Dr Artur Romaszewski
Jagiellonian University Medical College
Faculty of Health Sciences
Department of Medical Information Systems
Dr hab. Wojciech Trąbka
Jagiellonian University Medical College
Faculty of Health Sciences
Department of Medical Information Systems

Administrator of Information Security in health care entities

When analyzing the new Polish regulations of the Act[1] and the EU regulations on the processing of personal data in EU proposed for 2016 , it seems that the necessity emerged to appoint an Administrator of Information Security (AIS) in the majority of health care entities and in the IT system of the health care system.

The article presents the most important issues concerning the functioning and of AIS, the requirements, the necessity to register and the responsibilities.

The Polish regulations apply the term *Administrator of Information Security* (*AIS*), while the proposed EU regulation[2] uses the term *Data Protection Officer*.

The administrator of information security, who may be a full time employee of the data controller, should be able to perform the duties independently and should be specially protected against the removal from the function. The final responsibility should lie on the management of the entity.

AIS can be consulted particularly prior to designing, ordering, developing and implementing the systems of automatic personal data processing in order to ensure their compliance with the principles of privacy protection and the privacy by default already at the stage of design.

---

[1] Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 1997, No. 133, item 883

[2] Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

In the cases when the controller or processor is a public entity, AIS can be appointed for several organizational units of the entity with the consideration of its organizational structure.

Requirements regarding AIS and the qualifications

The Polish regulations define the requirements as regards AIS. It can be a natural person that

- has full capacity to perform legal acts and enjoys full public rights;
- has relevant knowledge in the field of personal data protection;
- has not been punished for intentional offence[3].

The requirements provided for the EU regulation are stricter. The Data Protection Officer should have at least;

- extensive knowledge of the substance and application of data protection law, including technical and organizational measures and procedures;
- mastery of technical requirements for privacy by design, privacy by default and data security;
- industry-specific knowledge in accordance with the size of the controller or processor and the sensitivity of the data to be processed;
- the ability to carry out inspections, consultation, documentation, and log file analysis; and the ability to work with employee representation.

The controller should enable the data protection officer to take part in advanced training measures to maintain the specialized knowledge required to perform his or her duties. The designation as a data protection officer does not necessarily require fulltime occupation of the respective employee[4].

Pursuant to the regulations of the act on personal protection AIS reports directly to the head of the organizational entity or to a natural person who is the data controller.

---

[3] Art. 36a5 Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 1997, No. 133, item 883

[4] 75 a Amendment 50, European Parliament legislative resolution of 12 March 2014 Recital 75 a on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

The data controller ensures the measures and organizational autonomy of AIS that are indispensable for an independent performance of his/her duties. The regulations do not prohibit the use of specialized external entities to perform the duties of AIS.

It is prerequisite for a correct emplacement in a health care entity that within 30 days after the appointment AIS should be notified to registration by GIODO (the Inspector General for Personal Data Protection). The data to be included in the notification are clearly defined[5]

1. specification of the controller (i.e. of the entity that runs the *register* of personal data),
2. data regarding AIS (name and surname; PESEL identification number or if the number has not been granted, name and number of document stating identity),
3. AIS appointment date,
4. AIS's statement on fulfilling the requirements of the full legal capacity, the possession of appropriate knowledge on personal data protection and being not punished for intentional crime.

GIODO may issue a decision on striking off the AIS from the register in the cases when:

- the AIS does not meet the requirements specified by the statement (or when his/her deputies do not meet the requirements);
- the AIS does not perform his/her tasks.

The dismissal of AIS should be notified to registration also within 30 days after the emergence of circumstances that resulted in the dismissal. AIS should also be dismissed when he/she ceases to fulfill the requirement of clean criminal record or has been deprived of public rights.

The title of *Administrator of Information Security* should be restricted only to AIS who are submitted to the register. Thus, a person who is temporarily in charge of personal data protection and is not submitted to the GIODO register should not be referred to as AIS but – for example - as a personal data protection specialist[6] .

