DATA PROTECTION IMPACT ASSESSMENT REPORT

on the processing of personal data implementing European Union financed Horizon 2020 programme's project "Regeneration and Optimisation of Cultural heritage in Creative and Knowledge cities" (ROCK))

2019-04-10, Vilnius

INTRODUCTION

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data was adopted (hereinafter – Regulation). Regulation is directly applicable European Union legislation. It has been applied in Lithuania, as in other European Union Member States, on 25 May 2018.

Article 35 Part 1 of Regulation provides that:

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."

Data protection impact assessment (hereinafter – DPIA) is a process for describing data processing and assessing, as well as, the necessity and proportionality of such processing, which helps to manage the risk to the rights and freedoms of natural persons, by assessing and indicating the means of eliminating it.

DPIA is an important means of accountability as it helps data controllers not only to comply with the Regulation but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation.

The aim of the DPIA is to systematically investigate new situations, new technological solutions to assess their compliance with data protection requirements, as well as, the impact on the rights and freedoms of natural persons.

Vilnius Gediminas Technical University (hereinafter – VGTU), in accordance with the compliance and reporting requirement of the Regulation, made a decision to carry out a DPIA on the processing of personal data implementing European Union financed Horizon 2020 programme's project "Regeneration and Optimization of Cultural heritage in Creative and Knowledge cities" (ROCK) (hereinafter – ROCK project).

The ROCK project is funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 730280. More about the programme: https://cordis.europa.eu/project/rcn/210174/factsheet/en.

Municipalities, universities, SMEs and companies, associations, data managers & developers, dissemination & networks, development and consulting groups, and other partners are involved in the ROCK project. In total there are 32 partners from 13 countries. The participating cities are divided into Role models and Replicators. From Lithuania Vilnius City Municipality and Vilnius Gediminas Technical University participate in this ROCK project.

Vilnius has been chosen as one of the exemplary cities that can convey its experience to other cities. It is a renovation of Vilnius Old Town – UNESCO World Heritage Site, presentation and promotion of heritage value, community heritage awareness-raising, inclusion in the renewal process.

VGTU has been chosen as the entity responsible for the scientific part of this project. VGTU has recommended the theme of Vilnius experience – optimal use of cultural heritage using multi-criteria, large data and text analysis guidance system. More about the project: https://rockproject.eu/consortium. ECOVIS ProventusLaw law office (hereinafter – Law Office) on behalf of VGTU carried out the ROCK project's DPIA, in accordance with Article 35 provisions of Regulation, Article 29 Data Protection Working Party's "Guidelines on Data Protection Impact Assessment (DPIA) and determining, whether the data processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" (Article 29 Data Protection Working Party Guidelines) and the 2019-03-14 Order of the Director of the State Data Protection Inspectorate No. 1T-35 (1.12.E) "On the approval of the list of data processing operations subject to the requirement to perform a Data Protection Impact Assessment" (hereinafter – State Data Protection Inspectorate Order).

After the analysis of the information provided by VGTU, the Law Office has prepared this DPIA report (hereinafter – Report).

We would like to draw your attention to the fact that the Report is based on the documents, explanations provided by VGTU, and the processes described with the assumption that the provided information is correct, the documents are comprehensive and final, the copies of the documents correspond to the originals and the processes proceed in accordance with the provided description.

The Law Office was provided with the following documents:

1. Description of the ROCK project;
2. Responses to Triangulum questionnaire;
3. Responses to communication with the Law Office, communication via e-mails;
4. VGTU provided scheme for the movement of personal data and applicable technical and organizational security measures dated on 4 April 2019;
5. Opinion of VGTU Data Protection Officer.

We would like to note that the Report is based on the expert understanding of the Law Office and the evaluation and interpretation of the provisions of the Regulation. Currently, there are no court or other institution practices in Lithuania on the application of the provisions of the Regulation. The evaluation provided by the Law Office does not exclude the possibility of a different interpretation, does not cover all individual circumstances and does not provide a guarantee for the successful outcome of the dispute, if it arises. The Report was prepared without evaluating the possible impact of new IT technologies on the process of processing personal data indicated in the Report, as well as, without carrying out audits of technical and organizational measures applied by VGTU. Law Office's recommendations are presented in a separate document.

The information contained in this Report is for the sole use of VGTU and may not be disclosed to any other person without the prior written consent of the Law Office, except for the ROCK project partners. The information contained in the Report is confidential. The Report and the information contained therein may not be used for any purpose other than those specified or quoted or indicated in any public document or made available elsewhere without the express permission of the Law Office.

Respectfully

ECOVIS ProventusLaw
Partner – Attorney at Law
Loreta Andziulytė

DATA PROTECTION IMPACT ASSESSMENT

1. Reasons why it is necessary to carry out data protection impact assessment

1.1. Description of activity to be carried out, its objectives and planned personal data processing operations. Explanation of necessity for a data protection impact assessment. If necessary, the relevant documents are attached to the form.

Description of activity: VGTU is implementing the ROCK project is funded by the European Union. Its objective is to identify the emotions of individuals with respect to specific areas of Vilnius and to use them to meet public interests and for scientific research. ***Emotions*** are captured by special equipment at places designated in Vilnius city (cheerful, sad, angry, surprised, appalled, disgusted, neutral; also valence and excitement), ***affective conditions*** (boredom, interest and confusion), ***physiological data*** (average composition of passers – by sex and age groups, pulse rate, respiratory rate). After capturing this data, it will be analysed, grouped and made with appropriate conclusions related to the ongoing project.

