AN OVERVIEW OF INFORMATION SYSTEMS AND DATA HANDLING OF HUNGARIAN LIVING COMMUNITIES FROM THE PERSPECTIVE OF GENERAL DATA PROTECTION REGULATION REQUIREMENTS AND INFORMATION SECURITY

Zoltán Som[1] and Zoltán Polgár[2]

DOI: 10.24989/ocg.v335.38

Abstract
There are multiple challenges present in the daily lives of living communities regarding legal and organizational matters, as well as issues concerning information technology and informational security, which demand a constant search for appropriate solutions. Reviewing these issues is especially important in Hungary, where one-fifth of the population lives in facilities that are maintained by the community itself. Moreover, the trends of the current real estate market point towards a rise in these numbers. Throughout our research, we have examined current Hungarian legal practices regarding data handling and information security. The central focus of our inquiry was to determine the typical behaviour of Hungarian officials working with, handling, storing and processing data of the country's living communities. This study analyses market solutions for these condominium buildings to comply with the legal requirements and also reviews the legal and economic limitations of such practices. Special attention is devoted to the handling and processing of personal data, with an emphasis on forecasted trends of cyber threat in 2018.

The central subjects of our study, then, are legislative practices relevant for living communities, the protection of personal data, and information security issues in general. Thus, we examine the typical and most widespread software solutions deployed by resident managers, while also shedding light, with empirical research methods, on the level of data protection in such software packages. Since barrier-free access to information on condominium resident managers and communities themselves, as well as annual financial reports will be mandatory from January 1, 2019, resulting in the creation of a national register for resident managers, we extend our inquiry to the relationship between public administration bureaus and such living communities in the predictive section of our study.

1. Market factors determining the room for manoeuvring of the residents' association

Since 1924, increasingly more dwelling-houses were built in order to meet the demands for condominiums. Within these buildings, some of the premises are suitable for dwelling, while some are not. The whole building consists of different types of condominium units and parts, some of

[1] National University of Public Service, Doctoral School of Public Administration Sciences, Information Security Department, H-1083 Budapest, 2 Ludovika tér, som.zoltan.kdi@office.uni-nke.hu
[2] National University of Public Service, Doctoral School of Public Administration Sciences, Information Security Department, H-1083 Budapest, 2 Ludovika tér, polg.zoltan@gmail.com

which are not private units. The whole area is the basis for the calculation of the ownership share, and the private ownership share is based on the whole area as well, which determines the later-discussed voting rights of persons concerned by data protection.

Not all condominium units of the building will be private property during the condominium registration, as there are parts of the building that are joint property. "Ownership of the same thing, by specific shares, can be claimed by two or more persons." [1]. The list of joint areas and private areas is included in the building's foundation document. The costs of the joint property are paid by the owners of the building. Joint property or jointly used areas occur in houses which operate as a condominium or in housing cooperative form. "A condominium is established when in a building at least two independent units for residential or non-residential purposes or at least one independent unit for residential and one for non-residential purposes defined in the bylaws and technically separated pass into the private ownership of condominium owners, whereas the building sections, building equipment, areas and flats, which are not owned individually, shall pass into the joint ownership of condominium owners." [2]

The rules of joint properties are described by the following laws:

1. Civil Code (Ptk.)

2. Act on condominiums (Tht.)

3. Act on housing cooperative (Lszt.)

The mentioned legal background forces the owners to decide during already the establishment, whose decision later determines the handling of data and the decision system. The system of building operation could be changed; thus, a condominium could be changed to a housing cooperative and a housing cooperative to a condominium. Buildings, which have six or less condominium units, can decide during the foundation whether they want to operate the building according to Ptk. or Tht.

According to a study by the Hungarian Central Statistical Office [3] there are 1.3 million condominiums in buildings which consist of four or more flats. The operation of these buildings is the following, according to the Office: 75% condominium, 13% housing cooperative and the remaining 12% cannot be classified. The importance of the topic is also shown in the fact that approx. 40% of the Hungarian population live in residential buildings operated as condominiums.

