Transkrypcja webinarium „Cyberzagrożenia- czego boją się Polacy?"

Dzień dobry, witamy na webinarium "Cyberzagrożenia - czego boją się Polacy". Temat wymagający, ale mamy solidne podstawy, aby się nim zająć w postaci autorskiego raportu z badań oraz oczywiście znakomite grono ekspertów, które zgodziło się je dla nas skomentować. Cyberzagrożenia pojawiły się wraz z cyfrową rewolucją, której wciąż jesteśmy, drodzy Państwo, świadkami. A ostatnie lata związane z pandemią, czy geopolityka pokazują niezwykłą wagę tego zagadnienia. W dzisiejszych czasach przeciętny ośmiolatek, zanim ukończy studia, spędzi ponad 10 000 godzin grając w gry komputerowe, oczywiście najczęściej w sieci, wyśle ponad 200 000 maili, przesiedzi przed telewizją ponad 10 000 godzin. Dla ciekawości dodam, że na czytanie książek przeznaczy zaledwie 4 do 5000 godzin. Rozwój internetu i nowych mediów jeszcze bardziej pokazuje dynamikę tych zmian, której jesteśmy świadkami. Tej swoistej rewolucji, która wciąż ma miejsce. Aby pozyskać 50 000 000 użytkowników radio potrzebowało aż 38 lat, telewizja 13-tu, a internet zaledwie 4. Dzisiejsze platformy internetowe, społecznościowe przede wszystkim tworzą najliczniejsze państwa na świecie. Ogrom informacji, z jakimi codziennie spotykamy się podczas naszego życia, spowodowało zjawisko zwane attention crush, czyli tzw. zablokowanie uwagi odbiorców. Codziennie wchłaniamy ponad 100 000 słów, w każdej minucie wysyłamy 12 000 000 SMS-ów, a każdego dnia prawie 300 000 000 000 maili. Syndrom zmęczenia informacją powoduje drodzy Państwo, że coraz więcej osób nie jest w stanie przyswoić nawet wiadomości. Mamy problemy z ich zrozumieniem, nie mówiąc o ich selekcji. Mija ponad 30 lat, kiedy analityk gier komputerowych Mark Prensky w magazynie "On the Horizon" opublikował znamienite dzieło, artykuł na temat cyfrowych tubylców i cyfrowych imigrantów, pokazując przepaść, jaka tworzy się w społeczeństwie. Od tego czasu zagrożeń niestety tylko przybywa.

Podczas dzisiejszego wydarzenia zostaną zaprezentowane wnioski z badania "Ochrona danych osobowych w 2022 roku", które przedstawiliśmy w dwuczęściowym raporcie - "Wiedza na temat bezpieczeństwa danych osobowych w Polsce" oraz "Cyberzagrożenia - czego boją się Polacy", która stanowi tytuł naszego dzisiejszego webinarium. Dla mnie to badanie stanowi swego rodzaju rejestr ryzyk. Dla każdej z osób fizycznych, jak i administratorów. Dzięki temu badaniu udało nam się, drodzy Państwo rozpoznać, czy Polacy mają świadomość nowych zagrożeń, jak sobie z nimi radzą, aby im przeciwdziałać, żeby z jednej strony minimalizować ich skutki, a z drugiej, żeby po prostu do nich nie dopuścić. To już druga edycja badania, które przeprowadził serwis ChrońPESEL.pl oraz Krajowy Rejestr Długów pod patronatem Urzędu Ochrony Danych Osobowych, który organizuje dzisiejsze webinarium. W pierwszej części naszego

dzisiejszego spotkania chciałbym Państwa serdecznie zaprosić do zapoznania się z wynikami badań, które przedstawi Pan Andrzej Kulik, rzecznik prasowy KRD. Po prezentacji wyników badania w drugiej części naszego spotkania odbędzie się debata z udziałem ekspertów, którą poprzedzi wystąpienie pana dr. inż. Jacka Oko, Prezesa UKE. Bardzo serdecznie już w tej chwili dziękujemy. A w samej debacie wezmą udział Pani dyrektor Monika Krasińska z Departamentu Orzecznictwa i Legislacji w UODO, Pani Dorota Grudzień-Barbachowska, dyrektor Departamentu Polityki Konsumenckiej w UKE, Pan Bartłomiej Drozd, ekspert serwisu chronPESEL oraz Pan Wiesław Paluszyński, Prezes Polskiego Towarzystwa Informatycznego, przewodniczący Sektorowej Rady do spraw Kompetencji Telekomunikacja i Cyberbezpieczeństwo.

Drodzy Państwo, nie przedłużając, zapraszam do wysłuchania prezentacji Pana Andrzeja Kulika, który widzę, że już jest gotowy. A w trakcie całego spotkania zapraszam do zadawania pytań, na które odpowiedzi przewidzieliśmy tuż po debacie. Panie Andrzeju, oddaję głos.