Activity objectives and planned personal data processing operations: The ROCK project is implemented in the public interest and for scientific research purposes. During this ROCK project, VGTU will seek to help with achieving the goals set for Vilnius city as a participant of the project, especially making the best use of public spaces. The ROCK project aims to determine what factors influence the positive or negative emotions of the population and make recommendations for improving the environment, develop innovative strategies for the regeneration of historic city centers, integrated urban management plans, using cutting-edge environmental models, urban marketing, enhancing urban security, promoting community initiatives. The data will be used to help urban planners to create a more comfortable, best-performing urban environment and a more accurate range of services to meet the needs of the city and its guests.

During the ROCK project video data, personal respiratory rate recordings will be captured, transmitted to a stationary VGTU computer, the video data will be computed, depersonalized, analysed and then stored on VGTU server (more about the data processing operations performed in Point 2.1. of this Report).

Necessity of carrying out data protection impact assessment: Article 35 Part 1 of the Regulation indicates that when new technologies are used, taking into account the nature, scope, context and purposes of the processing, it is likely to result in a high risk to the rights and freedoms of natural person, therefore, the data controller needs to carry out DPIA.

Article 29 Data Protection Working Party Guidelines indicate that DPIA can be carried out by data protection impact assessment on specific technological product, software.

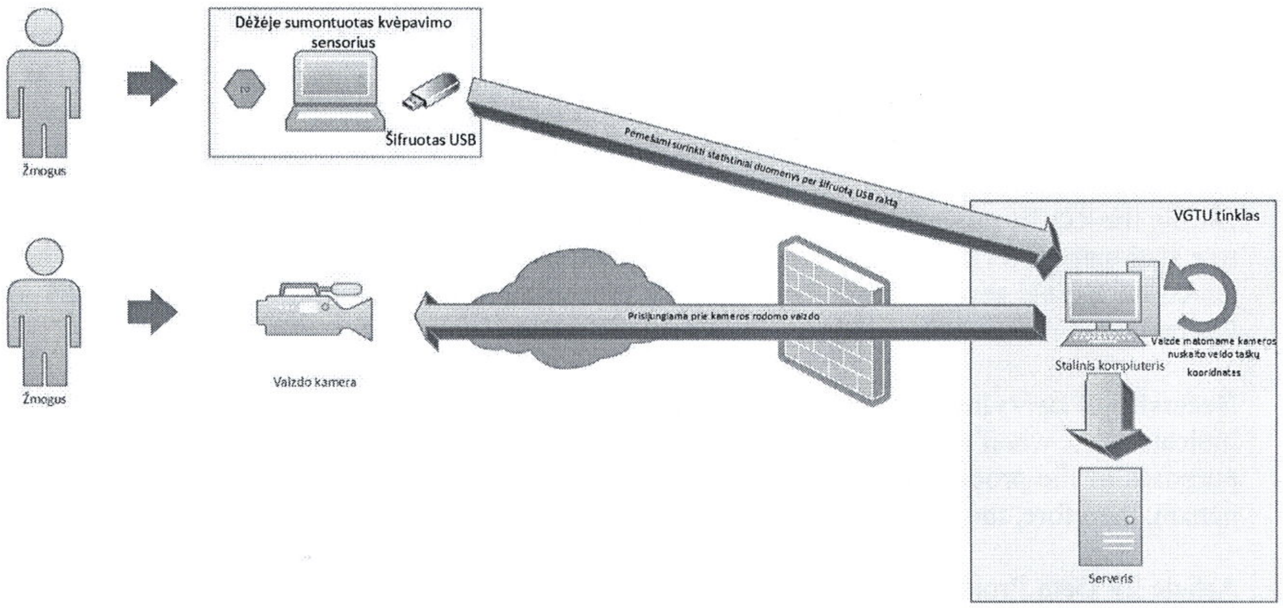
Points 6.1. and 8 of State Data Protection Inspectorate Order indicate that processing operations are subject to data protection impact assessment if they include the processing of video data when video surveillance is carried out in premises and/or areas that are not owned by the data controller or on other legitimate grounds when video surveillance is carried out in accordance with the Regulation (EU) 2016/679 sets out the principles relating to the processing of personal data or the processing of personal data using innovative technologies or the use of existing technologies in a new way when processing personal data of vulnerable data subjects.

During the ROCK project a technologically new IT solution is used, therefore, in accordance with the above-mentioned provisions of the Regulation, Article 29 Data Protection Group Guidelines and the State Data Protection Inspectorate, VGTU is performing a DPIA.

2. Description of the processing of personal data

2.1. Described actions for the collection, usage, storage and destruction of personal data, specifying the sources from which the data will be collected to which the data will be provided (action plan for the processing of personal data may be provided). It describes what actions of personal data processing may endanger the rights and freedoms of natural persons.

Indicated below is a graphical representation of personal data processing and processing scheme presented to the Law Office:



Žmogus
Dėžėje sumontuotas kvėpavimo sensorius
Šifruotas USB
Pernešami surinkti statistiniai duomenys per šifruotą USB raktą
VGTU tinklas
Žmogus
Vaizdo kamera
Prisijungiama prie kameros rodomo vaizdo
Stalinis kompiuteris
Vaizde matomame kameros nuskaito veido taškų kooridnates
Serveris

Below is a description of the processing of data collected during the ROCK project:

1. Video data capturing using cameras

1.1. The selected public places in Vilnius city have cameras that capture the view of the area of the camera, including people in the area. Video data captured by the cameras is transmitted via Internet to a computer on the VGTU premises.

