1) of the PDPA and keep a register of data processing, or have registered the processing of sensitive personal data with the Data Protection Inspectorate pursuant to subsection 27 (1) of the PDPA. Upon providing a health care service, personal data was collected only for an intended purpose and to the extent necessary for the achievement of determined purposes pursuant to law. All 12 audited medical spas also met the principles provided in section 6 of the Personal Data Protection Act and performed security measures arising from subsection 25 (2) by adhering to the objective and strategy of information security.

During the inspection, attention was also given to the compliance of information security with technical standards and requirements provided in other legislations, the performance of which is important with respect to the provision of a service, such as requirements for using video surveillance, also the performance of the requirement of confidentiality included in contracts entered into with employees and contractual partners. The results of the inspection allow us to confirm that medical spas largely adhered to the technical standards and requirements established for organisational security.

Summary

Estonian medical spas processed (collect and use) personal data in accordance with the law and only for the achievement of determined purposes, and they did not process the data for any other purpose. Data was processed both on paper and digitally. Paper documents were kept in a locked cabinet or safe in the doctor's office. Granting access to data included in the information system was in accordance with the rights given to users. There was no remote access to data.

The use of anti-virus software also ensured the performance of clause 25 (2) 7) of the Personal Data Protection Act. Data was backed-up regularly. Personal data was not communicated to third persons, including other authorities.

Video surveillance data was issued based on an application as required, for example to the police, and the issuing was recorded on site.

Data was destroyed (deleted) using document and data media destruction service in compliance with international standards; in case of data on paper media, a local paper shredder was also used.

Recommendations

Although the audit did not identify any significant risks or nonconformities to the requirements of subsections 25 (2) and 25 (3) of the PDPA, the Estonian Data Protection Inspectorate draws attention to the fact that information security is a continuous process that requires constant improvement and modernisation, also ensuring that employees are continuously up to date with any changes.

Legal documentation (manuals, regulations, procedures for use) must be kept up to date: revise regularly, amend and supplement existing documents as required. At the same time, the existence of documents and rules with similar content should be avoided.