INTERNATIONAL CONFERENCE
INFORMATION AND COMMUNICATION TECHNOLOGIES IN BUSINESS AND EDUCATION

CONFERENCE PROCEEDINGS

Publishing house "Science and economics"
University of Economics - Varna

International Conference

INFORMATION AND COMMUNICATION TECHNOLOGIES IN BUSINESS AND EDUCATION

Conference proceedings

INFORMATION AND COMMUNICATION TECHNOLOGIES IN BUSINESS AND EDUCATION

Proceedings of the International Conference dedicated to the 50th anniversary of the Department of Informatics

2019

University publishing house "Science and economics"
University of Economics – Varna

Published reports have not been edited or adjusted. The authors are solely responsible for the content, originality and errors of their own fault.

With the support of ADASTRA, 411 Marketing Business Services.

ISBN 978-954-21-1004-0

PROGRAMME COMMITTEE

Abdel-Badeeh M. Salem, Egypt
Aijaz A. Shaikh, Finland
Aleksandar Dimov, Bulgaria
Alexander Feldman, USA
Alexander Sergeev, Russia
Antoanela Naaji, Romania
Avram Eskenazi, Bulgaria
Dariusz Mrozek, Poland
Dimitrina Polimirova, Bulgaria
Dmitriy Berg, Russia
Elena Nechita, Romania
Emil Denchev, Bulgaria
Georgi Dimitrov, Bulgaria
Ivan Popchev, Bulgaria
Jeanne Schreurs, Belgium
Julian Vasilev, Bulgaria
Kameliya Stefanova, Bulgaria
Krasimir Shishmanov, Bulgaria
Maciej Czaplewski, Poland
Maciej Pondel, Poland
Maksim Medvedev, Russia
Maria Hristova, Bulgaria
Marian Cristescu, Romania
Marina Medvedeva, Russia
Michael Voskoglou, Greece
Nadezhda Filipova, Bulgaria
Nikola Nikolov, Ireland
Niv Ahituv, Israel
Pavel Petrov, Bulgaria
Rami Malkawi, Jordan
Sara Paiva, Portugal
Silvia Parusheva, Bulgaria
Snezhana Sulova, Bulgaria
Todorka Atanasova, Bulgaria

Valentin Kisimov, Bulgaria
Valery Trofimov, Russia
Veselin Popov, Bulgaria
Violeta Kraeva, Bulgaria
Vladimir Sulov, Bulgaria
Vladimir Zanev, USA
Zdzislaw Polkowski, Poland

ORGANIZING COMMITTEE

Chairman: Prof. Vladimir Sulov, PhD

Members:
Prof. Avram Eskenazi, PhD
Prof. Julian Vasilev, PhD
Assoc. Prof. Todorka Atanasova, PhD
Assoc. Prof. Silvia Parusheva, PhD
Assoc. Prof. Snezhana Sulova, PhD
Assoc. Prof. Pavel Petrov, PhD

Secretary: Tijen Talib

FOREWORD

These proceedings contain the papers of the International Conference "Information and Communication Technologies in Business and Education" which took place at the University of Economics – Varna, Bulgaria, 18 October 2019.

The international scientific conference is dedicated to the **50th anniversary of the Department of Informatics at the University of Economics – Varna.** The conference is also dedicated to the 100th anniversary of the University. The included papers describe recent scientific and practical developments in the field of information and communication technologies, information systems, and their applications in business and education.

The papers in the Proceedings are peer reviewed and are checked for plagiarism.