1.2. Cameras are placed in public places on traffic lights and/or street lights, out of reach of the individuals.

1.3. The video data captured by the cameras is not being recorded.

2. **Monitoring of respiratory rate with a special device and recording of data on a portable computer**

2.1. Respiration rate detecting device *xethru X4M200* is connected to a portable computer (respiratory rate monitoring program XeThryExplorer), which is mounted in a lockable box at a height of 3 meters on traffic lights and/or street lights next to the camera.

2.2. Device *xethru X4M200* captures the respiratory rate of the persons entering the coverage of the device. These data are not related to the specific persons captured by the camera. According to these data, it is not possible to identify or associate a particular person with the persons captured by the camera. The device only records the respiratory rate.

2.3. Respiratory rate information from portable computer is transferred to a USB flash drive and is then transferred to a VGTU stationary computer located on the VGTU premises at Saulėtekio al. 11, Vilnius in a separate locker room.

3. **Video data transfer to the VGTU on-premises computer and video data computing by the *Facereader* program. Transfer of respiratory rate information to a computer on VGTU premises.**

3.1. The video data captured by the cameras is transmitted via Internet to a desktop computer at the premises of VGTU, at Saulėtekio al.11, Vilnius. This computer is equipped with the *Facereader* program for computing video data.

3.2. *Facereader* program performs face detection actions to faces that are suitable for research purposes. Suitable faces are those whose points can be scanned. Suitability to scan face points is determined by the technical parameters of the equipment used. Suitability is not related to a person's physiological or other personal data being captured.

3.3. After *Facereader* program detects a person's face, it scans 500 facial points. Using *Facereader* program facial points are scanned and compared with thousands of emotional expressions already installed in the program, as well as, level of pattern strength and according to them, impersonal emotional state of the passer-by (cheerful, sad, boring, interest, angry, surprised, etc.) and its strength and physiological parameters (face temperature, pulse, age, sex) are identified. Each pattern of emotion level has its own numerical expression. This information is depersonalized, *Facereader* program does not record the prototype of a scanned facial points. Information is depersonalized using the method of randomization – permutation method and generalization – the method of aggregation and k-anonymity (for more details, see paragraph 7 of this Report). The data in the *Facereader* program is reflected in a form of numbers and expression of certain records that are not related to personal data. Depersonalized data are computed by converting it into statistics.

3.4. Respiratory rate information (respiratory rate per minute) from a USB flash drive is transferred to a VGTU stationary computer, located at Saulėtekio al.11, Vilnius, through which the respiratory data are transferred to the server database.

3.5. Both video data and respiratory rate information are transferred to the computer in separate streams, without interlinking.

3.6. Statistical and depersonalized data are sent to the VGTU data server.

4. Storage of statistical, anonymous data on VGTU server and database

4.1. From *Facereader* program an hourly average depersonalized information is transferred through *Facereader* API (filtering out invalid data, e.g. rejecting data received if the age of the person is less than 18 years) to data server where VGTU performs analysis of such depersonalized information and further uses depersonalized information for the ROCK project's implementation purposes. The records on the VGTU data server are approximate, the data parameters are correlative, and the expression of the statistical numbers is provided.

Provided below is the video data computing scheme using *Facereader* program that has been submitted to the Law Office:

Face detection – face and its position is detected using *Viola-Jones* classification algorithm which was primarily created for face detection. At this stage, the program detects a face that can be scanned.

Face modelling – at this stage a method called active appearance model (AAM) is used in order to synthesize an artificial face model with a detected face by scanning 500 facial points.

Face classification – points are spread out comparing to the patterns of thousands of already available expressions of emotion and their level of strength (thus, determining the human emotion). Each template of emotion level has its own numerical expression.

Data are processed using this equipment:

1. ***IP camera Hikvision PTZ DS-2DE4225IW-DE*** – camera is designed to transfer video data to the Facereader program installed on a computer on VGTU. The video data are not recorded;
2. ***Respiratory rate detection device xethru X4M200*** – for monitoring persons' respiratory rate
3. ***Portable computer Lenovo Miix 320*** – for processing persons' respiratory rate information;
4. ***USB flash drive*** – for transferring information on persons' respiratory rate to a VGTU stationary computer;
5. ***Stationary computer "Kilobaitas verslui"*** – for computing video data using *Facereader* program;
6. ***Program Noldus Facereader 8.0*** – designed to establish emotions used on a license basis (only works with a USB flash drive – license (unlimited time)). The scanned image is automatically depersonalized (video archive cannot be viewed);
7. ***Program Noldus Facereader API*** – designed to send (filtering and pre-computing) emotions from the software *Facereader* 8.0 to the database server;
8. **Server with Database** – for storing and processing depersonalized data.

Video data are being collected in public places in Vilnius city. Provided below are video data collecting addresses:

1. Pilies str. 1 / Šventaragio str. 2, Vilnius – 1 camera;
2. Gedimino av. 33 / V. Kudirkos str. (Lukiškių square), Vilnius – 1 camera;
3. Islandijos str. 6 / Pylimo str. 2, Vilnius – 2 cameras;
4. Kalvarijų str. / Ozo str. – 1 camera;
5. Santariškių str. 2, Vilnius – 1 camera;
6. Dariaus ir Girėno str. 2, Plungė – 2 cameras (cameras not connected).

