THE NEW GENERAL DATA PROTECTION REGULATION AND QUESTIONS OF ITS APPLICATION

József Baki

ABSTRACT

From 25 May 2018, new data protection norms will be introduced in the Member States of the European Union. From this point on, Member States will need to apply *Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation; hereinafter the GDPR or the Regulation).

Given that the leaders of credit institutions need to summarize the changes of the GDPR and their impact on credit institutions essentially in one page, I will attempt to carry out this task in the ten points below:

- From 25 May 2018, banks will have to reckon on operational risk some 300 times greater than at present, as a consequence of the increased penalty that may be imposed for non-compliance with data protection norms (EUR 20 million instead of HUF 20 million, or 4% of the annual global market turnover of the institution controlling or processing the data).
- The GDPR stipulates that data processing operations that began before the date of the Regulation's application must also be brought in line with the Regulation. This obligation means that all procedures at credit institutions that affect the processing of personal data, as well as the processing of personal data itself, must be comprehensively reviewed, which likewise entails significant additional tasks for practically all units of the organization concerned.
- As a principle rule, data protection incidents must be reported to the data protection authorities. If a given data protection incident entails a probably high risk to a natural person's rights and freedoms, then the data subject or subjects must be informed, which may entail numerous additional consequences (possible official procedure, penalty, customer complaint, customer claim for damages, injury to reputation, etc.).
- As a significant task entailing extra administration from May 2018, data controllers, based on the accountability principle, must carry out all data processing procedures – from planning through to initiation of data processing, and onwards up until the erasure of the processed personal data – in such a way as to be able to demonstrate at any given moment that they have conformed with the regulations on data protection.

- In certain cases that may be adjudged to be high-risk, the GDPR introduces the institution of the Data Protection Impact Assessment (DPIA), and – depending on the result of this – prescribes a preliminary data protection consultation with the relevant authorities in certain cases, the time aspect of which must also be taken into account in future with respect to the feasibility of introducing certain new procedures.
- The application of certain new legal titles under the GDPR (e.g. legitimate interest) will provide more flexible and "market-oriented" data processing options than at present; however, the classification of certain data processing procedures under new legal titles may also entail greater uncertainty and a higher compliance risk in future.
- The Regulation contains more detailed rules than at present pertaining to data processors, which make necessary the review and modification of every individual prior cooperation and contract concluded with all parties carrying out outsourced activity or other data processors (e.g. dependent agents) in order to bring them into line with the GDPR.
- Preparations for conformity with the GDPR also require IT developments (with respect to data erasure, data portability, pseudonymization, profiling rules, etc) which demand significant time and resources.
- The activity of those currently responsible for data protection will be carried out under the GDPR by a Data Protection Officer (DPO), whose employment will be mandatory across a broader spectrum than at present, with the Regulation containing numerous guarantees ensuring this officer's independence, and the organizational and operational conditions for their activity, more emphatically than before.
- In the course of preparing for application of the GDPR, taking into consideration the new institutions and procedures of data protection, it will be necessary to draw up new data protection regulations and to modify both the procedural order affecting the processing of other personal data and the documents pertaining to personal data processing, which will require a review of the entire internal regulatory structure and the amendment of many internal directives.

To summarize, preparation for the application of the GDPR is a complex task affecting the activities of numerous areas of speciality, where the success of preparations will greatly influence the future operational risks of each credit institution and its options for the legitimate exploitation of the wealth of data at its disposal, and where the consequences of potential non-compliance may impact the assessment of the given credit institution and even its competitive position on the market.

At the same time, preparing for the GDPR also represents an opportunity to thoroughly review a wealth of data of exceptional importance from a business perspective, with a view to handling this data as securely as possible and with the lowest possible operational risk, while ensuring optimal opportunities for its exploitation within the context of the given credit institution's sphere of activity.

JEL codes: G2, K23

Keywords: data protection, processing of personal data, financial institutions

1. PRINCIPAL CHANGES CONNECTED TO APPLICATION OF THE GDPR

With the GDPR, instead of the current European Union Directive 95/46/EC, regulatory procedures are carried out according to an EU Regulation with direct effect on individual Member States, characterized by a "one-stop shop" official jurisdiction spanning across EU borders. Based on these rules, therefore, a foreign data protection authority may proceed in Hungary in certain cases defined under the GDPR, as may the Hungarian data protection authorities abroad. These institutions may also carry out joint operations, delegate authority to one another in certain cases, co-operate for the sake of a unified mechanism, and so on. In the absence of relevant practical experience, the impact of such cross-border official jurisdiction on market players cannot yet be judged, but it already raises numerous questions today, some of which extend beyond the protection of personal data in the narrower sense.

The Regulation already contains changes on the level of underlying principles by formulating *requirements for data protection by design and by default*. The goal of this, on the one hand, is to ensure effective implementation of data protection principles, and on the other hand to incorporate into the data processing process the guarantees necessary for fulfilment of the requirements of the Regulation and protection of the rights of data subjects. Data protection by design and by default is a defining requirement of crucial importance in the processing and protection of personal data.

The GDPR codifies the *accountability principle*, on which basis Member States and supervisory authorities must, on the one hand, encourage the creation of data protection attestation mechanisms which prove that the data processing operations carried out by the data controller or data processor conform to the prescriptions of the Regulation, and on the other hand must be able to thoroughly document the legality of the data processing. They must always be able to demon-

strate the legal basis and purpose for their processing of data, and that the data is processed only to the extent necessary. All this also requires the development and internal regulation of a complex system of data protection records.

The Regulation also brings changes with respect to the *legal bases* that play a defining role in data processing. Replacing the current legal basis for data processing founded, as a principal rule, on the consent of the data subject or as provided by law ("obligatory" data processing), there will be six available legal bases and a narrower range of instances than before in which the consent of data subjects needs to be procured. There will be a separate legal basis for data processing if it is necessary for the performance of a contract, or if necessary for fulfilment of a legal obligation to which the data controller is subject, or if necessary for the assertion of the legitimate interests of the data controller or a third party. The start of application and appropriate selection of the legal basis according to the new provisions – considering the absence of relevant practical experience of the GDPR on the part of authorities and courts – may entail a compliance risk.

The Regulation also sets conditions for *data processing for purposes other than data collection*. Currently the use of existing data for other than the original purpose (based on original consent, notification, etc) qualifies as a new instance of data processing and may only be carried out in compliance with the original purpose (e.g. through renewed consent or notification). The GDPR establishes more flexible rules, determining a system of criteria for reconciling the divergent data processing process with the original goal.