	Operation of the building		
Types	Condominium		Housing cooperative
Subtypes	6 or less than 6	above 7 units	-
Foundation	Foundation document		Statutes
Laws	Ptk	Tht	Lszt
Decision-making body	General meeting, Partial General meeting		Congress
Representative	Condominium Board President Syndicate		Directorate
Decision formality	Decision Organisational and operational rules (SzMSz)		Decision Bylaws
Controlling	Court	Audit Committee Settlement clerk Court	Supervisory board Court of registration

Table 1. Structural forms according to laws
Source: according to laws, own edition

As the first table shows, the main aspects of building operation are implemented based on a similar set of criteria. Thus, in order to facilitate understanding, hereinafter we will use the term 'condominium'. What condominiums have in common is that the joint representatives use software products, which they usually (as we observed) lease, for bookkeeping, accounting, and keeping the records of residents. Within the context of our research, we contacted major software suppliers whom we selected based on a survey inquiring the participants about the Information Technology (IT) systems (software applications) they use for condominium management. We identified the 6 most-common software applications in a separate survey. We also treat the cluster where data are processed by using IT devices and software applications but on a local Personal Computer (PC) as a separate category. Legislative changes, however, imply that paper-based data management, if there is still any, presumably disappears due to the disclosure obligation.

In summary, we can conclude that it is necessary to develop condominiums in order to ensure housing. Due to the large-scale involvement of condominium associations, it is worth performing the review investigation of the compliance of the applied IT systems with the General Data Protection Regulation (GDPR) and IT security requirements.

2. Organisational responsibilities and challenges of owners' associations

Among the organisational responsibilities, we would first look at software selection, as this will determine the structure community management. This choice means that the officers of the condominium can, without any direct influence from the owners, decide on the IT data protection within the condominium.

Representation of the condominium and in most cases also the administration is performed by the elected representative. Their election is performed at the general assembly, which is the main decision-making body [4]. Both the knowledge and preparedness of the elected persons and the organisational form of the activity can vary a lot, just like the software products applied and the responses given to data security issues. Within the context of our study, we contacted the suppliers of condominium software applications, and we tried to explore their services and especially their compliance with the GDPR and IT security requirements. According to Paragraph (1) of Section 5 of Act CXII of 2011 on the Right of Informational Self-determination and the Freedom of

Information (hereinafter referred to as Infotv.), personal data may, as a general rule, be processed based on the consent of the data subject or the law (including statutory authorization as well). According to Paragraph (3) of Section 7 of the Infotv., controllers shall protect data by means of suitable measures against unauthorized access.

Realization of data management

The administrative work of a condominium's owner also includes data management [5]. To perform the administration, it is necessary to manage the data of the occupiers (e.g. owners, tenants). The Tht. lays down the general guidelines of data management, but it refers mainly to the SzMSz (Organizational and Operational Rules) to regulate that. The SzMSz of the condominium may contain the list data to be provided by the owners (Section 22 of the Tht.), but it is not obligatory. Among the before mentioned condominium entities (Condominium Board President, Syndicate, Audit Committee), it is mainly the Condominium Board that deals with data management. Anyone might need access the files during the administration, in practice however, in most cases the members of the Audit Committee or the person responsible for auditing the accounts will check the data besides the Condominium Board President.

To manage personal data [6] is necessary in order to reach the goals of the condominium. For this it is necessary to comply the commitments of the owners and to practice their rights. However, this is a thin line, as handling data which is beyond the aim of the community could constitute a criminal offense. There are other important moments in a condominium regarding data management. After the establishment of the condominium the person who becomes an owner by an agreement expressed by conduct accepts that the elected representatives of the condominium will manage his data. No implied contract is necessary for this. Furthermore, if the General Assembly agrees, the appointed person may get authorization for data management without the consent of the concerned person. In practice it is realized in keeping registry of residents. Usually it is the Condominium Board President who has the registry. Data that has not been announced by a joint proprietor cannot be handled by the Condominium Board President, even if the representative has gotten authorization by the Assembly. Data of the tenant or data regarding the number of people living in one condominium unit can only be asked by the representative, if it is to be used for calculating the cost of utilities. Data regarding the tenants must be announced by the owner. Data could be reported by the tenants as well, but in that case the data management will be not legitimate.