Video data and respiratory rate are computed on a VGTU stationary computer at Saulėtekio al. 11, Vilnius.

Anonymous and statistical data are stored on VGTU server at Saulėtekio al. 11, Vilnius.

VGTU stated that collected statistical data will be used for VGTU scientific research purposes and will not be shared with third parties.

Personal data processing activities that may endanger the rights and freedoms of natural persons:

According to the explanations provided by VGTU to the Law Office, data processing is carried out in the following equipment / devices: video cameras, respiratory rate device, portable VGTU computer, VGTU USB flash drive, stationary computer on VGTU premises, with installed *Facereader* program and VGTU server, database. It is necessary to evaluate the data processing steps for each equipment/device separately:

1. ***Video data capture using video cameras*** – captured video data are not recorded as it is transmitted over the Internet directly to a computer on the VGTU (*online*).

   1.1. Since the processing of personal data (video data capture and video data transmission) is carried out at this stage, the processing of personal data on a large scale and the monitoring of public places is assumed to include the capturing of video data by means of cameras that may endanger the rights and freedoms of natural persons it is, therefore, necessary to assess whether appropriate technical and organizational measures have been taken to address these risks.

2. ***Respiratory rate monitoring, using device xethru X4M200, respiratory rate information storing in VGTU portable computer and USB flash drive*** – respiratory rate of persons‘ entering the area captured by *xethru X4M200* is recorded. These data are recorded on a VGTU portable computer without linking them to the video data captured by the camera. These data are grouped with a certain periodicity. Respiratory device and cameras can capture data from different individuals, so there is no way to link them. Respiratory data from a portable computer is stored in a USB flash drive in order to transfer them to a VGTU stationary computer.

2.1. Since at this stage only the processing of respiratory rate information is carried out without linking it to a specific person, it is believed that the processing of such data does not jeopardize the rights and freedoms of individuals, since respiratory rate information cannot be linked to a specific person in case of a breach of data security. Also, if the respiratory rate information was matched with video data, there is no way to link the respiratory rate information to a specific person.

3. ***Video data transfer and data computing with the Facereader program installed on a VGTU computer*** – video data are transferred directly to a computer on the VGTU premises, where they are computed by making them anonymous with the help of *Facereader* program, converted into numbers and certain conditional records that are unrelated with personal data.

3.1. We shall distinguish two data processing operations from this data processing activity:

a) *Video data transfer to the computer* – the processing of personal data is carried out at this stage, as it is possible to see the view captured through the cameras on the computer. It is assumed that the transmission of video data to a computer falls within the scope of data processing operations which may endanger the rights and freedoms of natural persons, and it is, therefore, necessary to assess, whether appropriate technical and organizational measures have been taken to address these risks.

b) *Video data computing using Facereader program* – at this stage, *Facereader* program captures 500 facial points, convert them to anonymous, and group them according to specific parameters. It has been stated to the Law Office states that neither the computer nor *Facereader* program records video data and that the data are computed at the time when data are collected with the help of *Facereader* program. After computing this data, there is no possibility of identifying a particular person. The information is depersonalized using the method of randomization – permutation and generalization – aggregation and k-anonymity (for more details, see paragraph 7 of this Report), therefore, after applying these depersonalization methods there is no way of restoring them.

VGTU indicated to the Law Office that the facial points captured by the *Facereader* program are being depersonalized in accordance with the recommendations of the State Data Protection Inspectorate on the methods of depersonalization, based on Opinion 05/2014 on methods of depersonalization prepared by the European Commission's Article 29 Data Protection Working Party.

VGTU indicated that *Facereader* program computes video data and depersonalizes it in such a way that the data cannot be restored to the original personal data and linked to a specific person. From the available anonymous data: a) there is no possibility to distinguish an individual; b) there is no possibility of linking individual records to a particular individual; c) there is no possibility of retrieving data on the individual person from the derived data.

3.2. In the opinion of the Law Office, the risks to individual rights and freedoms at this stage may arise in the event of unauthorized access (or access granted) to the computer to which the video data are transmitted directly, and it is, therefore, necessary to assess, whether appropriate technical and organizational measures have been taken to eliminate these risks. The Law Office does not assess the functionality, modification, and the probability of an unauthorized access to the *Facereader* program.

3.3. In the opinion of the Law Office, the risks to the rights and freedoms of anonymous and statistical data on the computer are unlikely, as VGTU uses the appropriate methods of depersonalization, which are considered sufficient to prevent identification. The opinion of the Law Office does not cover the use of all possible information technologies and the creation or development of such technologies in the future, therefore, these circumstances are not assessed when expressing this opinion.

4. ***Storing and processing of statistical personal data on VGTU server and database*** – computed and depersonalized data via *Facereader* program is transferred to the VGTU server and database and further processed for scientific purposes.

4.1. Since anonymous, statistical data are transmitted to the VGTU server it is not possible to restore them to the original personal data and using these data to identify particular person, the risk to the rights and freedoms of natural persons is unlikely.

2.2. Described the extent of processing: what categories of personal data will be processed; whether specific categories of personal data or data on convictions and criminal offenses will be processed; how much data will be collected and used frequently; how long will personal data be stored; approximate number of data subjects and the geographical coverage of data processing indicated.

Categories of personal data processed: The following personal data are processed during the ROCK project: video data, facial points. The detailed processing of these data are described in Point 2.1 of this Report.

