RODO w szkolnej ławce. Przetwarzanie danych biometrycznych

Wykład online

28 kwietnia 2021 r.

URZĄD OCHRONY DANYCH OSOBOWYCH

Przetwarzanie danych biometrycznych w szkole

Natalia Holland
Departament Skarg

URZĄD OCHRONY DANYCH OSOBOWYCH

Zagadnienia

1. Czym są dane biometryczne – definicja danych biometrycznych.
2. Podstawy prawne dopuszczalności przetwarzania danych biometrycznych na gruncie przepisów RODO.
3. Wymogi dla wykorzystywania danych biometrycznych (ocena proporcjonalności, adekwatności, celowości).
4. Czy szkoły mogą przetwarzać dane biometryczne – odciski palców?
5. Dotychczasowe doświadczenia UODO dotyczące stosowania biometrii w szkole na przykładzie decyzji Prezesa UODO z 18 lutego 2020 r. o sygn. ZSZZS.440.768.2018.
6. Przetwarzanie danych biometrycznych przez szkoły na przykładzie europejskich organów nadzorczych.
7. Wytyczne dla administratorów w związku z przetwarzaniem danych biometrycznych.

Czym są dane biometryczne – definicja danych biometrycznych

- Zgodnie z art. 4 pkt 14 RODO dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

- Zgodnie z przywołanym przepisem dane biometryczne to wszystkie dane osobowe dotyczące np. kodu DNA, wizerunku twarzy, układu linii papilarnych, tęczówki oka.

Czym są dane biometryczne – definicja danych biometrycznych

- Poprzez specjalne przetwarzanie techniczne należy rozumieć wykorzystanie takich metod i środków, których celem jest dokonanie analizy cech biometrycznych i doprowadzenie do identyfikacji osoby fizycznej na podstawie przeprowadzonej analizy.

- Przykładem specjalnego przetwarzania technicznego może być na przykład skanowanie linii papilarnych czy tęczówki oka.

- Dana biometryczna jest szczególną cechą przypisaną do konkretnej osoby fizycznej i nie ulega ona zmianom na przestrzeni czasu. Ze względu na to są to dane szczególnie chronione i należy je wykorzystywać tylko w uzasadnionych przypadkach.

Podstawy prawne dopuszczalności przetwarzania danych biometrycznych na gruncie przepisów RODO

- Zgodnie z art. 9 ust. 1 RODO zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne, przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

Podstawy prawne dopuszczalności przetwarzania danych biometrycznych na gruncie przepisów RODO

- Zgodnie z art. 9 ust. 2 RODO wyżej wymieniony ustęp nie ma zastosowania, gdy zostanie spełniony jeden z wymienionych w tym przepisie warunków.

- Katalog wymieniony w art. 9 ust. 2 RODO jest zamknięty. Każda z przesłanek legalizujących proces przetwarzania danych osobowych ma charakter autonomiczny i niezależny. Oznacza to, że spełnienie co najmniej jednej z nich stanowi o zgodnym z prawem przetwarzaniu danych osobowych.

Podstawy prawne dopuszczalności przetwarzania danych biometrycznych na gruncie przepisów RODO

- Ten warunek występuje m.in. wtedy gdy osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1 (lit. a).

Podstawy prawne dopuszczalności przetwarzania danych biometrycznych na gruncie przepisów RODO

- Zgodnie z art. 4 ust. 11 RODO "zgoda" osoby, której dane dotyczą oznacza **dobrowolne, konkretne, świadome i jednoznaczne okazanie woli**, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Wymogi dla wykorzystywania danych biometrycznych (ocena proporcjonalności, adekwatności, celowości)

- Aby móc wykorzystać dane biometryczne należy spełnić kilka warunków.

Administrator musi ocenić zasadność zastosowania danych biometrycznych.

Aby dokonać takiej oceny, konieczne jest udzielenie odpowiedzi na poniższe pytania:

- czy biometria jest niezbędna do osiągnięcia celu, a cel jest naprawdę istotny
- czy istnieją inne mniej inwazyjne rozwiązania? Inne metody, dzięki którym ten cel da się osiągnąć
- czy można dać osobie, której dane dotyczą, wybór rozwiązania?

Wymogi dla wykorzystywania danych biometrycznych (ocena proporcjonalności, adekwatności, celowości)

- Administrator musi ustalić podstawę prawną wykorzystywania danych biometrycznych.
- Analiza tego czy administrator jest w stanie zapewnić właściwą ochronę w przypadku przetwarzania danych biometrycznych.

