Ministry of Education and Science of Ukraine

Odessa National Academy of Food Technologies

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2021

Information Technology, Automation and Robotics

Proceedings

Odessa, ONAFT 2021

UDC 004.01/08

Editorial board:

Black Sea Science 2021: Proceedings of the International Competition of Student Scientific Works. Information Technology, Automation and Robotics. / Odessa National Academy of Food Technologies; B.Yegorov, M. Mardar, S.Kotlyk (editors-in-chief.) [*et al.*]. – Odessa: ONAFT, 2021. – 526 p.

These materials of International Competition of Student Scientific Works «Black Sea Science 2021» contain the works of the contest participants in the section «Information technologies, automation and robotics» (not winners).

The author of the work is responsible for the accuracy of the information.

Organizing committee:

Prof. Bogdan Iegorov, D.Sc., Rector of Odessa National Academy of Food Technologies, Head of the Committee

Prof. Maryna Mardar, D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations of Odessa National Academy of Food Technologies, Deputy Head of the Committee

Prof. Stefan Dragoev, D.Sc., Vice-Rector for Scientific Work and Business Partnerships of University of Food Technologies (Bulgaria)

Prof. Baurzhan Nurakhmetov, D.Sc., First Vice-Rector of Almaty Technological University (Kazakhstan)

Prof. Mircea Bernic, Dr. habil., Vice-Rector for Scientific Work of Technical University of Moldova (Moldova)

Prof. Jacek Wrobel, Dr. habil., Rector of West Pomeranian University of Technology (Poland)

Prof. Michael Zinigrad, D.Sc., Rector of Ariel University (Israel)

Dr. Mei Lehe, Ph.D., Vice-President of Ningbo Institute of Technology, Zhejiang University (China)

Prof. Plamen Kangalov, Ph.D., Vice-Rector for Academic Affairs of "Angel Kanchev" University of Ruse (Bulgaria)

Dr. Alexander Sychev, Ph.D., Assoc. Professor of Sukhoi State Technical University of Gomel (Belarus)

Dr. Hanna Lilishentseva, Ph.D., Assoc. Professor, Head of the Department of Merchandise of Foodstuff of Belarus State Economic University (Belarus)

Prof. Heinz Leuenberger, Ph.D., Professor of the Institute of Ecopreneurship of University of Applied Sciences and Arts (Switzerland)

Prof. Edward Pospiech, Dr. habil., Professor of the Institute of Meat Technology of Poznan University of Life Sciences (Poland)

Prof. Lali Elanidze, Ph.D., Professor of the Faculty of Agrarian Sciences of Iakob Gogebashvili Telavi State University (Georgia)

Dr. V. Kozhevnikova, Ph.D., Senior Lecturer of the Department of Hotel and Catering Business of Odessa National Academy of Food Technologies, Secretary of the Committee

The jury for the section «Information technologies, automation and robotics»

Head of the jury:

Sergii Kotlyk – Ph.D., Associate Professor, Director of the P.M. Platonov Educational-Scientific Institute of Computer Systems and Technologies "Industry 4.0" of Odessa National Academy of Food Technologies (Ukraine)

Members of the jury:

Piotr Artiemjew - Dr hab., Associate Professor in Decision Systems of the Faculty of Mathematics and Computer Science,University of Warmia and Mazury in Olsztyn (Poland)

Francisco Antonio Augusto – Dr., International Relations Manager of Higher Institute of Information and Communication Technologies (Angola)

Andrey Kuprijanov – Ph.D., Associate Professor of the Department of Software for Computers and Automated Systems of Belarusian National Technical University (Belarus)

Simon Milbert – Vice-President of Xtra Information Management, Inc. (USA)

Ivan Palov – D.Sc., Professor of University of Ruse "Angel Kanchev" (Bulgaria)

Degla Gérard Hugues – Communications and Training Manager of "MAPCOM solutions informatiques" company group (Benin)

Nugzar Kereselidze - Academic Doctor of Informatics (Computer Science), Associate Professor of the Department of Natural Sciences, Mathematics, Technology and Pharmacy, Sukhumi State University (Georgia)

Etibar Seyidzade - Associate Professor of the Department of Computer and Information Technolohies, Baku Engineering University (Azerbaijan)

Vladimir Golenkov, D.Sc., Professor of the Department of Intelligent Information Technologies, Belarusian State University of Informatics and Radio Electronics (Belarus)

Zhanar Omirbekova - Ph.D., Associate Professor of the Department of Automation and Management, Satbayev University (Kazakhstan)

Ivan Palov - D.Sc., Professor of the Department of Power Supply and Electrical Equipment, University of Ruse "Angel Kanchev" (Bulgaria)

Siarhei Palavenia - Ph.D., Associate Professor, Head of the Department of Telecommunication Systems, Belarusian State Academy of Communications (Belarus)

Alexander Goloskokov - Ph.D., Professor of the Department of Software Engineering and Information Technology Management, National Technical University "Kharkiv Polytechnic Institute" (Ukraine)