C O N T E N T S

CHALLENGES OF GDPR COMPLIANCE IN CONSUMER FINANCING COMPANIES

***Monika Tsaneva*[1]**
[1] University of National and World Economy/Department of Information Technologies and Communications, Sofia, Bulgaria, mtzaneva@unwe.bg

Abstract

From the point of view of information systems, EU General Data Protection Regulation (GDPR) is traditionally associated with the imposition of strict procedures and restrictions on the storage, processing and transmission of personal data. The aim of this paper is to propose a comprehensive approach to implementing GDPR requirements in information systems and applications operating in the consumer financing area. The research is based on an analysis of the business process and the typical information infrastructure of a credit institution on one hand, and on specifics of GDPR compliance in this sector, on another. As a result of this development, basic guidelines are proposed for how, while implementing GDPR's requirements, business can be expanded by creating the fundamentals for introducing cutting-edge information technologies, upgrading existing applications, developing new integration solutions, and developing B2B platforms. The main conclusion made from this research is that when carefully planned and implemented with the right technological solutions, GDPR compliance in the consumer financing companies can open up new business and technological opportunities, thereby ensuring further optimization of company operation and eventually enhancing customer satisfaction.

Keywords: *GDPR, integration solutions, consumer financing applications.*

INTRODUCTION

Nowadays everyone is familiar with the main rules and regulations that comprise GDPR. Consumers associate them with the binding consent to the processing and storage of their personal data, IT professionals with the technological challenges to their implementation, and business - most often with restrictions that must be respected. This material addresses the major challenges and opportunities that GDPR compliance presents to Business Information Systems (BIS) operating in consumer credit companies.

1. TYPICAL INFORMATION INFRASTRUCTURE OF A CONSUMER FINANCING COMPANY

Whenever some significant new features of data storage and data processing must be implemented, the starting point must be the general architecture of the information infrastructure. This is because all the applications and system modules run as interconnected components of a system that serves the needs of the main business process of the company Tsaneva (2019, p. 8), consisting of three main stages – Apply, Contract and Perform (see Figure 1).

1. **Apply**: Both applicants and retailers use some front-end (web or mobile) system to apply or to register the application for a credit. On this stage the applicant signs a Consent for personal data storage and processing. An individual's consent for each specific type of financial operation must be requested. (Remoortel, 2016), so usually, as a part of this consent, the applicant authorizes the credit institution to perform an automated scoring of his application, and to share his personal data with other institutions like national registers, third party credit scoring companies and insurers. After its registration, the credit risk of each loan application must be scored. Usually, this assessment is performed automatically by a standalone system. The most significant specific of Credit risk scoring systems is that usually they work in compliance with the rules and restrictions established for accessing data in cloud systems (Lazarova, V. 2016) and do not store and visualise personal data, they just receive this data, perform the evaluations and return the score without jeopardizing GDPR requirements in any way. Another specific is that in the common scenario, the scoring involves some data requested and received via API from some National Registers (Central Credit Register - CCR, National Social Security Institute – NSSI, Directorate General Civil Registration and Administrative Services - GRAO etc.) and this data is sent back to the operational system as an additional information to the evaluated credit risk score. If the loan application is rejected by the scoring system, the customers personal data may be stored for 5 years (if the consent is not withdrawn earlier) and then must be deleted.