Wymogi dla wykorzystywania danych biometrycznych (ocena proporcjonalności, adekwatności, celowości)

- Przetwarzanie danych biometrycznych nie może się odbywać z pominięciem zasady minimalizacji określonej w art. 5 ust. 1 lit. c RODO.

- Zasada ta wymaga, aby proces przetwarzania danych był adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane.

Czy szkoły mogą przetwarzać dane biometryczne – odciski palców?

- Nie ma przepisu, który zezwalałby szkołom na pozyskiwanie od uczniów i pracowników odcisków palców w celu zapewnienia kontroli osób wchodzących do budynku. Nie uzasadniają tego nawet względy bezpieczeństwa oraz wyrażenie zgody przez zainteresowane osoby.

- To, jakie dane szkoły mogą pozyskiwać od swoich pracowników oraz uczniów regulują odpowiednio przepisy prawa pracy oraz przepisy sektorowe regulujące funkcjonowanie placówek oświatowych Żadne z nich nie zezwalają tym podmiotom na przetwarzanie, a więc m.in. pozyskiwanie i gromadzenie odcisków palca uczniów oraz nauczycieli i innych pracowników np. w celu kontroli dostępu do budynku.

Dotychczasowe doświadczenia UODO dotyczące stosowania biometrii w szkole na przykładzie decyzji Prezesa UODO z 18 lutego 2020 r. o sygn. ZSZZS.440.768.2018.

- Prezes UODO decyzją z 18 lutego 2020 r. nałożył karę na szkołę podstawową w związku z naruszeniem polegającym na przetwarzaniu danych biometrycznych dzieci.

- Prezes UODO po przeprowadzeniu z urzędu postępowania administracyjnego ustalił, że szkoła korzysta z czytnika biometrycznego przy wejściu do stołówki szkolnej, który identyfikuje dzieci w celu weryfikacji uiszczenia opłaty za posiłek.

Dotychczasowe doświadczenia UODO dotyczące stosowania biometrii w szkole na przykładzie decyzji Prezesa UODO z 18 lutego 2020 r. o sygn. ZSZZS.440.768.2018.

- W ukaranej szkole podstawowej, zgodnie z zasadami wydawania obiadów, umieszczonymi na stronie internetowej stołówki prowadzonej przez szkołę, uczniowie, którzy nie posiadają identyfikacji biometrycznej, przepuszczają wszystkich i oczekują na końcu kolejki.

- Tego typu zasady zdaniem Prezesa UODO wprowadzają nierówne traktowanie uczniów i ich bezpodstawne zróżnicowanie, ponieważ wyraźnie promują uczniów posiadających identyfikację biometryczną.

Dotychczasowe doświadczenia UODO dotyczące stosowania biometrii w szkole na przykładzie decyzji Prezesa UODO z 18 lutego 2020 r. o sygn. ZSZZS.440.768.2018.

- Prezes UODO w swojej decyzji stwierdził, że przetwarzanie danych biometrycznych nie jest niezbędne dla osiągnięcia celu, jakim jest identyfikacja uprawnienia dziecka do odebrania obiadu. Szkoła może przeprowadzić identyfikację za pomocą innych środków, które nie ingerują tak dalece w prywatność dziecka.

- W tym przypadku zgoda nie może być przesłanką legalizującą przetwarzanie danych biometrycznych → art. 106 Prawa Oświatowego w zw. z art. 6 ust. 1 lit. e RODO.

RODO w szkolnej ławce. Przetwarzanie danych biometrycznych

Wykład online

28 kwietnia 2021 r.

URZĄD OCHRONY DANYCH OSOBOWYCH

Przetwarzanie danych biometrycznych dzieci z perspektywy europejskich organów nadzorczych