Peter Nikolyuk - D.Sc., Professor of the Department of Computer Technology, Vasyl Stus Donetsk National University (Ukraine)

Vladimir Palagin - D.Sc., Professor, Head of the Department of Radio Engineering, Telecommunications and Robotics Systems, Cherkasy State Technological University (Ukraine)

Viktor Khobin – D.Sc., Professor, Head of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies (Ukraine)

Valeriy Plotnikov – D.Sc., Professor, Head of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

Sergii Artemenko – D.Sc., Professor, Head of the Department of Computer Engineering of Odessa National Academy of Food Technologies (Ukraine)

Fedir Trishyn - Ph.D., Associate Professor, Vice-Rector on Scientific and Educational Work, Odessa National Academy of Food Technologies (Ukraine)

Valerii Levinskyi – Ph.D., Associate Professor of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies (Ukraine)

Viktor Yehorov – Ph.D., Supervisor of the Laboratory of Mechatronics and Robotics of Odessa National Academy of Food Technologies (Ukraine)

Pavlo Lomovtsev – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

Yurii Kornienko – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

Serhii Shestopalov – Ph.D., Associate Professor of the Department of Computer Engineering of Odessa National Academy of Food Technologies (Ukraine)

Anatoly Galiulin - Ph.D., Associate Professor, Acting Head of the Department of Electromechanics and Mechatronics, Odessa National Academy of Food Technologies (Ukraine)

Secretary of the jury:

Oksana Sokolova – Senior Lecturer of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

IT SOLUTION REGARDING TO THE IMPLEMENTATION OF THE EU GDPR

Authors: ***Aurelian Gore, Ivan Postu***
Advisor: ***Rodica Bulai***
Technical University of Moldova (Moldova)

Abstract. *The main objective of the developed software is to implement the principles of the GDPR, the methodology for evaluating the impact of data protection, assessing the severity of the compromise of personal data within an organization and to keep track of personal data processing activities that are performed by responsible employees. The app also includes the possibility to manage the organization, the employee data and to process requests for personal data of those to whom the data belong.*

The functionality of managing an organization is creating it, modifying it by updating its information, deleting it, adding new departments, as well as editing the information about the departments. It is possible to evaluate the organization compliance with GDPR and to analyze statistically the results of the last evaluations.

The management of the departments of the organization includes creating it, changing its information, adding the head of the department, adding employees, displaying them in a list form and deleting it.

The basic functionality of managing the employees of the departments are adding them into respective departments, modifying, deleting their data and adding documents referring to the employee (especially necessary for that who is responsible for processing personal data to prove that he has the legal right to perform the given action). The decision if the employee can be responsible for personal data is made by answering a set of questions.

Keywords: *GDPR, confidentiality, personal data, impact evaluation, privacy, compliance, audit, protection, regulation, accountability.*

I. INTRODUCTION

By May 25, 2018, many of us woke up with dozens of emails in our inboxes from companies, politely asking us if we still wanted them to hold our personal data. The reason for this email campaign is the General Data Protection Regulation (GDPR).

The GDPR is considered the biggest change in the last two decades brought by the European Union legislation referring to data protection and having a global impact.

The strictness of the regulations and the colossal fines that were maximized in the media alarmed both EU and foreign companies. The created situation has become a gold mine for law firms and legal consultants, IT, offering GDPR consulting services at colossal sums.

Therefore, small companies found themselves in the situation of implementing the GDPR on their own, informing themselves on the requirements of the regulation found online, having too small budgets to use specialized consulting services and assuming the risks of deficiencies in compliance with the GDPR.

A law project transposed the EU GDPR to the Republic of Moldova and additions to Law 133 [12] were created based on the protection of personal data. Certain requirements of the regulation have been proposed, but have not yet been adopted.

However, some organizations tend to implement the requirements of the regulation, in particular those that are subsidiaries of European organizations or that collect and process data from European citizens.

II. ANALYSIS OF THE GENERAL REGULATION ON DATA PROTECTION IN A NATIONAL AND INTERNATIONAL CONTEXT

2.1. Evolution and current state of implementation of the GDPR

Data protection is a fundamental right within the European Union, as set out in Article 8 of the Charter of Fundamental Rights of the European Union and Article 16 (1) of the Treaty on the Functioning of the European Union (TFEU).

Until 25 May 2018, the main legal instrument for data protection in the European Union was Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data. [1]

The provisions of Directive 95/46 / EC have been transposed into the legislation of the Republic of Moldova by Law no. 133 of 08 July 2011 [12] for the protection of individuals with regard to the processing of personal data and on the free movement of such data. [2]

Fast rhythm of technological evolution has led to a colossal increase in the volume of data collected, used, transmitted and processed, which was not foreseen in 1995 when the directive was adopted, the internet being at an early stage and the major players in processing large volumes of data had not yet appeared on the scene (Google was founded in 1998, [3] and Facebook in 2004 [4]).

Increasingly, users have begun to make their personal information public, which has created new challenges in ensuring the protection of personal data.