The process to replace the authorized representation is also worth noting. There are no respective provisions of the Tht. that could apply on how the replaced Condominium Board President shall verify that he no longer possesses the data that have been handled by him. The Tht. does not regulate how the authorisation and/or data are passed to the new joint representative either. There is no such obligation to prove in practice; thusly the data management of the leaving Condominium Board President is not under control.

In summary, nor the form requirement neither the actual content of data management of the Condominium Board President is regulated by Tht., it is different in each condominium. Control varies depending on the general expectations of the owners' community and the efficiency of the controlling persons. According to the laws in force, data protection and data handing rules is expected to be written by such communities, where not data protection specialists are predominating. Controlling the principles of data protection is almost impossible upon the replacement of the Condominium Board President. We developed a questionnaire to compare the data-processing capabilities of the different software applications.

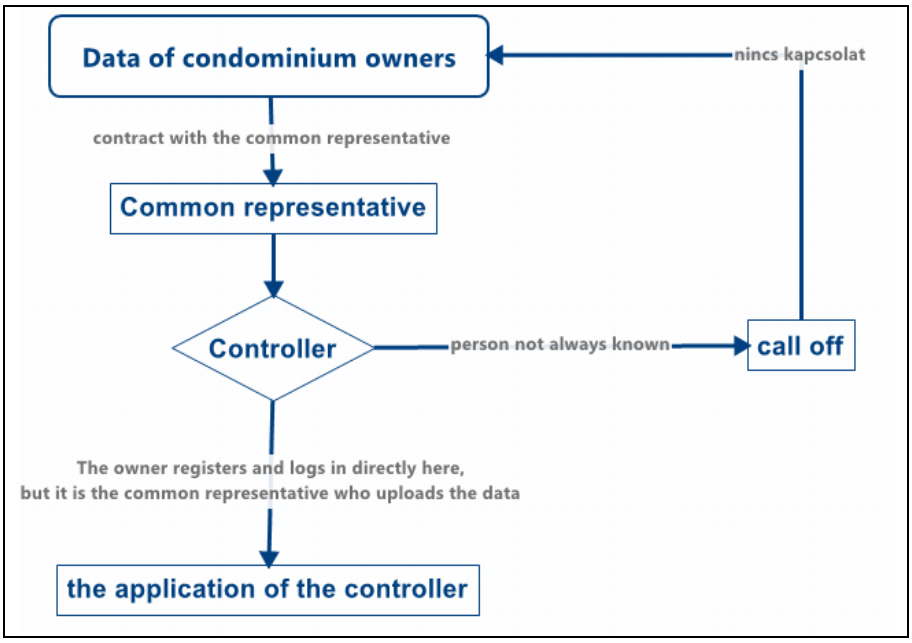

Figure 1. Processing the data of condominium owners
Source: own drawing

Hypotheses

- *H1:* The assumption is that GDPR compliance is a marketing feature for companies dealing with community data processing, allowing them to acquire data for the studies easily, because stressing and ensuring data security makes data-processing companies attractive.

- *H2:* The fact that the condominium management software is in the ownership of the joint representative does not serve the interests of the condominiums (i.e. the residents).

- *H3:* Condominium management programs better fit data-protection goals if they are owned by the residents' association.

3. Description of the research steps

In the second half of 2018, a group of 350 professionals was asked what software the joint representatives used to process condominium data. Based on the empiric observation, a portion of the potential answers were defined. Further software products could, however, also be named so that the decisions of the participants are not influenced. Based on the results, the study focused on 6 software products in total.

The next phase of the research defined and matched, based on the GDPR [7], the expectations that specify IT and IT security requirements specifically for community data processing.

In the third phase, we compiled a questionnaire for the software owners in which we formulated the questions in consideration of the typical operations based on the GDPR and we also paid attention to formulate the questions in consideration of the most-common non-industry-specific IT security “standards”.

Applied IT security standards

The most-common generally applicable standards provide a so-to-day "best practice" and they are MSZ ISO/IEC 27001:2014, NIST 800-53 R4, Act L of 2013 [8] and its implementing decree, Decree No. 41/2015. (VII. 15.) of the Minister of the Interior [9]. There are so-called cross-tables which make the standards consistent wither with each other or the GDPR requirements.