[5] Regulation of 10 December 2014 of the Ministry of Administration and Digitization on notification sample forms regarding appointments and dismissals of AIS, Journal of Laws 2014, item 1934

[6] CO Z TYM ABI? T.Osiej, M Bargiel –portal e-ochrona.danych.pl http://www.e-ochronadanych.pl/artykuly.php?news_id=2426

Responsibilities of AIS

The AIS's responsibilities include mainly the tasks presented in Fig 1:

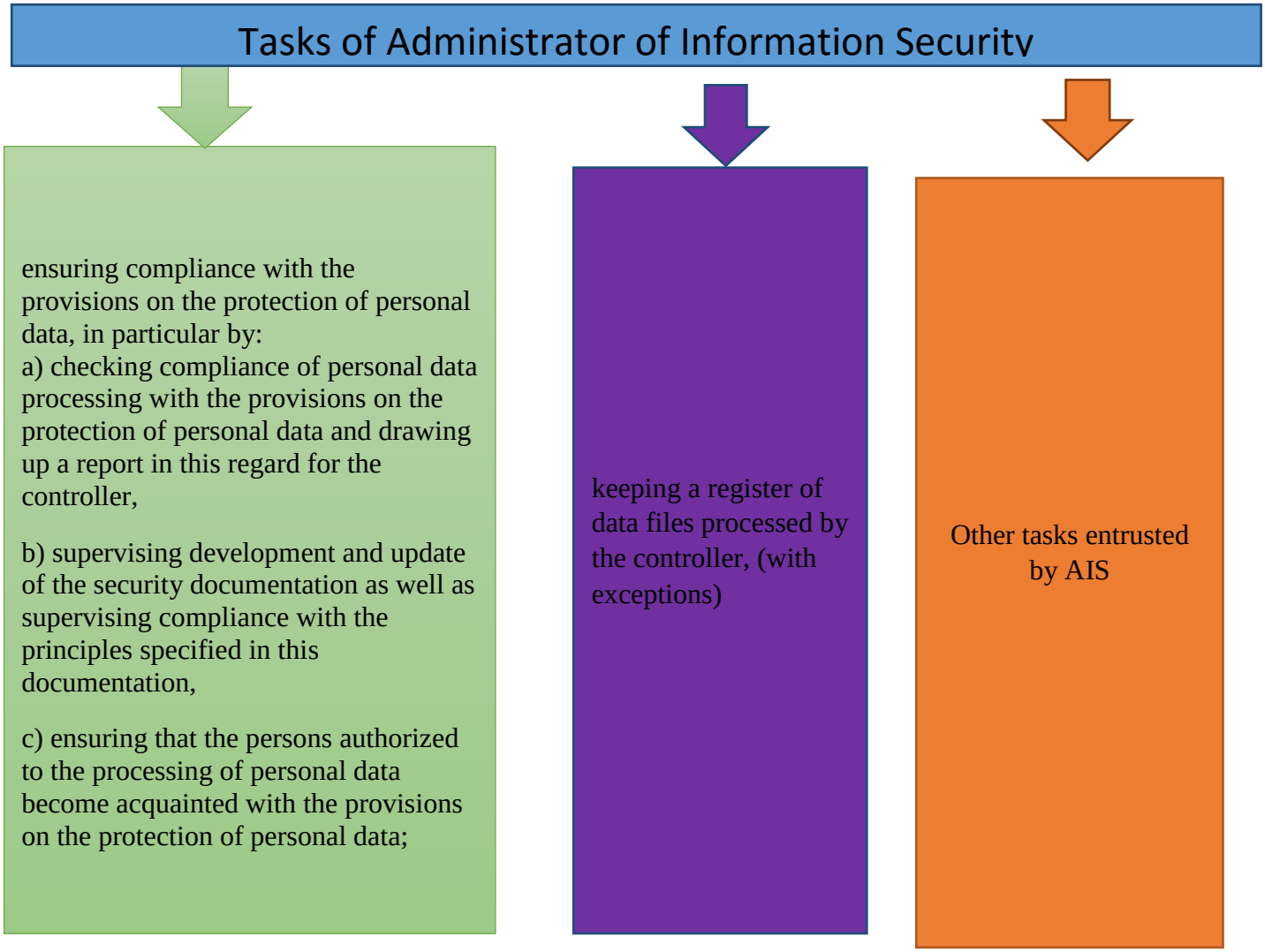

Figure 1. The tasks of Administrator of Information Security.