According to a study conducted by Javelin Strategy & Research, in 2016 a maximum share of online fraud involving identity theft had been reached [5]. Their growth trend was maintained in 2017 with 16.7 million victims. [6]

One of the most publicized and major breaches of personal data security is the Cambridge Analytica scandal, which has affected approximately 87 million users worldwide. In the European Union were affected users from all 28 Member States about 2.7 million Facebook accounts. The largest exploitation took place in Great Britain with 1,079 million and Germany with over 309,815 accounts. In Romania, 112,421 users were affected. [7]

In this digital environment, the need of modernization EU rules on the protection of personal data has become vital. Thus, in 2016 the European Commission adopted REGULATION no. 679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation), - GDPR - effective from 25 May 2018. [1]

In the Republic of Moldova, the supervisory authority is - the National Center for Personal Data Protection, based in Chisinau - https://datepersonale.md/. [8]

GDPR is legislation with a global impact. Its provisions are applied to all organizations (operators or persons empowered by the operator) operating in the territory of European Union countries. Even if the company's registered office is abroad or is fully established abroad, as long as the company processes personal data collected or processed in the EU, of individuals located in the EU, it must comply with the provisions of the regulation. [1]

According to a study by Hiscox among micro, small and medium-sized enterprises (SMEs) in the UK, more than a third of SME managers (39%) do not know who is affected by GDPR, while 1 of 10 respondents do not believe that the GDPR offers consumers new rights. The study showed that many SMEs still do not comply with the provisions of the GDPR. Also 96% of small business owners do not know what the maximum fine for violating the GDPR is. [9]

2.2. Current approaches in implementing and complying with GDPR

Given the global impact of GDPR provisions, the complexity of compliance processes, but also the complex specifics of some businesses, the provision of consulting services and the development of information systems to provide support in the implementation and compliance with the provisions of the regulation came naturally. .

Analyzing the GDPR market, the implementation and compliance solutions can be divided into several broad categories:

1. **Consulting services** provided by law firms, legal advisers, IT consultants specializing in GDPR - this option being necessary especially for large companies, corporations whose complexity of personal data processing actions are high and the automation of this process is weighty.

2. **GDPR kits** - templates with standardized documentation specific to GDPR (registers, procedures, forms, contracts), created by lawyers, in word and excel format that can be adapted to the specifics of organizations.

3. Various **software solutions**, which vary by the technologies used and by the way of approaching GDPR compliance, as well as by the purpose but also of the service delivered:

- Software products that provide the actual protection of personal data and / or infrastructures where they are processed (threat detection and prevention software, access management, application security, network security, DLP solutions, Endpoint Protection, etc...);

- Solutions that allow the identification of personal data, using machine learning and artificial intelligence technologies, with their subsequent labeling;
- Software that automates the process of implementing the requirements of the regulation but also the compliance flows, such as records of personal data processing operations, management of access requests from data subjects, notification of security breaches, creation of specific GDPR documentation, automation of the process of obtaining and recording the consents obtained from data subjects, data protection impact assessment, etc..

The list of software solutions presented is not exhaustive as technology evolves, which facilitates the creation of new horizons for automation of GDPR requirements but also creates new challenges in the process of personal data protection.

Analysis of software solutions

Further will be presented a brief analysis of several software tools that offer its customers the automation of GDPR requirements. This analysis aims to understand the strengths and weaknesses of these software, in order to create our own tool for automating the requirements of GDPR.

Ecomply.io - is an GDPR compliance solution created by a German company, which provides a step-by-step guide to the activities needed to be followed, making it easier to manage the data protection and compliance process. Ecomply covers the following areas:

- Governance and data protection objectives (art. 5. GDPR)
- Evidence of processing activities
- Requests for access from data subjects
- Supplier management
- Designation of the Data Protection Officer (DPO)
- Incident Management [10]

Fig. 2.1 Ecomply.io interface [10]

GDPR 365 - is a GDPR compliance solution created by a Dutch company, such as Ecomply.io, which facilitates the implementation of GDPR requirements, it

offers a series of templates as well as the possibility to export compliance reports, processing registers, etc. GDPR365 covers the following issues:

- Governance;
- Record of processing activities - Mapping of activities;
- Management of access requests from data subjects;
- Supplier management;
- Data transfer;
- Designation of the Data Protection Officer (DPO);
- Data Protection Impact Assessment (DPIA);
- Information of data subjects (templates);
- Employee training;
- Incident Management. [11]

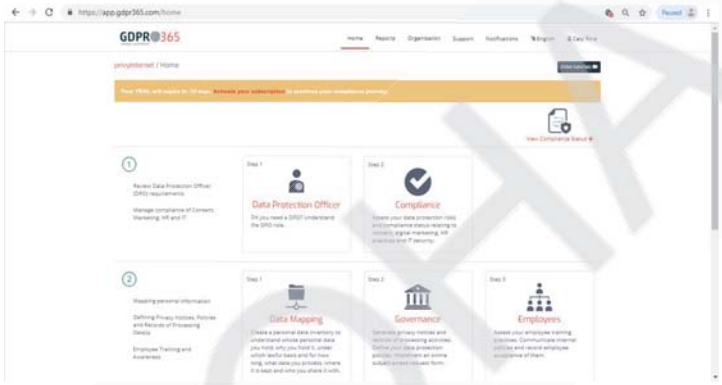

Fig. 2.2 GDPR 365 interface [11]

From all the range of solutions analyzed, including software products that were not presented above. GDPR 365 combines a wide range of GDPR compliance features into a dedicated product.