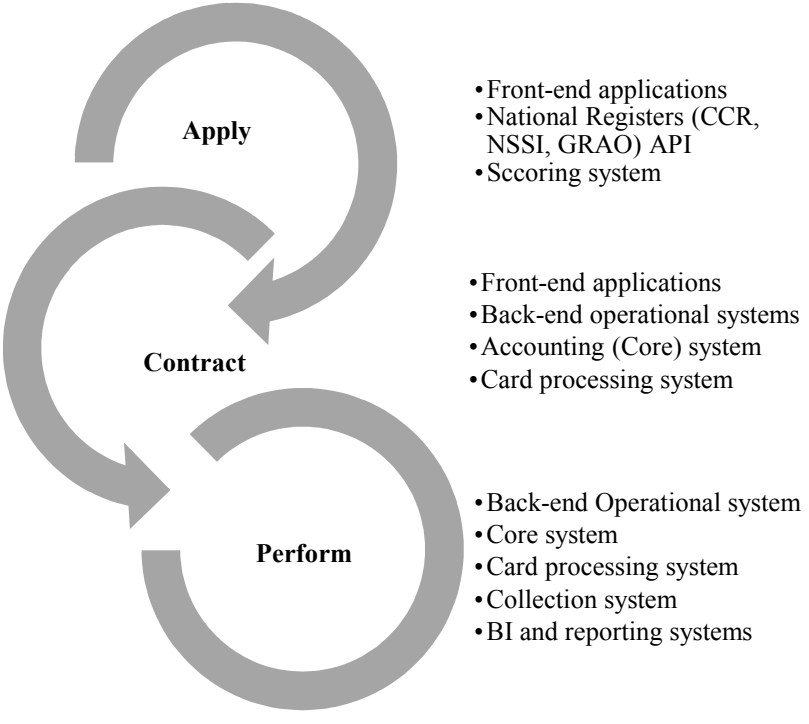

Figure 1. Typical information infrastructure of a Consumer Financing company

2. **Contract**: If the loan application is approved, a contract between the customer and the credit institution is signed. On this stage all the application/contract data is propagated from the operational system to the interconnected systems like the core (accounting) system, card processor (if a credit card has been contracted).

3. **Perform** (the contract): This stage includes all the administrative tasks that ensure regular loan repayment, quality communication with customers, reporting to company management and national regulators (Bulgarian National Bank -BNB, Central Credit Register - CCR etc.) On this stage additional data about bank or cash loan repayment transactions are collected on regular basis (usually monthly), all the communications (phone calls, e-mails, chats) with clients are recorded. On this stage

many indicators of contract performance are estimated. In the most common scenario, these indicators together with customers data are:

a) Exported in fixed record text files to national regulators on a weekly or monthly basis;

b) Loaded daily in the company's data warehouse. The company warehouse can be another relational database, or a Non-relational data store (Radoev, 2017, p. 153) to be presented to the management as dashboards providing informed data decision making abilities, so that business can continue to advance with the digital age (Mihova, Stefanov and Marzovanova, 2016, p 518);

c) Exported daily to Collection system or to another standalone company systems in files with predefined format.

All these activities are performed till the contract is fully repaid or terminated on some other legal basis.

Basically, all the above systems and modules have been developed during a long period of time and using completely incompatible information technologies, so the information infrastructure of a Consumer Financing company is heterogenous and ensuring the interoperability of its components in all the aspects including GDPR compliance is a complicated task

2. SPECIFICS OF GDPR COMPLIENCE IN CONSUMER CREDIT COMPANIES.

"GDPR another obstacle in an already complex system" and "Today's regulatory implementation, tomorrow's opportunity" – that's how the expectations of some managers (Kemp, 2017, p. 1) in financial business can be summarized.

MetaCompliance (2018, p.4) states the following GDPR principles:

- ✓ Lawfulness, fairness and transparency;
- ✓ Purpose limitation;
- ✓ Data minimisation;
- ✓ Accuracy;
- ✓ Storage limitation;
- ✓ Integrity and confidentiality.

Implementation of these principles in practice means (EY, 2018, p.6):

✓ Profiling is prohibited except when it is founded on a legitimate basis like explicit consent, performance of a contract and compliance with a legal obligation;

✓ Data protection impact assessments should take place prior to the processing of financial data and must serve to estimate the risks of processing data and to define mitigating measures;

✓ Services should adhere to data protection by design and by default principles which means that require service providers must think about the impact their services will have on data protection before delivering them;

✓ Data subjects always have the right of access to their information that is being processed and they have the right to receive a copy;

✓ Data subjects have the right of erasure which requires providers to take these rights into account when designing services, so that personal data can be deleted if requested and permissible.

