UDC 342.7
DOI https://doi.org/10.32849/2663-5313/2023.4.10

Daria Bulgakova,
Advocate, Ukrainian National Bar Association Member, Ph.D. in International Law, Visiting Scholar, Researcher, Law Department, Uppsala University, Munken 2, Västra Ågatan 26, Uppsala, Sweden, 75309, daria.bulgakova@jur.uu.se
ORCID: *orcid.org/0000-0002-8640-3622*

Victoriia Stupnik,
Pedagogue-Methodist of the Highest Category, Supervisor of Scientific Manuscripts on History and Law, Lecturer, Gymnasium No. 91 of Kryvyi Rih City Council of Dnipropetrovsk Oblast, 48 General Radievsky St, Kryvyi Rih, Ukraine, 50008, vikysjakrul@gmail.com
ORCID: *orcid.org/0009-0006-8953-2477*

Bulgakova, Daria, Stupnik, Victoriia (2023). The facial processing of the ticket holderat the ski resort in Austria. *Entrepreneurship, Economy and Law, 4*, 63–68, doi https://doi.org/10.32849/2663-5313/2023.4.10

THE FACIAL PROCESSING OF THE TICKET HOLDERAT THE SKI RESORT IN AUSTRIA

Abstract. ***Purpose.*** The presented article explores the case analysis of the 2020 Austrian Data Protection Authority investigation regarding the use of facial recognition technology at the ski resort for entrance management. ***Research methods.*** The article applies the case study approach and assesses of how the resort service is aligned with the special data technology in accordance with the General Data Protection Regulation (GDPR) of articles 6 (1, f) and 9 (1). ***Results.*** By relying on the research results and discussion, the authors have been confirmed that data protection standards of the European Union must be met in the scenario of any limitation of the fundamental right to privacy. The law-abiding practice for the lift-ticket holders' entrance control shall be legally demanded, admire the core of the rights, conform to the recognized interest objectives, and be necessary and proportional. ***Conclusions.*** The examination highlights the value of privacy in the design of face processing systems, attributing this matter to the contextual and culturally contingent nature of privacy, as well as the challenge of habilitating privacy goals into practical visions. Accordingly, the use of facial recognition technology at the Ski Resort is deemed justifiable, as it aligns with service level management and concedes with the lawfulness bars outlined in GDPR Article 6 (1, f) without exceeding the bounds of Article 9 (1). Consequently, the authors conclude that facial recognition technology can be used to verify the validity of lift ticket holders as long as this practice does not employ special techniques that direct a unique identification.

Key words: Austrian Data Protection Authority, customer identification, photo data collection, consent, right to privacy, personal data protection.

1. Introduction to facial recognition

In the Member States countries of the European Union facial data processing must follow General Data Protection Regulation (GDPR) criteria and standards to protect personal data. Facial identification compares a person's facial image with templates of other people stored in a database, on the other hand, authentication and verification similarity analogizes two templates of the same person. Thus, authentication and verification are different from identification.

Again, *facial identification* or designation is a technique of reaching an individual's facial shot with templates of different people reserved in a database to confine the identicalness of the individual in that shot. This method is exploited to pinpoint individuals in varied contexts, largely for security and law enforcement conditions. Facial algorithms could tag diverse segments of the face, likewise, the length between the eyes, the figure of the nose, and the silhouettes of the face, to liken the facial shot with the other database templates. At the same time, an algorithm is a method, an ordered set of operations, or a recipe and not a means to store biometric data (EDPS and Agensia Espanola Proteccion Datos, 2020, p. 1). It means facial identification could be done without the process of working with a biometric data of a person concerned as long as this function does not go beyond identification that led to unique (biometric) data workflow with further labelling of a person's distinctive traits. *Facial authentication* is a function of substantiating that a person is who he contends to be

by approximating his facial template of the shot with an already comprehended template kept in a database to inspect if his face matches a pre-existing record. This function is usually employed in household technology for security and access control systems, for example, unlocking a smartphone via facial credit or accessing home facility via facial validation. At the same time, according to the GDPR Recital 18, this Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities. *Facial verification* is a function of analogizing two templates of the same person to decide if they are a match. It is used to affirm the already known identity for a broad system by capturing a 'live image'. For example, it is practiced logging into bank accounts or inscribing into social media profiles.

