Deliverable D6.4
Data Protection Impact Assessment
IN2STEMPO Warsaw West station

Project acronym:	IN2STEMPO
Starting date:	01/09/2017
Duration (in months):	60
Call (part) identifier:	H2020-S2R-CFM-IP3-2017-01
Grant agreement no:	777515
Due date of deliverable:	Month 28
Actual submission date:	31/12/2019
Responsible/Author:	PKP/Piotr Sotomski
Dissemination level:	PU
Status:	Issued

Reviewed: Yes

This deliverable is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 777515.

Document history		
Revision	***Date***	***Description***
1	*13/11/2019*	*First issue*
2	20/12/2019	Second issue
3	*23/12/2019*	*QA*
4	05/10/2020	Final version integrating reviewer's comments

Report contributors		
Name	***Beneficiary Short Name***	***Details of contribution***
Piotr Sotomski	PKP	
Stephane Lorin	THA	
Aleksandra Wysocka	PKP	
Claudio Cavalletti	STS	
Artur Fojud	PKP	
Aneta Tumilowicz	NR	Reviewer no 1
Leonor Azevedo Mendes	IP	Reviewer no 2
Lorin Stéphane	THA	Reviewer no 3
Claudio Cavalletti	STS	Reviewer no 4

Table of contents

Table of figures

1. Executive Summary

This deliverable will present a data protection impact assessment that was undertaken before the largescale trial in Warsaw West station is initiated. This will advise on data collection, storage, protection, retention and destruction and compliance with national and EU legislation.

The overall objective of Work Package 6 (WP6) is to significantly improve customer experience and security in large and high capacity stations (especially large interconnected stations and multimodal hubs) both during standard operations, and in emergency cases. The IN2STEMPO Consortium will use the expertise in the areas of Video Analytics (to help assess the situation in real-time); behaviour models (to better simulate actual and observed behaviours) and (crowd simulation) - to model, analyse, measure and predict different scenarios that can be used in crowd management in large and high capacity stations. Using these three technologies at the same time enables new perspectives which should allow us to present recommendations for minimising and where possible, solving station over-crowding problems.

One operational prototype and real experimentation will be done in Warsaw West station in Poland under the supervision of project partner - PKP. This task will require real-time acquisition of data regarding people's movement and behaviour in the station. The presence and counting of people in the station will be ascertained using ticket gate information, validation machine and CCTV outputs, as well as specific counting devices already present in railway station or specifically installed for this purpose.

The data acquired from these multiple sensors and data sources will be normalized, anonymised when needed and loaded in a data collection system for analysis and interpretation by crowd counting dedicated algorithm. Then the data will be filtered to provide the necessary information to the station Managers and the SE-Star simulation system. These sets of data will be used as an input for the various Reference Use Cases defined in the project Grant Agreement.

However, the use of a surveillance camera system at Warsaw West station must consider the effect on individuals and their privacy. Use of a surveillance camera system is regulated by Regulation 2016/679/EU 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, and repealing Directive 95/46/EC, (hereinafter "General Data Protection Regulation", "GDPR")[1].

Systematic, automated monitoring of a specific space by optical or audio-visual means brings about collection and retention of pictorial or audio-visual information on all persons entering the monitored space that are identifiable based on their looks or other specific characteristics. Identity of these persons may be established on the basis of these personal details. It also enables further processing of personal data as to the persons´ presence and behaviour in the given space. The potential risk of misuse of these data grows in relation to the dimension of the monitored space as well as to the number of persons frequenting the space. This fact is reflected by the GDPR in the Article 35(3)(c) which requires the carrying out of a data protection impact assessment (DPIA) in case of a systematic monitoring of a publicly accessible area on a large scale.

This deliverable is a result of the DPIA conducted by PKP, to ensure that data collection and use for WP6 work at Warsaw West station is not in breach of the GDPR regulation.

2. Abbreviations and Acronyms

Abbreviation / Acronyms	***Description***
CA	Consortium Agreement
CBDK	PKP's Railway Stations Security Center located on Elektronowa Street, Warsaw (Centrum Bezpieczeństwa Dworców Kolejowych)
CCTV	Close-Circuit Television
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EU	European Union
GDPR	General Regulation on Data Protection - Regulation 2016/679/EU 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, and repealing Directive 95/46/EC (General Data Protection Regulation).
NVR	Network Video Recorder
PKP	Polish State Railways located at Aleje Jerozolimskie 142A, Warsaw (02-305), Poland (Polskie Koleje Państwowe Spółka Akcyjna, PKP S.A.)
PRM	People with Reduced Mobility
SAR	Subject Access Request
SOK	Railroad Guards (Straż Ochrony Kolei)
STS	Hitachi Rail STS
VCA	Video Content Analysis
WP	Work Package

3. Background

The present document constitutes the Deliverable D6.4 “Data Protection Impact Assessment” in the framework of the TD3.11 “Future stations”.

The primary objective of TD3.11 is to improve customer experience at stations. The TD is organised around four areas:

- BB3.11_1 Crowd management in high capacity stations
- BB3.11_2 Improved station designs and components
- BB3.11_3 Improved accessibility to train-platform interface
- BB3.11_4 Safety management in public areas

Shift2Rail project that deals with building block BB3.11_1 Crowd management in high capacity stations is IN2STEMPO project work package 6. The overall objective of WP6 is to significantly improve customer experience and security in large and high capacity stations (especially large interconnected stations and multimodal hubs) both during standard operations and in emergency cases, by using tools that enable crowds to be simultaneously modelled as a flow or a large group of persons with individual motivations.

This objective will be achieved with the development and use of passengers, users and crowd behaviour models within a realistic 3D simulation system that is relying on collected real time data for simulation alignment and validation and delivering short term prediction and staff training.