Maria Jęda
Departament Współpracy Międzynarodowej i Edukacji

URZĄD OCHRONY DANYCH OSOBOWYCH

Przykłady przetwarzania danych biometrycznych w szkole

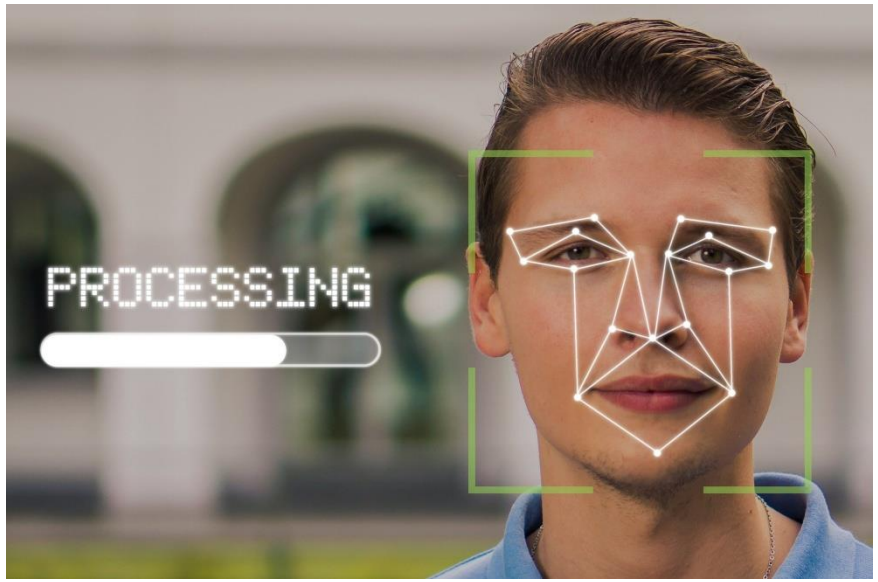
Szwecja	Francja
Rada Szkolnictwa Średniego w gminie Skellefteå	Dwie szkoły średnie w Nicei i Marsylii
Rozpoznawanie twarzy do monitorowania obecności 22 uczniów na lekcjach w ramach testu pilotażowego	Rozpoznawanie twarzy przy wejściu do szkół w ramach eksperymentu
Cel: łatwiejsze i skuteczniejsze rejestrowanie obecności na lekcjach	Cel: ułatwienie i zabezpieczenie dostępu do szkoły
Podstawą do przetwarzania była zgoda rodziców i uczniów	Podstawą do przetwarzania była zgoda rodziców i uczniów

Decyzja szwedzkiego organu ochrony danych (20.08.2019)

Rozpoznawanie twarzy uczniów było niezgodne z prawem z uwagi na:

- przetwarzanie danych osobowych uczniów w sposób bardziej inwazyjny z punktu widzenia integralności osobistej i obejmujący więcej danych osobowych niż jest to konieczne do określonego celu (monitorowanie obecności);
- przetwarzanie szczególnej kategorii danych osobowych (danych biometrycznych) bez spełnienia odpowiednich warunków;
- niespełnienie wymagań dotyczących oceny skutków dla ochrony danych i nieprzeprowadzenie uprzednich konsultacji ze szwedzkim organem ochrony danych.

Stanowisko francuskiego organu ochrony danych (17.10.2019)



- Zastosowanie urządzenia do rozpoznawania twarzy w szkole jest sprzeczne z głównymi zasadami proporcjonalności i minimalizacji danych określonymi w RODO.
- Cele polegające na zapewnieniu i usprawnieniu dostępu do szkół średnich można osiągnąć za pomocą środków, które są znacznie mniej inwazyjne pod względem prywatności i swobód, na przykład kontrola identyfikatorów.
- Urządzenia do rozpoznawania twarzy są szczególnie uciążliwe i stwarzają poważne zagrożenie dla prywatności i wolności osobistych.
- Prawdopodobnie stworzą również poczucie wzmocnionego nadzoru.

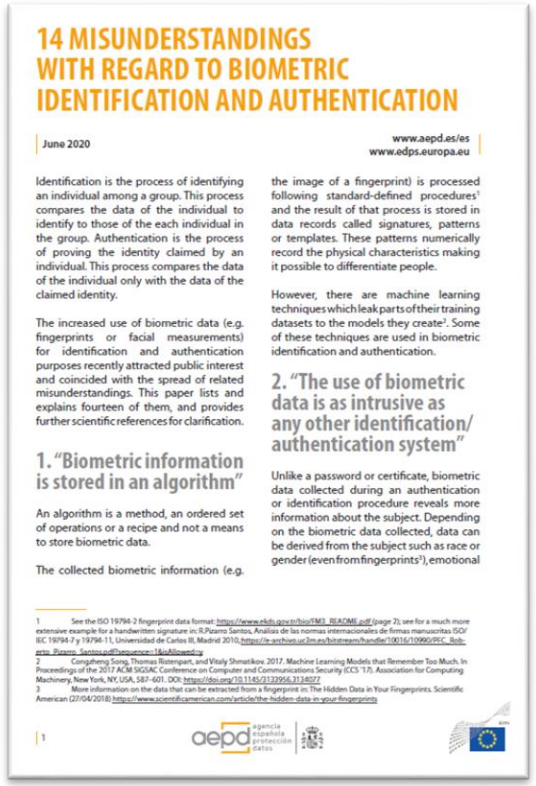
Orzeczenie Sądu administracyjnego w Marsylii z dnia 27 lutego 2020