The Regulation introduces the institution of *Attestation*, whereby Member States and supervisory authorities must encourage the creation of data protection attestation mechanisms which prove that the data processing operations carried out by the data controller or data processor conform to the prescriptions of the Regulation. Attestation presumably may have the effect of reinforcing trust and enhancing good reputation, and may thus even bring a business advantage.

The Regulation stipulates that Member States and supervisory authorities must encourage the elaboration of *sectoral codes of conduct*. The GDPR regulates information supply obligations in more detail than the present regulations, extending to the question of which information is to be made available when personal data has not been obtained from the data subject. The role of information supply, besides compliance with legal bases and data protection principles, is of heightened importance with respect to the validity of data processing.

As another essential new provision, the GDPR stipulates *the obligation to draw up an impact study* in the event of introduction of new technologies, in certain cases also prescribing consultations with data protection authorities. Elaborating the methodology and procedural rules for this impact study will be an important

task, for which Hungary's National Authority for Data Protection and Freedom of Information (NAIH) will publish relevant sets of criteria.

The Regulation also regulates *the requirement to maintain internal data protection records* with respect to the processed data and forwarding of data. Although Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (Privacy Act) currently contains provisions with respect to keeping records of forwarded data, it does not determine the content in detail. The GDPR defines the concept of a data protection incident more narrowly than the current definition under the Privacy Act; at the same time, it prescribes the obligation to inform the data protection authorities, and in certain cases even to inform the data subject(s). All this may entail significant consequences (official procedure, penalty, complaint by the data subject, claim for payment of damages, etc).

The GDPR also contains new provisions with respect to *data processors*. It determines the obligations of data processors with respect to certain contractual clauses, the employment of a Data Protection Officer, etc. The Regulation sets rules for joint data processing, the mandatory content of related contracts and the responsibility of joint data controllers, which, among other things, redefines the framework of data processing within banking groups. Joint data processing occurs when the goals and tools of data processing are determined jointly by two or more data controllers. Although the Privacy Act does not rule out joint data processing, the GDPR regulates it directly, determining the contractual content and the rules of accountability.

The GDPR regulates conditions for the applicability of *Binding Corporate Rules (BCRs)*. This provision is of particularly great significance for data controllers operating within corporate groups who forward personal data from within the European Union to a member of the group outside the European Union.

The rights of data subjects are augmented with a new right, the *right to data portability*. Data portability is the right of data subjects to receive and forward their personal data and, if this can be technically accomplished, to request the direct transfer of their data between data controllers. Questions of IT development and information security are among the issues that pertain to implementation of this right.

Compared to the current provisions of the Privacy Act pertaining to decisions made using automated data processing, the GDPR regulates *automated decision-making and profiling* in far greater detail. It is the right of the data subject not to be subjected to such a decision-making process. The data subject must be provided the opportunity to express their opinion or to raise an objection against a decision, as well as to request human intervention from the data controller. Decision-making by means of automated data processing may also occur based on the legal

authorization of a Member State; however, such laws must ensure appropriate guarantees. The making of automated decisions affecting data of a special nature is only permitted under additional conditions.

For security purposes, the Regulation introduces the institution of *pseudonymization*. According to the definition of the concept under the GDPR, pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject (natural person) without the use of additional information, provided that such additional information is stored separately and is subject to technical and organizational measures to ensure that the personal data cannot be attributed to an identified or identifiable natural person. The significance of application of pseudonymization also arises in the context of compliance with data protection by design and by default.

The *right to erasure* ("right to be forgotten") is an accentuated requirement of the Regulation. The Privacy Act hitherto already contained the obligation to erase personal data if the purpose of data processing has ceased to apply and there are no legal grounds for the continuing possibility or obligation to preserve the data. The GDPR regulates the right to erasure in more detail than the Privacy Act and places important emphasis on the "right to be forgotten" among the rights of the data subject.

With regard to *questions of data transfer*, the GDPR defines rules for data transfers at greater length and in greater detail than the provisions of the Privacy Act, setting the condition that the data controller or data processor should comply with the conditions for data transfer under the GDPR, with separate regulations for data transfers subject to appropriate safeguards.

The GDPR broadens the scope of obligatory employment of a *Data Protection Officer* (under the Privacy Act, currently the person responsible for data protection), strengthening their legal status and enhancing protection for this compliance control function, which will necessitate a rethink of the role of this sphere of tasks at credit institutions.

2, BRAVE NEW WORLD: THE NEW LEGAL BASES

Without the appropriate legal basis, data processing cannot be lawful. Consequently, the clarification of certain questions relating to the application of new legal bases under the GDPR constitutes an especially important part of preparations. Those applying internal data protection regulations must have access to adequate guidance when it comes to being able to determine the appropriate legal basis.

The essential difference in application of the provisions relating to legal bases under the GDPR and the Privacy Act, as they relate to credit institutions as well, is that while two principal conditions – voluntary consent and obligation under the law – currently serve as the legal bases for data processing in the case of the Privacy Act, the GDPR will add a number of additional legal bases that apply to data processing from 25 May 2018. Accordingly, in addition to other legal bases, the legislation expands and broadens the scope to include legal bases for data processing which are dependent on the performance of a contract, the assertion of legitimate interests, or the fulfilment of a legal obligation pertaining to the data controller.

Given that the processing of personal data will be characterized by a broader range of legal bases than the currently applicable practice under the Privacy Act, many questions remain open with respect to the application of these legal bases. Professional theoretical debates in the coming years with respect to the application and delineation of legal bases under the GDPR, together with practical experience on the part of authorities and courts, will result in a more settled practice. A thorough review of individual data processing goals, together with the determination and regulation of criteria for future classification under appropriate legal bases according to the GDPR, will be a prominent task for data controllers, involving all areas of specialization where personal data is processed or data processing goals are determined.

At the start of application of the GDPR on 25 May 2018, there will be a significant customer base for which the legal basis for data processing was voluntary consent. Although Article 7 of the currently operative EU Data Protection Directive, similarly to the GDPR, originally allowed for a variety of legal bases for data processing, data controllers were compelled by the restricting provisions of the Privacy Act to indicate the legal basis as voluntary consent. As far as we are aware at present regarding data processing operations currently in progress, there is no need to request a change or renewed consent – as stands to reason if the legal basis was appropriate at the time. Naturally, if a review of data processing operations finds that the process is not lawful, then it can only be legitimized if harmonized with the legal conditions, so that in given cases it may be necessary for data subjects to restate their positions.