4. Objective/Aim

This document has been prepared to provide Data Protection Impact Assessment (DPIA) for systematic monitoring of a publicly accessible area on a large scale in Warsaw West station.

Methodology for creating this document is based on guidelines published by President of the Personal Data Protection Office in Poland:

1. „Guidelines of President of the Office for Personal Data Protection regarding the use of CCTV" published in June 2018 [5];
2. „How to use risk-based approach in GDPR?" published in May 2018 [6].

Statutory requirements in GDPR are that DPIA must:

1. describe the nature, scope, context and purposes of the processing;
2. assess necessity, proportionality and compliance measures;
3. identify and assess risks to individuals;
4. identify any additional measures to mitigate those risks.

Statutory requirements in articles 37-39 of the GDPR are that if you are a public authority, or if you carry out certain types of processing activities, you must designate a Data Protection Officer (DPO) and always seek their advice when carrying out a DPIA.

5. Operational context

5.1 Introduction

WP6 aims at realising a real experimentation in a large station - Warsaw West station in Poland. It is the station with the highest number of train stops, and also one of the most crowded stations in Poland. PKP does not use any simulation tools and it is therefore an ideal opportunity to develop and enhance a suite of tools that will help them to proactively manage their station in the near future. Furthermore, station operators have close links with safety and security department to handle Video Content Analysis (VCA). Finally, PKP oversee the development of behavioural models and know this station in detail. Therefore, the models developed in this WP should reflect accurately the station reality. Because of systematic monitoring of a publicly accessible Warsaw West station area on a large scale and collecting behaviour models of passengers, DPIA required by GDPR and developed in this WP for Warsaw West station should reflect other large stations reality.

5.2 Warsaw West station (Warszawa Zachodnia) presentation

The station with the highest number of train stops

Warsaw West station is characterised by the highest number of train stops per day in Poland - about 900 trains and a balanced share of traffic types according to its range [8]:

1. agglomeration traffic trains - 314 per day;
2. regional trains - 342 per day;
3. Interregio trains - 12 per day;
4. long-distance trains - 227 per day.

Station capacity

Warsaw West station is one of the top ten busiest passenger stations in Poland. According to statistical data collected by the Office of Rail Transport, the daily exchange of passengers (according to the sold tickets) at this station exceeds 41 thousand passengers [8].

According to the data of the Polish Railway Transportation Office, the annual railway passenger number is on a rising trend since 2010 [8]. However, the rate of growth is disrupted by ongoing railway line closure due to construction works. The Polish railway system is currently in the process of general modernisation (both railway lines and stations). The trains are diverted to alternative detour routes or replaced with temporal bus transportation, which, in effect, makes the overall transport time longer and lowers the attractiveness of railway transportation on selected routes. This indicates that the system is not yet at peak saturation, which may lead to a rapid increase in passenger flow after the core transport corridor investments are finished.

In this context, the passenger and asset modelling, crowd forecasting and analysis tools developed in the project may be used by station management teams to develop optimal solutions in situations such as:

1. Crowded corridors and platforms management;
2. Emergency situation management.

Optimal solution will be to upgrade CCTV system installed in Warsaw West station with new video analytics and behavioural model systems.

CCTV system installed in Warsaw West station has been in operation for at least 10 years and was subject to review and total system upgrade in 2015. The upgrade included a total refit of the security control room and the installation of video recorders alongside flat screen monitors in the control room in Railway Stations Security Center located in Warsaw.

All information risks have been minimised and no complaints have been recorded for the past 5 years in respect of the operation and configuration of the system. CCTV is monitored by PKP Staff. Company T4B sp. z o.o. (T4B) is responsible for performing the maintenance of CCTV cameras, other devices and systems installed at the Warsaw West station.

The need for a DPIA is identified, as this is a project for large scale monitoring (hundreds of cameras for thousands of railway stations users and staff members and numerous visitors – compelling individuals to provide their data [Article 35(3)(c) GDPR]. After extending installed CCTV system will also be used for a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person [Article 35(3)(a) GDPR].

6. GDPR and its impact on WP6 works

6.1 GDPR: some definitions

The European General Regulation on Data Protection (GDPR) came into effect on 25 May 2018. Through the GDPR, the European Commission intends to strengthen and unify data security within the European Union. The Commission's primary objectives for the GDPR are to enable individuals to take back control of their personal data, and to harmonise the regulatory environment.

The regulation applies to all European companies and to companies outside the EU offering services to individuals in the EU. This regulation will have a major impact on any organisation, irrespective of where it is based or where it operates, that holds personal data on EU citizens. Organisations that do not comply will face severe penalties. Compliance requires both technical and organisational measures, and effective implementation must be documented at all times.

GDPR compliance calls for a careful combination of processes and technologies, backed by solid legal, IT and cybersecurity expertise.

Some definitions according to article 4 of GDPR are given here to highlight important factors regarding GDPR.

Personal data: means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Data minimization: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. PKP is the Data Controller because it is the owner of the CCTV systems in Warsaw West Station and is also responsible for creating DPIA;

Storage Limitation: kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the Data Subject [7].

6.2 Rules for personal data protection in IN2STEMPO Consortium Agreement (CA)

The IN2STEMPO CA [9] contains all the rules about the protection of the personal data used within the project IN2STEMPO. The CA was signed by the legal representatives of all the partners, therefore it represents a valid guarantee on data protection. The rules about the data protection are listed in the section 10 of CA "Non-disclosure of Confidential Information".

In summary, the partners of the IN2STEMPO Consortium, undertake to use the data made available by other partners only within the project itself, and undertake to not disclose them outside. In the particular case of WP6 and VCA, partner STS and subcontractor Aitek, guarantee that all the videos received from PKP, listed in section 7.1, will be used only for the scope of work of the project and will be deleted at the end of the project.

