Prepared by AmCham member

Data protection in healthcare

bnt
attorneys-at-law

With the passage of the new Act on Personal Data Protection, entrepreneurs should become more aware of personal data security. This topic concerns all subjects processing personal data of natural persons. One group of subjects to which this act applies is health care providers.

Under the new law, a controller is every person that alone or together with another person(s) specifies the purpose and conditions of personal data processing and that processes personal data on their own behalf. This means that any hospital or any private doctor that specifies a purpose for processing the personal data of a natural person, the "individual concerned", and processes data on their own behalf is considered a controller and is responsible for personal data processing.

The purpose of processing is mainly the personnel and wage agenda of hospital staff, patient records (medical records) or records of their family members, monitoring public spaces by CCTV, personal data processing for drugstore operation, etc. Personal data of natural persons are processed in what are called information systems (IS) that have to be labeled by the controller. Hospitals usually have several information systems for processing personal data for specific purposes, such as IS personnel and wage agenda, IS job applicants, IS CCTV, IS patients, IS drugstore, IS library, IS marketing.

Who are a processor and a sub-processor?

If the health care provider does not process personal data itself but, for example, through an external entity, it has to enter into a written agreement with that entity. Under the agreement, the controller is partly freed from responsibility for personal data processing since the processor has to follow the same rules as the controller. Under the new legislation, the processor can enter into an agreement with a third party that will process personal data, called a sub-processor. The processor is directly responsible for fulfilling obligations by the sub-processor. A practical example: a company owns a hospital with a drugstore, leases the drugstore to a pharmaceutical company which then enters into an agreement with a local entrepreneur for the operation of the drugstore. From the legal point of view the controller (hospital) is freed from responsibility for personal data protection by entering into an agreement with a processor (pharmaceutical company). This processor then authorizes a sub-processor (local entrepreneur) but remains responsible for fulfilling its obligations.

Legal basis for personal data processing

The new act explicitly states that a controller can process personal data only for specific legal reasons, or with consent of the individual concerned. In the case of health care facilities, the health care provider processes personal data mainly based on special provisions (Act No. 576/2004 Coll., Act No. 355/2007 Coll.), where the consent of the individual concerned is not required, or based on consent of the individual concerned. The direct legal basis for monitoring hospital space is the Act on Personal Data Protection where the space has to be clearly marked as monitored and CCTV data is considered sensitive data under special provision.

New obligations of hospitals and doctors as controllers

The controller, i.e., the doctor or the hospital, has several obligations. The controller must inform the individuals concerned before starting to process their personal data, about the data of the controller, the processor, the purpose and extent of the data, especially that the provision of data is optional, and the details of their rights (here a mere reference to legal provisions is not sufficient). The controller is also obliged to keep records about instructions to the individuals concerned about their rights and obligations during the processing of personal data. The existence of these notifications (several pages long) has to be proven to the Personal Data Protection Authority ("Authority").

The controller is also responsible for personal data security and has to adopt sufficient security measures. Depending on if personal data is processed in writing or on a computer with or without internet access, the controller has to draft a safety regulation or a safety project.

Does the hospital or doctor have to authorize a responsible person?

Under previous legislation, if an employer had more than five employees then a responsible person had to be authorized to supervise protection of personal data. Under the new act, the controller is only obliged to authorize a responsible person if more than 20 authorized people process personal data. An authorized person is a person who processes personal data for the controller and is in a legal relationship with the controller. This means that if more than 20 doctors and nurses who are in a legal relationship with the hospital process personal patient data, then the hospital is obliged to authorize a responsible person. The responsible person has to pass an exam before the Authority and also fulfill other legal requirements. Authorization of a responsible person has to be declared to the Authority. Authorizations under previous legislation remain valid until 30 June 2014 at the latest. If a controller is not obliged to authorize a responsible person, they have to register their information systems with the Authority (unless exempted by law).

Fees, sanctions and compliance

A doctor who, as health care provider, does not need to authorize a responsible person but processes personal data on a computer has to register with the Authority all IS where the doctor processes personal data with the consent of the individual concerned. The statutory fee is EUR 20 or EUR 50. The new sanctions for violating the rules are relatively high and are mandatory. The Authority must impose a penalty of up to EUR 300,000. Depending on the specific obligation, individual obligations must be harmonized with the new act during a temporary period from six to twelve months of the law coming into effect.

Zuzana Chudáčková
Partner, Attorney,
bnt attorneys-at-law

Katarína Babiaková,
Attorney,
bnt attorneys-at-law