Presentation of the situation in Poland regarding the notaryship of the Republic of Poland in relation to the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the revocation of Directive 95/46/EC (General Data Protection Regulation) [hereinafter: GDPR]

  becomes applicable on 25 May 2018

- The provisions of the applicable Act of 29 August 1997 on the Protection of Personal Data (Journal of Laws of 2016, item 922), hereinafter referred to as the “applicable Act” on the one hand contain regulations which are analogous to the provisions of the Regulation, e.g. as regards the definition of personal data, on the other hand they contain regulations which are different from those provided for in the Regulation, for example as regards the definition of the consent of the data subject.
- The applicable Act also contains regulations that are not provided for in the Regulation, e.g. in the scope of registration of data sets, but also lack of provisions regarding for instance certification in the applicable Act.
- **The GDPR will replace the existing Act.** The Polish provisions on the protection of personal data will also include the regulation of this part of the rules on the protection of personal data, which has not been regulated in the GDPR, i.e. certain rules for the processing of personnel data.

- In light of the above, it has become necessary to develop a completely new regulation in the field of personal data protection that would correspond to the regulations and standards for the protection of personal data adopted at EU level.
- **The provisions of the new Act establish a new body competent for the protection of personal data** - it will be the President of the Office for the Protection of Personal Data.
- In connection with the start of direct application of the GDPR as of 25 May 2018, **the Ministry of Digitization has prepared two drafts**: **the Act on the Protection of Personal Data** (hereinafter: PPD) and **the Act introducing the provisions of the Act on Personal Data Protection** (hereinafter: IP).

the Act on the Protection of Personal Data (PPD)

- **The PPD in the version dated 10 May 2018** (4 versions of the PPD draft have been prepared so far) **does not provide for any changes in the scope of application as regards the notaries**, but currently some exemptions for micro-entrepreneurs are provided, which may also apply to notaries.
- The PPD has been adopted by the Sejm (lower house of the Polish parliament) on 10 May 2018, whereas on 11 April 2018, the PPD and be adopted by the Sejm in May.

The Act introducing the provisions of the Act on Personal Data Protection (hereinafter: IP).

- **Direct changes in the scope of the GDPR application by the notaries will be provided for by the draft of the Introductory Provisions (IP),** and these will be changes that are important from a practical point of view.
- According to the information available at the moment, **the IP draft should not be expected before the end of June 2018,** but the legislative situation is dynamic.
- **The current version of the IP draft is not yet known**; according to currently available information, work on the project at the Ministry of Digital Affairs is to be finalised in June, and the new IP draft will be published only after the end of the consultations.
- **The original IP draft of September 2017 provided for the exclusion of application by the notaries of some obligations imposed by the GDPR and specifying the attitude to professional secrecy.**

The previous IP draft, related to the notaries connected with their obligations as regards the protection of personal data can be found below:

- **Art. 78b. § 1. The administrators of personal data processed in order to perform tasks, duties, or rights under the Act are respectively: (...)**
- 2) **The National Notarial Council - as regards personal data processed:**
- a) in the course of administrative proceedings conducted by this body, proceedings regarding complaints and applications and other provided for by the Act or legal acts issued pursuant to the Act of notarial self-government bodies, proceedings concerning notaries, notary's apprentices, notarial deputies or persons applying for appointment to the office of a notary public or an entry on the list of notary apprentices, as well as persons taking the entrance and notarial examination,
- b) to the extent necessary for the proper implementation of public tasks specified in the Act and supervision arising from the Act,
- c) in the course of disciplinary proceedings conducted by the Supreme Disciplinary Court;
- 3) **councils of notarial chambers** - in the case of personal data processed:
- a) in the course of administrative proceedings conducted by this body, proceedings regarding complaints and applications and other provided for by the Act or legal acts issued pursuant to the Act of notarial self-government bodies, proceedings concerning notaries, notary's apprentices, notarial deputies or persons applying for appointment to the office of a notary public or an entry on the list of notary apprentices, as well as persons taking the preliminary and notarial examination,
- b) to the extent necessary for the proper implementation of public tasks specified in the Act and supervision arising from the Act,
- c) in the course of disciplinary proceedings conducted by a disciplinary court of a notary chamber;
- 4) **qualification and appeal commissions** - in the case of personal data processed in the course of the admission procedure for the entrance and notarial examinations as well as in the course of the appeal proceedings against the results of these examinations;
- 5) **notaries** - in the case of personal data obtained during the performance of notarial actions.
- § 2. For the processing of personal data referred to in § 1, the provisions of art. 13- 15 secs. 1 and 3, 18, 19, and 21 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and revoking Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the EU L 119 of 4.05.2016, page 1), hereinafter referred to as "Regulation 2016/679", shall not apply.
- § 3. The exclusions referred to in § 2 shall apply to personal data necessary to ensure the correct implementation of the tasks, duties or entitlements referred to in § 1.
- § 4. The provision of art. 16 of the General Data Protection Regulation does not apply, unless specific provisions provide for a separate procedure for rectification.
- § 5. The personal data referred to in § 1 are subject to safeguards to prevent abuse and unlawful access or disclosure, resulting from legal procedures in which course they are processed.

Retention period – 10 years

Art. 78c. In the case of personal data that a notary or a processor has received or obtained as a result or for the performance of notarial actions and is obliged to keep the secret referred to in art. 18 § 1, the provisions of Art. 58 sec. 1 e and f of Regulation 2016/679 shall not apply. Art. 78d. **The period of storage of personal data referred to in Art. 78b § 1, shall be determined by the administrator in accordance with the purposes of their processing, taking into account the separate provisions regarding deadlines, however, in the case of personal data obtained while performing notarial actions, it may not be longer than the storage period referred to in Art. 90 of the Act.„**

Conclusions

The correct and purposeful implementation of the GDPR in a notary's office **should take into account the provisions of the GDPR and the PPD as well as the IP.**

According to currently known projects, starting 25 May 2018, notaries will apply the GDPR in its entirety, and then their obligations will be reduced on the basis of the IP and LP and PPD.

As a result, notaries in Poland will be able to prepare the **final, ultimate documentation and instructions for the application of the GDPR in their offices in July 2018 at the earliest**.

On the other hand, notaries in connection with the application of the GDPR as of 25 May 2018 **cannot wait with the implementation of the GDPR procedures for the entry into force of the Polish provisions on the protection of personal data, i.e. PPD and IP.**

The practical aspects of the GDPR implementation at a notary's office - the role of a notary public in the protection of personal data

- **What personal data is processed by the notary public pursuant to the GDPR**

Personal data is processed in the notary's office - two typical groups of personal data can be identified, which are processed at every office:

1) Personal data related to the performance of notarial actions: name, surname, and address (or information about persons acting on behalf of legal entities), information about the actions, documents collected, etc. This group also includes personal data, e.g. of participants in the land and mortgage register proceedings.

2) Personal data of employees and cooperating persons: include information about persons employed under a contract of employment and on the basis of other so-called contracts under Civil Law, personal details of cooperating deputies of notaries and notary apprentices. This group also includes personal data of notarial applicants, in relation to which notaries act as patrons.

Personal data shall also be processed in connection with the performance of obligations related to the employment of employees, in particular for the purpose of performing social security obligations and tax obligations.

Who is a notary public in relation to personal data being processed

- In relation to personal data of employees and cooperating persons, the notary public is entitled to the status of personal data administrator - on general terms, as, for example, every employer is entitled to the status of personal data administrator in relation to personal data of their employees. On the basis of the GDPR and the accompanying Polish provisions on the protection of personal data - in accordance with the original draft Act on the Introductory Provisions to the Act on the protection of personal data, it is to be decided that notaries will act as personal data administrators in relation to personal data processed within the performance of their profession.
- **A notary public in relation to personal data processed related to the performance of notarial actions should therefore be considered as the administrator of personal data.**

How should a notary public protect personal dataj

The GDPR deviates from the practice of specifying in the provisions of the law of specific measures to secure personal data to be implemented by the data administrator.