6.3 Impact on WP6

Personal data used in the project mostly rely on the exploitation of video analysis to estimate passenger density and flows inside stations. The process may be described in three steps:

- **Video Content Analysis (VCA)**
  The VCA technology is able to draw "virtual" sensors onto images for real-time detection of dangers and threats at stations and track-sides, such as yellow line trespassing, loitering, vandalism, track crossing, intrusion into forbidden areas, abandoned luggage and overcrowding detection. These highly-sophisticated software modules automatically generate alarm signals that are promptly forwarded to the supervisory system for immediate action (e.g. the issuing of customer warnings and announcements).
  Once VCA has been processed, only statistical and aggregated information is available and no more information regarding any data subject is available.
- **Crowd simulation**
  In this second step, we are in a virtual world representing the station environment, in which virtual actors move inside the station. Thanks to advanced behavioural models, the simulation tool developed in the project provides a very sophisticated set of capabilities in human simulation. Indeed, each virtual actor is a truly situated agent meaning it is able:
  - to **perceive** its own immediate surrounding environment through different sensors with their precisions and perceptual aliasing: virtual eyes with occultation, virtual ears with hearing illusions and virtual nose;
  - to **take its own decisions** according to its perceptions and its own internal variables, character traits and motivations;
  - to **act** in its environment in order to achieve its decisions and satisfy its own needs. In this virtual environment, no data come from the real world and so no data regarding any data subject is present.
- **Simulation calibration with VCA results**
  With calibration, the goal is to obtain a simulation that is the closest to the reality and to "bridge the gap between simulation and reality". Statistics and aggregates produced by VCA will be used to populate the simulation with the same number of people, in the same location in the space. Thanks to calibration, better crowd management scenarios will be created.

A more detailed presentation may be found in the IN2STEMPO deliverable *D6.1 Reference use cases, scenarios & KPI for standard & emergency operations* [8].

To sum-up, the only data subjects that will be used will come from video data in the very beginning of the global process developed in the project. For this step of the process and to be compliant with GDPR requirements, a DPIA – Data Protection Impact Assessment – has been conducted by PKP to define rules to guarantee that privacy of travellers will be respected, and data collated will be handled in accordance with GDPR requirements and regulations.

The next section describes the DPIA with the rules defined in PKP to respect GDPR regarding the exploitation of these video data that will be collected inside PKP network and that will not be shared with entities other than IN2STEMPO partners.

7. Data Protection Impact Assessment

7.1 Areas under surveillance of CCTV system

PKP's Warsaw West station CCTV system has over 135 cameras. All cameras are located inside Warsaw West station's secure perimeter. The field of coverage of PKP's CCTV system extends to the access and exit points to and from the PKP secure premises. The cameras monitor locations where one can enter or exit from the premises, for example, near the exits from the stairways, as well as near emergency exits of the train station. In addition, the system, to a certain extent, monitors sensitive areas where extra physical security is required, such as:

1. the IT technical rooms where end-user network connections to the PKP corporate network or to the PKP CBDK secure network are physically distributed;
2. security guards' room where live CCTV footage is available;
3. few railway ticket offices.

For collecting data and creating behaviour models of passengers in IN2STEMPO project 34 cameras will be used. Most cameras in Warsaw West station have native resolution of 1080p (1920 x 1080). For collecting data will be used lower-quality/resolution videos (640x480, 768x432, 900x600) in order to facilitate the provision of data to the IN2STEMPO project partners. Tools used in project can work with this lower quality data and deliver the same results. Thanks to usage of low-resolution video, passengers faces cannot be recognized.

Except for ticket offices, none of the cameras monitor areas where staff would be continuously present and there are no instances where a staff member working in a certain area would be constantly in the field of vision of a camera. There are also no cameras in individual offices, near or in restrooms, or in other areas where staff members and visitors would expect a high degree of privacy. The list of the cameras, their location and resolution used in project:

#	Camera	Camera location	Resolution
1	02.KZ-P2-028 (29MP) (02/LPD-02/01)	platform 2	900 x 600
2	02.KZ-P2-038 (29MP) (02/LPD-03/08)	platform 2	640 x 480
3	02.KZ-P2-032 (02/LPD-03/02)	platform 2	640 x 480
4	02.KZ-P2-033 (02/LPD-03/03)	platform 2	640 x 480
5	02.KZ-P2-034 (02/LPD-03/04)	platform 2	640 x 480
6	02.KZ-P2-035 (02/LPD-03/05)	platform 2	640 x 480
7	02.KZ-P2-036 (02/LPD-03/06)	platform 2	640 x 480
8	02.KZ-P2-038 (29MP) (02/LPD-03/08)	platform 2	900 x 600
9	02.KZ-P3-039 (29MP) (02/LPD-04/01)	platform 3	900 x 600
10	02.KZ-P3-040 (02/LPD-04/02)	platform 3	640 x 480
11	02.KZ-P3-042 (02/LPD-05/02)	platform 3	640 x 480
12	02.KZ-P3-043 (02/LPD-05/03)	platform 3	640 x 480
13	02.KZ-P3-044 (02/LPD-05/04)	platform 3	640 x 480
14	02.KZ-P3-045 (02/LPD-05/05)	platform 3	640 x 480
15	02.KZ-P3-046 (02/LPD-05/06)	platform 3	640 x 480
16	02.KZ-P3-048 (29MP) (02/LPD-05/08)	platform 3	640 x 480
17	02.KZ-P6-073 (29MP) (02/LPD-11/01)	platform 6	900 x 600
18	02.KZ-P6-074 (02/LPD-11/02)	platform 6	640 x 480

