Serdica J. Computing **13** (2019), No 3–4, 155–170

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

IMPLEMENTATION OF GDPR REQUIREMENTS IN THE INFORMATION SYSTEMS OF CONSUMER FINANCING COMPANIES

Monika Tsaneva

Abstract. From the point of view of information systems, the 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 drawn from this research is that when carefully planned and implemented with the right technological solutions, GDPR compliance

ACM Computing Classification System (1998): C.2.4, D.2.11, H.3.5.

Key words: GDPR compliance, integration solutions, consumer financing applications, Information Systems of Consumer Financing Companies, implementation of GDPR requirements.

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.

1. 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 paper addresses the major challenges, implementation considerations and opportunities that GDPR compliance presents to Business Information Systems (BIS) operating in consumer credit companies and proposes some practical guidelines for the gradual implementation of GDPR requirements.

2. 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 [10], 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. [9] 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 [3] 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

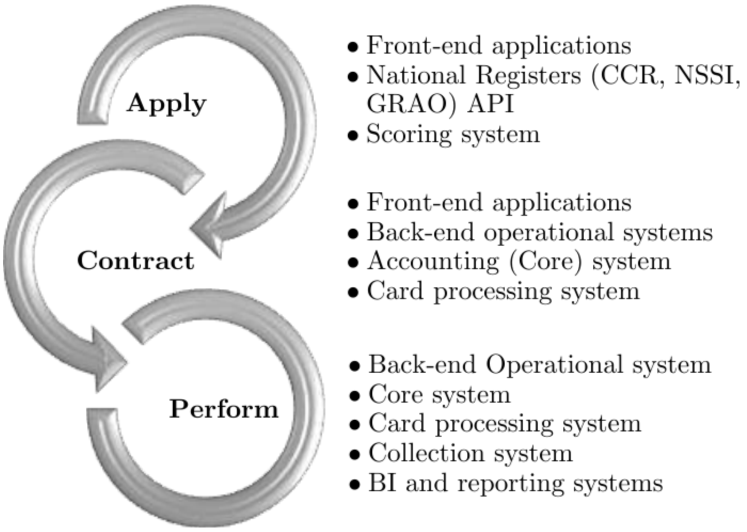


Fig. 1. Typical information infrastructure of a Consumer Financing company

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.

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 [8] 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 [6];

(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.

3. Specifics of GDPR compliance in consumer credit companies. "GDPR: another obstacle in an already complex system" and "Today's regulatory implementation, tomorrow's opportunity"—this is how the expectations of some managers [2] in financial business can be summarized.

MetaCompliance [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 [1]:

- 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;

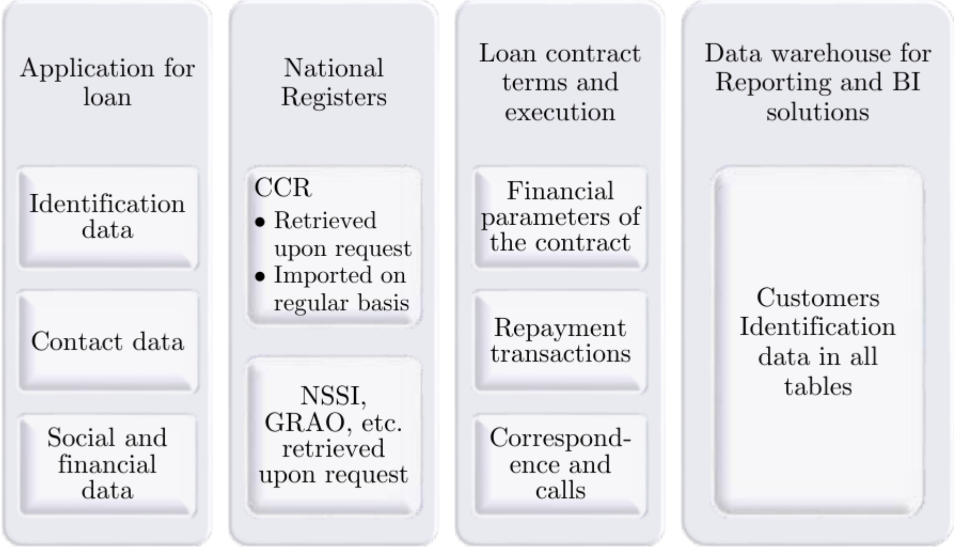

Application for loan
Identification data
Contact data
Social and financial data
National Registers
CCR
• Retrieved upon request
• Imported on regular basis
NSSI, GRAO, etc. retrieved upon request
Loan contract terms and execution
Financial parameters of the contract
Repayment transactions
Correspond-ence and calls
Data warehouse for Reporting and BI solutions
Customers Identification data in all tables

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

- 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.