Instead**, the GDPR introduces the so-called a risk-based approach**.

The essence of a risk-based approach boils down to saying that every entity that processes personal data should independently determine what specific data security measures should be implemented.

The choice of security measures should be based on:

- a. the nature, scope, context, and purposes of the processing,
- b. the risk of violation of the rights or freedoms of natural persons with various likelihood of the occurrence and the severity of the threat,
- c. the state of the art,
- d. the implementation cost.

- **Each entity that processes personal data, including a notary public, should:**
- a. determine what personal data, in what capacity, why and in what environment they process,
- b. determine the risk of violation of the rights or freedoms of natural persons associated with such processing,
- c. choose appropriate data security measures, taking into account the existing technical capabilities and own financial capabilities.

Example - personal data processing by a notary public

■ **data scope**: the risk increases when personal data regarding property ownership and other things, the health condition or family situation, financial situation of clients, etc. are processed

■ **processing purposes**: the risk increases when the data are processed for purposes related to notarial actions, as such data may be disclosed as part of the actions performed

■ **the risk increases** when data are processed on external servers with which communication is carried out in an unencrypted manner using public networks, and decreases when data is processed on own servers

The GDPR does not impose the usage of any specific data security means.

The GDPR only indicates only examples of technical and organisational measures that can be used to achieve this objective, i.e. **to ensure a level of security corresponding to the risk.**

These are in particular:

- personal data pseudonymisation and encrypting;
- the ability to continually ensure the confidentiality, integrity, availability, and resilience of processing systems and services;
- the ability to quickly restore the accessibility and access to personal data in the event of a physical or technical type incident;
- regular testing, measuring, and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

The risk-based approach assumes that every entity that processes data will consciously decide on the security measures to be used. This is all the more important since this entity is liable in the event of violation of the personal data security.

Examples of activities to be applied in a notary's office are:

- **preparation and implementation of personal data protection documentation in the notary's office** - preparation of instructions for storing personal data and internal risk protection documentation, including in particular the legal obligation to inform about security related incidents involving personal data, i.e. preparing an internal procedure to demonstrate that personal data are processed and secured in accordance with the legal requirements
- **creation of a catalogue of data security rules**, e.g. encryption of notarial deed drafts containing personal data sent via electronic mail, e.g. an e-mail password will be sent to the customer's phone, access to computers, folders containing confidential, password protected data, given only to certain office employees, no access to computers for external devices of the USB type, all documents (not only the original notarial deeds), but also all documents provided by the client to the office - must be stored in closed safes, conclusion of entrustment agreements for personal data processing, etc.

How to conclude an entrustment agreement for personal data processing?

- In connection with the profession of a notary public, personal data processing is very often entrusted - **A notary public should conclude an agreement with the data processor to order, the so-called entrustment agreement, in which the principles of data processing shall be determined**

Examples

- using the services of an external entity providing accounting services,
- using the services of an IT specialist
- using the services of an entity ensuring electronic mail services,
- ordering an external entity to destroy documents containing personal data,
- ordering an external entity to archive documents containing personal data,

the GDPR introduces new - significantly extended - requirements as to the contents of the entrustment agreement (In relation to the Act of 29 August 1997 on the protection of personal data)

These are the obligations of the data processor to:

- a. process data only on a documented request of the administrator,
- b. ensure that persons authorised to process personal data have committed themselves to secrecy or to be subject to an appropriate statutory obligation of secrecy,
- c. take measures to secure the data as required by the GDPR and help the administrator in meeting these obligations,
- d. observe the terms of using the services of another data processor - the so-called the sub-entrusting of data processing is allowed only with the consent of the data administrator,
- e. assist the administrator in fulfilling their duty to respond to requests of the data subject in the exercise of his/her rights as set out in the GDPR,
- f. delete the data or return the data to the data administrator after processing, as decided by the administrator,
- g. make available to the administrator all the information necessary to demonstrate compliance with their obligations and to enable the administrator or auditor authorised by the administrator to carry out audits.