As far as the future practical application of the GDPR is concerned on the part of financial organizations, *four legal bases* for data processing of the six specified in the Regulation are particularly worth mentioning, namely where:

- Data processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract; or

- Data processing is necessary for compliance with a legal obligation to which the data controller is subject; or
- Data processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which necessitate the protection of personal data, in particularly where the data subject is a child; or
- The data subject has given their consent.

In addition to the four above-mentioned legal bases, the remaining two legal bases under the GDPR (data processing in the public interest, or in order to protect the vital interests of the data subject) are typically less likely to arise in daily practice in connection with the activities of financial organizations. Voluntary consent as a legal basis will presumably apply in future only to a narrower range of instances than under the provisions of the current Privacy Act, since the legal bases connected to contracts and the applicability of legitimate interests will supersede a significant portion of the legal basis of voluntary consent as currently applied.

The legal criteria for voluntary consent are elaborated in more detail by the GDPR than under the Privacy Act, and greater attention will need to be paid to the application of these requirements. Consent must be freely given, specific, informed and clearly affirmative of the data subject's agreement to the processing of their personal data. Silence or pre-ticked checkboxes, for example, do not constitute active consent. If data processing is based on consent, then the data controller must be able to verify that the data subject has consented to the processing of his or her personal data. If the data subject has given their consent in the form of a written statement which also applies to other matters, then the request for consent must be submitted in a way that can be unequivocally differentiated from these other matters, in a comprehensible and easily accessible form, and in clear and simple language. Any part of such a statement which contains the consent of the data subject, but which infringes the Regulation, will not have binding force. The data subject is entitled to withdraw their consent at any time. The withdrawal of consent does not affect the legitimacy of data processing based on consent prior to the withdrawal. As regards legitimate interest as a legal basis founded on the weighing of interests, the currently valid Privacy Act permits its application only in an extraordinarily narrow range of circumstances. The GDPR opens the way to application of this legal basis much more broadly than under the legal regulations currently in force.

3. LEGITIMATE INTEREST: A NEW "MIRACLE WEAPON" AND QUESTIONS OF ITS APPLICATION

With respect to the legal bases to be applied under the GDPR, a "legitimate interest" determined on the basis of an assessment of interests can be expected in future to be used as the legal basis in numerous cases where data controllers have hitherto been obliged to obtain voluntary consent. Such cases may include, for example, when the legitimate interest of a credit institution can be deduced from a given law; however, this will not be determined in a direct manner as a legal obligation under the GDPR. In the case of labour-related data processing, legitimate interest will constitute the legal basis almost exclusively, while also arising in certain instances related to direct marketing (e.g. the sending of newsletters).

The Privacy Act currently in force permits legitimate interest to be applied only in a narrow range of cases. Accordingly, as things presently stand, voluntary consent represents the legal basis even in cases where there might otherwise also be a legitimate interest under Article 7 of the currently operative EU Data Protection Directive. The Hungarian regulations currently in force, however, are more restrictive in nature than the provisions of the Directive.

In several of its recommendations and resolutions, the National Authority for Data Protection and Freedom of Information (NAIH) already accepts the direct application of legitimate interest in accordance with Article 7, point (f) of the Directive, while in certain cases (in the case of employment relationships) it regards this legal basis as a principle rule to be applied.

In its resolution reached in case no. NAIH/2015/515/3/H. – /NAIH-1116/2014/H/, the NAIH refers, with respect to Article 7, point (f) of the Directive, to the ruling of the Court of Justice of the European Union, made in a preliminary decision-making procedure, that this point of the Directive has direct effect, so that anyone can cite it before the court of a Member State. In its resolution, the NAIH also stated that, since the Privacy Act did not adequately transplant Article 7, point (f) of the Directive, the authority had carried out an interest assessment test based on Article 7, point (f) of the Directive, as discussed in detail in Opinion 06/2014 of the Data Protection Working Party set up under Article 29 of the Data Protection Directive.

The NAIH's recommendation of 23 January 2013, regarding the fundamental requirements for electronic surveillance systems used in the workplace, refers to the position repeatedly taken by the Article 29 Data Protection Working Party that the possibility of voluntary consent is questionable within the employer-employee relationship, and consequently the application of other legal bases specified in

the Data Protection Directive is justified in the context of labour law. In its Opinion 15/2011 on definition of the concept of consent, the Data Protection Working Party also stated that consent may not be the sole legal basis for lawful data processing, but that the other legal bases specified in Article 7 of the Data Protection Directive may also be applied with respect to data controllers.

Despite all this, data controllers currently still remain cautious in application of legitimate interest as a legal basis with respect to the provisions of the Privacy Act now in force.

Within the direct scope of the GDPR, the path will clearly be opened in future to *data processing on the grounds of legitimate interest* at credit institutions, subject to an appropriate assessment of interests. At the same time, applying this legal basis means stepping on thin ice since instances of its application cannot be defined on a case-by-case basis, while the result of the interest assessment may be disputed by the customer or deemed to be without basis by the data protection authorities. The EU's Article 29 Data Protection Working Party also dealt with questions of the application of legitimate interest. The notion of "interest" applied by the Working Party is a broader category than the goal of data processing, where even general basic principles are to be taken into account alongside itemised material legal rules. With respect to the Google Street View (GSV) service, the NAIH accepted that Google had a legitimate interest connected to introduction of the GSV service, the implementation of which might necessitate the processing of the data of data subjects. This interpretation, it seems, has opened the way to economic interest in the broad sense being defined as legitimate interest.

At the same time, in the practice of the courts, legitimate interest "must always be tied to some interest appearing in a way specified in law, failing which 'legitimate' interest would be replaced by 'interest worthy of recognition'." Application of this legal basis therefore demands a great degree of caution and self-restraint, as if the legal basis does not prove well-founded, this may result in invalid processing of data with potential unforeseeable consequences with respect to mass data processing.

In short, therefore, although currently there are instances and opinions of data protection authorities in connection with the application of legitimate interest, overall it can be assumed that it will only be possible to apply this legal basis more securely with the benefit of several years of experience on the part of data protection authorities and courts. The question of where data processing goals may present themselves within the activities of credit institutions, where this legal basis might reasonably occasion the need for voluntary consent as before, must be subject to separate analysis. For data processing to be lawful on this legal basis as well, it is also implicitly necessary to observe data processing principles and

conditions for the provision of information. Legitimate interest, therefore, is no business "miracle weapon," but its careful application based on an assessment of interests makes the practice of credit institutions simpler and more realistic without infringing on the rights of data subjects.