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 front-end 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.

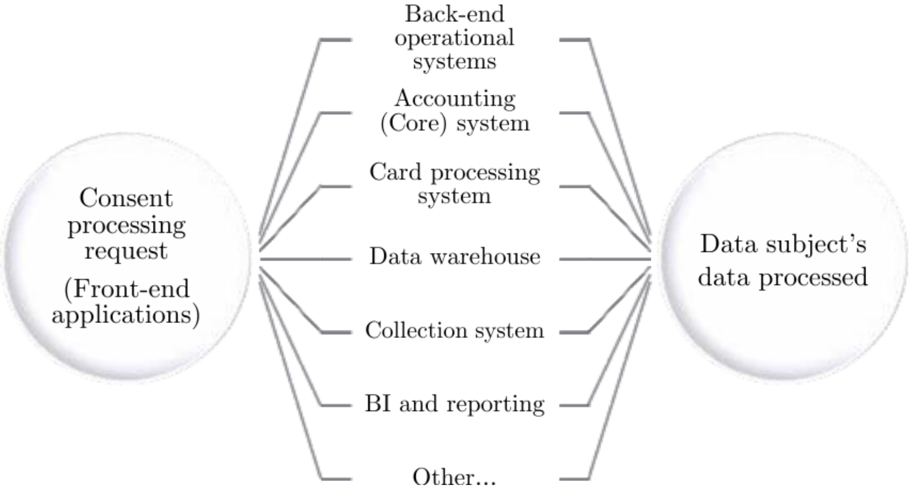


Fig. 3. Single-entry "Consent processing" module for data subjects

4. Consider and implement the "anonymize" instead of "forget" personal data functionality. The main reason for such a consideration is the process of

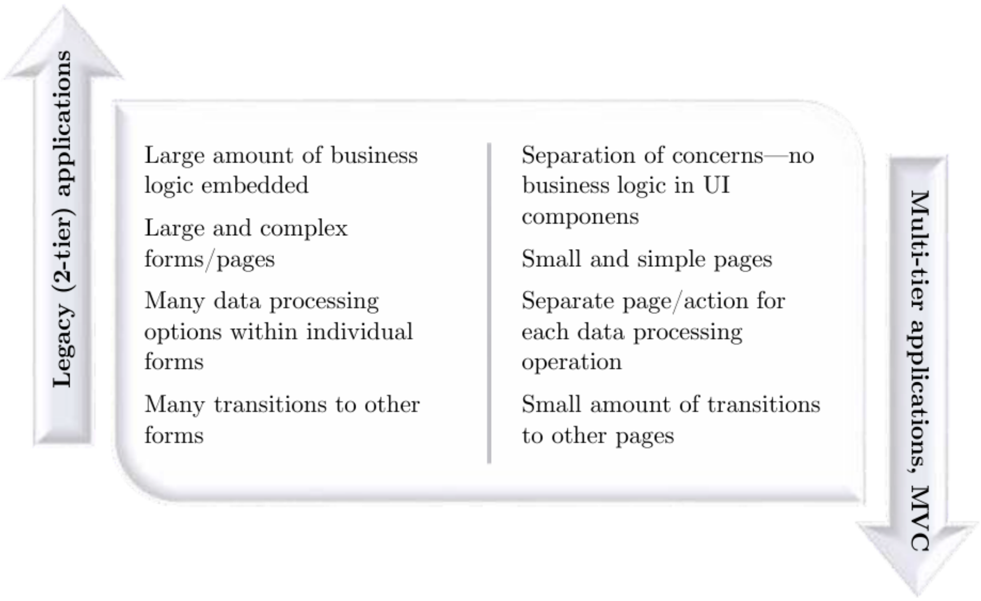
score card development for loan application assessment. Usually the content of a score card is based on contract performance indicators estimated for different customers segments depending on contract point of sale, purchased goods, customers age, education, social and financial status etc. So, the simple 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 an individual. 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.