A proper data subject consent gives the consumer credit companies legitimate basis to perform profiling in order to evaluate the credit risk of each loan applicant, so the prohibition of profiling is actually not an issue, but an opportunity for further automation of one of the most time and resource consuming activities which is credit risk assessment. This opportunity is extended by developing advanced integration modules for data retrieval from national registers via API provided by CCR, NNSI and other Bulgarian national institutions.

The following points need to be considered during the design process of GDPR compliance of information systems and their integration solutions:

1. Properly determine the scope of personal data (see Figure 2) that needs protection and must be ready to be delivered to the data subject in a machine readable format or be deleted (”forgotten”).

Based on the business process, the scope of personal data that must be returned to the data subject or must be “forgotten” upon request is:

✓ Personal data registered as a part of the application for a loan like names, addresses, e-mails, phones and other contact data, education, workplace, incomes, depts and so on;

✓ Data received from national registers – from NSSI retrieved during application assessment, from CCR retrieved both during application

assessment and imported on regular basis (monthly) during loan repayment;

✓ Terms and conditions of the loan that have been contracted like purchased goods, loan amount or credit card limits, credit card numbers, bank accounts numbers, insurances, loan duration, interest percentages and so on;

✓ Data collected during contract performance about regular payments (bank or cash transactions) made by the client, customer calls, correspondence regarding collection process and so on;

✓ All the data that is transferred to the company data warehouse and can be used to identify a customer including names, EGN, identification card, addresses, phones, e- mails, workplace etc.

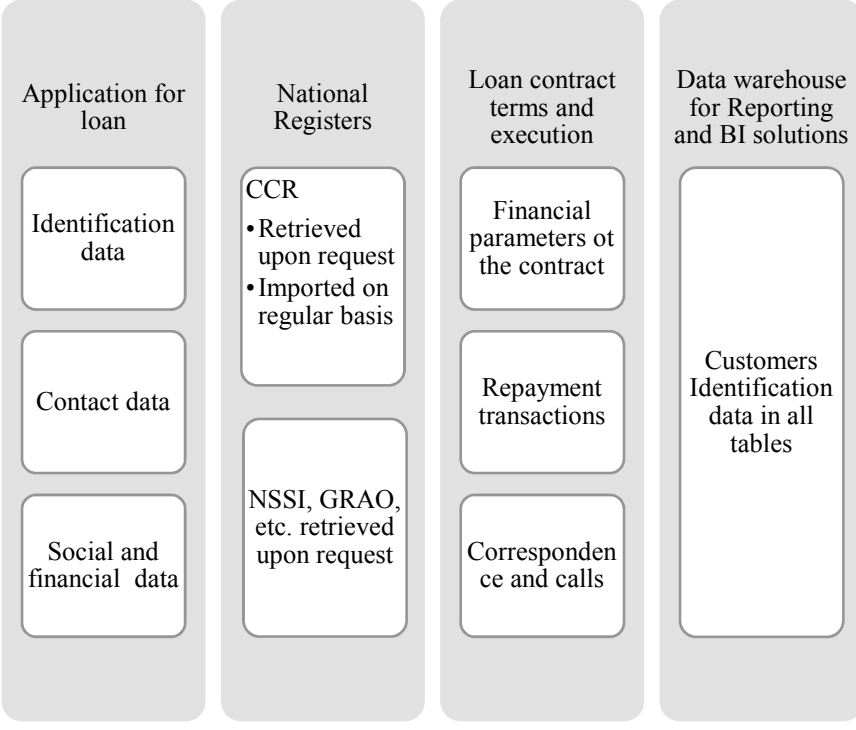

Figure 2. Scope of personal data that must be returned or "forgotten"

In addition to this, when a customer or employee needs to be forgotten, all the backups of the databases that are not currently destroyed must also be included in the scope of deletion. All drives/folders that contain obsolete data exported by legal obligations for national institutions must also be checked and cleared.

