Polityka ochrony wideo w Parlamencie Europejskim

przyjęta przez
Dyrektor Generalną ds. Bezpieczeństwa i Ochrony
Parlamentu Europejskiego

Aktualizacja w styczniu 2022 r.

Spis treści

1. Zakres stosowania

Dyrekcja Generalna ds. Bezpieczeństwa i Ochrony Parlamentu Europejskiego (zwana dalej „DG SAFE") stosuje ochronę wideo w celu **monitorowania określonych obszarów, wydarzeń, działań lub osób za pomocą systemu monitoringu wizyjnego** zwanego telewizją przemysłową (CCTV).

W niniejszym komunikacie dotyczącym polityki ochrony wideo **opisano system ochrony wideo Parlamentu Europejskiego, jego cel i zastosowanie oraz zabezpieczenia** wprowadzone w celu ochrony praw osobowych osób, których dane dotyczą, zgodnie z rozporządzeniem (UE) 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje Unii (zwanym dalej „rozporządzeniem (UE) 2018/1725").

2. Ograniczenie celu

System ochrony wideo stanowi wsparcie w zapewnianiu bezpieczeństwa i ochrony zgodnie z przepisami dotyczącymi bezpieczeństwa i ochrony w Parlamencie Europejskim[1].

DG SAFE wykorzystuje system ochrony wideo w celu **zapobiegania ewentualnym zagrożeniom dla porządku i bezpieczeństwa, powstrzymywania ich lub zarządzania nimi, co oznacza też nieupoważniony dostęp fizyczny** do pomieszczeń Parlamentu Europejskiego lub do stref zastrzeżonych lub wrażliwych, infrastruktury informatycznej lub informacji.

DG SAFE może ponadto wykorzystywać nagrania z kamer telewizji przemysłowej **w ramach dochodzeń dotyczących bezpieczeństwa i dochodzeń pomocniczych** prowadzonych w ramach jej mandatu.

Przekazywanie nagrań z kamer telewizji przemysłowej odbywa się wyłącznie zgodnie z warunkami określonymi w punkcie 6.2: „Ujawnianie i przekazywanie".

System ochrony wideo nie jest wykorzystywany do żadnych innych celów[2].

3. Podstawa prawna

Korzystanie z systemu ochrony wideo Parlamentu Europejskiego regulują następujące podstawy prawne:

- Parlament Europejski – decyzja Prezydium z dnia 15 stycznia 2018 r. w sprawie przepisów regulujących kwestie bezpieczeństwa i ochrony w Parlamencie Europejskim (2018/C 79/04);

[1] Decyzja Prezydium Parlamentu Europejskiego z dnia 15 stycznia 2018 r. w sprawie przepisów regulujących kwestie bezpieczeństwa i ochrony w Parlamencie Europejskim (2018/C 79/04).
[2] Artykuł 4 rozporządzenia (UE) 2018/1725.

- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia nr 45/2001 i decyzji nr 1247/2002/WE;
- Parlament Europejski – decyzja Prezydium z dnia 17 czerwca 2019 r. w sprawie przepisów wykonawczych dotyczących rozporządzenia (UE) 2018/1725;
- decyzja Prezydium Parlamentu Europejskiego z dnia 15 kwietnia 2013 r. dotycząca przepisów regulujących postępowanie z informacjami poufnymi w Parlamencie Europejskim, Dz.U. C 96 z 1.4.2014, s. 1;
- Polityka bezpieczeństwa informacji w Parlamencie Europejskim z dnia 2 czerwca 2020 r., Geda (D(2020)14287).

4. Strefy chronione

DG SAFE podejmuje decyzje o lokalizacji kamer, kątach widzenia i strefach objętych ochroną wideo, w pełni uwzględniając wytyczne Europejskiego Inspektora Ochrony Danych[3].

Kamery są rozmieszczane po przeprowadzeniu oceny ryzyka, aby zagwarantować ich skierowanie wyłącznie na najbardziej istotne miejsca, strefy i widoki wewnątrz i na zewnątrz budynków, a tym samym zagwarantować właściwą zgodność ze wspomnianą polityką.

Dokładniej rzecz biorąc, kamery są instalowane w celu monitorowania punktów wejścia i wyjścia z budynków oraz ich bezpośredniego sąsiedztwa, w tym stref dostępu publicznego (takich jak główne wejścia, wyjścia ewakuacyjne i przeciwpożarowe, wejścia na parkingi, miejsca wysiadania VIP-ów, Esplanada itp.). Ponadto kamery monitorują kilka ważnych klatek schodowych lub punktów połączeń, a także wyjątkowo ważne strefy, które wymagają dodatkowego zabezpieczenia, takie jak miejsca, w których przechowuje się cenne aktywa, poufne i wrażliwe informacje lub tak zwane „pomieszczenia sensytywne” i strefy o ograniczonym dostępie.