4. Basic technological considerations about implementation of GDPR requirements in the information systems of consumer financing companies. From a technological point of view, the main mandatory tasks that need to be performed for the implementation of GDPR requirements in the information systems of consumer financing companies are analysis, design/redesign, reengineering and development of at least the following front-end and back-end software modules:

- User access control to these front-end modules that display and process personal data according to the consent given by the data subject;
- Back-end modules for generation of a machine-readable copy of each subject's personal data that is stored and processed in all interoperable systems and applications;
- Back-end modules for anonymization of each subject's personal data that is stored and processed in all interoperable systems and applications;
- Single-entry "Consent processing" front-end modules for data subjects and corresponding back-end modules for exclusion of data subject from activities not included in the consent.

Some additional (optional) activities to consider may be the implementation of some data encryption. These include both data bases used by individual information systems and/or integration solutions (intermediate/interface data base schemes) and data files exported to third parties like National Credit Registers, National Insurance Institute, National Revenue Agency etc.

The effort for front-end software implementation changes strongly depends on current solution pattern and varies from total redevelopment of legacy 2-tier desktop applications (fat clients) to small changes like new data annotations of some model properties in MVC (Model View Controller) web applications (see Figure 4). As main factors that influence the effort needed for front-end redevelopment may be considered:



Large amount of business logic embedded	Separation of concerns—no business logic in UI componens
Large and complex forms/pages	Small and simple pages
Many data processing options within individual forms	Separate page/action for each data processing operation
Many transitions to other forms	Small amount of transitions to other pages

Fig. 4. Factors that influence the effort needed for front-end redevelopment

- Amount of business logic embedded into the software component—The more business logic is embedded into some front-end software components, the bigger is the effort needed for its redevelopment. Usually legacy 2-tier applications (like Windows Forms and similar solutions) have their business logic encapsulated within the user interface components, so the redesign of such a user interface only is practically impossible and GDPR compliance requires almost total redevelopment of the entire application software. On the contrary—web applications, especially MVC ones, implement the concept of separation of concerns, so data visualization is completely isolated in specialized views (including partials) thus providing some easy ways to hide or protect personal data by simply changing its annotations or attributes.

- Complexity of user interface components (forms, web pages) including the number of data sections displayed in each form and the variety of their content. The greater number of fields in each form, and the larger variety of its content and usage requires more complex organization of access rights and may impose total redesign of user interface to ensure that only data that is processed for the same purpose and to which an individual user has the access rights is visible at a time. From this point of view, it is very possible that legacy 2-tier applications will require total redesign and reprogramming because their user interface is usually organized in large multi-tab and multi-section forms, that contain miscellaneous data. On the contrary—best practice MVC web applications consist of simpler forms in which data is retrieved when needed, not when the page is initially displayed. This makes the structure of the program code more appropriate for the seamless integration of a new consumer rights organization for personal data access.

- The number and variety of data processing actions available in each individual form and the available transitions to other forms containing personal data must be reduced in order to minimize the need for redevelopment of user access control concepts. Commonly used user interface design practice of legacy client server applications is to include many options for personal data processing (including different types of updates and redirects to other data pages) depending on business logic and business rules encapsulated in the same software component. On the contrary—modern MVC web applications usually implement each processing activity in a separate page or at least separate action or HTTP verb handler, which makes control and changes of user access to personal data much easier.

To summarize the above considerations, in most cases compliance of the legacy applications with the requirements of the GDR requires a complete recreation of the front-end part. Efforts to do so are likely to be comparable (in some cases larger, especially if one considers the risk of introducing errors in such processing) than if a completely new front-end that meets modern standards and uses high-tech technology is built. This does not necessarily apply to the administration module of the application system, which by default is used only by the system administrator who has full access rights to the user accounts including their personal data.

The situation with back-end modules for data subject anonymization and personal data export is quite different for the following reasons:

- These software modules did not exist before GDPR adoption, so they may be developed as encapsulated software components which are easy to integrate with a heterogeneous environment like web services or data base procedures.