Consequently, while facial identification is demarcating the identity of a person by comparing their facial shot with templates of other people reserved in a database, facial authentication, and verification apply two templates of the exact individual to decide if they are identical.

2. A face-check system for costumers at the ski resort in Austria

According to the GDPR Article 51 (1) each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority'). Thus, the research refers to the case analysis of the Austrian Data Protection Authority (Datenschutzbehörde/ADPA) investigation that started on 07 January 2020, decided on 23 November 2020, and published on 11 April 2022 about the entrance management solution at the Ski Resort through the shot of costumers' facial data. The Ski Resort operator used a face-check system requiring customers to take their photos and further store for an automatic open-door system according to the tickets possession respectively. Therefore, the problem question is how the execution of service level agreement (SLA) aligns with the data technology to the needs of its customers according to the GDPR Articles 6 (1, f), 9 (1).

The research has shown, based on the GDPR Article 77(1) without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation. Notably, on 07 January 2020 the ADPA under the GDPR Article 57 (1) started an investigation based on Robert A***'s privacy complaint (complainant) against N*** Lift GmbH (respondent) represented by the lawyers Dr. Rudolph L*** & Dr. Sebastian L***. The respondent, Ski Resort, is the sole operator of the lift system on the Z***berg that checked the validity of the lift ticket for access management by taking a visitor's photo and a comparison measurement of this photo with a previously stored reference to the photo which runs while customer purchased a lift ticket. The consent to take photos linked to the use of the lift ticket. In the event of disagreement, the lift system cannot be used. The complainant indicates an opt-in procedure analogously linked to the e-mail addresses of the applicant respectively and breaks privacy. The complainant used this lift from 27 December 2019 to 29 December 2019 and sent various photos, screenshots, and e-mail correspondence as enclosures.

On 06 March 2020, the respondent confirms a reference photo of the lift ticket holder for access control management on the scene equipped with a camera when first stepping through the entry, specifically on the Turnstile at the valley station of the Z***bergbahn I and the valley station of the *** gondola. This access control has a permissible form because it is only practiced at the particular entry points of the Z***bergbahn I. Valley station. As evident respondent, there are two access areas: one northwest, and one east. The reference photo is only used when a person passes through the northwest access system, where, among other things, appropriate stickers and information signs additionally announce such measures. Besides, the company informed the public about that measure in the check area by notice and this warning was posted on the public service homepage. Also, it was pointed out that the capture, storage, and processing of photo data are exclusively for management-alike control purposes to avoid improper use of the ticket card. These data, as a rule, are based on the validity period of a ski pass and would expire at the end of each year when data is deleted.

It is believed that such a measure suits every ski guest to traverse free to one of the two areas. Besides, at the mountain station, ten other lifts

are available as an alternative, with neither one reference of control photo to be taken. Indeed, there is the possibility to purchase hourly tickets for which no reference photo is taken meaning that the lift system use is not critically tied to the respective data consent. Notably, a control photo taken at the entrance is deleted within 30 minutes after passing through the turnstile. Technically, the photo files are encrypted with further access through the log into the system with a password. Hence, the data control is not automated, and based solely on the personal information management system (PIMS).

