



Country or jurisdiction report

SLOVENIA

Website: www.ip-rs.si

Major case law

The Personal Data Protection Act defined conditions under which biometric measures are to be allowed. These measures can, if not stipulated in a specific act, be performed only in cases when absolutely necessary to carry out business practices, for safety of people and property or to protect confidential data and business secrets. In such cases biometric measures controllers must provide the supervisory body for the protection of personal data with prior description of the biometric measures planned and the reasons for their introduction. The performing of biometric measures is allowed only after the receipt of the supervisory body's decision granting the performance of biometric measures. A problem however arose as the law failed to stipulate the course of action for those controllers performing biometric measures already prior to the adoption of the new law. With regard to this matter the Information Commissioner argued that also such controllers are obliged to provide the supervisory body with a description of biometric measures and reasons for their introduction, and are allowed to continue using biometric measures only after the receipt of the supervisory body's decision granting biometric measures.

In 2006 the Information Commissioner issued a total of nine decisions regarding the execution of biometric measures, four of which to private legal persons and five to public legal persons, all from areas of banking, healthcare and telecommunications.

In 2006 the Commissioner issued several decisions widely publicized by the national media:

1. A decision on minor offence of a clothing retail company, which carried out video surveillance of working premises in its department store, specifically in changing rooms, thus violating the provisions of Personal Data Protection Act, prohibiting video surveillance in changing rooms, elevators and rest rooms. The supervision established that video tapes were stored, access to video surveillance system inadequately protected, while at the same time no traceability of data-recording to removable media was ensured. The Commissioner ordered the offender to immediately cease performing video surveillance in changing rooms, with which the latter promptly complied. Additionally, the Commissioner issued a fine as a result of breaching of lawful provisions, as the offender committed a grave infringement on privacy and dignity of persons using

the changing rooms in question, thus also violating their constitutional rights to personal dignity, safety and privacy.

2. A decision on minor offence of a publishing company, which in its weekly newspaper published names of a competitive company's 86 employees receiving highest net and gross salaries, thus illegally using, processing and presenting to public the personal data of 86 employees, even though it had neither a statutory basis nor the individual's personal consent to process such data. The case in question entailed processing of personal data of private sector employees, regulated in further detail by the Labour Relations Act¹.
3. A decision on minor offence of a newspaper for publishing autopsy reports on three minors succumbing to injuries in a night club crush incident. As in the previous case the offender appealed to freedom of expression as well as to public interest. The stated could however not be the legal basis for the processing of personal data in the private sector, especially processing of sensitive medical personal data including data of the deceased, specifically defined in the PDPA's provisions. Additionally the processing of personal data was not carried out in accordance with the collection's original purpose. The autopsy reports were namely initially intended for use in the criminal proceedings against the night-club owner and not for the publication in public media.

The Information Commissioner also examined legality of personal data processing in clinical drug-testing trials, the method of protecting patient personal data and methods of access to such data. With regard to collecting prior individual written patient's statement of consent for participation in medical trials, no irregularities were established. It was however uncovered that no catalogues of personal data filing systems containing data relating to clinical trials were made, additionally that no records on viewing access to medical records archives were kept, and also that traceability was not ensured. During the inspection supervision, the medical institution raised a question as to the state supervisor's competency in the debated case. The latter should, according to medical experts, need to obtain, prior to examining any personal data, the patient's explicit consent. Medical experts also argued that by providing the state supervisors with requested documentation, the doctors would violate the code of medical deontology and thus endanger the doctor-patient confidentiality. For the stated reason the medical institution refused to allow review and delivery of the patients' written statements of consent and moved to stay the proceedings, in spite of unequivocal meaning of statutory provisions (Articles 2 and 8 of the Information Commissioner Act and Articles 51 and 52 of the PDPA), that supervision over protection of personal data and over implementation of provisions of PDPA and other regulations governing protection or processing of personal data, lies in exclusive competency of the Information Commissioner as the national authority for data protection.

In 2006 the Information Commissioner lodged two requests for judicial review:

1. Judicial review of paragraphs 7 and 8 of Article 128 of the Aviation Act², regulating the movement of persons on premises of the public airport as well as on premises of the air-traffic control service. In the Commissioner's view the challenged provision is

¹ Official Gazette of the RS, No. 42/2002, 79/2006.

² Official Gazette of the RS, No. 18/2001, 110/2002, 49/2006, 79/2006.

inconsistent with Articles 2, 15 and 38 of the Constitution and Article 8 of the European Convention on Human Rights; the Commissioner therefore moved for its annulment and until the Constitutional Court's final judgement the stay of its execution.

2. Judicial review of paragraph 1 of Article 96, paragraph 2 of Article 98, Article 100, paragraphs 5 and 6 of Article 103 and paragraph 1 of Article 114 of the Real-Estate Recording Act³, which among else regulates real-estate recording, real-estate register, issuing of data and other real-estate related questions. The Act's challenged provisions stipulates the collection of several personal data, however failing to provide a clear purpose for such collection, leaving it inaccurate, too broad and vaguely defined. Without a statutorily defined purpose of collection it is impossible to define the type and number of personal data needed for processing.

Major specific issues

The Personal Data Protection Act specifies in considerable detail the conditions under which video surveillance of entries to business premises, apartment buildings and working areas can be allowed. In accordance with these provisions the persons executing video surveillance do not need to obtain permission of the Supervisory body to establish video surveillance. The persons executing video surveillance are only required to align their implementation of video surveillance with the provisions of the law, that is, to adopt a decision on video surveillance execution, publish an appropriate notice, inform its employees in writing, obtain the consent of apartment buildings co-owners, consult the syndicates, etc. Most of the video surveillance controllers however failed to adjust their practice with the provisions of the law which led to a large number of appeals filed with the supervisory body.

Several inconsistencies were caused also by provisions relating to contractual processing of personal data. Experience showed that contracts concluded between personal data controllers and contractual processors are often inadequate, as they lack a specific definition of the contractual processor's competencies. These contracts also inadequately specify procedures and measures to protect personal data when in the hands of the contractual processor.

One of the persisting key problems in the area of personal data can also be discerned from the fact that most of the personal data controllers have yet to notify the supervisory body with a description of their personal data filing systems and enter them into the register of filing systems managed by the supervisory body. The register of filing systems is published on the Information Commissioner's web page and allows everyone to review in a simple manner information on filing systems controllers in the Republic of Slovenia, information on filing systems managed by the individual controllers, types of personal data contained in individual filing systems, the purpose of processing, etc.

In 2006 the state supervisors for the protection of personal data (as of April 2006, there are seven supervisors employed with the Commissioner) carried out 231 supervisions, of which 87 in public and 143 in private sector.

³ Official Gazette of the RS, No. 47/2006.