19	02.KZ-P6-075 (02/LPD-11/03)	platform 6	640 x 480
20	02.KZ-P6-077 (02/LPD-11/05)	platform 6	640 x 480
21	02.KZ-P6-078 (02/LPD-11/06)	platform 6	640 x 480
22	02.KZ-P6-081 (02/LPD-12/03)	platform 6	640 x 480
23	02.KZ-P6-083 (02/LPD-12/05)	platform 6	640 x 480
24	02.KZ-P6-084 (02/LPD-12/06)	platform 6	640 x 480
25	02.KZ-P6-085 (02/LPD-12/07)	platform 6	640 x 480
26	02.KZ-P6-087 (02/LPD-13/01)	platform 6	640 x 480
27	02.KZ-P6-090 (29MP) (02/LPD-13/04)	platform 6	900 x 600
28	02.KZ-DW-120 (02/LPD-18/07)	Tunnel	768 x 432
29	02.KZ-DW-121 (02/LPD-18/08)	Tunnel	768 x 432
30	02.KZ-DW-080 (02/LPD-12/02)	Tunnel	768 x 432
31	02.KZ-DW-079 (02/LPD-12/01)	Tunnel	768 x 432
32	02.KZ-DW-020 (02/LPD-1/05)	Tunnel	768 x 432
33	02.KZ-DW-019 (02/LPD-1/04)	Tunnel	768 x 432
34	02.KZ-DW-016 (02/LPD-1/01)	Tunnel	768 x 432

According to IN2STEMPO deliverable D6.1 Reference use cases, scenarios & KPI for standard & emergency operations [8] two main use cases are:

1. Offline machine learning trainings to create a working demonstrator;
2. Online test in which the output of the live video system is plugged to the input of the simulation, thanks to Video Analytic.

Detailed information of data flows for both uses cases may be found in the diagrams 16-18 in deliverable D6.1.

Camera records to be used during offline trainings will be collected and delivered to the IN2STEMPO project partners in 2 stages. First short sample camera recordings (about 10-15 seconds each) from all cameras will be delivered to project partners to check which cameras are useful for the project i.e. are suitable for machine learning. Sample CCTV outputs (images and video files) will be supplied to project partners using Acronis Access Advanced internal cloud system. Acronis Access Advanced is a secure access, sync, and share solution that provides enterprise IT with complete control over business content to ensure security, maintain compliance. Acronis Access Advanced lets PKP employees use any device - desktop, laptop, tablet or smartphone – to securely access and share content with authorized internal and external constituents, including employees, customers, partners, and vendors.

After selecting the cameras for the test, the material of about 90 minutes will be downloaded from each camera from few consecutive days: Friday, Saturday, Sunday, Monday, and for the following times: 6am-7.30am; 11am-12.30am; 4.30pm-5.30pm and some period in the evening.

It would be very difficult to transfer over 500 large video files via FTP or Acronis Access Advanced to partners, so a hard drive will be used. The hard drive will be transferred directly between the PKP employee and the IN2STEMPO partner's employee, so the risk of losing data will be minimal and there will be no need for data encryption. At the end of the test, the hard drive will be returned to PKP in the same way.

In order to conduct an online test, the PKP CCTV network will have to be connected to the network of the project partner. The network in which the CCTV monitoring system of the Warsaw West Station operates is a separate network of PKP S.A.

In order to preserve the confidentiality of the transmitted information, access to these networks during online tests can be provided via an encrypted site-to-site VPN (Virtual Private Network) connection tunnel.