Source: Authors research

The checking procedure plays a significant role[7]; the Check includes activities that aim at the verification of the compliance of personal data processing with the provisions on personal data protection [8,] (Figure 2)

[7] based on art. 16a and 36a par.2 point 1 of the Act on personal data protection

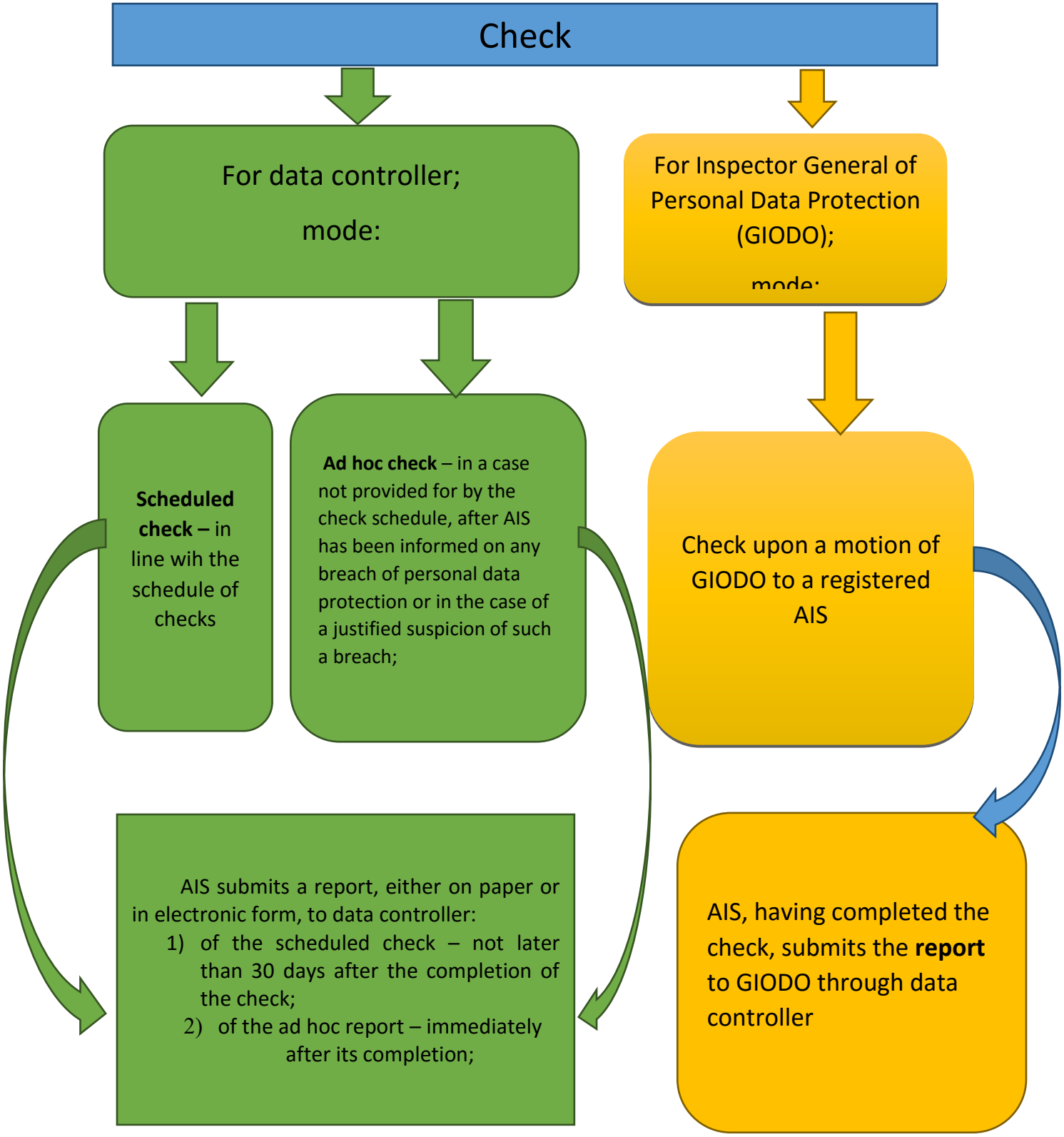

Figure 2. Diagram of various options of the checking procedure conducted by AIS

[8] Draft regulation of 4 March 2015 of the Ministry of Administration and Digitization on procedures to ensure compliance of provisions on personal data protection by data controllers , http://legislacja.rcl.gov.pl/projekt/268582/katalog/268589#268589

In the check schedule, the AIS takes into account particularly:

- personal data files and the IT systems for processing the data
- the necessity to verify the compliance of data processing with the provisions of the Act.