2.3. Difficulties in defining a unitary framework for implementing GDPR

Implementing and complying with the provisions of the GDPR can be difficult for any organization regardless of size or area of activity, each leading its own battle in the war of conformity.

The challenges of implementing GDPR differ from organization to organization, due to the heterogeneity of personal data processing, IT systems processing, storage, etc., internal operational processes, organizational structure, number of employees who have access to personal data, the company's area of activity, etc.

Although the need for a system that will facilitate the difficult implementation process came naturally, the creation of such a magic wand is virtually impossible for large companies, as the complexity of the challenges requires a consultation of lawyers and IT consultants specializing in GDPR, and the heterogeneous nature but also the large volume of constraints that may arise, makes it impossible to transpose the implementation process on the architecture of a single implementation system.

However, the landscape described above is at the opposite pole in the case of small companies, so the possibility of creating a system that will facilitate the implementation of GDPR takes shape.

III. IMPLEMENTATION MODEL OF THE EU GDPR

3.1. Key requirements of the EU GDPR

The EU General Data Protection Regulation is a set of rules on how companies should process the personal data of data subjects. The GDPR establishes the responsibilities of organizations to ensure the confidentiality and protection of personal data, gives data subjects certain rights and assigns regulators to demand liability demonstrations or even to impose fines in cases where an organization does not comply with the requirements of the GDPR:

1) Legal, fair and transparent processing
2) Limitation of purpose, data and storage
3) The rights of the data subject
4) Consent
5) Personal data breaches
6) Privacy by design
7) Data protection impact assessment
8) Data transfers
9) Responsible for data protection
10) Awareness and training

It is important to understand these requirements and their implications for the company and to implement them in the company context.

3.2. EU GDPR implementation

As it is implemented, it is important to understand whether the established plan is going in the right direction. The key GDPR implementation steps that the project must include are:

1) *Preparation of the GDPR project*.
2) *Defining the policy on personal data and other higher level documents.*
3) *Creating an inventory of processing activities.*
4) *Defining an approach for managing the rights of the data subject*.
5) *Implementation of a Data Protection Impact Assessment (EIPD).*
6) *Secure transfer of personal data.*
7) *Modification of third party contracts*.
8) *Ensuring the security of personal and sensitive data.*
9) *Defining data breach management*.

3.3. Data Protection Impact Assessment (DPIA) methodology according to the EU GDPR

EU GDPR implementation model Article 35 of the EU GDPR provides a specific analytical tool for assessing the impact of GDPR in depth, gradually.

In terms of methodology, Article 35.7 of the Regulation provides for the minimum elements to be assessed, which are described below in five steps:

Step 1 is essentially a detailed list of data processing, including the data it uses, the details of the operators and processors, the legal basis or retention periods applied to the data.

Step 2 identifies the legal and risk management controls that are currently being implemented. This phase involves the current and existing set of measures from a legal, technical, physical and organizational point of view.

Step 3 lists the sources of risk for data processing. This raises the question: "Will my business suffer from this new data processing and, if so, where and when will it suffer?" This phase focuses on possible intrusions of confidentiality and an assessment of corporate risks, damage to reputation or financial costs. It takes imagination, especially to browse a fair amount of sources of risk against the company.

Step 4 refers to the analysis and listing of potential negative events and threats to data processing. Its distinction from step 3 is that it will focus on the personal data of the data subjects and on the potential impact of the new processing on these data. If the events are internal or external, human or non-human (technical), this phase is relevant in terms of technological developments. New technologies may not have a clear introduction of privacy-friendly protection measures and thus expose people to threats such as hacking, phishing and spam. Its purpose is to determine what kind of threats your processing may be exposed to.

Finally, **step 5** takes the form of a report and summarizes the analysis, current controls, business risks and threats to personal data. The report sets out the organization's options for addressing each identified risk, threat and defect. Indicate whether each option would eliminate, reduce or accept the risk as it stands. The report will be recorded, kept and presented to the main managers of the organization. These managers can thus decide whether actions have been taken or should be taken and follow up on such actions.

Such an evaluation provides a powerful opportunity to review documents, prepare for project implementation, build or adapt policies, update technical issues, and strengthen controls. In short, the EIPD empowers staff to make changes and raise awareness of the protection of personal data within the company.

Demonstrating compliance with data protection authorities is what must be considered and must be kept on record. In the case of an audit, these records may be submitted. In addition, the company's customers and data subjects will have the guarantee of data protection and reputation.