Association of the legal approach of the GDPR and IT security requirements

Association of legal and IT security requirements is necessary because it allows for the specification of the technical requirements a software application must meet, i.e. an instruction for the software developer (operator and other contributing party) to ensure compliance of the software product and its operation with the law. Community data processing also knows the term "Software as a service" (SaaS), because condominium management companies cannot, and probably not always want to, develop their own software applications. And the developer, as service provider, may also use further services (PaaS), see Table 3.

Szádeczky pointed out that "Current Hungarian IT security regulations are not uniform, and the areas which are regulated to different degrees are distinguishable and categorizable." [10] Szádeczky saw that these findings are verified; the basis of the research projects is, therefore, the association made in Table 2 which is transparent and can be useful for future research projects as well.

GDPR reference	*Studied areas*
CHAPTER II Principles	
Article 5 Principles relating to processing of personal data	
1. Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').	Security of internal communication Physical security Border control Access management ITS processes Security of external relationships Save Encryption Protection against harmful codes (virus protection)
CHAPTER III Rights of the data subject	
Section 2 Information and access to personal data	
Article 13 Information to be provided where personal data are collected from the data subject	
1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: 2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:	Application functionality

GDPR reference	*Studied areas*
Section 3 Rectification and erasure	
Article 16 Right to rectification	
The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.	Application functionality Save Erasure procedures
Article 17 Right to erasure (‘right to be forgotten’)	
1. The controller shall have the obligation to erase personal data without undue delay	Application functionality Save Erasure procedures
Article 20 Right to data portability	
1. shall receive the personal data provided to a controller in a structured, commonly used and machine-readable format	Application functionality
CHAPTER IV Controller and processor	
Section 1 General obligations	
Article 24 Responsibility of the data controller	
1. shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation	ITS processes
Article 25 Data protection by design and by default	
1. The controller shall ... implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. ... In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.	Application functionality security Access management Security testing (vulnerability test)
Article 28 Processor	
1. ... the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	Verification of compliance with relevant requirements at the processor as well Audit procedures (external, 3rd party)
Section 2 Security of personal data	
Article 32 Security of processing	
1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical	Pseudonymisation Audit procedures (external) Security of internal communication Physical security Border control Access management ITS processes Risk assessment Security of external relationships Save Security testing (vulnerability

GDPR reference	*Studied areas*
incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.	test) Encryption Protection against harmful codes (virus protection) Restoration
Article 33 Notification of a personal data breach to the supervisory authority	
3. (c) describe the likely consequences of the personal data breach; 5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.	Records of data breaches Management of security breaches Log management, assessment Monitoring
Article 34 Communication of a personal data breach to the data subject	
3. The communication to the data subject shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;	Encryption
Article 35 Data protection impact assessment	
1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.	Data-protection impact assessment Risk assessment

Table 2. Association of the legal approach of the GDPR and IT security requirements
Source: own edition

- *H1:* The assumption is that GDPR compliance is a marketing characteristic of companies dealing with community data processing, allowing them to acquire data for the studies easily, because stressing and ensuring data security makes data-processing companies attractive.

The study revealed that the companies concerned do not provide data and will not fill in the questionnaires sent to them either.

- *T1:* Stressing the GDPR does not generate any benefits for the marketing activities of the community data processing companies covered by the study. The non-provision of answers allowed us to conclude that the companies do not want to disclose their GDPR compliance, i.e. they do not think it is important to express this openly towards their customers.

After formulating Thesis 1 (T1), we continued our study based on data that are accessible without approval, i.e. by way of open collection of information.
Information collected during the observations

Information were studied in compliance with the requirements of the GDPR. The study found that 4 of the 6 examined websites had privacy statements. Only one of these privacy statements was dated, it was issued on 1 May 2016. There was another privacy statement, on a subpage of one of the websites, it was issued on 24.05.2018.

On the whole, it was hard, or even impossible, for us to find GDPR-relevant information; thus, taking the non-filling of the questionnaire into consideration, we are on the opinion that further studies and research of this topic would be justified. Due to the large-scale involvement of the communities.