The check schedule is prepared by AIS for a period not shorter than a quarter and not longer than a year. The schedule is submitted to the data controller not later than one month before the commencement of the period in question. The check schedule covers at least one check

The data files and IT systems for processing or protecting personal data should be subject to the check at least once every two years.

An ad hoc check is conducted immediately after AIS has been informed on any breach of personal data protection or in the case of a justified suspicion of such a breach. AIS notifies the data controller about the commencement of the ad hoc check before undertaking the first step of the check. After the completion of the check, AIS makes a report.

One of the most important responsibilities of AIS is to supervise the data processing documentation (Table 1). When supervising the data processing documentation, AIS verifies the security documentation and takes necessary measures after revealing any breach (Figure 3)

AIS responsibilities as regards the supervision of security documentation
1) verification of completeness of the data processing documentation;
2) assessment of the compliance of the data processing documentation with the provisions of law;
3) analysis of the actual state of personal data processing;
4 assessment of the conformity of actual processing to the technical and organizational measures against the risks to personal data protection as specified by documentation;
5) assessment of the compliance of rules and responsibilities specified in the data processing documentation

Table 1. The responsibilities of AIS as regards the supervision of security documentation.

Source: Authors' research based on a draft regulation of the Ministry of Administration and Digitization on procedures and methods of implementing measures to ensure the observance of the regulations on personal data protection by Administrator of Information Security (10.04.2015)

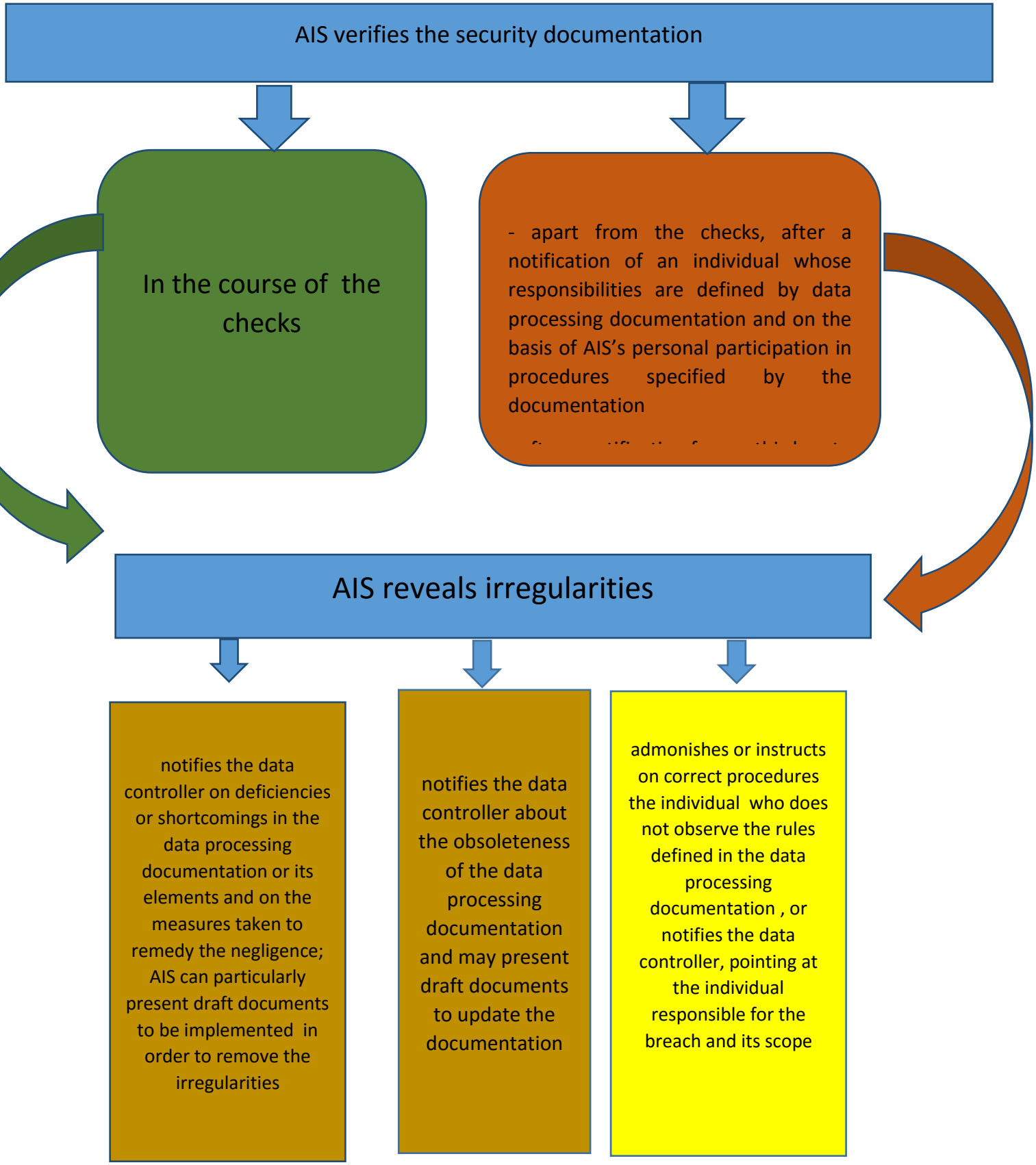
AIS verifies the security documentation
In the course of the checks
- apart from the checks, after a notification of an individual whose responsibilities are defined by data processing documentation and on the basis of AIS's personal participation in procedures specified by the documentation
AIS reveals irregularities
notifies the data controller on deficiencies or shortcomings in the data processing documentation or its elements and on the measures taken to remedy the negligence; AIS can particularly present draft documents to be implemented in order to remove the irregularities
notifies the data controller about the obsoleteness of the data processing documentation and may present draft documents to update the documentation
admonishes or instructs on correct procedures the individual who does not observe the rules defined in the data processing documentation , or notifies the data controller, pointing at the individual responsible for the breach and its scope