Nie monitoruje się miejsc, w których można oczekiwać bardzo dużej prywatności, takich jak indywidualne biura lub miejsca wypoczynku.

Monitorowanie poza terenem Parlamentu jest ograniczone do minimalnego obszaru niezbędnego do zapewnienia realizacji niniejszej polityki i odbywa się zgodnie z odpowiednimi przepisami unijnymi i krajowymi.

4.1. Doraźna ochrona wideo

W uzasadnionych przypadkach DG SAFE może stosować doraźną ochronę wideo, w określonym celu i przez ograniczony czas.

Kamery wykorzystywane do doraźnej ochrony wideo są instalowane po złożeniu pisemnego wniosku i uzyskaniu uprzedniego pisemnego zezwolenia Dyrektora Generalnego DG SAFE.

[3] Wytyczne są dostępne na stronie https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf oraz na stronach https://edps.europa.eu/data-protection/our-work/publications/guidelines/video-surveillance-follow_en

Doraźna ochrona wideo może być stosowana maksymalnie przez jeden miesiąc. Każde przedłużenie tego okresu będzie wymagało powtórzenia ww. procedury.

Kamery nagrywają tylko w uprzednio określonych godzinach.

Obrazy zarejestrowane w ramach doraźnej ochrony wideo nie będą przechowywane, z wyjątkiem sytuacji, gdy zostaną uznane za istotne dla celów dochodzenia w sprawie bezpieczeństwa, w którym to przypadku będą przechowywane wraz z materiałami z dochodzenia.

W uzasadnionych przypadkach i po konsultacji z Inspektorem Ochrony Danych doraźna ochrona wideo może zostać zainstalowana w sposób ukryty.

5. Gromadzone dane osobowe i specyfikacje techniczne systemu

System ochrony wideo Parlamentu Europejskiego jest standardowym systemem telewizji przemysłowej. Wszystkie kamery pracują 24 godziny na dobę przez 7 dni w tygodniu.

Większość kamer rejestruje jedynie zmiany w pikselach, co oznacza, że dostęp do właściwych obrazów jest uzależniony od wykrycia ruchu przez system. System rejestruje każdy ruch wykryty przez kamery w chronionej strefie, wraz z godziną, datą i lokalizacją. W takim przypadku jakość obrazu pozwala na identyfikację osób lub innych szczegółów na nagraniu.

Wszystkie kamery, niezależnie od tego, czy wykrywają ruch, czy nie, podlegają takim samym rygorystycznym środkom bezpieczeństwa.

W systemie nie stosuje się obecnie telewizji przemysłowej rejestrującej dźwięk. Parlament Europejski nie wykorzystuje kamer internetowych do ochrony wideo.

Zgodnie z art. 10 rozporządzenia (UE) 2018/1725 system ochrony wideo nie jest przeznaczony do gromadzenia szczególnych kategorii danych.

6. Dostęp do obrazów i ujawnianie informacji

6.1 Prawa dostępu dla pracowników i administratorów systemu

Wyłącznie Dyrektor Generalny DG SAFE (zwany dalej „administratorem danych”) jest uprawniony do przyznawania, zmiany lub unieważniania praw dostępu.

Prawa dostępu są przyznawane użytkownikom na zasadzie wiedzy koniecznej (osobom, dla których dostęp jest niezbędny do wykonywania ich zadań) i są ograniczone do celów ww. polityki CCTV oraz technicznej konserwacji systemu.

DG SAFE prowadzi wewnętrzny rejestr praw dostępu i systematycznie rejestruje wszystkie przypadki pozyskiwania materiału filmowego. Pozyskiwanie materiału filmowego do celów konserwacji technicznej odbywa się bez wizualizacji obrazu.

6.2 Ujawnianie i przekazywanie

DG SAFE może ujawniać lub przekazywać nagrania z kamer telewizji przemysłowej służbom bezpieczeństwa innych instytucji europejskich lub organom bezpieczeństwa, sądowym lub ścigania państwa członkowskiego UE. Takie przekazywanie nagrań może być dokonywane wyłącznie na wniosek takich stron – nie są to działania regularne ani rutynowe – oraz zgodnie z procedurą opisaną w niniejszym rozdziale[4].

Każde ujawnienie lub przekazanie nagrań wymaga zgody administratora danych, rygorystycznej oceny konieczności takiego ujawnienia lub przekazania oraz zasięgnięcia opinii Wydziału Prawnego Parlamentu Europejskiego.