3.4. Methodology for assessing the severity of the compromise of personal data (ASCPD) according to the EU GDPR

Methodology for assessing the severity of personal data breaches, in line with

the views of the Article 29 Working Party "Guidelines on the notification of personal data breaches under Regulation 2016/679" and "Recommendations for a methodology for assessing the severity of personal data breaches ”issued by the European Union Agency for Network and Information Security (ENISA), is also based on the assessment of the severity of data breaches in organizations in different fields of activity and is intended to provide a simple and comprehensive model for assessing data breaches .

The methodology is based on an objective approach, while trying to remain flexible enough to be adopted by various companies. Depending on different requirements, the scoring of some categories can be adjusted to produce the most appropriate results.

In order to assess the general severity of the data breach and to obtain a result that will be easy to interpret, the following formula is proposed:

SC = CPD x UI + CC, where

SC means Severity of compromise,

CPD means **Context of data processing (possible values 1,2 or 3),**

UI means **Ease of identification, (possible values 1 or 2),**

CC means **Violation circumstances (possible values 1 or 2).**

After obtaining the exact value of the severity of the compromise (SC), you can consult the table below to check the impact on affected data subjects, the possible consequences for data subjects and the company's notification obligations in case of data breach.

Table 1. Assessment of the severity level of data compromise

SC value	Impact on affected data subjects	Possible consequences for data subjects	Obligation to notify
SC is less or equal than 3	Little probability to lead to a risk	Individuals will either not be affected, or they may encounter some inconveniences, which they will overcome without any problem (time spent reintroducing information, upset, irritations, etc.).	Data breach should only be recorded in a register
SC = 4	There may be a risk	People may experience significant inconveniences, which they may be able to overcome despite some difficulties (additional costs, refusal of access to commercial services, fear, lack of understanding, stress, minor physical ailments, etc.).	Data breaches should be reported to the supervisory authority.
SC is equal or greater than 5	More probability to lead to risk	People may experience significant, or even irreversible, consequences that may prove difficult or impossible to overcome (embezzlement, blacklisting by banks, property damage, job loss, subpoena, worsening health, financial distress, such as be substantial debts or incapacity for work, long-term psychological or physical illness, death, etc.).	Data breaches should be reported to the supervisory authority as well as to the data subjects affected.

Although the notification obligations required by the EU GDPR may seem

quite simple, in practice, many infringement scenarios are unclear and require careful case-by-case assessment. The methodology provides a common approach to ensuring accountability and compliance with the EU GDPR provisions on data compromise notification and allows operators to have a clear approach when assessing the seriousness of personal data breaches. The correct assessment of a data breach is essential in the light of the new sanctions that will be applied by the supervisory authorities, as failure to report the data breach, as necessary, can lead to administrative fines of up to EUR 10,000,000 or, in the case of an undertaking, up to 2% of total annual global turnover in the preceding financial year.

Finally, even if the EU GDPR only requires operators to notify data breaches, if processors become aware of a data breach, they must notify the controller without undue delay in order to allow the controller to comply with its notification obligations.

IV. IT SOLUTION REGARDING THE IMPLEMENTATION OF GDPR

The main objective of the information system design is to provide the necessary support in the implementation of the provisions of the GDPR, to a small organization, by:

1. Detailed analysis of the provisions of the GDPR
2. Defining functional and data requirements for key processes:
    - Designation Responsible for data protection
    - Processing register
    - Data protection impact assessment
    - Evidence of requests from data subjects
    - Register of incidents of personal data breach
3. Modeling of modules and flows using UML language and stimulus-response sequences
4. Formalization of functional and non-functional requirements of the system

4.1. Building the system

Implementations of the system were made with much accuracy to maintain all the functionality in a simple interface. The desktop application is cross-platform to maintain the availability for all users. On the other hand the server (web application) with the desktop app and with the Database system the break apart to maintain the security and integrity of data.

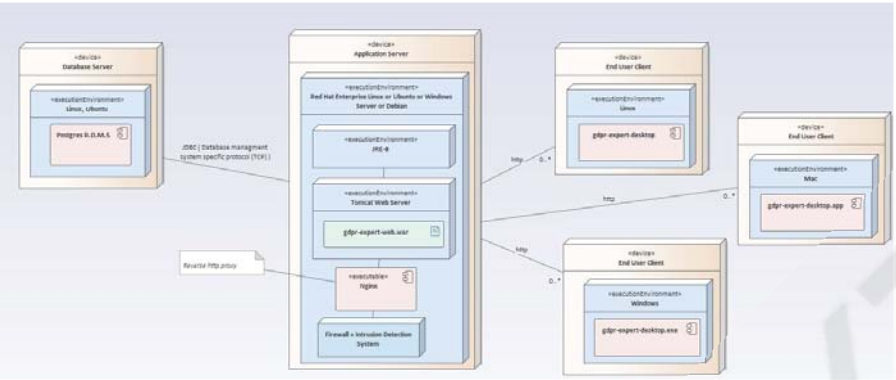

Fig. 4.1 Deployment diagram

In the deployment diagram (Fig. 4.1) is represented the basic scenario in which applications are placed on real environments, the process of interaction - through http between the desktop application on the frontend that can be placed on multiple workstations and running web application on the server using the tomcat container servlet and JVM. The diagram also shows the server for RDMS - PostgreSQL with which the web application interacts.