3. The law-abiding practice for the lift-ticket holders' entrance control

The use of facial recognition technology for access management vision is becoming more prevalent, and it is essential to ensure that it is used lawfully. Observing the entry into force of the Lisbon Treaty, the Charter of Fundamental Rights of the European Union (CFREU) evolved the leading relation for evaluating compliance with fundamental rights. The Court of Justice of the European Union (CJEU) has affirmed that an investigation of the facts of a requirement of secondary EU law must be undertaken solely in light of the fundamental rights guaranteed by the Charter, likewise, in the case C-199/11, Otis and Others, paragraph 47, case C-398/13 P, Inuit Tapiriit Kanatami and Others v Commission, paragraph 46, and case C-601/15 PPU, J.N. v Staatssecretaris van Veiligheid en Justitie, paragraph 46. Furthermore, the CFREU Article 8 (2) as well as EU data protection law, provide for the right of access, correction, and deletion of one's own data that are stored (FRA, Opinions on Biometrics).

The case highlights the issues of data protection and privacy concerns when it comes to the use of facial recognition technology. There is a lack of awareness and understanding of how to exercise the right of access, correction, or deletion of inaccurate data that are stored (FRA, Opinions on Biometrics). The cumbersome nature of the processes, administrative hurdles, language barriers, and lack of specialized lawyers also explain why few persons try to exercise these rights (FRA, Opinions on Biometrics). It raises questions about the level of consent required for the use of the facial technology in question and the transparency of data collection and processing. Societies must, therefore, be able to control cheaters (free riders) and prevent excessive status-seeking (Burk, 2021).

To be lawful, any limitation on the exercise of the fundamental rights protected by the CFREU must comply with the following criteria, laid down in Article 52(1) (EDPS, 2017, p. 4):

– it must be provided for by law,
– it must respect the essence of the rights,
– it must genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others,
– it must be necessary, and
– it must be proportional.

The complainant's objection is justified because he was not given a free choice to use the territorial addenda of the respondent without consenting to data processing. These findings have demonstrated the assertion of the complainant to obtain his consent at the first place otherwise ticket use would be limited. Hence, the consent to data processing did not occur voluntarily because the use of the facilities conjoined to consent. On the other side, according to the GDPR Recital 40, in order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. *Twofold consent to the processing of non-contractual personal data with the conclusion of a contract is generally not voluntary unless there are special circumstances that articulate its voluntariness. Since the respondent in this case expressly does not rely on the consent of those affected for the data processing in question, these considerations can be disregarded.* Thus, the service with data collection for further photo comparison to a reference photo is to verify the validity of the lift ticket possession and to prevent improper use of the lift ticket is the legitimate interests *provided for by* GDPR Article 6 (1, f) which is enough to evaluate the processing to be lawful because para 1 of the mentioned article refer to the lawfulness assessment when 'only if and to the extent that at least one of the following applies' such as stipulation 'f' used in the case in question. Besides, consent should not, as a rule, be the legal ground used for facial recognition performed by public authorities given the imbalance of powers between the data subjects and these authorities (CE, 2021, p. 9). For the same reason, consent should not, as a rule, be the legal ground used for facial recognition performed by private entities authorized to carry out tasks similar to those of public authorities (CE, 2021, p. 9). At the same time, it must respect the essence of the rights as well as the legitimate interest shall not be 'overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data' as per GDPR Article 6 (1, f).

In the authors' view, the respondent shows respect and not overridden facial technology practice, since as stated, the data concerns amount of photo shot only, it is obtainable through a password, deleted to the extent of the processing, provide customers with PIMS and therefore, meet the technical and organizational requirements of the GDPR Article 25 para 2 about obligation 'to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility'.

Furthermore, in the view of the authors, the photo processing measure through access control with image comparison *protects those who are authorized*. It means that the respondent processing is based on their principal legitimate interests under GDPR Art. 6 (1, f) and ought to be estimated. This point of view took into account the legitimate interests of the complainant and whether they align with the respondent's and third parties' interests respectively to the use of personal (image) data of ski lift card users. Significantly, the complainant has a legitimate interest in keeping his data, specifically his photograph. Hence, private entities shall not deploy facial recognition technologies in uncontrolled environments such as shopping centers, especially to identify persons of interest, for marketing purposes, or private security purposes (CE, 2021, p. 12). On the other hand, the respondent has a legitimate interest in ensuring that their contractual partners behave according to the SLA (Hosseinifard et al., 2022) as well as the tariff conditions are overseen by service level management (Looy, 2013) to deter the unauthorized transfer of the ski pass. This is particularly consequential since a day or multi-day credentials are correspondingly more cost-effective than hourly tickets. *Hence, the system implemented by the respondent is reasonable because its guarantee the admission management and execute contractual intention*.