2. Check and, if necessary, redesign the user access control system, in order to guarantee, that every user of each system will have access to read and/or modify only to this data that are relevant to his job description. Some hard choices must be made because such changes usually require a large amount of work for user interface components redevelopment especially for legacy desktop systems. When new functionality is designed, data visualization must be organised considering data usage defended by Data Protection Officer (DPO) for different user roles. An alternative approach like using data encryption options embedded in modern databases must also be considered. Generally, database embedded data encryption is more suitable for new systems development. When applied to existing systems, this approach will require both data migration and redevelopment of application's data access tier, which can become a very big issue for large size databases that need a large amount of time to be migrated.

3. Choose and develop a proper single-entry module for data subjects (see Figure 3) who want to withdraw their consent, change its individual permissions, receive a copy of their data or request to be "forgotten". Opposed to traditional vision, this module is not a simple form (or a web page) containing a set of checkboxes, an "I accept" and a "Reject" button. Such a "Consent processing" module is an integration solution that includes substantial business logic and eventually results in a sequence of method invocations in all the interconnected modules and systems that store a particular set of personal data.

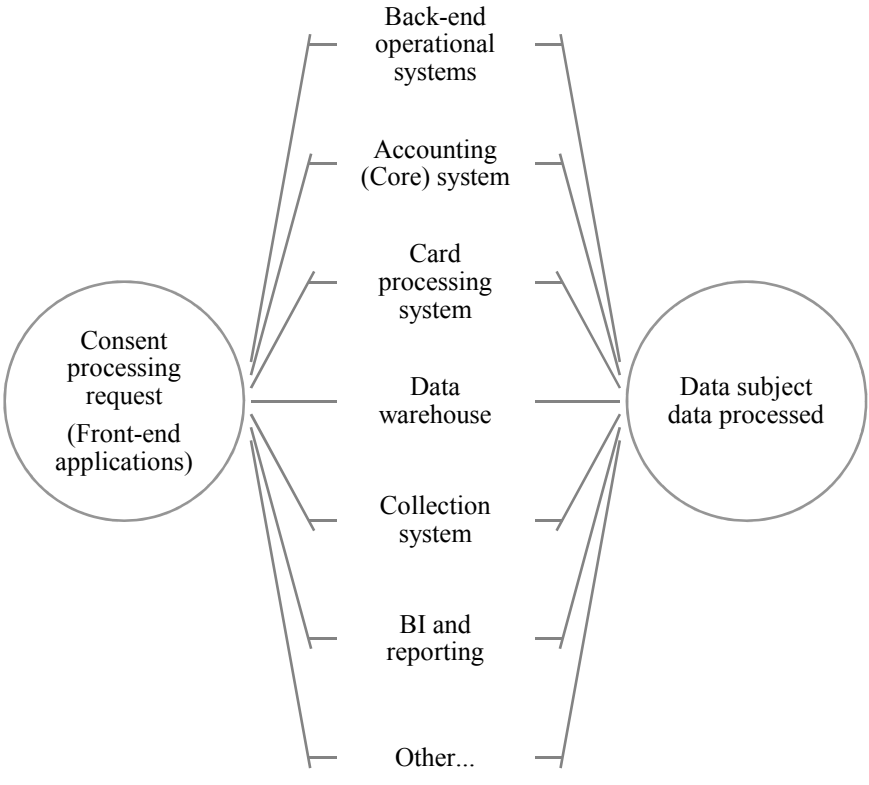

Figure 3. Single-entry "Consent processing" module for data subjects

4. Consider and implement the "anonymize" instead of "forget" personal data functionality. The main reason for such a consideration is the process of score card development for loan application assessment. Usually the content of a score card is based on contract performance indicators estimated for different customers segments depending on contract point of sale, purchased goods, customers age, education, social and financial status etc. So the simple deletion of the customer and all his related data (as required by relations in the data base) is not a suitable option. The more flexible approach that can be implemented is to anonymize all the sensitive data that can be used to identify a particular per-

son. A simple option is to replace all these actual values with hash codes, thus guaranteeing on one hand consistency of data and database relations and on the other - the impossibility of unauthorized sensitive data recovery. Anonymization must be performed simultaneously over all the data bases and data warehouses in the company thus ensuring both GDPR compliance and reporting systems operability.