The date is missing in many cases; this is important, because the service provider can also not prove when it uploaded the document to its website.

The IP address range revealed that the service providers are not located in Hungary in all the cases, implying that considerable conflicts of laws must be resolved in case of legal disputes.

Given that residential buildings having 6 or more apartments correspond to at least 39% of all the apartments in Hungary, we can say with great probability that the software products studied process the personal data of at least the same number of persons.

Partly based on the CEH exploration methodology, we examined the following factors regarding the websites concerned from open (i.e. publicly accessible on the Internet) sources of information.

8 service providers were examined in this phase of the research project; data stored on personal computers (i.e. in local databases) are not applicable; hence they were not examined.

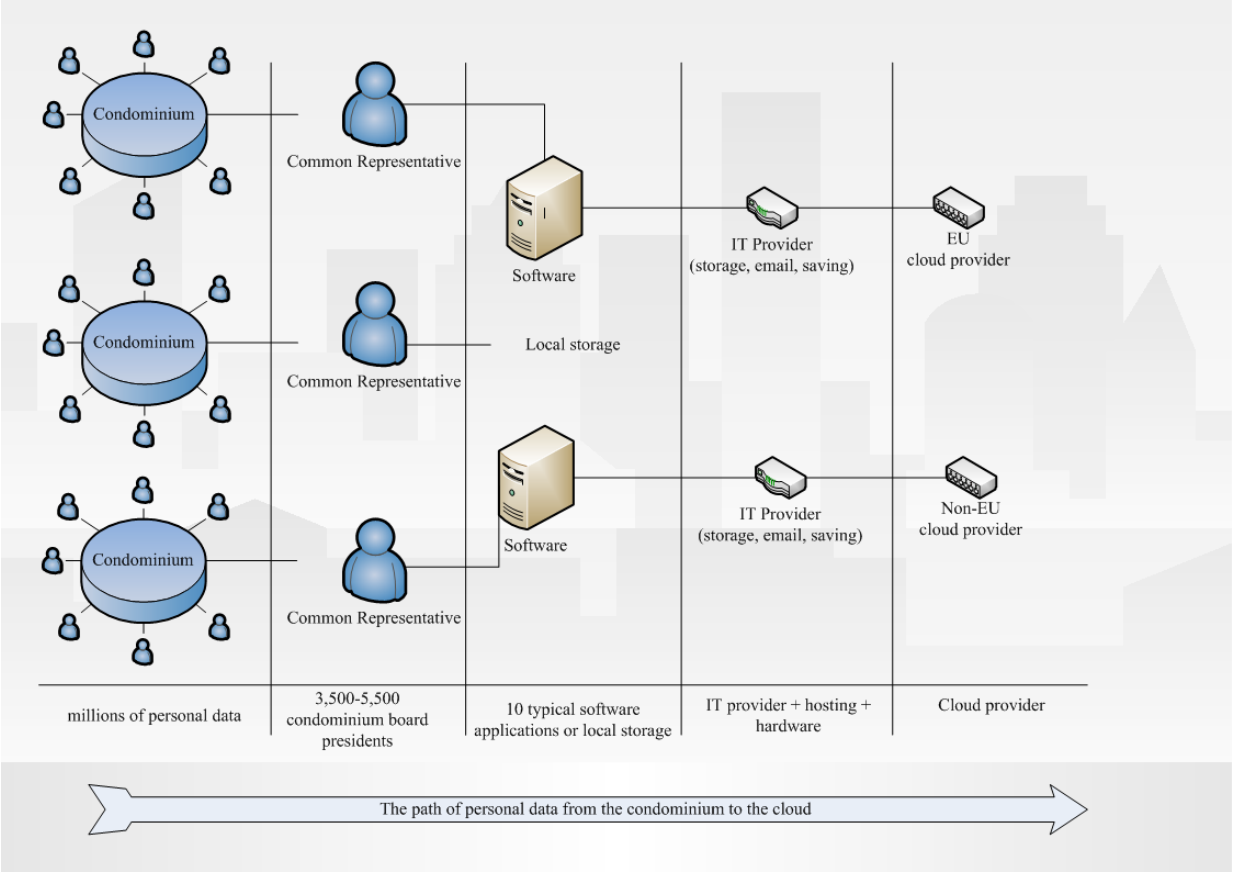

Figure 2. The path of personal data from the condominium to the cloud
Source: own drawing

In case of the service providers studied:

- in 50% of the cases, the site was accessible via http connection as well. This means that data traffic, login or personal information may be intercepted, or even stolen.