- Both modules have similar scope (data than needs to be "forgotten" or exported are basically the same), so an approach based on a dictionary of personal data elements looks appropriate. Such a dictionary may be designed and implemented in many ways—as an extension of MS—Identity [Personal data] annotations [6], as an especial set of data base tables etc. but it must have hierarchical structure and must contain at least the following attributes—data base scheme (or system) name, table name (or synonym), column name, data type, resource identifier of the label for export etc. (see Figure 5). Probably this is not the cheapest or the fastest solution to implement, but it is the most flexible and scalable one. There is a high probability for all the consumer financing information systems to expand (as grows the business itself), and as a consequence, the scope of personal data will extend. In such a case the new attributes must only be added to the dictionary and no further development will be required. Another future usage of personal data dictionary may be binding with data subject consent allowances so that automatic exclusion of corresponding individuals from

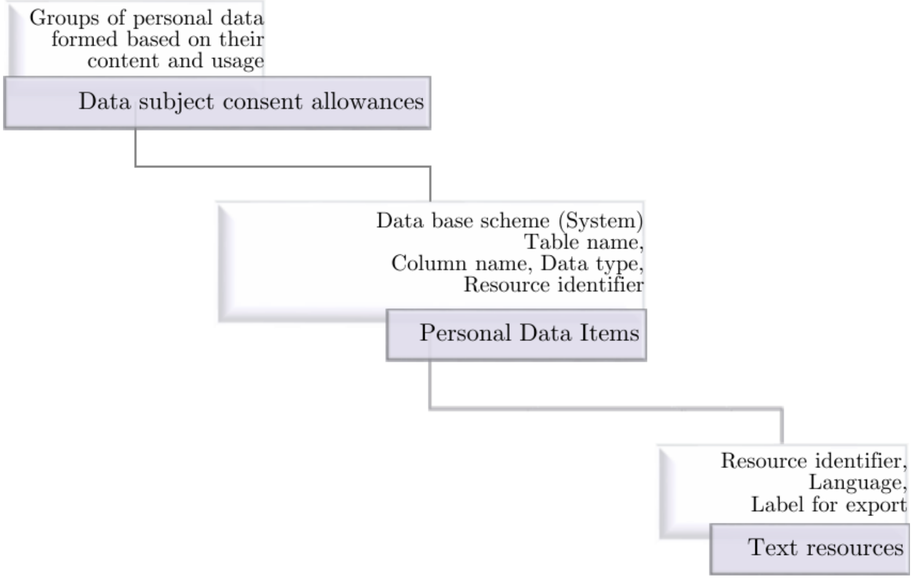


Fig. 5. Structure of a Personal Data Dictionary

some processing to be achieved.

GDPR defines the implementation of personal data encryption as an optional task. The approach to be considered depends on the data storage type and data breach risks arising therefrom:

- Encryption of data bases used by individual information systems and/or integration solutions (intermediate/interface data base schemes) is a task that can be postponed, because their storage media is usually well protected, and the data contained therein cannot be accessed directly, but only via database management and development environments.

- Data files exported to third parties like National Credit Registers, National Insurance Institute, National Revenue Agency etc. are stored and transferred in a plain text format which makes them much more vulnerable. To be safe, these files must be stored encrypted or at least they or the storage media itself must be password protected. Based on a legal obligation, a secure communication channel for this data transfer has always been used, but currently the encryption of the content itself cannot be implemented because of the counterpart's inability to decrypt before processing.

Basic conclusion that can be made from all the above is that the guide line of GDPR compliance implementation are the flexibility, extensibility and scalability of the technological solution that has been chosen. In all circumstances the development and the deployment (including possible data migrations) will be risky and resource consuming, but future maintenance and evolution of the system will be much easier and faster.

5. 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 flexible, scalable, well thought-out, technology-relevant and business-friendly solutions can achieve serious competitive and strategic benefits for the company (see Figure 6).

The GDPR is not the only regulation which targets financial services industry, but consumers will also benefit from Payment Services Directive (PS-DII), 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