3. BUSINESS AND TECHNOLOGICAL OPPORTUNITIES GIVEN BY GDPR COMPLIANCE IN CONSUMER CREDIT COMPANIES.

GDPR compliance is a time consuming and costly process because it involves significant redevelopment of data base structures, API methods and user interface components in a complex heterogeneous environment. Implementing well thought-out, technology-relevant and business-friendly solutions can achieve serious competitive and strategic benefits for the company (see Figure 4). The GDPR is not the only regulation which targets financial services industry, but consumers will also benefit from Payment Services Directive (PSDII), which requires financial services companies to open their data and payments infrastructure to promote increased competition. “PSDII, actually provides an opportunity for the financial services industry. This directive should allow innovative banks to improve their customer experience, increasing value to corporate customers” (Kemp, 2017, p. 1) because the treatment of data under PSDII must also comply to GDPR requirements.

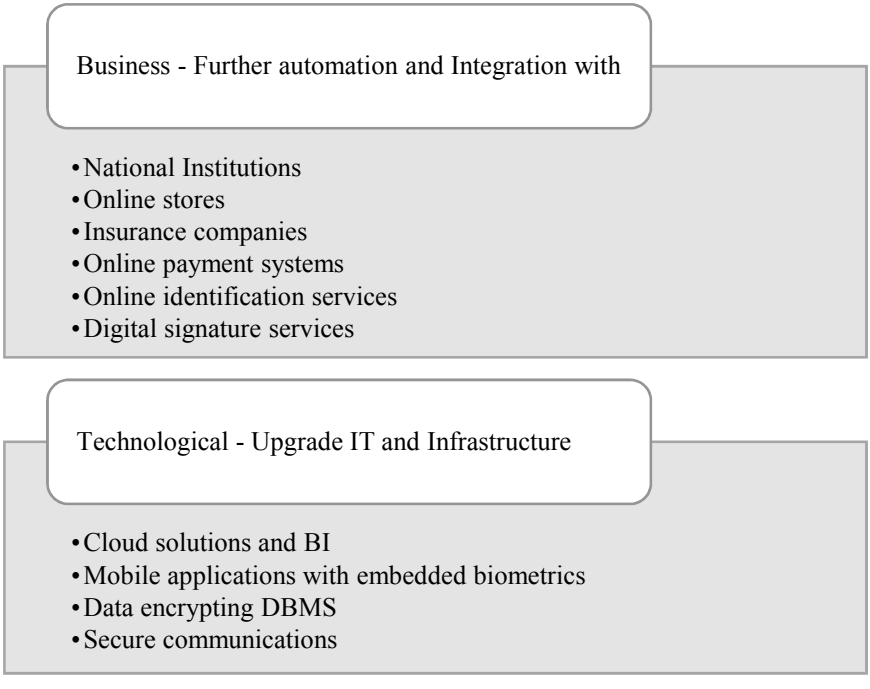

Figure 4. Opportunities given by GDPR compliance

Many new business opportunities are opened by data portability - the right to transfer consumers personal data in a structured, commonly used and machine-readable format. That way further automation of business activities and data entry reduction are achieved. A variety of additional services may be offered via Integration via API with third party systems for common business solutions.

✓ Integration with some national institutions like CCR, BNB, NSSI using the API they provide;

✓ The commonly used interoperability between digital (online) stores and credit institutions is greatly facilitated;

✓ Thanks to the GDPR-regulated data exchange, financial institutions and insurers offer common products and their overall business process is fully automated using specialized API methods. Additional options may be sought in the direction of automating periodic calculations

and reporting between them, for which the use of API is not the most appropriate option due to the large volumes of data exchanged;

✓ Common business solutions can also be implemented with external online payment systems (like ePay, EasyPay etc.), although most credit institutions encourage customers to use the implemented internal modules and applications;

✓ A very modern and promising area is the integration of services for electronic identification and electronic signature of documents (credit agreement, insurance policies, even the consent for processing personal data).