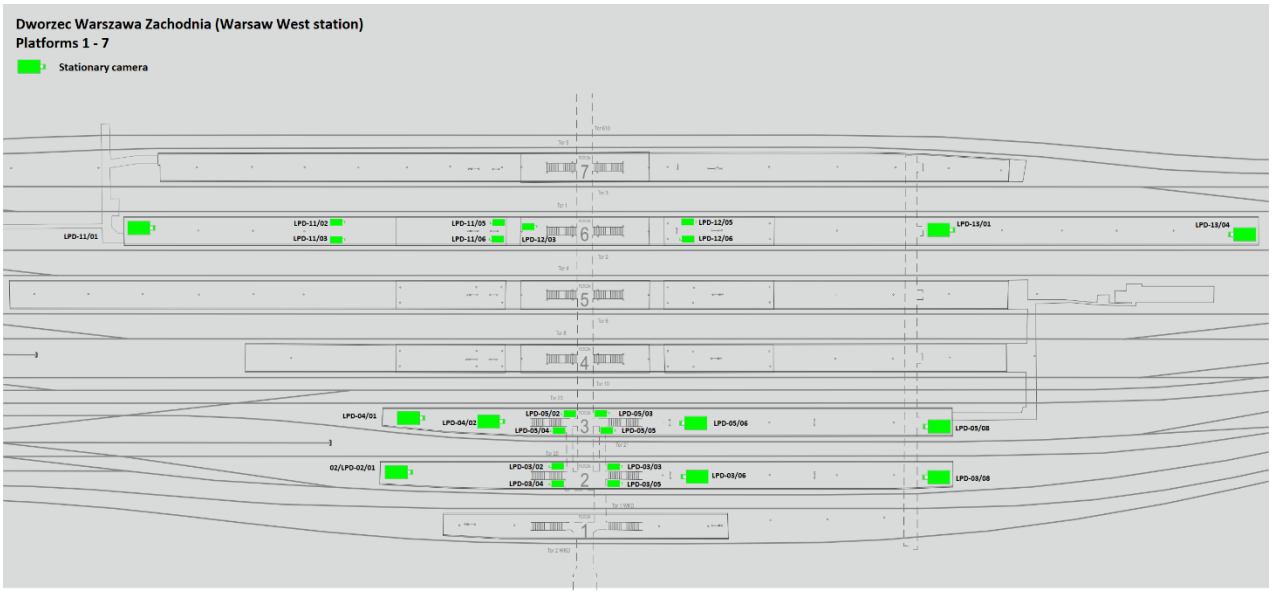

Figure 1. Warsaw West Station cameras on platforms 2, 3 and 6

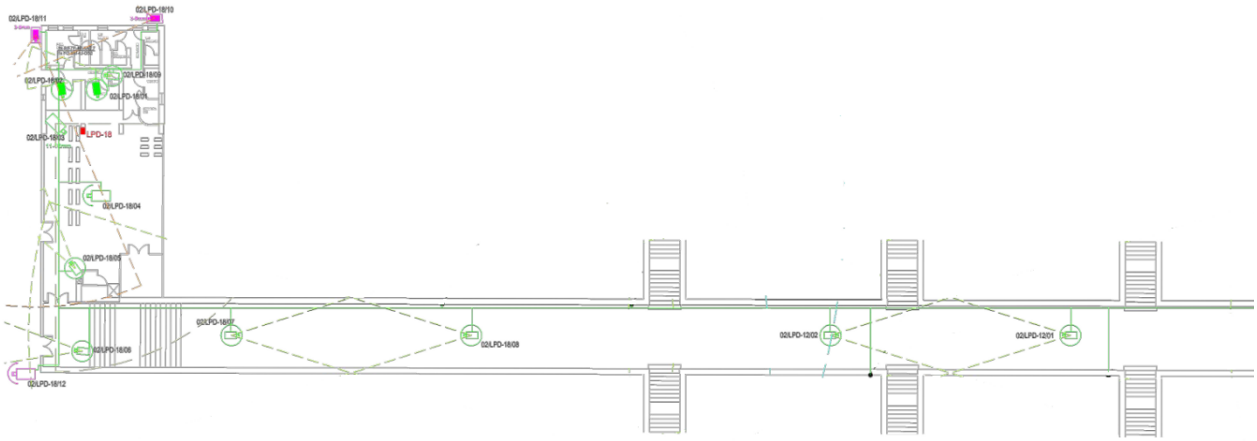

Figure 2 Warsaw West Station cameras in the tunnel (part 1 of 2)

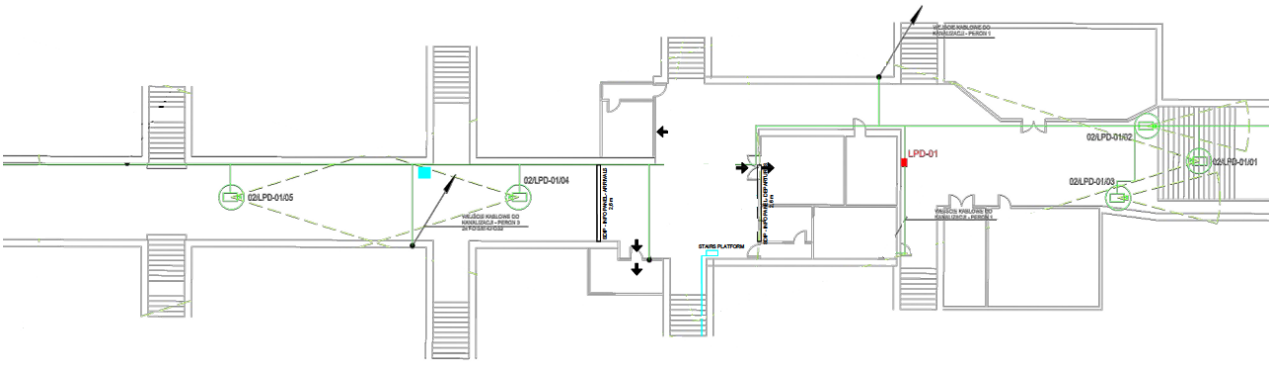

Figure 3 Warsaw West Station cameras in the tunnel (part 2 of 2)

7.2 Purpose for using the surveillance CCTV system

The use of the CCTV system shall be for the purpose of:

1. To protect Staff, railway travellers and other railway station users;
2. To increase personal safety and reduce the fear of crime;
3. To reduce incidents of violence and aggression to staff members and railway travellers;
4. To support the Police, SOK and security guards in reducing and detecting crime (including countering terrorism);
5. To assist in identifying, apprehending and prosecuting offenders;
6. To provide a deterrent effect and reduce criminal activity;
7. To deter or reduce the incidence of vandalism, graffiti, and other environmental crime;
8. To discourage anti-social behaviour including alcohol and drug-related elements;
9. To provide passengers, users and crowd behaviour models;
10. To help in emergency situation management;
11. To assist in all aspects of railway station management.

The CCTV cameras are all used as a proportionate response for crime, disorder and wider community safety purposes.

The CCTV system is not used for any other purpose. Neither is the system used as an investigative tool (other than investigating physical security incidents such as thefts or unauthorised access). It is only in exceptional circumstances that the images may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation.

PKP's CCTV system in Warsaw West station has no webcams or Body Worn Cameras.

7.3 The legal basis of the video-surveillance CCTV system

The use of our video-surveillance system is necessary for the management and functioning of PKP's Warsaw West station. Therefore, we PKP has a lawful ground for the video-surveillance.

The legal basis for processing personal data captured by the CCTV is under:

1. Article 6(1)(c) GDPR: "processing is necessary for compliance with a legal obligation to which the controller is subject";
2. Article 6(1)(f) GDPR: „processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".