The following diagram represents the management of the data processing activities, which includes creating of a new data processing activity, visualizing them, updating and changing their information. For every such activity can be implemented an assessment of data protection impact and / or a severity compromising evaluation. All actions, which can be made to data processing activities, are shown in figure 4.2.

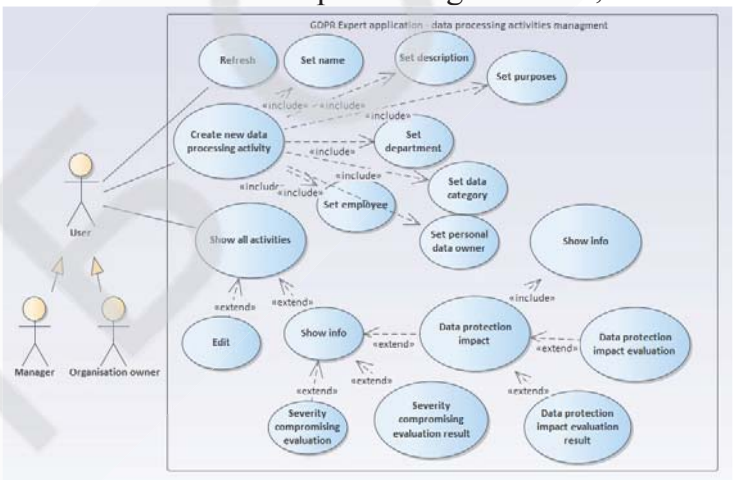

Fig. 4.2 Data processing activity

4.2. The technologies used to create the system

For implementing the GDPR solution was used React + Electron (for desktop app), Java Spring Framework and Gradle (for web app) and postgreSQL with Docker for RDMS (Relational Database Management System).

```
async fetchQuestions(): Promise<void> {
 const response = await getDataResponsibleQuestions()
```

```
    if (!this._isMounted) return

    if (!UnsuccessResponseData.isUnsuccessResponseData(response)) {
      const data = response as Array<GetDataResponsibleQuestionsResponse>
      this.setState({ isLoad: false, questions: data, questionId: data[0].id })
    } else {
      const err = response as UnsuccessResponseData
      if (err.isSessionExpired) {
        this.props.clearAuthDataActionCreator()
      }
    }
  }
```

In this piece of code is a request to the server to get the list of questions and answers that will be displayed on the UI. Depending on the chosen answer, it is determined whether the person can be responsible for personal data or not.

Also, in the following peace of code was written the logic part of determining the responsible person for personal data.

```
    @RequestMapping(value = "", method = RequestMethod.POST)
     public ResponseEntity<?> evaluateOrganisation(@AuthenticationPrincipal AuthUserEntity
user,
       @RequestBody GDPREvaluationQuestionsResultDto dto) {
      Validator validator = Validation.buildDefaultValidatorFactory().getValidator();
      List<String> errorMessages = validator.validate(dto).stream().map(a ->
a.getMessage()).collect(Collectors.toList());
      if (errorMessages.size() > 0) {
        return ResponseEntity.status(HttpStatus.BAD_REQUEST).body(errorMessages);
      }
      gDPREvaluationService.saveEvaluationResult(dto.getOrganisationId(),
dto.getPercentages());
      return ResponseEntity.status(HttpStatus.CREATED).build();
    }
```

Following the assessment of the organization's compliance with GDPR, an HTTP request to the server is sent, which validates it, extracts the data and keeps the result in the database.

4.3. GDPR Expert system functionalities

After the registration of the user and creating the organizations, the list of all companies appears. In the figure 4.3 are shown a list of companies and the user can make modifications on the organizations, create others, or access the site menu to view all the possibilities.

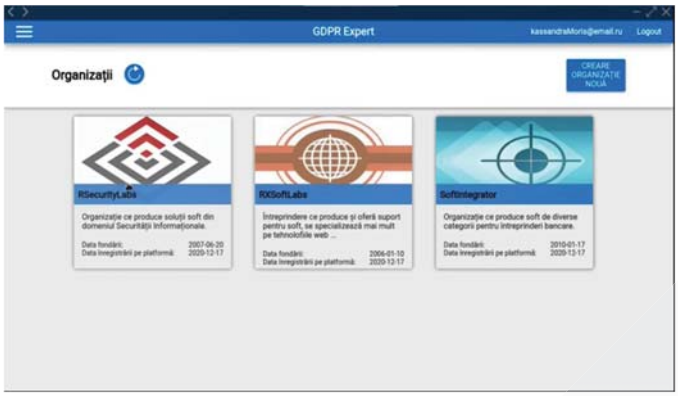

Fig. 4.3 List of organizations

Accessing an existing company in the organization list, it displays all the information about it, showing some functionality, like viewing departments, assessing the conformity with GDPR and viewing previous data processing activities (figure 4.4).