4. APPLICATION OF THE GDPR AND OTHER RELATED REGULATIONS OF THE LAW

Numerous laws on the Hungarian statute books currently contain provisions which give rise to the processing of personal data within the activities of credit institutions. In connection with the application of the GDPR, it is an inescapable necessity to review these laws, and furthermore to examine other norms – not on the level of laws, but still affecting the processing of personal data – to see how they are harmonized with the provisions of the GDPR, as well as how the new legal bases under the GDPR impact the processing of personal data managed in connection with these norms after 25 May 2018.

An examination of the laws reveals significant differences with regard to the method of defining data processing, which in turn determine the specification of the given legal basis. Some of these laws directly stipulate obligatory data processing, itemising the individual data to be processed, as well as the conditions for the transfer of this data (e.g. the law on the prevention of money laundering and financing of terrorism (Pmt.), the act on the Central Credit Information System (KHR), etc). In the case of the latter laws, it is clear at present that the legal basis for data processing is an obligatory stipulation under the law.

In other cases, the processing of personal data is generated indirectly by provisions of the law, but the law does not determine the personal data to be processed. Between these two, there are also provisions of the law where the processing of personal data is a requirement that is more easily circumscribed, but where the definitions are not entirely in harmony with the requirement of the Privacy Act pertaining to obligatory data processing, which determines the processing of data on a case-by-case basis. Besides laws, there are also governmental and ministerial decrees that affect the processing of personal data, where – in the absence of authorization under the law – voluntary consent is currently the legal basis for data processing. After application of the GDPR, based on fulfilment of a legal obligation or legitimate interest, classifying such instances of data processing under the appropriate legal basis will appear more manageable.

Looking ahead to the provisions of the GDPR entering into force in future, an essential question is whether certain laws will be amended by the time of its application. For example, if current regulations pertaining to the transfer of banking and

securities secrets under the Act on Credit Institutions and Financial Enterprises (Hpt.) and the Act on Investment Firms and Commodity Exchange Service Providers (Bszt.) are not amended with respect to the legal basis of legitimate interest or other legal obligations, then these more "market-oriented" provisions would not be applicable, which might also present more opportunities for transfers of data among companies in a group in respect of other possible contractual relationships.

Representatives of the advertising profession and direct marketing experts are also looking ahead to the GDPR with great anticipation, seeing in it opportunities in, for example, the application of legitimate interest in certain other contexts (e.g. in the sending of newsletters). However, unless there is an amendment of the main regulation of the Advertising Act (Rktv.) pertaining to the sending of advertising messages based – aside from a narrow range of exceptions – on prior consent, then the GDPR would scarcely signify any substantive change in this area should the Advertising Act qualify as a *lex specialis*. It is another matter how a data controller should proceed if they encounter a provision of the law which, in their interpretation, is not in harmony with the provisions of the GDPR, in an area where the GDPR does not provide a different regulatory option within the jurisdiction of a Member State.

5. QUESTIONS OF THE FRAMING OF A SECTOR-SPECIFIC CODE OF CONDUCT FOR DATA PROTECTION: A SAFETY BELT OR A RESTRICTION ON FREEDOM?

The GDPR stipulates that Member States and supervisory authorities must encourage the drawing up of sector-specific codes of conduct. One advantage of such a code, in the event of the given authority accepting certain provisions of the code (e.g. with regard to the application of legal bases, such as the criteria for establishing legitimate interest in particular), would be that it would reduce the compliance and operational risks, functioning as a kind of safety belt. At the same time, we know that a safety belt simultaneously restricts free movement, and – despite the risk entailed – not everybody believes in using one. Nevertheless, to enhance its good reputation, a credit institution would surely consent to such a code as adopted by the data protection authorities.

The process of elaborating the content of a sector-specific code and securing its acceptance by the authorities might drag on for several years, and at present it remains unknown (and would require a preliminary survey to discover) which credit institutions would demand or submit to such a code. At the same time, preparation of a code at the sector-specific level might in itself already help credit

institutions to develop a uniform practice of legal interpretation for application of the GDPR. Other solutions might also be sought outside of the code for the establishment of a safer, more uniform practice with respect to application of the GDPR; for example, the elaboration of a given sector-specific methodology for applying legal bases and its possible auditing by authorities, or even the defining of requirements for the content of a code specific to data protection as a sector in itself, and its auditing by authorities.

6. FROM "PERSON RESPONSIBLE FOR DATA PROTECTION" TO "DATA PROTECTION OFFICER": A CHANGE OF NAME OR ROLE?

With the application of the GDPR, the rather unfortunate concept of "person responsible for data protection" (*adatvédelmi felelős*) will disappear from the Privacy Act under Hungarian law, to be replaced by the Data Protection Officer (DPO). The current definition of the DPO as the "person responsible for data protection" may also be misleading for those less familiar with the tasks of the office under the law. The practice whereby this sphere of "responsible" data protection tasks is most frequently performed by legal counsels attached to the legal department likewise appears to reinforce this, as if a legal counsel specializing in a specified area were predestined to carry out operative tasks and services at the administrative level.

At the same time, it is clear that the person responsible for data protection, with respect to their tasks legally defined under the Privacy Act, is the senior independent agent supervising the observance of data protection norms within the organization, who – beyond their supervisory obligations – cooperates and supports decision-making connected with data processing, as well as safeguarding the rights of data subjects. The latter could be defined as a kind of advisory activity, or as the activity of a type of internal ombudsman within an organization responsible for clients and employees as data subjects. With their tasks under the law, and by virtue of being directly under the supervision of the head of the given body based on the relevant provision of the law, the person responsible for data protection is positioned at the same level as other compliance controls under the law, since the object of their supervisory activity is to monitor observance of laws pertaining to the protection of personal data and the stipulations of data protection regulations.

Given that at credit institutions there is scarcely any process or unit of the organization which is not involved in the processing of personal data, it is hardly an exaggeration to say that the scope of compliance control of the person responsible

for data protection – or the Data Protection Officer, as they will come to be known – extends to almost all activities of the credit institution.

The GDPR broadens the scope of obligatory employment of a Data Protection Officer, strengthening their legal status and enhancing protection for this compliance control function. Contrary to the regulations currently in force in Hungary, the GDPR does not require specific academic (legal, IT) qualifications for fulfilment of the tasks of a DPO, but instead regards "professional aptitude and particularly professional knowledge of data protection law and practice" and suitability for the fulfilment of tasks defined under the Regulation as the primary criteria for selection.