'Necessity' is also a data quality principle and a recurrent condition in almost all the requirements on the lawfulness of the processing of personal data stemming from EU data protection secondary law (EDPS, 2017, p. 5). For example, Article 6 (1, c) and 7 of Directive 95/46, Article 4 (1, c) and 5 of Regulation 45/2001, Article 5 (1, c) and 6(1) of Regulation 2016/679 as well as recital (49), which emphasizes the strict necessity test regarding the processing of personal data to guarantee network and information security of the systems of the controller, and Article 8(1) of Directive 2016/680. Thus, it is *proposed for a view to the extent of whether the facial processing technique employed at the Ski Resort is prohibited for practice in means of GDPR Article 9 (1)*. The research has shown, facial recognition is the automatic processing of digital images containing individuals' faces for identification or verification of those individuals by using face templates (CE, 2021, p. 5). The use of facial recognition technologies in the private sector can only take place in controlled environments for verification, authentication, or categorization purposes (CE, 2021, p. 11). The context of the processing of images is relevant to the determination of the sensitive nature of the data, as not all processing of images involves the processing of sensitive data (CE, 2021, p. 5). Images shall only be covered by the definition of biometric data when they are processed through a specific technical means that permits the unique identification or authentication of an individual (CE, 2021, p. 5.). The condition is also seen from the Paragraph 59 of the Explanatory Report to Convention 108+. *Thus, a simple digital photo at the Ski Resort stored for visual comparison purposes and displayed on a screen not being subjected to special technical processes does not meet the definition of the processing of special data categories according to GDPR Art. 9 (1)*. Consequently, the case of a Ski Resort operator in Austria employing facial recognition technology through photo characterization for lift ticket access control demonstrates compliance with the GDPR in means that the company has not used technology to uniquely identify, otherwise this practice would be prohibited. *Instead, company-operated photo data match that demonstrates avoidance of specific technical recognition and that is not banned under GDPR Article 9 (1)*.

Embracing a preventive approach and also marking Articles 5 and 6 of Convention 108+, the study tenses up to the proportionality assessment based on the risk posed from the policy, design, performance, and function of the digital facial recognition system at the Ski Resort. A 'risk' is a scenario describing an event and its consequences, estimated in terms of severity and likelihood (A29, 2017, p. 6). 'Risk management', on the other hand, can be defined as the coordinated activities to direct and control an organization with regard to risk (A29, 2017, p. 6). In practice, this means that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is 'likely to result in a high risk to the rights and freedoms of natural persons' as per the GDPR Article 35(1) (A29, 2017, p. 6). The GDPR Article 35(3) models of when a processing is 'likely to result in high risks': '(a) a systematic and extensive evaluation of personal aspects relating to natural persons which are founded 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 per-

son; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offenses referred to in Article 1013; or (c) a systematic monitoring of a publicly accessible area on a large scale'. In the view of the authors, none of mentioned applies to the case study meaning the minimum interference with claimed right to privacy. *In such cases, the controller should justify and document the reasons for not carrying out a data protection impact assessment (DPIA) and include/record the views of the data protection officer* (A29, 2017, p. 12). At the same time, it depends on the technology used and the circumstances, perception, and culture of each user, and can negatively affect the user's perception: Feeling of invasion of privacy, failures in biometric systems that prevent access to services, non-biometric alternatives lacking completely or not being suited to provide the same service, as well as the need to perform enrolment processes in each entity (ibid., p. 4). Since this information is 'built-in', the user cannot prevent the collection of additional information (EDPS and Agensia Espanola Proteccion Datos, 2020, p. 2) such as email address in the case. The establishment of a 'one-stop-shop procedure' for receiving requests to access, correct, and delete data could simplify procedures (FRA, Opinions on Biometrics).