Fig. 4.4 Company information

The interface of adding a department to an organization, of adding an employee to a department and adding documents to an existing employee are shown in figure 4.5 a, b and c.

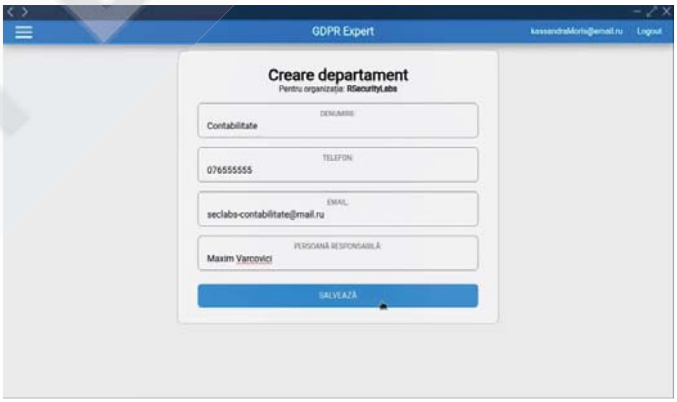

Fig. 4.5. a - Adding a new department

Fig. 4.5. b - Adding a new employee

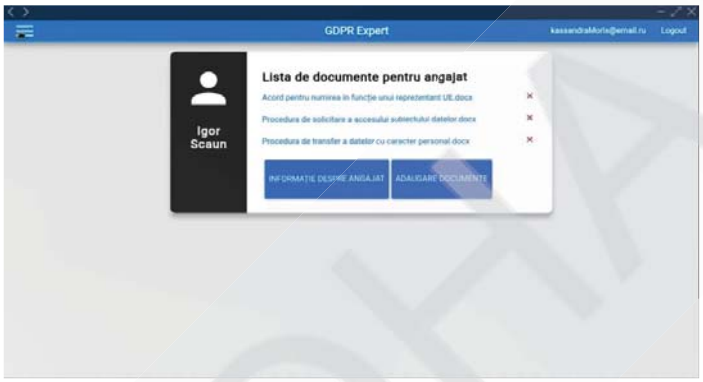

Fig. 4.5. c - Adding personal documents to the existing employee

4.4. Assessment of compliance with the GDPR

It is very important that the system provides a way to assess compliance with EU GDPR requirements. Following the analysis of the main requirements imposed by the Regulation, those essential compartments that can demonstrate an organization's compliance with the GDPR have been established, which are presented below. 1. Principles related to the processing of personal data 2. The rights of data subjects during processing and access to their information 3. Data transfers to third parties 4. Private information 5. Data leaks 6. Data protection impact assessment The review of the EU GDPR conformity assessment questionnaire and the visualization of the current results, as well as the comparison with the previous evaluations are presented in figure 4.6 a, b, c, d and e.

Fig. 4.6. a - GDPR conformity assessment questionnaire

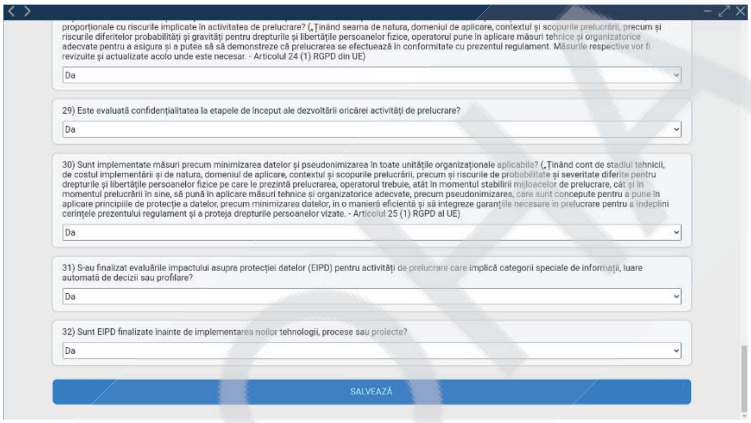

Fig. 4.6. b - GDPR conformity assessment questionnaire GDPR (ending)