After computing the data with the help of *Facereader* program, 6 parameters are applied: emotion, affective condition, sex, age groups, pulse, respiratory rate. Further actions (analysis, grouping, systematization) are only carried out with regard to the depersonalized and statistical data.

If program *Facereader API* detects a person younger than 18 years, his/her face points are not read and not sent to the database, these points are not recorded/saved. The accuracy of age determination is about 60-70% and age is determined by smaller groups, for example 15-20 years; 20-25 years and so on, so the accuracy of the age determination is low (the error depends on whether the person is wearing glasses, the angle at which the face is turned, the weather conditions, etc.). The program does not have any possibility of identifying other socially vulnerable natural persons groups. If an approximate age category on the *Facereader* program is set, the *Facereader API* open source program can be programmed to scan and send data into the database.

How much data will be collected and used frequently; how long will personal data be stored; the approximate number of data subjects and the geographical coverage of data processing indicated:

During the ROCK project, it will be collected approximately 10504690 records for each parameter (6 in total). Data are collected continuously, in automated ways. The approximate number of data subjects is between 30 and 120 people per hour. The ROCK project will last until 2020 and the results of the project must be retained for at least 10 years after the completion of the ROCK project.

Geographic coverage of personal data processing is as follows:

1. Pilies str. 1 / Šventaragio str. 2, Vilnius;
2. Gedimino av. 33 / V. Kudirkos str. (Lukiškių square), Vilnius;
3. Islandijos str. 6 / Pylimo str. 2, Vilnius;
4. Kalvarijų str. / Ozo str.;
5. Santariškių str. 2, Vilnius;
6. Dariaus ir Girėno str. 2, Plungė (cameras not connected).

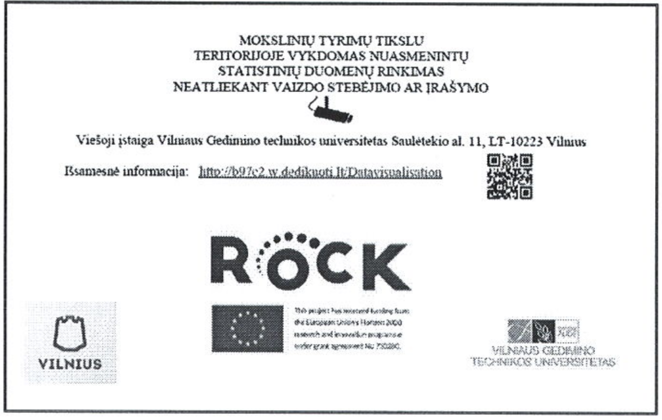
In each of the above-mentioned areas the video data capture is about 1.5 square meters area parameter from the camera mounting location. The facial points are fixed at a distance of 20-30 meters from the camera mounting location.

Video data and respiratory rate information are computed on a VGTU stationary computer at Saulėtekio al. 11, Vilnius.

Anonymous and statistical data are stored on VGTU server at Saulėtekio al. 11, Vilnius.

2.3. Described the nature of data processing: what kind of relationship links your company with data subjects; whether data subjects will have the opportunity to control data processing; whether data subjects can foresee that their personal data will be processed in this way; whether the data of children and other vulnerable persons will be processed; assess whether such data processing is secure; whether the data processing technologies are new or whether existing technologies will be used in a different way; what is the level of technology development in this field; are there any public or other problems or issues to consider; indicated whether there is an obligation to comply with an approved code of conduct or an approved certification mechanism.

VGTU collects and processes personal data at random from persons entering the area where video data are captured and respiratory rate is recorded. Persons who fall into the camera's video data capture area and those who fall within the respiratory rate monitoring range are not specifically selected. There is no relationship between VGTU and data subjects. Due to the nature of the actions performed, data subjects have no control over the processing of data.
Data capture zones include information tables that provide information on data collection (size 20x10 cm).



MOKSLINIŲ TYRIMŲ TIKSLU
TERITORIJOJE VYKDOMAS NUASMENINTŲ
STATISTINIŲ DUOMENŲ RINKIMAS
NEATLIEKANT VAIZDO STEBĖJIMO AR ĮRAŠYMO

Viešoji įstaiga Vilniaus Gedimino technikos universitetas Saulėtekio al. 11, LT-10223 Vilnius

Išsamesnė informacija: http://b97c2.w.dedikuoti.lt/Datavisualisation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 730280.

Are data processing technologies new: VGTU stated that data processing technologies are contemporary and modern, yet reliable and secure.

Will the existing technologies be used in another way: VGTU stated that existing technologies would not be used in any other way.

What is the level of technology development in this area: VGTU has stated that the level of technology development in this area is ordinary.

Are there any public or similar problems or issues to consider: The Law Office has not been provided with any questions or problems that need to be addressed in the processing of such coverage data.

Is there an obligation to comply with an approved code of conduct or approved certification mechanism: VGTU undertakes to follow its own internal processing policy (link online: https://www.vgtu.lt/universitetas/duomenu-saugumas/296093#296105) as well as Code of Ethics: http://www.vgtu.lt/files/876/43/2/9_0/81-2.5.%20Akademines%20etikos%20kodeksas.pdf).

2.4. Describe the purposes of the processing of personal data: what impact the result will have on natural persons; what is the benefit of processing such data for your company and others.

The purposes of data processing are the satisfaction of the public interest, scientific research. It should be noted that video data and personal face points are collected only at the initial data processing stage, i.e. only until they are computed with the help of the *Facereader* program and depersonalized. The purpose of the ROCK project is not to analyse the personal data collected prior to their processing in the *Facereader* program. The purpose of the ROCK project is to analyse, and report findings based on data depersonalized and grouped according to the *Facereader* program parameters.