- Sąd uznał, że decyzja o zainstalowaniu w dwóch szkołach technologii rozpoznawania twarzy nie była zgodna z RODO, ponieważ uczniowie nie mogli wyrazić „zgody na zbieranie danych osobowych w sposób dobrowolny i świadomy”, ze względu na stosunek zwierzchnictwa wiążący uczniów z administracją szkoły.
- Ponadto sąd przychylił się do stanowiska francuskiego organu i orzekł, że rozpoznawanie twarzy jest środkiem nieproporcjonalnym do kontroli wejść do szkoły, zwłaszcza że istnieją alternatywne środki.
- *„Region używa młota pneumatycznego, aby uderzyć mrówkę"*.

Blaski czy raczej cienie biometrycznej identyfikacji?

Czy systemy biometrycznej identyfikacji:

- są inwazyjne?
- są zawsze dokładne?
- są zawsze precyzyjne?
- są odpowiednie dla wszystkich?
- można obejść?
- są bezpieczne?



14 MISUNDERSTANDINGS WITH REGARD TO BIOMETRIC IDENTIFICATION AND AUTHENTICATION

June 2020

www.aepd.es/es
www.edps.europa.eu

Identification is the process of identifying an individual among a group. This process compares the data of the individual to identify to those of the each individual in the group. Authentication is the process of proving the identity claimed by an individual. This process compares the data of the individual only with the data of the claimed identity.

The increased use of biometric data (e.g. fingerprints or facial measurements) for identification and authentication purposes recently attracted public interest and coincided with the spread of related misunderstandings. This paper lists and explains fourteen of them, and provides further scientific references for clarification.

1. "Biometric information is stored in an algorithm"

An algorithm is a method, an ordered set of operations or a recipe and not a means to store biometric data.

The collected biometric information (e.g. the image of a fingerprint) is processed following standard-defined procedures[1] and the result of that process is stored in data records called signatures, patterns or templates. These patterns numerically record the physical characteristics making it possible to differentiate people.

However, there are machine learning techniques which leak parts of their training datasets to the models they create[2]. Some of these techniques are used in biometric identification and authentication.

2. "The use of biometric data is as intrusive as any other identification/ authentication system"

Unlike a password or certificate, biometric data collected during an authentication or identification procedure reveals more information about the subject. Depending on the biometric data collected, data can be derived from the subject such as race or gender (even from fingerprints[3]), emotional

1 See the ISO 19794-2 fingerprint data format: https://www.nbib.gov.tr/bio/FM3_README.pdf (page 2); see for a much more extensive example for a handwritten signature in: R.Pizarro Santos, Análisis de las normas internacionales de firmas manuscritas ISO/IEC 19794-7 y 19794-11, Universidad de Carlos III, Madrid 2010, https://e-archivo.uc3m.es/bitstream/handle/10016/10990/PFC_Roberto_Pizarro_Santos.pdf?sequence=1&isAllowed=y

2 Congzheng Song, Thomas Ristenpart, and Vitaly Shmatikov. 2017. Machine Learning Models that Remember Too Much. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). Association for Computing Machinery, New York, NY, USA, 587–601. DOI: https://doi.org/10.1145/3133956.3134077

3 More information on the data that can be extracted from a fingerprint in: The Hidden Data in Your Fingerprints. Scientific American (27/04/2018) https://www.scientificamerican.com/article/the-hidden-data-in-your-fingerprints

1

Źródło: 14 nieporozumień odnośnie identyfikacji i uwierzytelniania biometrycznego opr. hiszpański organ nadzorczy, Europejski Inspektor Ochrony Danych

RODO w szkolnej ławce. Przetwarzanie danych biometrycznych

Wykład online

28 kwietnia 2021 r.

URZĄD OCHRONY DANYCH OSOBOWYCH

Biometria w dokumentach Rady Europy

Iwona Piórkowska-Kapica
Departament Współpracy Międzynarodowej i Edukacji

URZĄD OCHRONY DANYCH OSOBOWYCH

Ochrona danych osobowych w kontekście biometrii w Radzie Europy

Rada Europy	Europejska Konwencja Praw Człowieka	Artykuł 8 Prawo do poszanowania życia prywatnego i rodzinnego
Komitet Konsultacyjny Konwencji nr 108 Rady Europy (T-PD)	Konwencja nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych 28.01.1981 r. oraz Protokół zmieniający Konwencję nr 108 (2018)	Artykuł 6 Szczególne kategorie danych