An entrustment agreement for personal data processing should also specify:

a. the subject and duration of processing,
b. the nature and aim of processing,
c. type of personal data,
d. data subject categories,
e. the administrator’s obligations and rights.

The entrustment agreement may be concluded in writing and in electronic form, provided that the document’s integrity and authenticity in electronic form is ensured.

Poland - What significantly differs entrusting of data processing pursuant to the GDPR from the Act of 29 August 1997 is the legal obligation to choose such a data processor that guarantees adequate protection of personal data. A notary public can have practical difficulty in choosing such an entity - especially when data processing is to be carried out by reputable suppliers. In this case, the so-called procedure for certification of personal data processors is helpful. Certificates will be issued to certify compliance of data processing by a certified entity. Thus, it will be a guideline for those who are looking for an appropriate personal data processor - the choice of entities holding
a certificate.

The obligation for the notary public to notify about cases of data protection violation

- **The GDPR imposes on the entities that process personal data a legal obligation to inform about security incidents regarding personal data.** *This is a very significant change in relation to the Act of 29 August 1997 which did not contain any such provisions at all.*
- **The security incident is called violation of personal data protection in the provisions of the GDPR and it may consist in:**
- a. violation of security leading to accidental or unlawful destruction, loss, or modification of personal data,
- b. violation of security leading to unauthorized disclosure or unauthorized access to personal data sent, stored, or otherwise processed.

Examples in a notary’s office:

- loss of a carrier containing personal data,
- obtaining access to the data by an unauthorised person,
- breaking into the system used for processing of personal data.

The supervisory authority (President of the Personal Data Protection Office) should be informed about the occurrence of the incident. The information should be sent promptly, however no later than within 72 hours from the discovering the violation. In some cases, the data subject should also be informed about the incident - it will be in a situation when the violation may cause a high risk of violating the rights and freedoms of the data subject, e.g. loss of the client’s original documents.

The right to being forgotten by the notary public

- The right to be forgotten is one of the new rights granted by the GDPR to the data subjects.

This right consists of two powers:

- a. the possibility for the data subject to request the deletion of his/her personal data by the data administrator,
- b. the possibility of requesting the data administrator to inform other data administrators to whom they have disclosed personal data that the data subject requires that those administrators delete any links to those data or a copy thereof.

In notarial practice, these will be situations in which the data subject withdraws the consent given or raises an objection.

Specific cases limiting the right to be forgotten

- In the event of exercising the right to be forgotten, the data administrator or notary public should stop processing personal data and delete the data, unless there are specific cases limiting the right to be forgotten. Among them, particular attention should be paid to:
- **a. the existence of a legal provision that orders the processing of personal data,**
- **b. a situation in which data processing is necessary to establish, seek redress, or defend claims.**

The right to be forgotten does not apply to those data that a notary public processes for purposes related to the profession of notary public, e.g.

sending copies/extracts of notarial deeds to the municipal/communal offices, city mayor, commune head or town mayor, to the district office, tax office, and the land and mortgage register court.

In other cases, in particular in relation to personal data processed for purposes related to hiring employees or collecting data for the purpose of sending information materials to clients, the right to be forgotten is granted on general terms.

Example

- the party to a notarial action after the signing/concluding of the notarial deed cannot exercise the right to be forgotten and effectively request removal of their personal data from the original notarial deed or from the Notarial Repository,
- a participant of a notarial action cannot exercise his/her right to be forgotten and effectively request the removal of his/her personal data from the Notarial Repository.