According to the provisions of the GDPR, the DPO must be provided with the resources necessary for the fulfilment of their tasks under the Regulation and the maintenance of knowledge to an expert level, so that they are able to participate in a timely manner in cases related to the protection of personal data. In addition, it is necessary to ensure that the DPO accepts no instructions from any party regarding fulfilment of their tasks, that they are directly answerable to the "senior management," and that the data controller or data processor "cannot dismiss or sanction [the DPO] in connection with the performance of their tasks."

Under the Regulation, data subjects may appeal directly to the DPO. Besides ensuring independence, the monitoring of potential conflicts of interest is also worthy of special attention within the activities of the DPO. A solution where the DPO comes into contact with another area of activity in which the determination and actual processing of personal data occurs is scarcely compatible. Such spheres of activity may include compliance, for example, which typically involves data processing falling within the DPO's personal compliance control activity (personal data processed in connection with insider trading, trading on own account, conflicts of interest, etc).

An example of the determination of independence of a control function is Recommendation 7/2017 (VII.5) of the National Bank of Hungary on the protection of IT systems, which states (under point 13.1.2): "*Independence should be taken to mean that the control department cannot be involved in the planning, selection, implementation or operation of the control measures to be monitored, and is not in a subordinate relationship with the monitored department.*"

Looking at the new sphere of action of the DPO, it points more emphatically in the direction of an independent compliance control function and the related sphere of management tasks. An examination of the new organizational and personnel conditions of data protection compliance control, and of the relationship between control functions, merits a separate study in itself, with consideration for the risk-based internal control approach as well.

7. A MEETING OF PAST AND FUTURE: HOW DO WE PREPARE FOR APPLICATION OF THE GDPR?

The GDPR must be applied from 25 May 2018, but data processing operations that began before the date of its application must also be "brought in line" with the GDPR within two years of the Regulation entering into effect (on 24 May 2016) – so basically by the time of the Regulation's application. A twofold task is thus incumbent on data controllers:

– on the one hand, they must be ready to "spring to action" for application of the new data protection norms by 25 May 2018, and – by means of internal regulations and ensuring other organizational, personnel and IT conditions – the execution of the provisions to be applied from this date;
– on the other hand, by this date they must also review all procedures that entail the processing of personal data and harmonize these data processing tasks with the provisions of the GDPR.

The process of preparation can be broken down into a number of stages and tasks, which can be distinguished thus:

a) assessment of ongoing data processing operations;
b) review of the legality of ongoing data processing operations, and observations with respect to the legality of the data processing operations;
c) in the event of potential non-conformity with the law, determination and execution of the necessary measures;
d) examination of the conditions for harmonization of data processing operations with the GDPR, determination and execution of the necessary measures;
e) with respect to the review of procedures and data processing operations, framing of internal data protection regulations and related other internal regulations for application of the GDPR;
f) implementation of the organizational, personnel, IT and other technical conditions necessary to ensure compliance with the GDPR by the time of its application;
g) a special, heightened focus on the carrying out of educational tasks;
h) assessment of the procedures in preparations for application of the GDPR, assessment of the regulation and effective legality of data processing operations, quasi internal audit in certain defined cases, or potential external audit.

Execution of the tasks related to the above stages of preparations requires the detailed elaboration of these tasks, and of separate but related sets of criteria and other documents.

7.1 Assessment of ongoing data processing operations

The successful assessment of ongoing data processing operations is of key importance since it will serve as the starting point for examination of the legality of data processing, harmonization with the GDPR, elaboration of data protection records, and compliance with the accountability principle. Any aspect of the review of data processing that is potentially omitted from this assessment may linger on as a latent compliance risk.

Earlier internal data protection records and the data inventory may provide help in this, but a review necessitates that every data processing operation is re-examined – taking each data processing goal in turn – in every process that involves the processing of personal data. Consequently, processes in product development, the extension of credit, credit management, claims management, payment services, investment services activity, direct marketing, compliance, HR, labour issues, bank security and so forth must be reviewed, as must every data processing operation in the context of data transfers, the keeping of records, recording in IT systems, crossovers between systems, erasure of data from systems, selection of documents for destruction, etc. A review taking each data processing goal in turn requires an examination of products and services to be conducted practically at product level.

A review of ongoing data processing operations requires the elaboration of a complex set of criteria. Consequently, there is good reason to develop uniform data questionnaires, and instructions for filling them out, in order to assess data processing and data transfers, as well as a set of criteria needed for determining legality, data cleansing and GDPR harmonization tasks, with particular attention to the accountability principle and the elaboration of records according to the GDPR.

Such criteria for the assessment of ongoing data processing operations include: designation of the given data processing operation; categories of data subjects; the data processed; goal and legal basis of the data processing; source of the data; method of data collection; where the data is recorded and stored; who are the data processors; whether any data transfer occurs outside the bank or abroad; whether automated data processing is applied; whether profiling is used on the data; how long the data will be preserved, etc. It is also important to assess and analyse the nature of current data processing notifications related to individual data processing operations.

For application of the GDPR on 25 May 2018, all data processing notifications will need to be reframed (general homepage and cookie notices; notifications pertaining to use of individual products and services; data processing notifications contained in contracts; notifications relating to audio and video recordings; no-

tifications related to access control systems, direct marketing, job applications, labour-related data processing operations, and so on).

Within financial organizations engaged in data processing, the specific activities of various individual units of the organization mean that significant differences appear with respect to the data processing they perform in the broader sense. In this way, for example, there are units of an organization which determine the range of personal data to be processed as part of their activity, but which do not actually "process" any personal data. Such is the case with activity in the development and elaboration of new products, which relies on earlier experiences that entail the use of personal data. Preventive compliance control is of key importance in terms of data processing determined by various departments, and related internal rules and procedures.

The processing of personal data specifically arises in the activity of other units of an organization (credit or risk management departments, claims management, etc). There are also units of an organization specializing in data transfer (e.g. a department carrying out regular data provision for the National Bank of Hungary (MNB), Hungarian State Treasury (MÁK), etc, or a department or organizational unit providing responses to requests from authorities). Data processing may likewise take a different form in the marketing department, for example, where personal data may be determined, collected, recorded and processed on the basis of relevant specific laws – e.g. the Advertising Act (Rktv.).

Elsewhere, the processing of personal data of third parties not qualifying as customers may typically take place (e.g. at secretariats of a company, the personal data of external members of committees according to the Act on Credit Institutions and Financial Enterprises (Hpt.), external supervisory board members, shareholders, etc).