Dokumenty T-PD dot. ochrony danych osobowych w kontekście biometrii

Wytyczne dot. ochrony danych dzieci w środowisku edukacyjnym

20 November 2020 T-PD(2019)06BISrev5

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

Children's Data Protection in an Education setting

Guidelines

Directorate General of Human Rights and Rule of Law

Wytyczne dot. rozpoznawania twarzy

28 January 2021 T-PD(2020)03rev4

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

Guidelines on Facial Recognition

Directorate General of Human Rights and Rule of Law

Wytyczne dot. ochrony danych dzieci w środowisku edukacyjnym

Dobre praktyki przetwarzania danych biometrycznych w sektorze oświaty:

1. Nie stosowanie przetwarzania danych biometrycznych w sposób rutynowy
2. Stosowanie odpowiednich zabezpieczeń przewidzianych w przepisach
3. Zwrócenie uwagi na wrażliwość przetwarzania danych dotyczących ciała i danych behawioralnych dziecka
4. Spełnienie warunków dotyczących zgody

Wytyczne dot. rozpoznawania twarzy

Wskazówki dla podmiotów wykorzystujących technologie rozpoznawania twarzy:

1. Oparcie się na podstawach prawnych odpowiednich dla sektora i celu, a tym:
   - zapewnienie rzetelności i przejrzystości, w tym określenie polityki prywatności rozpoznawania twarzy
   - ograniczenie celu, minimalizacja danych i ograniczenie czasu przechowywania
   - prawidłowość
2. Zapewnienie bezpieczeństwa danych biometrycznych
3. Zapewnienie odpowiedzialności i rozliczalności
   - uwzględnienie odpowiednich środków organizacyjnych
   - podjęcie niezbędnych środków technicznych w celu zapewnienia jakości danych biometrycznych
4. Dokonanie oceny skutków dla ochrony danych

Podsumowanie

- Dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.
- Nie ma przepisu, który zezwalałby szkołom na pozyskiwanie od uczniów i pracowników odcisków palców w celu zapewnienia kontroli osób wchodzących do budynku.
- Praktyka pokazuje, że konieczności przetwarzania danych biometrycznych nie uzasadniają nawet względy bezpieczeństwa oraz wyrażenie zgody przez zainteresowane osoby.
- Co do zasady – nie przetwarzamy danych biometrycznych w szkole, jeśli nie jest to konieczne.
- Jeśli zachodzi uzasadniona konieczność – należy pamiętać o tym, by przetwarzanie było zgodne z obowiązującymi przepisami prawa.
- W celu ułatwienia procesu przetwarzania danych biometrycznych, warto zapoznać się z dobrymi praktykami i wskazówkami, np.
  - Wytycznymi dot. ochrony danych dzieci w środowisku edukacyjnym
  - Wytycznymi dot. rozpoznawania twarzy

Źródła – część I

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
- https://uodo.gov.pl/pl/138/1943
- https://uodo.gov.pl/pl/138/1453
- Decyzja Prezesa UODO z 18 lutego 2020 r. sygn. ZSZZS.440.768.2018

Źródła – część II

- Opinia Grupy Roboczej Art. 29 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych (WP 193), 27.04.2012 r. https://archiwum.giodo.gov.pl/pl/1520111/4676
- Wytyczne Europejskiej Rady Ochrony Danych 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń wideo, https://uodo.gov.pl/pl/414/1332
- Dokument: 14 nieporozumień odnośnie identyfikacji i uwierzytelniania biometrycznego *(ang. 14 misunderstandings with regard to biometric identification and authentication)* *https://edps.europa.eu/data-protection/our-work/publications/papers/14-misunderstandings-regard-biometric-identification_en*
- Dokument*:* „Stan biometrii" Informacje od Europejskiego Inspektora Ochrony Danych (ang. "The State of Biometrics" Update from the European Data Protection Supervisor), 7.10.2020 https://edps.europa.eu/sites/default/files/publication/20-10-07_edps_biometrics_speech_en.pdf

Źródła – część III

- Europejska Konwencja Praw Człowieka https://www.echr.coe.int/Documents/Convention_POL.pdf
- Konwencja nr 108 (zmodernizowana protokołem z 2018 r.) https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf
- Wytyczne dot. ochrony danych dzieci w środowisku edukacyjnym https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b, wersja w jęz. polskim https://uodo.gov.pl/pl/138/1824
- Wytyczne dot. rozpoznawania twarzy https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 (polska wersja w przygotowaniu)

Dziękujemy za uwagę!

URZĄD OCHRONY DANYCH OSOBOWYCH