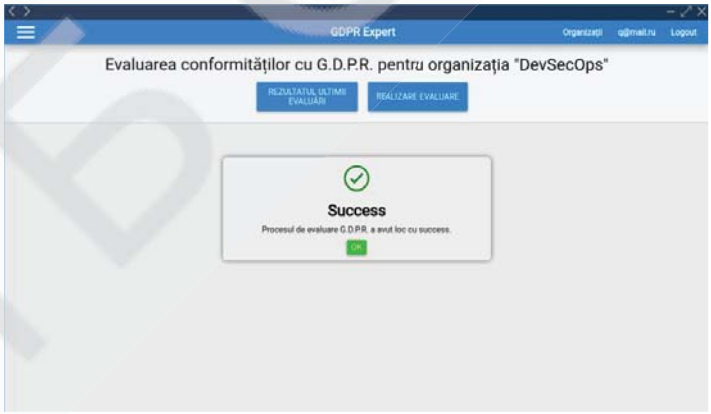

Fig. 4.6. c – Assessment of compliance with the GDPR

Fig. 4.6. d – The result of the last GDPR conformity assessment

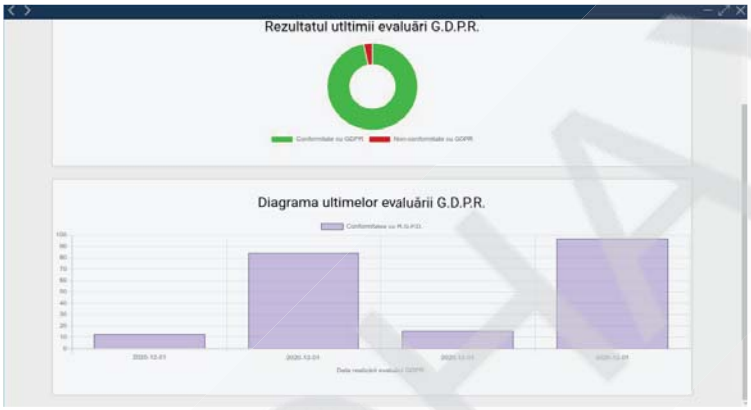

Fig. 4.6. e – Comparison with previous GDPR conformity assessments

V. CONCLUSIONS

The harmonization of the legislation in the field of personal data protection with the legislation of the European Union will be a progressive step in order to obtain the recognition of the Republic of Moldova as a state that ensures an adequate level of protection of personal data. This achievement will increase the credibility of the Republic of Moldova in the eyes of the financial institutions of the European Union, will create optimal conditions for attracting investments and for developing sustainable economic relations.

In this project we tried to conceptually design a solution that will facilitate the implementation of the General Regulation on Data Protection and to materialize the given concept in a software solution.

The analysis of the provisions of the General Regulation of Data Protection competing on the market facilitated the creation of a system that comes to automate and facilitate the process of implementation and monitoring of GDPR compliance.

The system seeks to cover the essential aspects of a small to medium-sized organization in the process of compliance.

Since the purpose proposed in this project is to create a universal solution that can be used by small companies regardless of their field of activity. The complete automation of the implementation process is not feasible at the moment, being necessary the manual adjustment of the provided documentation templates. Full automation would only be possible if the system was created for a certain field of

activity.

The system automates a series of processes and facilitates the implementation of the provisions within small and medium-sized organizations regardless of their field of activity, reducing much of the costs in case of using consulting services at law firms and / or IT consultants.

VI. REFERENCES

1. Jurnalul Oficial al Uniunii Europene. REGULAMENTUL nr. 679 din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), [cited 10.09.2020]. Available: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32016R0679
2. Sorina-Elena ANGHELUȚĂ. 2015 *Protecţia datelor cu caracter personal în contextul angajării.* Internet Documentation, [cited 10.09.2020]. Available: https://www.juridice.ro/401834/protectia-datelor-cu-caracter-personal-in-contextul-angajarii.html
3. *From the garage to the Googleplex*, [cited 17.09.2020]. Available: https://about.google/our-story/
4. Facebook – Company info, [cited 10.09.2020]. Available: https://newsroom.fb.com/company-info/
5. Al Pascual, Kyle Marchini, Sarah Miller. *2017 Identity Fraud: Securing the Connected Life.* Internet Documentation, [cited 20.09.2020]. Available: – https://www.javelinstrategy.com/coverage-area/2017-identity-fraud
6. Al Pascual, Kyle Marchini, Sarah Miller. *2018 Identity Fraud: Fraud Enters a New Era of Complexity.* Internet Documentation, [cited 21.09.2020]. Available: https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity
7. Catherine Stupp | EURACTIV.com. *Cambridge Analytica harvested 2.7 million Facebook users' data in the EU.* Documentaţie Internet, [cited 10.09.2020]. Available: https://www.euractiv.com/section/data-protection/news/cambridge-analytica-harvested-2-7-million-facebook-users-data-in-the-eu/
8. Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, [cited 03.10.2020]. Available: https://datepersonale.md/
9. *GDPR still a mystery to SMEs: the risks of non-compliance* , january 2019, [cited 07.10.2020]. Available: https://www.hiscox.co.uk/business-blog/gdpr-still-mystery-smes-risks-non-compliance/
10. Ecomply.io, Internet Documentation, [cited 13. 09.2020]. Available: https://ecomply.io/
11. GDPR 365, [cited 21.09.2020]. Available: https://www.gdpr365.com/software-features/
12. Legea nr. 133 din 8 iulie 2011 privind protecţia datelor cu caracter personal.

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2021

Information Technology, Automation and Robotics

Proceedings

Odessa National Academy of Food Technologies

The collection includes student works of the participants of the competition, which were not included in the number of prize-winners. The texts of the competitive works are published in the form in which they were submitted by the authors. The authors of the articles are responsible for the content and form of submission of the material.

Responsible for the issue: Sergii Kotlyk

Computer typesetting and layout: Oksana Sokolova

Odessa 2021