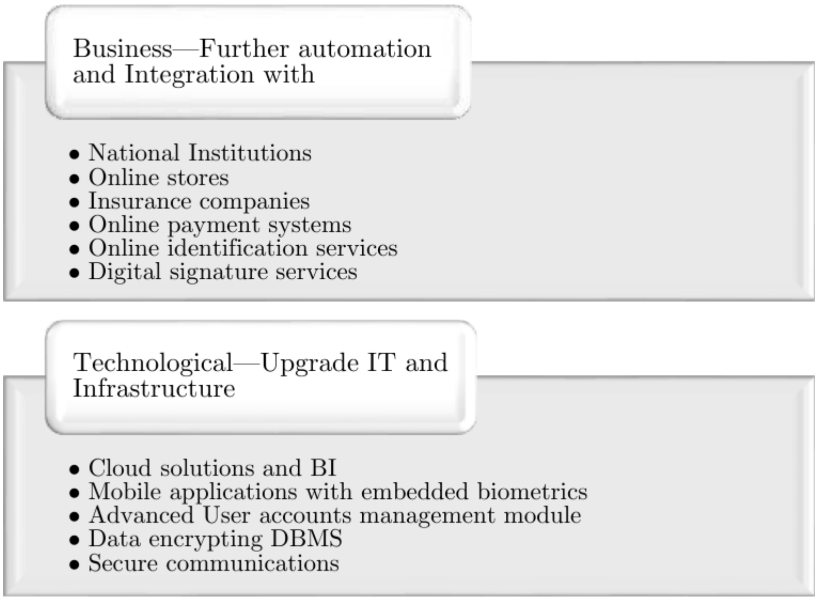

Business—Further automation and Integration with
• National Institutions
• Online stores
• Insurance companies
• Online payment systems
• Online identification services
• Digital signature services
Technological—Upgrade IT and Infrastructure
• Cloud solutions and BI
• Mobile applications with embedded biometrics
• Advanced User accounts management module
• Data encrypting DBMS
• Secure communications

Fig. 6. Opportunities given by GDPR compliance

customers” [2] because the treatment of data under PSDII must also comply to GDPR requirements.

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 multi-touch user interface [4] and embedded biometric data for secure consumer identification;
- Developing an advanced module for managing the users' access to information and functions of the system, using best practices and established environments and libraries, through which much of the development is automated, significantly reducing the risks and errors
- 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.

The benefit of the approach suggested above will not come easily and suddenly. In the first place, the business information system will become more flexible, more convenient and less expensive to maintain and develop. In addition, businesses will lay the foundations for next-to-come compliance of Know Your Customer (KYC) and Anti-Money Laundering (AML) politics and regulations which is of highest importance for companies in the consumer financing sector.

6. Conclusions. 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] Navigating the PSD2 and GDPR challenges faced by banks. *EY*, 2018. 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, 31 August 2020.

[2] Kemp J. GDPR: A challenge for the financial services industry. *Euractiv*, 7 September 2017. https://www.euractiv.com/section/economy-jobs/opinion/gdpr-a-challenge-for-the-financial-services-industry, 31 August 2020.

[3] Lazarova V. Managing User Access to Cloud Services by Company Administrators. *TEM Journal*, **5** (2016), No 3, 289–293.

[4] Marzovanova M. Building Multi-Touch User Interface. In: Proceedings of the 4th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE-2014), 701–704. http://icaictsee.unwe.bg/past-conferences/ICAICTSEE-2014.pdf, 31 August 2020.

[5] GDPR Best Practices Implementation Guide. *MetaCompliance*, 2018. https://www.infosecurityeurope.com/__novadocuments/355669?v=636289786574700000, 31 August 2020.

[6] Decentralized Identity—Own your digital identity. *Microsoft Corporation*, 2018. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY, 31 August 2020.

[7] Mihova V., G. Stefanov, M. Marzovanova. Cognos Mobile—dashboards design and implementation technology. In: Proceedings of the 6th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE 2016), Sofia, Bulgaria, 2–3 December 2016, 514–519. http://icaictsee.unwe.bg/past-conferences/ICAICTSEE-2016.pdf, 31 August 2020.

[8] Radoev M. A Comparison Between Characteristics of NoSQL Databases and Traditional Databases. *Computer Science and Information Technology*, **5** (2017), No 5, 149–153. http://www.hrpub.org/download/20171130/CSIT1-13510351.pdf, 31 August 2020.

[9] Van Remoortel F. Financial institutions and the General Data Protection Regulation. *Financier Worldwide Magazine*, November 2016. https://www.financierworldwide.com/financial-institutions-and-the-general-data-protection-regulation#.XS2i4OgzaHt, 31 August 2020.

[10] Tsaneva M. A practical approach for integrating heterogeneous systems. *Business Management*, **2** (2019), 5–15. http://bm.uni-svishtov.bg/title.asp?title=1383, 31 August 2020.

Monika Tsaneva
Department of Information Technologies and Communications
University of National and World Economy
1700 Sofia, Bulgaria
e-mail: mtzaneva@unwe.bg

Received October 22, 2019
Final Accepted January 28, 2020