Another set of review criteria is required by the IT department, where, on the one hand, the systems through which personal data are actually processed, the nature of the data and the purpose of its processing is subject to review, as is the nature of transfers involving this data, and the extent to which IT systems conform to the legal requirements, currently of the Privacy Act, and subsequently of the future GDPR. Such requirements may include, for example, the technical conditions for erasure, ticking or blocking of data, or aspects of automated data processing, profiling, pseudonymization and data portability.

The review also affects the full range of GDPR harmonization and information security tasks, demanding the elaboration and application of its own set of review and harmonization criteria.

Preparatory work affecting information security and IT security is an area requiring its own separate set of criteria. The applied concepts and questions of compli-

ance with various laws impacting this specialized area, as well as the examination of the related control function aspect in particular, merits an independent study.

Reviews of the activities of every data processor with respect to the requirements of the GDPR, as well as the subsequent amendment of contracts, will be subject to separate review, likewise demanding its own set of criteria in turn, as well as a review of all data processing activity and amendment of all related contracts. As an issue not to be disregarded, the changes of the GDPR will presumably generate numerous IT developments, which will be connected to outsourced activity and implemented at the data processors. Issues of the time and cost aspects of such developments will arise, impacting the content of other contractual relationships between credit institutions and those carrying out outsourced activity.

At the same time, the ultimate goals of all sets of criteria relating to GDPR preparations must be harmonized. The set of review criteria must be elaborated so that the legality of data processing can be assessed based on the content of data questionnaires and tables, so that additional measures to be taken to ensure harmonization can be determined, and – keeping the accountability principle in mind – so that the transparency of data processing is guaranteed and can serve as a basis for the creation of internal data protection records in compliance with the expectations of the Regulation.

It is an important task to map out and audit the network of laws, internal regulations and procedures that regulate the activities of individual departments and related processing of personal data, both from the point of view of the Privacy Act and GDPR harmonization (via necessary amendments).

7.2 Tasks following the assessment of ongoing data processing operations

One of the main tasks following the assessment of data is to examine the legality of data processing operations, which must be carried out for each data processing goal. We can only speak of lawful data processing if it has an appropriate legal basis, if it complies with the relevant principles of data processing, and if the data subject has been adequately informed in accordance with legal requirements. The elaboration of a set of criteria taking these requirements into account is justified for the examination of legality. Such an examination must be carried out, on the one hand, by taking the provisions of the Privacy Act currently in force into consideration, with a view to eliminating any data processing operations that may qualify as unlawful; and on the other hand, by determining the new legal bases for the future with respect to data processing operations begun for the same purposes from 25 May 2018.

Under the GDPR, provided data processing operations were based on consent under Directive 95/46/EC currently in force, and provided the data subjects have

given their consent in keeping with the conditions set down in the Regulation, there is no need to request renewed consent. A more problematic situation potentially arises if the examination of legality uncovers some deficiency, whereby some element does not fully conform under the law. Here the question may be whether the shortcoming can be remedied (for example, via notification), or if the invalid aspect cannot be eliminated for some other reason (for example, if with respect to some data processing task, it does not conform to the principle of data frugality).

An essential question is to establish which of the provisions of the GDPR must be applied with respect to ongoing data processing operations, and which exclusively with respect to data processing begun after 25 May 2018. In this way, for example, the obligation to carry out a Data Protection Impact Assessment does not extend to ongoing data processing begun earlier.

At the same time, however, compliance with new principles of data processing such as the accountability principle must be interpreted as a requirement for every data processing operation under way as of 25 May 2018. In other words, it must be possible to document the legality of data processing at any time. This requirement already appears in the Privacy Act currently in force, to the extent that in court proceedings the data controller must prove that data processing is lawful, which already constitutes an outline of the accountability principle.

Obviously it is also necessary to conform to internal data protection records under the GDPR, both before application of the Regulation and with respect to data processing begun thereafter. The keeping of internal data protection records is currently already a requirement, although the content is not defined under the Privacy Act. The GDPR, on the other hand, already contains provisions in this regard.

By the time of application of the GDPR, all notifications pertaining to data processing (product descriptions, marketing prospectuses, website information, information related to sound recording or camera surveillance, etc) must be reviewed and, where necessary, reframed to bring them into line with the GDPR, as must various customer declaration forms – again, where necessary. Based on new provisions pertaining to multiple data controllers or data processors, contractual relationships must be reviewed and amended. Practically all contracts relating to data processors (to those carrying out outsourced activity, independent intermediaries, agents or other data processors) are to be reviewed and amended, taking into consideration the set of criteria under the Regulation. An important aspect is the configuration and regulation of a set of conditions and processes in accordance with the principle of data protection by design and by default.

Data cleansing may also be connected to the outcome of the review, together with the necessary IT developments (e.g. technical IT implementation of data erasure, records related to processing and transfer of data, in connection with the new right to data portability or the new rules on profiling). Where erasure cannot be guaranteed within the appropriate time, steps must be taken to mitigate related risks (blocking, restrictions on access, etc).

It is also expedient to tie into preparations issues related to the mapping of operational risks, determination of monitoring points, and generally the development and regulation of management oversight built into the process. As a related task following assessment of ongoing data processing operations, it is reasonable – taking the principles of data processing into account – to re-examine the handling of authorization, to review and (where necessary) re-regulate who may access personal data, for what purpose and to what extent.

It is likewise justified to examine fulfilment of the tasks of the Data Protection Officer, as well as the conditions necessary for carrying out these tasks, and to take steps as needed to ensure conformity with the Regulation. Based on the "accountability principle" under the GDPR, it must be possible to fully document the legality of data processing operations and, with this in mind, to shape the order of data processing and the obligatory keeping of records under the GDPR, as well as the system of documentation in support of the latter.

7.3 Data protection regulations and other related internal regulations

For application of the GDPR from 25 May 2018, new data protection regulations must be drawn up. The earlier expectation of Hungary's data protection authorities was that data protection regulations should be required to function as a kind of handbook. It follows from this that data protection regulations will not conform to their own content requirements if they merely contain written norms. It is another matter that in practice, regulations operate on several levels when it comes to credit institutions, and that even in the case of data protection regulations that contain still more detailed requirements, certain executive provisions will be implemented via various separate regulations (e.g. the recording of telephone conversations under call centre procedures, or special data processing rules for claims management under their own relevant procedures). Moreover, some changes may also affect a credit institution's Organizational and Operational Rules at the regulatory level with respect to individual tasks, even broken down to the level of individual job descriptions.