The project aims to develop innovative strategies for the regeneration of historic city centers, integrated urban management plans, using innovative environmental models, urban marketing, increasing urban safety, promoting community initiatives. From collected data, scientists will develop integrated maps of emotional, physiological and air pollution conditions (temperature, wind, precipitation) and will provide recommendations to help urban planners create a more environmentally-friendly and socially-friendly environment that meets the needs of the population and city guests.

The data collected during the project will be used for scientific purposes and for the implementation of the ROCK project.

3. Consultations

3.1. Described how the opinion of interested parties is planned to know or why it is not necessary to do so: whose opinion is planned to know; who will be recruited by your company or whether or not data processors will be involved; whether it is planned to consult with data security experts or experts in other fields.

Opinion of the data subjects: VGTU stated that they did not ask the opinions of the data subjects, as asking of such opinion would be disproportionate to the activities carried out and would not guarantee the purpose of evaluating such opinion, as it is not possible to identify the specific data subjects who are included in the observation area and the assessment of public opinion is inexpedient.

The ROCK project is funded by the European Union, additional resources to conduct general surveys, research is not provided.

VGTU stated that the data processors will not be used.

Opinion of VGTU Safety Specialist: Justinas Rastenis, Head of VGTU Centre of Information Technology and Systems Infrastructure Department, presented his conclusion on technical and organizational security measures used by VGTU in this data processing process (Annex 1).

4. Assessment of necessity and proportionality

4.1. The legality and proportionality of the processing of personal data are described: the basis for lawful processing is specified; assessed whether personal data will help to achieve Your goal; whether the same result can be achieved in another way; how to avoid malfunctions; how data quality and data minimization will be implemented; what information will be provided to data subjects; how your company plans to implement data subjects' rights; how it will be ensured that the data processor complies with the requirements; how the security of personal data provided to foreign countries will be ensured.

During the ROCK project VGTU aims to help with implementing the goals set for Vilnius city as a project participant to use public spaces in the most optimal way . The ROCK project aims to find out what factors have an impact on the positive or negative emotions of the population and to develop recommendations for improving the environment, developing innovative strategies for the regeneration of historic city centers, integrated urban management plans using innovative environmental models, urban marketing, enhancing city security, promoting community initiatives. The data will be used to help urban planners to create a more comfortable, best-performing urban environment and a more accurate range of services to meet the needs of the city and its guests.

These goals can only be achieved by VGTU after analysing the data computed and depersonalized with the help of the *Facereader* program and after some research is carried out. These actions are not possible without the initial stage of collecting personal data.

On the basis of the above-mentioned ROCK project‘s objectives, it must be concluded that the processing is carried out on the basis of Article 6 Point 1 Peart e of the Regulation, i.e. the processing of personal data is lawful when processing the data is necessary for the performance of a task carried out in the public interest.

The purpose of the ROCK project is to link Vilnius city spaces with the emotions of individuals, therefore, the identification of emotions is necessary for the proper implementation of this project.

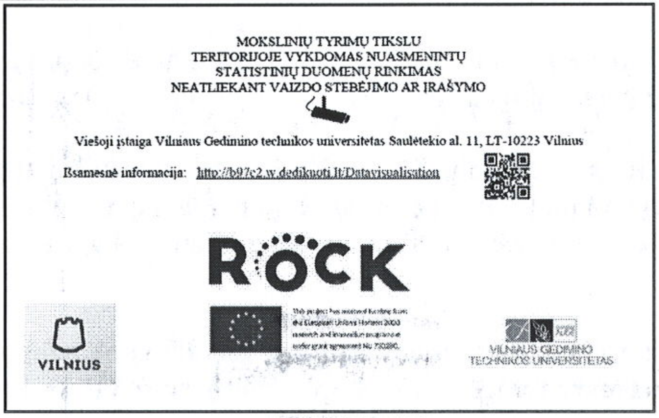
The selected method of capturing video data and facial points in the *Facereader* program is the most appropriate, because it:

1. provides a large number of individuals that ensures sufficiently large amount of data is analysed and that the conclusions are as accurate as possible;
2. ensures the reliability of the emotions of individuals, because emotions are determined by natural reaction of individuals to certain places, without creating played, false emotions;
3. ensures same application of the methodology for identifying people's emotions, as only a specific program can provide a certain conclusion using same computing criteria and algorithms;
4. ensures the accuracy of emotion detection and compliance with the purpose of the ROCK project by capturing emotions from a person's face, unlike e.g. a method of interviewing which may include errors in expressing emotions, describing them, and so on.

Considering that after capturing video data and facial points personal data are depersonalized and converted into statistics, there is no impact on the rights and freedoms of data subjects in further analysing such data. It must, therefore, be concluded that the chosen method of processing personal data is proportionate to the objective pursued.

The VGTU uses two different ways of depersonalization: method of randomization – permutation and method of generalization – aggregation and k-anonymity (for more details see paragraph 7 of the Report).

Data subjects are informed about the ongoing data collection:



MOKSLINIŲ TYRIMŲ TIKSLU
TERITORIJOJE VYKDOMAS NUASMENINTŲ
STATISTINIŲ DUOMENŲ RINKIMAS
NEATLIEKANT VAIZDO STEBĖJIMO AR ĮRAŠYMO

Viešoji įstaiga Vilniaus Gedimino technikos universitetas Saulėtekio al. 11, LT-10223 Vilnius

Bsamesnė informacija: http://b97c2.w.dedikuoti.lt/Datavisualisation

ROCK
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 730280.
VILNIUS
VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

VGTU stated that it will not employ data processors and data are and will not be provided to foreign countries.