4. Conclusions

According to THE FRA research, very few lawyers are specialized in seeking to enforce the right of access, correction, and deletion of data stored in IT systems, making it even more difficult for the persons concerned to exercise their rights (FRA, Opinions on Biometrics). Under the study, privacy is important when designing facial processing systems. Reasons for this include the contextual and often culturally dependent concept of privacy and the difficulty of translating privacy objectives into actionable requirements (EDPS, 2018, p. 12). The ENISA (European Union Agency for Network and Information Security) has administered a breakdown of the state of the art of how to engineer privacy by design (ENISA, 2014). While some privacy engineering methodologies mainly focus on the requirements phase or the measures to implement, privacy engineering must consider the whole life cycle of a service or a product, from initial planning to service/product disposal (EDPS, 2018, p. 15). *Adequate governance and management structures and procedures in the organization are then needed to enable the overall approach* (EDPS, 2018, p. 15). Therefore, *the service at the Ski Resort aligning to the facial processing technology is justified due to service level management as the basis for the lawfulness of the processing under the GDPR Article 6 (1, f) and that is not gone beyond Article 9 (1)*. Consequently, the complainant's objections are unsupported.

References:

Article 29 Data Protection Working Party (A29) (13 October 2017). Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is 'likely to result in a high risk' for the purpose of Regulation 2016/79. Available online: https://ec.europa.eu/newsroom/article29/items/611236 (last visited 03 May 2023).

Austrian Data Protection Authority (Datenschutzbehörde) (2020). Robert A***'s privacy complaint (complainant) against N*** Lift GmbH (respondent), represented by the lawyers Dr. Rudolph I*** & Dr. Sebastian I***, ECLI:AT :DSB:2020:2020.0.759.615; National Case Number: 2020-0.759.615.

Burk, D.L. (2021). ALGORITHMIC LEGAL METRICS. *The Notre Dame Law Review*, *96*(3), 1147–.

Council of Europe (CE) (June 2021). Guidelines on facial recognition adopted by the Consultative Committee of the Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108). Available online: https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751 (last visited 03 May 2023).

Council of Europe (CE) (June 2018). Convention 108+, Convention for the protection of individuals with regard to the processing of personal data. Available online: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (last visited 03 May 2023).

ENISA (December 2014). Privacy and Data Protection by Design – from policy to engineering. Available online: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (last visited 03 May 2023).

European Parliament and the Council (04 May 2016). Regulation (EU) 2016/679 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), OJ L 119, 1–88.

European Union Agency for Fundamental Rights (FRA), Opinions on Biometrics. Available online: https://fra.europa.eu/en/content/fra-opinions-biometrics (last visited 04 May 2023).

European Data Protection Supervisor (EDPS) and Agensia Espanola Proteccion Datos (24 June 2020). Joint Paper on 14 Misunderstandings to Biometric Identification and Authentication. Available online: https://edps.europa.eu/data-protection/our-work/publications/papers/14-misunderstandings-regard-biometric-identification_en (last visited 04 May 2023).

European Data Protection Supervisor (EDPS) (11 April 2017). Assessing the Necessity of Meas-

ures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit. Available online: https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf (last visited 04 May 2023).

European Data Protection Supervisor (EDPS) (31 May 2018). Opinion 5/2018, Preliminary Opinion on privacy by design. Available online: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (last visited 04 May 2023).

Explanatory Report to Convention 108+. Available online: https://rm.coe.int/ cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a (last visited 03 May 2023).

