41. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności

21-24 października 2019 r., Tirana

Rezolucja dotycząca czynnika ludzkiego jako przyczyny naruszeń ochrony danych osobowych

41. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności:

Zważywszy, iż w celu ochrony prywatności i budowania zaufania do gospodarki opartej na danych wymagana jest globalna reakcja organów i organizacji zajmujących się ochroną danych i prywatności ze względu na wzrost liczby, wielkości i wagi naruszeń ochrony danych osobowych, wspólne źródło ich przyczyn, międzynarodowy charakter konsekwencji i szkód, które mogą z nich wyniknąć,

Uznając, że wdrożenie systemów zgłaszania naruszeń ochrony danych osobowych w niektórych jurysdykcjach państw członkowskich doprowadziło do znacznego wzrostu zgłaszania naruszeń ochrony danych osobowych, co dostarczyło cennych informacji na temat ich przyczyn oraz pozwoliło lepiej zrozumieć, w jaki sposób można ich uniknąć i określić potencjalne strategie zapobiegawcze;

Podkreślając, że zgłoszenia naruszeń ochrony danych osobowych, działania regulacyjne w niektórych jurysdykcjach państw członkowskich, a także badania krajowe i międzynarodowe pokazują, że naruszenia ochrony danych osobowych często wiążą się z błędami ludzkimi, w szczególności takimi jak nieumyślne ujawnienie danych osobowych przez pracowników osobom nieuprawnionym lub oszukiwanie osób w celu pozyskania ich danych uwierzytelniających, pozwalających na dostęp do ich informacji i systemów;

Uznając, że wspólną zasadą dla przepisów dotyczących prywatności i ochrony danych na całym świecie jest konieczność ochrony danych osobowych poprzez odpowiednie zabezpieczenia przed zagrożeniami takimi jak: utrata danych lub nieuprawniony do nich dostęp, a także zniszczenie, wykorzystanie, modyfikacja lub ich ujawnienie;

Potwierdzając, że rola czynnika ludzkiego w naruszeniach ochrony danych osobowych podkreśla znaczenie budowania kultury w miejscu pracy, w której prywatność i bezpieczeństwo są organizacyjnymi priorytetami, w tym poprzez okresowe wdrażanie programów szkoleniowych, edukacyjnych i informacyjnych, uwzględnianie ochrony prywatności w fazie

projektowania, wykorzystania systemów i praktyk i zarządzanie nimi, a także wdrażanie rozwiązań technologicznych;

Odnotowując, że Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności uprzednio stwierdziła potrzebę pracy na rzecz globalnej polityki, standardów i modeli oraz zapewnienia wyższego poziomu współpracy regulacyjnej w celu wzmocnienia skutecznego zapobiegania problemom związanym z prywatnością i ochroną danych oraz ich wykrywaniu i rozwiązywaniu, a także w celu zapewnienia spójności i przewidywalności systemów nadzoru w gospodarce opartej na danych;

Zważywszy na trwające prace Organizacji Współpracy Gospodarczej i Rozwoju (OECD) w celu zapewnienia, aby bezpieczeństwo cyfrowe i ochrona prywatności sprzyjały rozwojowi gospodarki cyfrowej oraz prac mających na celu ulepszanie bazy dowodowej dla tworzenia polityki bezpieczeństwa i prywatności, w tym porównywalności w zgłaszaniu naruszeń danych osobowych;

Zauważając, że Spis Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności z 2017 r. wykazał, że systemy zgłaszania naruszeń danych osobowych różnią się w poszczególnych jurysdykcjach państw członkowskich – odnotowano zarówno brak posiadania takich systemów, jak i posiadanie dobrowolnych oraz obowiązkowych systemów zgłaszania naruszeń ochrony danych osobowych, mających zastosowanie do wszystkich lub poszczególnych sektorów;[1]

Podkreślając, że gromadzenie, klasyfikacja, analiza i publikacja statystyk dotyczących naruszeń ochrony danych osobowych zgłoszonych organom ochrony danych i prywatności, w tym z podaniem ich przyczyn, ma zasadnicze znaczenie zarówno dla rozwoju globalnej polityki, jak i reakcji na przyczyny naruszeń ochrony danych osobowych;

