



AUDIT ON DATA PROTECTION CONCLUDES

Press summary on the audit of the domestic framework of data protection and various priority data registries
(17061)

The State Audit Office of Hungary has concluded its audit of the domestic framework of data protection and various priority data registries for the 2011-2015 period. The SAO concluded that the level of internal regulation of the data processing activity of data controller organisations adequately ensured the protection of national data assets that are part of national assets. The data controllers applied the provisions aimed at secure data management and the outsourcing of data processing appropriately. In respect of the appropriate protection of data, it represented a vulnerability risk that the classification of the electronic systems used for data management according to security class and the classification of the whole of the organisation according to security level was not carried out in line with legal provisions in each case, to which the absence of an official audit also contributed.

National data assets that are part of national assets are made up of data of public interest managed by organisations performing public tasks, personal data and data made public on the grounds of public interest. Ensuring the security of such data assets is essential in the interest of reinforcing the trust of citizens placed in the state and of the continuous and uninterrupted operation of public administration. Through its audit, the SAO promotes the enforcement of 'good governance', contributes to protecting national assets and supports audited entities in complying with increased social expectations aimed at establishing transparency.

During the audit of the 2011-2015 period, the SAO evaluated whether the domestic framework of data protection is appropriately established; and whether the data controller organisations selected for auditing appropriately applied the provisions aimed at secure data management, the outsourcing of data processing and especially the protection of personal data and national data assets. Among registries falling into the category of national data assets, the SAO audited data processing through the activities of six key data controller organisations: the National Tax and Customs Administration (NTCA), the National Health Insurance Fund (NHIF), the Central Administration of National Pension Insurance (CANPI), the Hungarian State Treasury (Treasury), the Educational Authority (EA) and the Central Office for Administrative and Electronic Public Services (COAEPS). The audit also extended to assessing the activities of authorities exercising data protection and data security supervision over data controllers, such as the National Authority for Data Protection and Freedom of Information (NADPFI) and the National Electronic Information Security Authority (NEISA).

The SAO concluded that the level of internal regulation concerning the management, processing and transfer of data at the data controller organisations adequately ensured the protection of national data assets. However, of the supervisory authorities, the NEISA failed to perform its audit tasks set out by law, and the NADPFI failed to fulfil all its obligations related to decision-making and taking actions. The internal regulation of data transfers to third parties was set up by data controller organisations in line with legal regulations. During the performance of tasks, the determination of scopes of responsibility; authorisation, approval and control procedures; access to documents and IT systems and the levels of such access; and reporting and accountability were appropriately regulated in internal control instruments, in line with legal provisions. In practice, the data controller organisations applied the provisions aimed at secure data management, the outsourcing of data processing and the protection of national data assets appropriately and regularly. The transfer of data that are part of national data assets was in each case carried out in line with the given legal mandate and objective, in compliance with the provisions of internal regulations and with the involvement of persons authorised to do so.

At the same time, the SAO audit revealed that in respect of the appropriate protection of data, it represents a vulnerability risk that the security classification of the electronic systems used for data management, as well as the security classification of the whole of the organisation, was either not carried out by the audited data controller organisations in line with legal provisions in each case or they failed to carry out this classification. As a result, the protection measures established are not at the level expected in respect of the managed data assets. In the area in question, the audit lines of defence did not function appropriately either as the deficiencies were not uncovered by the internal audits of the data controller organisations, and furthermore, the official external audits of the NEISA regarding security classifications (to be implemented pursuant to applicable laws) were also absent.

The audit formulated a recommendation addressed to the Presidents of NADPFI, the Treasury and EA, the heads of NEISA and NTCA, the Director General of CANPI and the National Health Insurance Fund (as NHIF's legal successor), as well as the Minister heading the Ministry of the Interior (as the head of the legal successor of COAEPS), in respect of which the above persons must prepare an action plan within 30 days of the receipt of the SAO report.

Further information, press relations:

Bálint Horváth, Head of Department

State Audit Office of Hungary, Department of Communication and Public Relations

Phone: +36 1 484 9145 Mobile: +36 20 238 6939 E-mail: sajto@asz.hu