Legal obligations (Article 6(1)(c) GDPR) to which the PKP is subject are:

1. Article 58 (3) of Railway Transport Act of 28 March 2003 (Journal of Laws of 2019, Item 710) which states that "Managers and rail operators shall ensure law and order on railway area as well as on trains and other rail vehicles.";
2. Article 5a (1) of Act of 16 December 2016 on the principles of state property management (Journal of Laws of 2016, Item 2259 as amended) which states that "The management of state property also includes ensuring the security of property, which allows possible application of security measures, including physical security measures and technical measures enabling image registration (monitoring) on the property and in buildings constituting the state property, as well as on the area

around such properties and facilities if it is necessary to ensure the security of managed state property.";

3. Article 22(2) of Act of 26 June 1974 - Labour Code (Journal of Laws of 2019, Item 1040 consolidated text) which states that "If it is necessary to ensure the safety of employees or the protection of property or the control of production or to keep in confidentiality information, the disclosure of which may expose the employer to harm, the employer may introduce special supervision over the workplace or the area around the workplace in the form of technical measures enabling image registration (monitoring)".

Legal obligations (Article 6(1)(f) GDPR – PKP's legitimate interests)

Video surveillance is lawful if it is necessary in order to meet the purpose of a legitimate interest pursued by a controller (PKP) or a third party, unless such interests are overridden by the data subject's interests or fundamental rights and freedoms (Article 6 (1) (f)). Legitimate interests pursued by a controller or a third party can be legal, economic or non-material interests. Given a real and hazardous situation, the purpose to protect property against burglary, theft or vandalism constitutes a legitimate interest for video surveillance.

Creating DPIA in Warsaw West station is also required because of document "List of Types of Personal Data Processing Operations Requiring Data Protection Impact Assessment published on 17.06.2019 by the President of the Personal Data Protection Office in Poland. In section 3 of this document it is written that DPIA is required when there is: *systematic monitoring on large places publicly exploiting recognition elements features or properties objects that are made in monitored space*.

7.4 Processing of special categories of data in CCTV system

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, are prohibited unless an exception can be found in article 9 of GDPR.

As noted in deliverable D6.1 scenarios implying PRM people have been largely studied in FAIR Stations project and will not be studied in In2Stempo, except maybe for the impact on an evacuation scenario. Additionally, low quality of recordings from cameras will make it impossible to recognize faces of PRM, e.g.: people in wheelchairs. Therefore CCTV system used for IN2STEMPO project will not collect special categories of data mentioned in article 9 of GDPR and will not transfer it to project partners. The use of our video-surveillance system is necessary for the management and functioning of PKP's Warsaw West station. Therefore, PKP has a lawful ground for the video-surveillance.

7.5 Who has access to the information and to whom is it disclosed

The PKP's staff are the only people to have direct access to the system for monitoring and reviewing any footage. PKP's Security Policy for video-surveillance specifies and documents who has access to the video surveillance footage and/or the technical architecture of the video-surveillance system, for what purpose and what those access rights consist of. In particular, the document specifies who has the right to view the footage real-time, view the recorded footage, or download, delete, or alter any footage.

All personnel with access rights, were given their data protection training. Training is provided for every new member of the staff and periodic workshops on data protection compliance issues are normally carried out at least once every two years for all staff with access rights.

All personnel with access rights are statutory staff bound by the staff regulation and cannot disclose any information.

All transfers and disclosures outside the security group are documented and subject to a rigorous assessment of the necessity of such transfer and the compatibility of the purposes of the transfer with the initial security and access control purpose of the processing.

PKP will only share data with:

1. The Police – where the images recorded would assist in a specific criminal inquiry;
2. Prosecution agencies – for example Public prosecutor's office;
3. Relevant legal representatives – such as lawyers and barristers where legal advice is sought;
4. Persons recorded and whose images are retained where disclosure is required by virtue of Data Protection Legislation.

7.6 Data protection features adopted to reduce privacy intrusion

Transmission types used for the CCTV at the Warsaw West station are Fibre optic and Hard wired. There are no wireless connections used in CCTV system.

CCTV images (digital recordings) go from a camera to a Network Video Recorder (NVR) unit – a data store. There will be NVR's on site, located in secure offices at Warsaw West station IT technical room. There are NVR's in PKP CBDK on Elektronowa Street in Warsaw site to allow better flow of network traffic around system. The CCTV system has been designed to allow redundancy so if one of NVRs failed the others would be able to take the loading on the system.

The PKP staff are the only people to have direct access to the system for monitoring and reviewing any footage.

Footage is automatically deleted after retention period of about 60 days except where data has been extracted for internal or external investigations. Under these certain circumstances only authorised persons from PKP's staff may override the retention period, e.g. retained for prosecution agency. All retained data will be stored securely and permanently deleted as required by PKP data retention schedule. Recorded data is kept secure on the PKP network in drives allocated in CBDK Elektronowa site. This is to ensure their evidential value and to protect the rights of the people whose images have been recorded.

Data being used for an investigation will be stored on storage device until the investigation is completed then they will be promptly deleted, unless data retention requirements state otherwise i.e. for a serious incident which may require up to few years retention.

The CCTV system captures visual images only with no audio recording to ensure the minimum intrusion of privacy.

7.7 How members of the public can verify, modify or delete their information?

Under the GDPR, individuals have the right to obtain confirmation that their personal information is being collected/processed/stored. PKP process for assuring this is as follows:

1. Individuals have the right to submit a SAR (Subject Access Request) to gain access to their personal data in order to verify the lawfulness of the processing.
2. PKP will verify the identity of the person making the request before any information is supplied.
3. A copy of the information will be supplied to the individual free of charge; however, PKP may impose a 'reasonable fee' to comply with requests for further copies of the same information.

4. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format. CCTV outputs (images and video files) will be supplied using Acronis Access Advanced internal cloud system.
5. Requests by persons for viewing or copying disks, or obtaining digital recordings, will be assessed by the PKP Security Department (Biuro Bezpieczeństwa), who will consult the DPO (Data Protection Officer), on a case-by-case basis with close regard to data protection legislation.
6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
7. All fees will be based on the administrative cost of providing the information.
8. All requests will be responded to without delay and at the latest, within one month of receipt.
9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
10. Where a request is manifestly unfounded or excessive, PKP holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority (Urząd Ochrony Danych Osobowych - UODO) and to a judicial remedy, within one month of the refusal.
11. In the event that a large quantity of information is being processed about an individual, PKP will ask the individual to specify the information the request is in relation to.
12. It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.
13. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law.
14. Requests for access or disclosure will be recorded and the person in charge (Head) of the Security Department (Biuro Bezpieczeństwa) will make the final decision as to whether recorded images may be released to persons other than the police.

7.8 Providing information about video-surveillance to the public

PKP provides information to the public about the video-surveillance in an effective and comprehensive manner. PKP follows a multi-layer approach, which consists of a combination of the following two methods:

1. on-the-spot notices to alert the public to the fact that monitoring takes place (first layer);
2. posting of this Video-Surveillance Policy on PKP's internet sites for those wishing to know more about the video-surveillance practices of PKP (second layer).

The first layer information (warning sign) should generally convey the most important information, e.g. the details of the purposes of processing, the identity of controller (PKP) and the existence of the rights of the data subject, together with information on the greatest impacts of the processing. This can include for example the legitimate interests pursued by the controller (PKP) and contact details of the PKP's data protection officer. It also has to refer to the more detailed second layer of information and where and how to find it. In addition, the sign should also contain any information that could surprise the data subject. In case of IN2STEMPO project that will be, for example, transmissions to third parties, the storage period and also information about Video Analytics used to help assess the situation in real-time and using behaviour models on station visitors. Second layer should convey other information required by article 13 of GDPR.

Figure 4 First layer GDPR information about video surveillance used by PKP in Warsaw West station

7.9 Risk identification and assessment

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	Likelihood of Harm	Severity of Harm	Overall risk
Hacking	Unlikely	Significant / Severe	Low
Unauthorised disclosure	Possible/Probable	Significant /Severe	Medium
Unjustified invasion of privacy / right to privacy	Possible/Probable	Significant	Medium
Loss of recorded data	Unlikely	Significant / Severe	Low
Covert Monitoring	Unlikely	Severe	Low
Unauthorised usage of data collected by behaviour models and crowd simulation systems	Unlikely	Low	Low

Because of technical and organisation measures used by PKP to protect data collected by CCTV on Warsaw West station overall risk in most cases is defined as Low. In two cases it's required to identify additional measures PKP could take to reduce or eliminate risks identified as medium.

7.10 Measures to Reduce Risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure Approved**
Hacking	All cameras to be hard cabled and system will require password to be entered to be accessible	Reduced	Low	YES
Unauthorised disclosure	Internal guidance will be provided in the form of a CCTV policy (Regulamin systemów monitoringu wizyjnego w PKP S.A.). Privacy notices and signage will allow individuals to be informed of CCTV usage. Privacy notices will be available in form of a sign on railway station and on the PKP's site e.g. www.pkp.pl/RODO/IN2STEMPO. Limited access to recordings. Retention is 60 days in the usual course of events. Only the selected Staff members will have access to the system and all viewings will be logged. PKP will only share data with selected authorities: The Police, public prosecutor office etc.	Reduced	Low	YES
Unjustified invasion of privacy	Cameras will not be installed in or nearby toilets and other such sensitive areas. No audio recording. Cameras installed in few railway ticket offices that monitor employees are justified by possibillity of theft. Where video is being captured, faces can be blurred out that are not part of any incident. Staff have been informed via the formal consultation process.	Reduced	Low	YES
Loss of recorded data	No data will leave the PKP site without protection. Data will sit on password protected NVR's on as secondary network not on the main PKP network. Camera records will be sent to partners using encrypted cloud service or via site-to-site VPN tunnel. Camera records downloaded to the hard drive will be transferred directly between employees.	Eliminated	Low	YES
Undisclosed monitoring	There will be no undisclosed or covert monitoring taking place on the site. Privacy notices and signage will be public facing to promote the right to be informed.	Eliminated	Low	YES

Unauthorised usage of data collected by behaviour models and crowd simulation systems	Installed by IN2STEMPO Consortium video analytics, behaviour models and crowd simulation systems will not use potentially harmful technologies like for example face recognition. There will be little (if any) danger for PKP staff and railway station visitors if collected by CCTV and IN2STEMPO systems data would be used unauthorised.	Eliminated	Low	YES

7.11 Sign off and record outcomes

The volume and situation of the CCTV cameras creates risks. There are several factors to consider:

Hacking - the risk of hacking into the CCTV system has been reduced by the design of the technology. PKP will not retain data for a long period of time. The WWK CCTV system has password protected access and the cameras are hard-cabled. The impact of hacking is unknown, although it will depend on a case by case basis. PKP has adequately considered and reduced this risk.

Unauthorised disclosure - PKP have stringent measures in place. All CCTV cameras and CCTV management systems have password protected access. PKP created a CCTV policy for PKP staff. Small retention periods (60 days), encrypting downloaded personal data, security measures around data stores, limiting the geographical scope of the recordings to the Warsaw West station, not audio recording and limiting access to the office where the monitors are to be displayed, including that of remote access.