5. Determination and assessment of risk

5.1. Risk is a scenario describing an event and its consequences, estimated in terms of severity and likelihood. "Risk management", on the other hand, can be defined as the coordinated activities to direct and control an organization with regard to risk.

Assessing the risk to individual rights and freedoms it is necessary to distinguish these data processing operations and equipment used for it: 1) Video data capture (using cameras); 2) Respiratory rate monitoring using *xethru X4M200* device, transferring this information to portable VGTU computer and USB flash drive; 3) Video data transfer to computer in VGTU premises and video data processing using *Facereader* program (using VGTU desktop computer and *Facereader* program); 4) Storage of statistical, anonymous data on VGTU server and database (using VGTU server).

Justinas Rastenis, Head of VGTU Centre of Information Technology and Systems Infrastructure Department, presented his conclusion on technical and organizational security measures applied to the equipment used in the data processing process (Annex 1), therefore Law Office assesses the risk to individual rights and freedoms according to the provided conclusion.

Law Office does not assess technical decision and level of security of *Facereader* program and respiratory rate monitoring device *xethru X4M200*, also functionality, modification, reprogramming, installment or modification of programs, and the probability of an unauthorized access is not assessed, thus conclusion on these IT technologies and their security and impact shall not be provided by the Law Office.

	5.2. Described nature of the risk and the impact on the individual. If necessary, the related business risk is described.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1.	*Possible risk to the rights and freedoms of data subjects during video data capture and transfer to the VGTU computer* **Nature of the risk:** According to the information provided by VGTU, video data will be captured, using cameras, in public sites of Vilnius city. Captured video data via Internet will be transferred to computer on VGTU premises in order to process data using *Facereader* program. When assessing potential risk, it is believed that unauthorized access to the camera and unauthorized receiving of video data is possible. **Sources of the risk:** A potential source of risk may be unauthorized and external access to the cameras. **Severity and probability of the risk:** VGTU stated that the security measures listed in Annex 1 of this Report have been taken, so the probability of a personal data breach is low. Additionally, the camera does not perform video data recording, so even in the case, where connection with the camera would be made, only the currently visible view would be available. **Impact on rights of data subjects:** In the event of a data breach and the unauthorised access to data, there may be some impact on the rights and freedoms of the data subjects. The impact on the rights and freedoms of data subjects depends on the circumstances of use of such data, the scale and the development of information technology. The opinion of the Law Office does not cover the use of all possible information technologies and the creation or development of such technologies in the future; therefore, these circumstances are not assessed when expressing this opinion.	**Low likelihood**	**Minimal**	**Low**

2.	*Possible risk to the rights and freedoms of data subjects during respiratory rate monitoring, transfer of this data to portable computer, VGTU USB flash drive and transfer of this data to VGTU computer* **Nature of the risk:** According to the information provided by VGTU, respiratory rate will be monitored, using *xethru X4M200* device, in public sites of Vilnius city. All respiratory rate information will be recorded in portable VGTU computer, which will be mounted in a lockable box next to the cameras. Later this data using USB flash drive will be transferred to VGTU desktop computer on VGTU premises. Respiratory rate information cannot be associated with particular person, but for the purpose of completeness of this Report, the risk to the rights and freedoms the individual is assessed in relation to used equipment. **Sources of the risk:** A potential source of risk may be unauthorized access to a portable computer that records respiratory rate information or loss of USB flash drive or unauthorized access to the USB flash drive. **Severity and probability of the risk:** VGTU stated that the security measures listed in Annex 1 of this Report have been taken, so the probability of a personal data breach is low. Also, it shall be noted that respiratory rate information is not associated with particular individuals captured using cameras, therefore these data are not considered as personal data. According to these data, it is not possible to identify a particular person or to associate it with the persons captured by the camera, so even in the event of a security breach, the risk to the rights and freedoms of individuals shall not arise. **Impact on rights of data subjects:** In the event of a data breach and the unauthorised access to data, there would be no impact on the rights and freedoms of the data subjects, as there is no possibility of identifying the person and the unlawful interception of the respiratory rate information would not have consequences for data subjects.	**Low likelihood**	**Minimal**	**Low**

3.	*Possible risk to the rights and freedoms of data subjects during video data transfer from cameras to VGTU stationary computer and personal facial points capture using Facereader program* **Nature of the risk:** According to the information provided by VGTU, captured video data will be transferred to VGTU stationary computer on VGTU premises at Saulėtekio al. 11, Vilnius, where its computing will be carried out. Assessing possible risk, two situations shall be distinguished: a) unauthorized access to the computer to which the video data is transferred; b) unauthorized connection to a computer when computing video data by scanning 500 person's facial points. **Sources of the risk:** A potential source of risk may be unauthorized access to a desktop computer. **Severity and probability of the risk:** a) Unauthorized access to the computer to which the video data is transferred - VGTU stated that the security measures listed in Annex 1 to this Report have been taken, so the probability of personal data breach is low. In addition, VGTU indicated that the computer does not perform video data recording, so even when connected to a computer, only the currently visible view would be available. b) Unauthorized connection to a computer while computing video data by scanning 500 person's facial points - VGTU explained that facial points scanned with the *Facereader* program are not stored and at the time when data are collected computed and depersonalized, therefore, even when unauthorized connected to a computer, it is not possible to get access to a particular person's scanned facial points (prototype). Law Office does not assess technical decision and level of security of *Facereader* program, as well as, its functionality, modification, reprogramming, installment or modification of programs, and the possibilities of granting unauthorized access is not assessed, thus conclusion on this program and its security or impact on	**Low likelihood**	**Minimal**	**Low**