National data protection regulations, therefore, beyond individual data protection regulations, must pay attention to all other internal regulations that affect the processing of personal data, and must cover the whole network of such regulations. The regulations must be practically focused. Besides processes, the regula-

tions demand the new legal institutions of the GDPR to be elaborated, necessitating IT developments and related separate regulations.

When amending data protection regulations, or rather when drawing up new data protection regulations, it is expedient to draw attention to the *following considerations of content*:

- provisions pertaining to basic concepts and principles, to be supplemented and reworded to reflect changes under the GDPR;
- the application of new legal bases, and the relevant methodology, to be regulated, with particular regard – in the case of current data processing goals – to data processing operations begun from 25 May 2018, which, unlike the previously applied legal bases, must be classified under several legal bases from this date onwards;
- new legal institutions and their procedural rules to be elaborated in the regulations, such as instances of obligatory impact studies, and changing new rules for profiling, data portability and pseudonymization as data protection incidents;
- attention to be paid to the importance of regulations pertaining to the rights of data subjects, with particular regard to the "right to be forgotten" and requirements for data erasure;
- as a sub-area that cannot be neglected, the regulation of data processing for purposes other than data collection, and elaboration of aspects of joint data processing.

Beyond the above, another important task is to develop a new set of requirements for data processors with respect to the protection of personal data. Elaboration and regulation of a suitable system for notifying data subjects also remains an essential task. Careful examination of the sphere of action of the Data Protection Officer, and elaboration of his or her independent control function, is similarly deserving of special attention.

As a priority, the regulations must serve compliance with the accountability principle, so that the legality of data processing operations can be confirmed at any time based on the regulated activity and internal records of data processing and transfer.

Assisting compliance with the law, and the activities of employees in the protection of personal data, are numerous auxiliary materials forming appendices to the data protection regulations (e.g. data forms used for determining new data processing operations, or for opinions of the Data Protection Officer, data protec-

tion incident report forms, etc).

Information security is typically a separate regulatory area at credit institutions, with its own regulations, so that its investigative and regulatory system is not examined within the present framework.

7.4 Other tasks related to preparations for the GDPR

Organizational, personnel-related, IT and other technical conditions necessary to ensure compliance with the GDPR must be put in place by the time of the Regulation's application. At credit institutions and bank groups carrying out more complex activities, the drawing up of data protection regulations means reviewing the regulation – and, where necessary, the amendment – of all processes that entail the processing of personal data. Based on the set of criteria for application of the new legal bases, data processing notifications must also be reviewed and reframed. This affects all product descriptions, but also other website information, notifications related to camera or sound recordings, etc.

Based on new provisions pertaining to multiple data controllers or data processors, contractual relationships must also be reviewed and amended. Practically all contracts relating to data processors (to those carrying out outsourced activity, independent intermediaries, agents or other data processors) are to be reviewed and amended, taking into account the set of criteria under the Regulation. An important aspect is the configuration and regulation of a set of conditions and processes in accordance with the principle of data protection by design and by default, including defining the tasks and persons responsible for protection of personal data.

As part of compliance with the law and preparations for application of the GDPR, it is reasonable to carry out an internal or – depending on a decision to this effect – external audit.

7.5 Educational tasks

Special emphasis in preparations must be given to the education of employees and data processors (those carrying out outsourced activity, agents qualifying as data processors, and other data processors).

Education through e-learning of a more general nature, extending to all and failing to take disparate peculiarities of individual areas of specialization adequately into account, spells "certain death." What is needed is education in data protection which (in a documented manner) ensures that employees or agents in given areas of specialization proceed with a "tailor-made" knowledge of data protection in the execution of their daily tasks. Although general knowledge extending to all is undoubtedly also necessary, those determining new data processing pro-

cedures in product regulation, for example, or employees of organizational units expressly specializing only in data transfer, need to be able to consciously apply specific knowledge to ensure routine compliance with data protection requirements in their daily work. Education must keep these specific aspects in mind.

8. THE IMPACT OF THE GDPR ON MARKET COMPETITION

As for the future, it can be expected that the penalties of hundreds of millions, or even billions, of forints to be imposed on credit institutions for violation of norms on the protection of personal data following application of the GDPR will create more of a stir in the media and society than the official fines of a few million forints that can currently be imposed.

Customers might judge a credit institution differently if it has been slapped with a fine of hundreds of millions or even several billion forints, irrespective of whether the nature of the violation is similar to one for which a fine of just a few million forints would currently be imposed. If an incidence arises – in the context of data processing information published on a website, data processing operations initiated there, product-related printed matter accessible to anyone, or direct marketing procedures – where failure to comply with the provisions of the GDPR is clearly demonstrable in some regard, this may have many consequences, depending on who examines the procedure concerned and to what purpose. It may be a case of conscious checks by data protection authorities, or it may happen otherwise. A violation of the law that the authorities sanction with a sizeable fine may also heighten the appetite for claims under civil law, in the hope that the magnitude of sanctions might put the assessment of such civil claims on a different scale than at present with regard to the amounts that may be awarded.

When something unlawful occurs, we need not think of it as being diabolically wicked. Lawful data processing is conditional on the appropriate legal basis, compliance with data processing principles (purpose limitation, data minimization, etc), and the adequate content of prior notification of data subjects. If one of these is violated, then data processing is unlawful.

The new legal bases of the GDPR – particularly until the relevant official and judicial practice has evolved – do not exclude the possibility that an erroneous legal basis will be determined, since no itemised regulation exists, or can exist, in this regard. Moreover, even with respect to other conditions (e.g. the notification obligation), the compliance risk cannot be entirely ruled out, particularly in individual recommendations of the data protection authorities and bearing in mind expectations formulated in other official documents. Compliance with basic principles may also be subject to debate; whether every piece of data is really necessary

for the attainment of the data processing goal, whether the least invasive methods are to be used – or, when debatable legitimate interest is applied, the result of the assessment of interests.

The application of data protection norms under the GDPR, while it may present more opportunities, also entails the possibility of a far greater compliance risk, at least in the coming years until the relevant official and judicial practice has evolved. Each new data processing operation may entail risks with respect to the appropriate determination of legal bases, compliance with every principle of data protection, adequate notification, subsequent lawful use of data, and processing of this data for only the appropriate period of time.