Figure 3. The AIS's supervision over data processing documentation

Source: Authors' research based on a the Regulation of 11 May 2015 of the Ministry of Administration and Digitization on procedures and methods of implementing measures to ensure the observance of the regulations on personal data protection

Personal data register as an alternative to the registers of the Inspector General

With the consideration of signals concerning the work on EU regulations, certain less strict provisions have been implemented as regards the notification of data files to registration by the Inspector General (GIODO). The principle has been implemented that if the processor has appointed an AIS, all personal data files to be processed in files that are not digitized and are paper-based, are not subject to the obligation of registration[9].

The registration is not obligatory in the case of personal data files, including the ones that are processed electronically, for controllers who have appointed AISs and notified the fact to registration by the Inspector General .[10]

However, the obligation to register sensitive data and the right to process the data after the decision of the registration has been made, has remained unchanged .

The obligation of file registration has been replaced by the AIS's obligation to conduct a data file register[11]. The data register consists of a list of data files that includes information separately for each file. The register may be in paper or electronic form.

When the register is in an electronic form, it is shared by AIS:

- on the controller's website; the homepage includes a link directly to the register or
- at the access point of the controller's IT system, located in the controller's office or place of residence,
- through a printout of the register from the controller's IT system.

When the register is run in a paper form, AIS shares the data for browsing in the office or the place of residence to anyone interested .

[9] Art. 43 par.1 point 12 , Act of 29 August, 1997 on the protection of personal data (Journal of Laws of 1997, No. 133, item 883)

[10] Art. 43 par.1a , Act of 29 August, 1997 on the protection of personal data (Journal of Laws of 1997, No. 133, item 883)

[11] Stowarzyszeni Administratorów Bezpieczeństwa Informacji **KALENDARIUM NOWELIZACJI USTAWY O OCHRONIE DANYCH OSOBOWYCH - USTAWA DEREGULACYJNA** http://www.sabi.org.pl/page8.php

Within the framework of running the register, the AIS

1. enters the data file to the register prior to processing,
2. updates the information regarding the data file in the register – in the case of the changes in the information entered;
3. erases the data file from the register – in the case when the processing of the personal data in the file has been stopped;
4. shares the register for browsing.