Przypominając, że 31. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności w 2009 r. przyjęła „*Międzynarodowe Standardy Ochrony Danych Osobowych i Prywatności"* („*Rezolucja Madrycka*"), które obejmowały zasady ukierunkowane na ochronę danych osobowych poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych (Zasada 20 - Środki bezpieczeństwa) i środków proaktywnych, w tym okresowe wdrażanie

[1] Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności, Grupa Robocza ds. Wskaźników Ochrony Danych *„Polegając na Rzecznikach: Wysoki poziom wyników Spisu 2017 ICDPPC"* (2017) https://globalprivacyassembly.org/icdppc-census-report-2/.

programów szkoleniowych, edukacyjnych i informacyjnych oraz audytów przez niezależne strony (Zasada 22 - Środki proaktywne);

Przypominając, że 32. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności w 2010 r. postanowiła zachęcić do przyjęcia Podstawowych Zasad Prywatności w Fazie Projektowania jako domyślnego sposobu działania organizacji;

41. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności postanawia wezwać:

1) TYCH CZŁONKÓW Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności, którzy zbierają, analizują i publikują statystyki dotyczące naruszeń ochrony danych osobowych zgłoszonych w ramach dobrowolnego lub obowiązkowego systemu zgłaszania naruszeń ochrony danych osobowych, do:

i. klasyfikowania i zgłaszania przyczyn naruszeń ochrony danych osobowych oraz do rozważenia dodania kategorii naruszeń, które są wynikiem czynniku ludzkiego; oraz

ii. ciągłego uwzględniania zaleceń organów eksperckich, takich jak OECD czy Grupy Roboczej ICDPPC ds. Wskaźników Ochrony Danych, dotyczących pomiaru naruszeń danych osobowych.

2) WSZYSTKICH CZŁONKÓW Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności do promowania odpowiednich zabezpieczeń w celu zapobieżeniu błędom ludzkim, które mogą prowadzić do naruszeń ochrony danych osobowych, w tym:

i. Tworzenia kultury w miejscu pracy, w której prywatność i bezpieczeństwo danych osobowych stanowić będą priorytety organizacyjne, poprzez m.in. okresowe wdrażanie programów szkoleniowych, edukacyjnych i informacyjnych dla pracowników na temat ich obowiązków w zakresie prywatności i bezpieczeństwa oraz wykrywania i zgłaszania zagrożeń dla bezpieczeństwa danych osobowych;

ii. Ustanowienia solidnych i skutecznych praktyk, procedur i systemów ochrony danych i prywatności, w tym poprzez:

a. uwzględnianie prywatności w fazie projektowania, wykorzystanie systemów i praktyk i zarządzanie nimi oraz inwestowanie w poprawę ogólnego stanu zabezpieczeń zgodnie ze znanymi zagrożeniami dla bezpieczeństwa; oraz

b. na poziomie użytkownika: wdrażanie technologii uzupełniających edukację użytkowników w zakresie ograniczania ryzyka naruszenia danych uwierzytelniających i nieumyślnego ujawnienia danych osobowych nieuprawnionym odbiorcom;

iii. Dokonywania oceny praktyk, procedur i systemów ochrony prywatności w celu zapewnienia ciągłej skuteczności, w tym poprzez wdrożenie proaktywnego przeglądu, tj. monitorowania systemów i przeprowadzania audytów.

3) WSZYSTKICH CZŁONKÓW Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności do współpracy z odpowiednimi sieciami międzynarodowymi i regionalnymi w celu promowania niniejszej rezolucji.

4) ORGANIZACJE (W TYM RZĄD I PRZEDSIĘBIORSTWA PRYWATNE), aby zrozumiały i uznały, że naruszenia ochrony danych osobowych często dotyczą czynnika ludzkiego i podjęły działania wdrażające odpowiednie zabezpieczenia, które mogą obejmować zabezpieczenia wymienione w punkcie (2) powyżej.