W sprawach z udziałem posłów wymagana jest formalna zgoda Przewodniczącego Parlamentu Europejskiego. W przypadku pracowników wymagana jest formalna zgoda sekretarza generalnego.

O każdym takim ujawnieniu lub przekazaniu danych powiadamiany jest inspektor ochrony danych Parlamentu Europejskiego.

DG SAFE dokumentuje proces w całości.

7. Okres przechowywania

DG SAFE przechowuje nagrania telewizji przemysłowej przez jeden miesiąc.

Materiał filmowy uzyskany w ramach dochodzenia w sprawie bezpieczeństwa jest przechowywany przez okres trwania przedsięwzięcia, a w razie potrzeby archiwizowany wraz z dochodzeniem przez okres do 10 lat. DG SAFE skrupulatnie dokumentuje takie przechowywanie.

8. Środki ochrony

Parlament Europejski korzysta z najlepszych dostępnych rozwiązań technologicznych sprzyjających ochronie prywatności, zgodnie z zasadami „prywatności w fazie projektowania” i „minimalizacji danych”.

DG SAFE opiera się na szeregu technicznych i organizacyjnych środków bezpieczeństwa w celu ochrony danych zawartych w materiałach z telewizji przemysłowej.

W związku z tym system telewizji przemysłowej nie jest połączony z żadnym innym systemem poza Parlamentem Europejskim, a dostęp do niego mają wyłącznie specjalnie

[4] DG SAFE nie przyjmuje wniosków dotyczących „eksploracji danych”, czyli procesu analizowania danych z różnych perspektyw i przedstawiania ich w formie użytecznych nowych informacji.

upoważnieni pracownicy DG SAFE. DG SAFE szyfruje zarchiwizowane pliki wideo w okresie ich przechowywania i skrupulatnie rejestruje wszelkie czynności w systemie.

Ponadto DG SAFE uzależnia uzyskanie prawa dostępu od odbycia obowiązkowego szkolenia wewnętrznego i złożenia zobowiązania do zachowania poufności.

DG SAFE systematycznie zamazuje materiał filmowy, który mógłby doprowadzić do identyfikacji osób niebiorących udziału w dochodzeniu w sprawie bezpieczeństwa lub dochodzeniu pomocniczym.

Podjęto niezbędne kroki w celu zapewnienia, że system ochrony wideo Parlamentu Europejskiego będzie mógł działać w przypadku przerwy w dostawie prądu, aby zapewnić minimalne warunki bezpieczeństwa i ochrony.

9. Informowanie społeczeństwa

Parlament Europejski informuje opinię publiczną o systemie ochrony wideo poprzez:

- wydawanie powiadomień na miejscu, aby poinformować opinię publiczną o monitoringu oraz aby przekazać jej istotne informacje na temat przetwarzania takiego monitoringu;
- udostępnianie streszczenia zasad ochrony wideo w recepcjach i na stronie internetowej Parlamentu Europejskiego;
- udostępnienie polityki ochrony danych osobowych w intranecie i na stronie internetowej Parlamentu Europejskiego.

W przypadku wszystkich tych trzech metod podany jest adres poczty elektronicznej, pod którym można zadawać dalsze pytania i uzyskać informacje o prawach przysługujących osobom, których dane dotyczą.

10. Prawa osób, których dane dotyczą

DG SAFE powiadamia indywidualnie każdą osobę zidentyfikowaną w materiale wideo, jeżeli zachodzi którakolwiek z poniższych sytuacji:

zawsze, gdy DG SAFE:

- przechowuje tożsamość takiej osoby w aktach;
- przechowuje tożsamość po upływie zwykłego okresu przechowywania;
- wykorzystuje materiał filmowy w postępowaniu z udziałem tej osoby;
- ujawnia lub przekazuje obraz poza DG SAFE.

Członkowie społeczeństwa mają prawo do wykonywania swoich praw w zakresie ochrony danych osobowych na mocy rozporządzenia (UE) 2018/1725, kierując wszelkie żądania do administratora danych:

Administrator danych z monitoringu wideo w Parlamencie Europejskim
Dyrektor generalny ds. bezpieczeństwa i ochrony

Rue Wiertz 60, B-1047 Bruksela
Adres e-mail: SAFE.dataprotection@europarl.europa.eu

DG SAFE wysyła osobie, której dotyczą dane, **potwierdzenie otrzymania** wniosku w ciągu pięciu dni roboczych od jego wpłynięcia[5].