The CCTV Policy will aid the appropriate safeguards around monitoring, accessing, disclosing and storing CCTV. PKP has confirmed that security measures will be in place in regard to downloaded personal data for investigatory purposes, such as the prevention and detection of crime. PKP's staff with access to CCTV monitoring should ensure that they have sight of the CCTV policy which mentions remote viewing specifically, alongside GDPR training. Those using the CCTV infrastructure should have relevant training where appropriate and also have sight of the CCTV policy before using the system. This reduces the 'high risk' that recording on a large scale and of 'vulnerable subjects' poses.

PKP should consider what will occur in the event of important members of PKP staff (for example Head of the PKP Security Department) being absent/ill or unable to utilise access to remote working. If the responsibility is passed to someone else, it should be documented how that employee has been trained/informed in appropriately using the system with GDPR compliance.

Adequate and relevant training regarding GDPR and CCTV must take place when a new employee with access to CCTV begins. These employees should have regard to the PKP CCTV Policy guidance.

Maintenance of the cameras made by „T4B Sp. z o.o." company does not include access to personal data, therefore mitigating the risks of a breach via a processor and eliminating the need for an Article 28 (GDPR) compliant contract.

Loss of recorded data - PKP must have regard to the possibility of data loss. In general, no CCTV recordings will leave PKP site without some protection. Downloaded CCTV data onto e.g. a portable device can be encrypted (Symantec Endpoint Encryption) and this must be stored securely, preferable in a lockable

location. Data loss in terms of a failure of an NVR unit has been mitigated by ensuring there are multiple units active and these have the ability to take on the loading system, thus reducing the risk of a loss of data.

Undisclosed monitoring - signage must be adequate and well-informed. All individuals subject to CCTV monitoring must be notified. This should be done prior to processing their data (i.e. placing signage on each of West Station entrances) and on the PKP webpage with privacy notices. The record retention schedule must be updated to reflect any changes in the new system. There will be no covert monitoring. Staff and visitors each have their own privacy notice. Notices for visitors must be public facing and publication on the PKP's website is strongly advised.

Necessity and proportionality - the high volume of cameras and, ultimately, personal data that will be processed poses a risk to the rights and freedoms of individuals. PKP must document their detailed reasoning for the quantity of security cameras used as the volume of installed cameras seems 'excessive' and 'disproportionate'. They must be able to document the reasons for its necessity, balancing between individuals' rights and the PKP's documented purposes. Previously, the CCTV system included less cameras and this was not enough to achieve the purpose of protecting the PKP sight, its assets and the health and safety of those on the PKP site. The CCTV system also did not include behaviour models and crowd simulation technologies.

Thanks to all abovementioned options all residual risk was reduced to low values. Because of probability of new risks, DPIA should be regularly reviewed (at least every 2 years).

7.12 Monitoring and review

This policy will be monitored and reviewed every two years by the DPO, and PKP's Head of the Security Department (Biuro Bezpieczeństwa) and the Management Board of PKP. The Management Board of PKP will be responsible for monitoring any changes to legislation that may affect this policy and make the appropriate changes accordingly. PKP's Security Department will communicate changes to this policy to all members of PKP staff. The scheduled review date for this policy is December 2021.

8. Conclusion

Work described in this deliverable will be continued and enriched during the project with exchanges between the different data project officers of the different entities implied in the works.

The conclusion reached at this stage and highlighted in this report is that data protection compliance is a responsibility of data controller who uses CCTV systems with video analytics for systematic monitoring of a publicly accessible area on a large scale. Conduction of the DPIA confirmed that PKP is compliant with GDPR and local GDPR supervisory authority's CCTV guidelines. Consequently, in case of any incident (for example, data breach) during IN2STEMPO project, it will be less probable that data controller (PKP) will be penalised with an administrative fine from the supervisory authority. The confirmation of compliance with GDPR and national regulations around data collection and handling, means that work defined in WP6 can be conducted without the risk of legislation breach.

DPIAs are important tools for managing the privacy and data protection risks for 'riskier' processing operations. Going through the assessment process provides evidence that the business owner thought about these risks and chose justifiable means for managing them. When the GDPR supervisory authority of each European Union Member State where the data controller has its main establishment checks how it complies with its data protection obligations, business owner can be sure that auditors will have a look at DPIAs. Failure to do DPIAs when required may result in an administrative fine from the supervisory authority.

There is no one unified methodology to create DPIAs (especially for CCTV) valid for all European Union states. In each EU state local supervisory authority usually publish their own guidelines for creating DPIAs. Therefore, going forward, to minimise risk of administrative fines, each business owner should always check their local GDPR supervisory authority's web page for newest guidelines.

9. References

[1] Official Journal of the European Union – "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, and repealing Directive 95/46/EC (General Data Protection Regulation)" – 2017, Official Journal of the European Union nr L119/1 [https://eurlex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=PL];

[2] The European Data Protection Board – "Guidelines 3/2019 on processing of personal data through video devices" – 2019, Version for public consultation adopted on 10 July 2019;

[3] The International Organization for Standardization – "ISO/IEC 29134:2017 Information technology – Security techniques – Guidelines for privacy impact assessment" – 2017, Vol. 1

[4] President of the Personal Data Protection Office in Poland – "List of Types of Personal Data Processing Operations Requiring Data Protection Impact Assessment - Annex to the notification of the President of the Personal Data Protection Office of 17 June 2019" – 17.06.2019, Vol. 1;

[5] President of the Personal Data Protection Office in Poland – "Guidelines of President of the Office for Personal Data Protection regarding the use of CCTV" – 06.2018, Vol. 1;

[6] President of the Personal Data Protection Office in Poland – "How to use risk-based approach in GDPR?" – 05.2018, Vol. 1;

[7] https://gdpr-info.eu/art-4-gdpr/;

[8] IN2STEMPO D6.1 *Reference use cases, scenarios & KPI for standard & emergency operations*;

[9] IN2STEMPO Consortium Agreement, Version 1, July 2017.