Federal Legal Information System (Rechtsinformationssystem des Bundes (RIS) (in DE)), Lift GmbH (2020). NOTICE, Data Protection Authority decides on Robert A***'s complaint of January 7, 2020, against N***. Available online: https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20201123_2020_0_759_615_00/DSBT_20201123_2020_0_759_615_00.pdf (last visited 16 March 2023).

Hosseinifard, Z., Shao, L., & Talluri, S. (2022). Service-Level Agreement with Dynamic Inventory Policy: The Effect of the Performance Review Period and the Incentive Structure. *Decision Sciences,* 53(5), 802–826. https://doi.org/10.1111/deci.12506

Looy, B. van, Dierdonck, R. van, Gemmel, P., & Dierdonck, R. van (Roland). (2013). *Service management: an integrated approach* (3rd ed.). Pearson.

Дар'я Булгакова,
адвокат, член Національної асоціації адвокатів України, доктор філософії з міжнародного права, запрошений науковець, дослідник, Департамент права, Уппсальський університет, Мюнкен 2, Востра Огатан 26, Уппсала, Швеція, 75309, daria.bulgakova@jur.uu.se
ORCID: *orcid.org/0000-0002-8640-3622*

Вікторія Ступнік,
педагог-методист вищої категорії, науковий керівник дослідницьких робіт з історії та права, викладач, Криворізька гімназія № 91 Криворізької міської ради Дніпропетровської області, Кривий Ріг, Україна, 50008, vikysjakrul@gmail.com
ORCID: *orcid.org/0009-0006-8953-2477*

ОБРОБКА ОБЛИЧЧЯ КОРИСТУВАЧА ВХІДНОГО КВИТКА НА ГІРСЬКОЛИЖНОМУ КУРОРТІ АВСТРІЇ

Анотація. ***Мета.*** Представлена стаття досліджує справу 2020 р. за фактом розслідування Австрійським органом із захисту даних щодо використання технології обробки даних обличчя на гірськолижному курорті. ***Методи дослідження***. У статті застосовано підхід прикладного дослідження з вивчення практики країни – члена Європейського Союзу щодо розгляду справи про захист персональних даних особи. Так, надано оцінку про те, як в Австрії застосовуються статті 6 (1, f) та 9 (1) Загального регулювання захисту даних (GDPR). ***Результати.*** Завдяки проведеному аналізу автори підтвердили, що європейські стандарти про захист даних мають бути дотримані у разі будь-якого обмеження права на приватність, зокрема під час обробки персональних даних. Зокрема, практика вхідного контролю користувачів ліфт-квитків має вимагатися законом, поважати основні права, відповідати визнаним інтересам, бути необхідною та пропорційною. ***Висновки.*** Дослідження переконалося у цінності приватності під час дизайну систем обробки обличчя шляхом співставлення з контекстуальним та культурно зумовленим характером розуміння приватності, а також виклику адаптації цілей обмеження приватності до практичних бачень. Відповідно, використання технології обробки обличчя на гірськолижному курорті вважається виправданим, оскільки воно узгоджується з управлінськими умовами обслуговування клієнтів та враховує вимоги, викладені у статті 6 (1, f) GDPR, а також водночас практика застосування досліджуваних технологій на гірськолижному курорті Австрії не стосувалася межі статті 9 (1) GDPR. Отже, автори роблять висновок, що справа про обробку обличчя на гірськолижному курорті Австрії показала, що технологію з розпізнавання обличчя дозволено використовувати для перевірки особистості користувача/власника квитка, наприклад під час сходження на підйомник, однак за умови якщо така практика не використовує спеціальних технологічних методів, що спрямовані на досягнення мети унікально ідентифікувати таку особу.

Ключові слова: Австрійський орган із захисту даних, ідентифікація людини, збір фотоданих, згода, фундаментальне право на приватність, захист персональних даних.

The article was submitted 17.10.2023
The article was revised 07.11.2023
The article was accepted 28.11.2023