The penalties that may be imposed in future under the GDPR (EUR 20 million, or 4% of the annual global market turnover of the institution controlling or processing the data) lend greater emphasis to the elaboration of procedures for managing compliance risk as efficiently as possible, as well as the most efficient possible operation of compliance control by the Data Protection Officer. Beyond fines imposed by the data protection authorities, other potential consequences must also be addressed. An order to erase personal data in the event of unlawful data processing may have many consequences with respect to the operation of the database itself or its role within the IT system (e.g. for identification purposes). The GDPR provides data subjects with the right to compensation, while prevailing Hungarian law envisages several situations under criminal law. Good reputation may be damaged by an official fine, or in the context of notification of customers in connection with data protection incidents.

Development of the organizational and personnel-related conditions for personal data protection controls and their efficient operation can thus be expected to play a more significant role in the coming years.

Perhaps it is no exaggeration to state that the legality of processing of personal data by a given credit institution, its transparency to customers, or its non-compliance and the sanctions that potentially follow, may impact the competitive position of the given credit institution in terms of trust or loss of trust. All these risks may reinforce the idea of examining the creation of a new type of data protection control organization that departs from current practice.

9. QUESTIONS OF THE CREATION OF A NEW TYPE OF DATA PROTECTION CONTROL ORGANIZATION

The creation of an efficient data protection control organization affects numerous operational and personnel-related conditions, but changes in attitude should also not be ignored. Internal supervision and compliance control functions, in light of their historical development, are already more advanced in terms of their place and acceptance within an organization. At larger credit institutions, they typically already function at the level of the board of directors, or at least a key department within the organization. The person responsible for data protection – who often also has other tasks – is the "youngest son" among those responsible for control functions.

In so far as we take risk-based control as the starting point, based on the size of the area to be overseen, the scale of potential compliance risks and official penalties, as well as other consequences (erasure of data, compensation, injury to reputation, etc), the question arises as to how to reconsider the role of the personal data protection control function and its organizational and operational conditions.

As far as the area to be supervised is concerned, there is almost no process or organizational unit of a credit institution which is not connected to the processing of personal data in some way. There are numerous instances of data processing situations, from the point at which someone enters a bank branch; where video recording by cameras takes place; where the customer fills out forms containing personal details or signs a contract; where processing of personal data begins, electronically or otherwise, in connection with the utilization of products and services; where direct marketing declarations are filled out; where personal data are processed in connection with claims management; or where mass data transfer occurs within the context of regular data supply or based on ad hoc requests for the authorities, etc.

Presumably one task among others in the future will be the theoretical elaboration of methods of data protection compliance control with a greater historical perspective in the case of other supervisory control functions. The future will sooner or later probably see a system of data protection control at credit institutions which will collaborate efficiently in numerous processes that entail the processing of personal data, through conscious and wide-reaching, risk-based oversight, promoting the lawful and secure processing of data and mitigating compliance and operational risks.

All this will require a Data Protection Officer – essentially a manager supervising data protection – who, beyond legal knowledge of the protection of personal data, is able to review the processes of the given credit institution in a way that permits

them to give advice to assist lawful data processing and the development of a comprehensive system of controls pertaining to processes that entail the protection of personal data.

10. SUMMARY

The success of preparations for application of the GDPR from May 2018 will have a decisive impact on the future operational risks of credit institutions. Presumably few would dispute the accentuated role played by a credit institution's database as a business resource. At the same time, studies discussing databases cite the finding (backed up by our own experience) that organizations typically still do not employ an independent person responsible for data who – positioned somewhere on the border between business operations and IT – would promote the most efficient possible exploitation of available data.

At the same time, questions of complex data processing lead to the examination of related operative and supervisory tasks, the links and necessary demarcations between them, and the relevant organizational and personnel-related conditions, since it is only through the coordination of activities among several areas of specialization that data may be processed in a lawful manner, with the lowest compliance risk and optimization of benefits for business.

REFERENCES

CMS (2016): The new EU General Data Protection Regulation and the Privacy Act [Az EU új Adatvédelmi Rendelete és az Infotv. – a 25 legfontosabb különbség]. November 2016.

EC (2016): Article 29 Data Protection Working Party. Guidelines on Data Protection Officers ('DPOs'). Adopted on 13 December 2016. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

European Parliament and the Council (2016): Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; GDPR).

Hungarian Government (2011): Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (Privacy Act).

Jóri, András – Soós, Andrea Klára (2016): *Data Protection Law – Hungarian and European Regulations* [Adatvédelmi Jog – Magyar és európai szabályozás]. Budapest: HVG ORAC Lap és Könyvkiadó Kft.

Kővári, Attila (2015): Responsible for Data [Adatvagyon felelős]. BI Projekt, 18 June, http://wwww.biproject.hu/blog/Adatvagyon-felelos.htm.

Liber, Ádám (2011): The ASNEF/FECEMD Ruling of the European Court of Justice – Decision on Data Processing Based on Legitimate Interest [Az Eu Bíróság ASNEF/FECEMD ítélete – döntés a jogos érdeken alapuló adatkezelésről]. DataPrivacy.hu, 27. 11. 2011, http://www.dataprivacy.hu/?p=864.

Liber Ádám (2012): Data Processing Based on Legitimate Interest [A jogos érdeken alapuló adatkezelésről]. *Infokommunikáció és Jog*, 2(49), pp. 79–88, https://infojog.hu/liber.adam-a jogos eredeken-alapuló adatkezelesrol-20122-49-79-8.

MNB (2016): *Recommendation 5/2016 (VI.06) of the National Bank of Hungary on the establishment and operation of internal lines of defence, and on the management and control functions of financial organizations* [A Magyar Nemzeti Bank 5/2016. (VI.06.) számú ajánlása a belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról]. https://www.mnb.hu/letoltes/5-2016-belso-vedelmi-vonalak-kialak-es-muk.pdf.

MNB (2017): *Recommendation 7/2017 (VII.5) of the National Bank of Hungary on the protection of IT systems* [A Magyar Nemzeti Bank 7/2017. (VII.5.) számú ajánlása az informatikai rendszer védelméről]. https://www.mnb.hu/letoltes/7-2017-informatikai-rendsz-ved.pdf.

Péterfalvi, Attila [ed.] (2012): *Data Protection and Freedom of Information in Everyday Practice* [Adatvédelem és információszabadság a mindennapokban]. Budapest: HVG ORAC Lap és Könyvkiadó Kft.

Szabó, Endre Győző (2016): *Questions on the European Union's General Data Protection Regulation: I. Data Portability and the Data Protection Impact Assessment* [Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről I. Az adathordozhatóság és az adatvédelmi hatásvizsgálat]. Pázmány Law Working Papers 26, http://plwp.eu/evfolyamok/2016/182-2016-26.