Jeśli chodzi o treść pytania, DG SAFE **udziela odpowiedzi osobie, której dane dotyczą, w ciągu 30 dni kalendarzowych**, chyba że z uzasadnionego powodu administrator danych nie może dotrzymać tego terminu. Administrator danych informuje osobę, której dane dotyczą, o wszelkich możliwych opóźnieniach i ich przyczynach.

Aby uzyskać dostęp do swoich danych, osoba, której dane dotyczą, musi w sposób niebudzący wątpliwości udowodnić swoją tożsamość, wskazać – o ile to możliwe – datę, godzinę, miejsce i okoliczności wykonania nagrania, do którego chce uzyskać dostęp, oraz dostarczyć aktualną fotografię, która umożliwi DG SAFE zidentyfikowanie jej na podstawie przeglądanych zdjęć.

Administrator danych może odmówić podjęcia działań na wniosek osoby, której dane dotyczą, jeśli jest on ewidentnie nieuzasadniony lub nadmierny, w szczególności ze względu na jego powtarzalność[6]. DG SAFE ocenia to indywidualnie w każdym przypadku. Na administratorze danych spoczywa ciężar wykazania, że wniosek jest ewidentnie nieuzasadniony lub nadmierny.

W przypadku bardzo skomplikowanego wniosku lub gdy wniosek może spowodować zagrożenie dla praw i wolności lub dla innych osób, których dane dotyczą, administrator danych konsultuje się z inspektorem ochrony danych Parlamentu Europejskiego.

Parlament Europejski nie pobiera od wnioskodawców opłat za to, że korzystają ze swoich praw do ochrony danych.

Administrator danych może zastosować ograniczenia praw przyznanych osobom, których dane dotyczą, na mocy rozporządzenia (UE) 2018/1725, jeżeli **skorzystanie z takiego prawa zagroziłoby celowi dochodzenia w sprawie bezpieczeństwa[7]**. DG SAFE analizuje tę możliwość w poszczególnych przypadkach i w stosownych przypadkach należycie dokumentuje ten proces oraz informuje inspektora ochrony danych Parlamentu Europejskiego o każdym takim ograniczeniu.

11. Prawo do złożenia skargi

Każda osoba fizyczna ma prawo do złożenia skargi do Europejskiego Inspektora Ochrony Danych (adres e-mail: edps@edps.europa.eu), jeśli uzna ona, że jej prawa wynikające z rozporządzenia (UE) 2018/1725 zostały naruszone w wyniku przetwarzania jej danych osobowych przez Parlament Europejski. DG SAFE zaleca, aby przed podjęciem takich

[5] Potwierdzenie odbioru nie jest konieczne, jeżeli w tym samym terminie pięciu dni roboczych zostanie udzielona merytoryczna odpowiedź na wniosek. Odpowiedź przesyła się osobie, której dane dotyczą, w terminach przewidzianych w art. 14 ust. 3 i art. 14 ust. 4 rozporządzenia (UE) 2018/1725.
[6] Art. 14 rozporządzenia (UE) 2018/1725.
[7] Artykuł 25 rozporządzenia (UE) 2018/1725 i załącznik I do decyzji Prezydium Parlamentu Europejskiego z 17 czerwca 2019 r. ustanawiającej przepisy wykonawcze dotyczące rozporządzenia (UE) 2018/1725.

działań osoby fizyczne starały się uzyskać dodatkowe informacje, kontaktując się z następującymi podmiotami:

Administrator danych z monitoringu wideo w Parlamencie Europejskim:
Dyrektor generalny ds. bezpieczeństwa i ochrony
Rue Wiertz 60, B-1047 Bruksela
Adres e-mail: SAFE.dataprotection@europarl.europa.eu

lub

inspektor ochrony danych osobowych w Parlamencie Europejskim
Telefon: +352 4300 23595
Adres e-mail: data-protection@ep.europa.eu

Pracownicy PE mogą również odwołać się od decyzji organu powołującego na mocy art. 90 regulaminu pracowniczego.

12. Konsultacje i kontrola wewnętrzna w zakresie ochrony danych

Parlament Europejski stosuje swój system ochrony wideo w pełnej zgodności z rozporządzeniem (UE) 2018/1725.

Przy opracowywaniu niniejszej polityki DG SAFE konsultowała się z inspektorem ochrony danych Parlamentu Europejskiego.

DG SAFE przeprowadza okresowe przeglądy ochrony danych, aby ocenić, czy:

- prawidłowo wdraża politykę ochrony wideo (audyt zgodności);
- nadal istnieje potrzeba stosowania systemu ochrony wideo;
- system nadal służy założonemu celowi;
- odpowiednie alternatywne rozwiązania pozostają niedostępne;
- regularnie przeprowadza się minimalizację danych.