	VGTU equipment shall not be provided by the Law Office. **Impact on rights of data subjects:** In the event of a data breach and the unauthorised access to data, there may be some impact on the rights and freedoms of the data subjects. The impact on the rights and freedoms of data subjects depends on the circumstances of use of such data, the scale and the development of information technology. The opinion of the Law Office does not cover the use of all possible information technologies and the creation or development of such technologies in the future; therefore, these circumstances are not assessed when expressing this opinion.			
4.	*Potential risks to the rights and freedoms of data subjects, depersonalized data transfer, analysis, and storage of such data on the VGTU server and database* **Nature of the risk:** According to the information provided by VGTU, after scanning of the person's facial points, all the data are computed and depersonalised at the time when data are collected, with the help of the *Facereader* program, using two methods of depersonalisation: the method of randomization-permutation and the method of generalization-aggregation and k-anonymity (for more details, see paragraph 7 of this Report). VGTU explained that there is no way of restoring the original depersonalized and processed data to initial personal data, therefore, in the event of a data breach with regard to such depersonalized data, the risk to rights and freedoms of the data subjects is low. **Sources of the risk:** A potential source of risk may be unauthorized access to the VGTU server. **Severity and probability of the risk:** VGTU indicated that scanned facial points are depersonalized at the time when data are collected. From the available anonymous data: a) there is no possibility to distinguish a particular person; b) there is no possibility of linking individual records to a particular person; c) it is	**Low likelihood**	**Minimal**	**Low**

	not possible to obtain data on a particular person from the derived data, therefore, the Law Office considers that the risks to rights and freedoms of the data subjects should not arise at this stage. In accordance with the State Data Protection Inspectorate on the methods of depersonalization, based on Opinion 05/2014 on methods of depersonalization prepared by the European Commission's Article 29 Data Protection Working Party, depersonalized data are not subject to data protection legislation. Point 26 of the preamble to the Regulation states that the principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes. **Impact on rights of data subjects:** In the event of a data breach and the unauthorised access to statistical, depersonalized data, it is likely that there would be no impact on the rights and freedoms of the data subjects. The opinion of the Law Office does not cover the use of all possible information technologies and the creation or development of such technologies in the future; therefore, these circumstances are not assessed when expressing this opinion.			

6. Conclusion

According to the information provided in Point 5 of this Report, in the opinion of the Law Office, the overall level of risk is low.

7. Opinion by the data protection officer

An opinion by the data protection officer should be submitted regarding the legality of processing data on individuals, planning means to minimise or eliminate risks and the possibilities for continuing to handle personal data.

Opinion by Raimonda Bublienė, VGTU Data Protection Official:

The basis for data gathering conforms with Article 6 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, indicating the lawfulness of data processing. Data are gathered and processed in the public interest whereby processing is essential for performing a task in the public interest or executing the functions entrusted to an official authority.

The data controller applies for collected data in an integrated manner two different methods for depersonalizing of the data: randomization - permutation method and generalization - aggregation and k-anonymity. Application of these two methods of depersonalization assures the anonymity of the information. Anonymous information is processed for statistical and scientific research purposes.

Statistical information is stored in the database, where relevant organizational and technical measures are employed to assure security: limitation and control of database user rights; persons dealing with the personal are bind with statutory confidentiality obligations; software programs are consistently updated and equipped with firewalls and antivirus programs.

The data controller suitably assures the provision of the information on the collecting of personal data to data subjects foreseen by Article 13 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Information about the project, the data controller and the purpose of processing of the data are provided on the informational board at all the sites where data are being collected. Informational boards are prepared according to the recommendations provided by the State Data Protection Inspectorate.

Upon assessing the use of the collected data and the actions regarding their storage and deletion, as well as, the technical and organizational measures, a conclusion can be reached that the risk to data security is low, and no risks arise to the rights and freedoms of individual persons. Properly executed depersonalization of data on individuals constitutes an appropriate strategy for safeguarding benefits and reduction risk, which is implemented during the execution of this Project. Based on the information mentioned above it might be concluded that the application of the depersonalization method is suitably organized. The data collected during the Project are depersonalized at the time when data are collected, and the information is anonymous, i.e., the anonymity of the data on individuals is assured in such a way that the identity of any data subject cannot be established.

Raimonda Bublienė	*Name, surname, date, signature*

8. Indication of consideration of the data protection officer's opinion

VGTU informed the Law Office that during the implementation of ROCK project the opinion of the data protection officer was taken into account.

9. Opinions from other persons

No opinions from other persons were received.

10. Person designated to be responsible for supervising the assessment of the impact on data protection

Note: The data protection officer shall supervise the processing of personal data to assure the compliance with the conclusions and decisions indicated in the Data Protection Impact Assessment.

Raimonda Bublienė, VGTU Data Protection Official	
	Name, surname, date, signature

Annex:

1. The scheme of the movement of personal data and applicable technical and organizational security measures provided by Justinas Rastenis, Head of the ITSC Department of Infrastructure at VGTU on 4 April 2019.