Investment in bringing information systems and GDPR compliance can increase their effectiveness if combined with upgrading the entire IT infrastructure by:

✓ Deploying cloud technologies, that ensure complete and much more secure control over user access to company services and data;

✓ Development of mobile applications using embedded biometric data for secure consumer identification;

✓ Migrating to the latest DBMSs that have built-in data encryption capabilities for whole tables or individual table columns;

✓ Construction of advanced network equipment with encrypted communication channels and high level of intrusion protection.

CONCLUSION

Implementation of GDPR compliance solutions in consumer financing companies requires hard work and significant amount of time and finances. But when carefully planned and implemented with the right technological solutions, this process can open new business opportunities and create prerequisites for technological upgrading of the information infrastructure, thereby ensuring further optimization of business processes eventually enhancing customer satisfaction. Financial sector companies passed the first easy and cheap steps – they have legal basis to store and process the personal data of their customers and have implemented the minimum GDPR requirements by designating DPOs and demanding data subjects to sign an individual consent for each purpose. To reap the potential benefits of GDPR compliance, the firm's business strategy must be updated, and information technology and infrastructure evolution strategy must be aligned with it,

then development and investment priorities must be set, and finally a detailed plan for their realization must be created and implemented.

REFERENCES

1. EY, Navigating the PSD2 and GDPR challenges faced by banks (2018), [Online], Available from https://www.ey.com/Publication/vwLUAssets/ey-navigating-the-psd2-and-gdpr-challenges-faced-by-banks/$FILE/ey-navigating-the-psd2-and-gdpr-challenges-faced-by-banks.pdf [Accessed 17/08/2019].
2. KEMP, J. (2017) GDPR: A challenge for the financial services industry, [Online], Available from: https://www.euractiv.com/section/economy-jobs/opinion/gdpr-a-challenge-for-the-financial-services-industry// [Accessed 15/08/2019].
3. LAZAROVA, V. (2016). Managing User Access to Cloud Services by Company Administrators. 2016 TEM Journal, 5(3), p.289-293
4. MetaCompliance (2018) GDPR Best Practices Implementation Guide, [Online], Available from https://www.infosecurityeurope.com/__novadocuments/355669?v=636289786574700000 , [Accessed 17/08/2019].
5. MIHOVA, V., STEFANOV, G., MARZOVANOVA, M. (2016). Cognos Mobile -dashboards design and implementation technology, 6th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education ICAICTSEE 2016 UNWE, Sofia, Bulgaria, 2-3 December 2016. [Online] pp. 514-519. Available from: http://icaictsee.unwe.bg/past-conferences/ICAICTSEE-2016.pdf, [Accessed 17/07/2019].
6. RADOEV M. (2017), A Comparison Between Characteristics of NoSQL Databases and Traditional Databases, Computer Science and Information Technology, Vol. 5(5), 2017, San Jose, CA, USA, [Online], pp. 149 – 153, Available from: http://www.hrpub.org/download/20171130/CSIT1-13510351.pdf [Accessed 16/07/2019].
7. REMOORTEL, FR.,(2016), Financial institutions and the General Data Protection Regulation, Financier Worldwide Magazine, November 2016, AVAILABLE from: https://www. financierworldwide.com/financial-institutions-and-the-general-data-protection-regulation#.XS2i4OgzaHt [Accessed 16/07/2019].

8. TSANEVA, M. (2019) A practical approach for integrating heterogeneous systems. Business Management 2/2019 [Online] pp. 5-15. Available from: http://bm.uni-svishtov.bg/title.asp?title=1383, [Accessed 17/08/2019].