The aim of the above mentioned responsibilities of the data controller and AIS is to ensure a better protection of data and an effective prevention against breach. A breach of personal data protection results in a security breach which leads to a coincidental or unlawful destruction, loss, modification , unlawful disclosure or access to personal data that are transmitted, stored or processed in other ways; these provisions of law do not apply to deeply encrypted data in the case when there are proofs that the cipher code has not been cracked.

A breach of personal data protection , when there is no adequate and prompt reaction, may result in a significant economic loss and social harm, including identity fraud, to the individual concerned. Therefore, the data controller should notify the breach to the supervisory authorities without undue delay, which should be presumed to be not later than 72 hours. If applicable, an explanation of the reasons of the delay should accompany the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay[12].

[12]Amendment 43, Proposal for a regulation of the European Parliament of 12 March 2014, Recital 67 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with

Bibliography

1. Osiej M. Bargiel CO Z TYM ABI? http://www.e-ochronadanych.pl/artykuly.php?news_id=2426
2. Regulation of 10 December 2014 of the Ministry of Administration and Digitization on notification sample forms regarding appointments and dismissals of AIS, Journal of Laws 2014, item 1934
3. KALENDARIUM NOWELIZACJI USTAWY O OCHRONIE DANYCH OSOBOWYCH – Calender of amendments to the act on personal data protection – a a deregualtory act http://www.sabi.org.pl/page8.php
4. Regulation of 11 May 2015 of the Ministry of Administration and Digitization on procedures and methods of implementing measures to ensure the observance of the regulations on personal data protection by *Administrator of Information Security*, Journal of Laws 2015, item 745
5. Regulation of 11 May 2015 of the Ministry of Administration and Digitization on the methods of running data *register* by *Administrator of Information Security*, Journal of Laws 2015, item 719
6. Ł. Onysyk Jak prowadzić rejestr zbiorów danych osobowych http://blog.e-odo.pl/2015/01/13/jak-prowadzic-rejestr-zbiorow-danych-osobowych/
7. P.Janiszewski Projekt rozporządzenia w sprawie realizacji zadań przez ABI http://blog.e-odo.pl/2015/01/05/projekt-rozporzadzenia-w-sprawie-realizacji-zadan-przez-abi/
8. K.Chylińska Nowe rozporządzenie w sprawie abi http://blog.e-odo.pl/author/katarzyna-chylinska/
9. K.Witkowska Reforma ochrony danych osobowych - nowe obowiązki, nowe korzyści https://www.portalodo.com/entry/reforma-ochrony-danych-osobowych-nowe-obowiazki-nowe-korzysci.
10. P. Wierzbicki Jest szansa na unijne rozporządzenie o ochronie danych (2014.02.11) Obserwator Konstytucyjny http://www.obserwatorkonstytucyjny.pl/debaty/jest-szansa-na-unijne-rozporzadzenie-o-ochronie-danych/
11. K. Witkowska Ochrona danych osobowych 2015 – zmiana przepisów, nowe obowiązki i nowe korzyści. http://ksiegowosc.infor.pl/obrot-gospodarczy/dzialalnosc-gospodarcza/703554,Ochrona-danych-osobowych-2015-zmiana-przepisow-nowe-obowiazk

regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

Abstract

When analyzing the new Polish regulations of the act and the EU regulations on the processing of personal data in EU proposed for 2016 , it seems that the necessity emerged to appoint an Administrator of Information Security (AIS) in the majority of health care entities and in the IT system of the health care system.

The article presents the most important issues concerning the functioning and of AIS, the requirements, the necessity to register and the responsibilities. It is a prerequisite for a correct emplacement in a health care entity that within 30 days after the appointment AIS should be notified to registration by GIODO (the Inspector General for Personal Data Protection). The most important responsibility of AIS is to ensure the compliance of the provisions on personal data protection, which includes keeping the register of personal data files, preparing reports and the supervision of the data processing documentation