- The DNS and IP address queries allowed for the identification of hosting providers. This allows for the conclusion that these service providers use further service providers as well.

- 62.5% of the hosting providers are Hungarian companies; we, therefore, assume that data are physically stored in Hungary. For the rest, we assume the opposite, due to the involvement of foreign service providers. We can also presume that non-EU service providers are also involved.

- The mapping of mailing services (MX records) provided similar results. In other words, it is presumable that further service providers are involved. This is a relevant issue because the practice we studied included frequent adding of personal data to the correspondence.

- On 62.5% of the examined sites, we could find a notice related to data management; their respective contents were, however, up-to-date and dated in one case only. Despite the fact that in more than one third of the cases the mentioned sites had only form fields, data processing can be carried out easily, even by asking a single question.

- There are systems that allow for the uploading and storing of special personal data, e.g. photos or any other optional data.

- As we have observed, none of the sites applies multifactor authentication.

- Based on the opinions of the independent experts, each hold a CEH qualification, we asked, 75% of the sites in question are vulnerable to misuse or have potential attack vectors.

All that allows for the assumption that each examined service provider has involved one or more other service providers which (as data processors) they do not provide any information of. It can be seen, as a result of the research project, that large quantities of personal data are stored in a limited number of systems.

4. Summary, comparison of hypotheses and theses

We checked the software products named by professional users and we found that software owners are very reluctant to disclose any data. The research focused, therefore, on publicly accessible data.

Hypotheses and theses

- *H1:* The assumption is that GDPR compliance is a marketing feature for companies dealing with community data processing, allowing them to acquire data for the studies easily, because stressing and ensuring data security makes data-processing companies attractive.

- *T1:* Stressing the GDPR does not generate any benefits for the marketing activities of the community data processing companies covered by the study. The non-provision of answers allowed us to conclude that the companies do not want to disclose their GDPR compliance, i.e. they do not think it is important to express this openly towards their customers.

- *H2:* The fact that the condominium management software is in the ownership of the joint representative does not serve the interests of the condominiums.

- *T2:* The research project could neither refute nor verify this. Further study would be justified.

- *H3:* Condominium management programs better fit data-protection goals if they are owned by the residents' association.

- *T3:* The research project could neither refute nor verify this. Further study would be justified.

It was, against this background, justified that this is a current topic, and a great deal of personal data are processed. It was revealed that the service providers currently do not put any emphasis on disclosing their “GDPR compliance”. The absence of any market pressure can, presumably, contribute to this. These and similar issues and the hypotheses not proven in the foregoing justify further studies (research projects). Software products identified in the research project. We have prepared a table associating GDPR and IT security requirements. We used publicly accessible information to prepare the table comparing the software products identified, allowing for further conclusions concerning the storage of data and other GDPR- and IT-security-related compliance.

5. References

[1] Section 5:73 of the Civil Code of Hungary

[2] Section 5:83 of the Civil Code of Hungary

[3] SÁGHI, G., Lakásviszonyok az ezredfordulón. (Dwelling status in the millennium) Budapest, KSH, Budapest, 2005.

[4] Section 27 of the Condominiums Act (Tht.)

[5] Paragraph (1) of Section 22 of the Condominiums Act (Tht.)

[6] Section 27 of the Condominiums Act (Tht.)

[7] The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC

[8] Act L of 2013 on the Electronic Information Security of State and Municipal Organisations

[9] Decree No. 41/2015. (VII. 15.) of the Minister of the Interior on the Requirements on Technological Security and Secure IT Equipment Specified in Act L of 2013 on the Electronic Information Security of State and Municipal Organisations and the Classification into Security Classes and Security Levels

[10] SZÁDECZKY, T., Regulated security. Theory and practice of regulating IT security and the methodology set up to facilitate application.] (PhD dissertation) Pécs, 2011.