Dziękuję. Dzień dobry Państwu, bardzo się cieszę, że mogę dzisiaj Państwu zaprezentować wyniki tego badania, o którym wspominał pan Adam Sanocki. Cieszę się też przede wszystkim Państwo przyjęli nasze zaproszenie na webinar. Cyberzagrożenia to jest temat coraz bardziej modny, coraz bardziej głośny. No pewnie, dlatego że to zjawisko przybiera na sile. Oczywiście, za chwilę Państwu przedstawię wyniki badania, które przeprowadziliśmy pod koniec marca, wspólnie z ChrońPESEL i Krajowy Rejestr Długów pod patronatem Urzędu Ochrony Danych Osobowych. Wyniki tego badania zapisane w dwóch raportach, o których pan Adam Sanocki wspominał przed chwilą, są dostępne na stronie serwisu chronPESEL.pl i na stronie Urzędu Ochrony Danych Osobowych w Aktualnościach. Zachęcam do ich pobrania, do zapoznania się z tymi wynikami. Gdybym miał tak w skrócie scharakteryzować, streścić wynik tego badania i odpowiedzieć na pytanie "Czy Polacy wiedzą, jakie zagrożenia czyhają na nich w cyberprzestrzeni, z jakimi konsekwencjami się to wiąże i jak się przed nimi bronić?" to powiedział bym tak, że jest znaczny postęp w porównaniu, jeszcze z czasem sprzed 5 lat, kiedy tak naprawdę większość Polaków uważała, że jedynie zagrożenie dla ich bezpieczeństwa, czy bezpieczeństwa ich danych osobowych było tylko wtedy, kiedy utracili dowód osobisty. Dzisiaj już rozumiemy, że dowód osobisty jest tylko jednym z wielu nośników danych osobowych. Jego utrata, nawet jeżeli będziemy ten dowód trzymali w bezpiecznym miejscu, nie stracimy go, nigdy nie udostępniamy nikomu, kto nie jest do tego powołany, to i tak nasze dane osobowe nie są bezpieczne, bo one są zgromadzone w wielu różnych miejscach. I co do części jakby, mamy możliwości reagowania, znaczy możemy je zabezpieczyć. Czyli te miejsca, gdzie sami przechowujemy te dane, ale są też takie miejsca, na których sposób działania, zabezpieczenia nie mamy wpływu. I ta świadomość jest coraz większa, ale wydaje mi się, że ciągle jeszcze niewystarczająca i to będziemy też Państwu chcieli tutaj

pokazać w tym badaniu i myślę, że pojawi się ten wątek też w dyskusji. Tylko ja niestety nie mogę przewinąć prezentacji do kolejnego slajdu. Bardzo bym prosił o wsparcie ze strony…

Panie Andrzeju, Ewelina Janczylik-Foryś z tej strony. Już działamy, mam nadzieję, że za chwilę będzie mógł Pan przewinąć prezentację.

Tak, mamy małą przerwę techniczną. Za chwilkę będę mógł tą prezentację dalej Państwu… o już, już mamy. Dziękuję bardzo. Proszę Państwa, więc na poziomie deklaracji ta świadomość zagrożeń, świadomość własnych umiejętności w zapewnieniu bezpieczeństwa swoich danych osobowych jest bardzo wysoka. Gdy w tym badaniu, o którym wspominałem, zapytaliśmy, "Czy potrafisz zadbać o bezpieczeństwo swoich danych osobowych ?", to ponad 90% ankietowanych deklarowało, że wie, w jaki sposób zadbać o to bezpieczeństwo. No ale to jest taki wynik powiedziałbym nie do końca odpowiadający prawdzie, bo gdy dopytaliśmy bardziej szczegółowo, to takich zdeklarowanych zwolenników pewnych na 100 procent jest tylko 17 procent. Całej reszcie wydaje się, że są w stanie zadbać o bezpieczeństwo tych danych osobowych. A gdy pogłębiliśmy jeszcze to pytanie okazało się, że tak naprawdę mamy wiedzę, albo wydaje nam się, że mamy wiedzę na temat tego, jak rozpoznać fałszywy e-mail, fałszywy SMS, fałszywy telefon, którym ktoś próbuje, podszywając się pod kogoś innego, czy pod Sanepid, na przykład, to było bardzo modna forma oszustwa w czasie pandemii, czy pod jakiś inny urząd czy instytucję, podszywając się pod ten urząd czy instytucję próbuje od nas te dane osobowe wyłudzić. Jest to w zasadzie jedyne oszustwo, które prowadzi do utraty danych osobowych, które zdaniem większości potrafimy rozpoznać, aczkolwiek nie do końca jesteśmy pewni, że w 100 procentach.

Jakie natomiast Polacy identyfikują źródła zagrożeń dla danych ich osobowych. To się nie zmieniło od zeszłego roku. Mamy mniej więcej, mniej więcej ta kolejność też jest taka sama, czyli najwyżej w hierarchii to są wyłudzenia przez oszustwo, tu przed chwilą też o tym wspominałem, że to jest jedyne zagrożenie dla danych, które w miarę dobrze potrafimy już teraz rozpoznawać. Na drugim miejscu wycieki danych z firm prywatnych i instytucji publicznych, a na końcu atak hakerów na telefon lub komputer.

Tylko gdyby rozebrać to jeszcze, ten wynik na czynniki pierwsze to okazałoby się, że ta kolejność jest trochę inna. Bo myśmy zsumowali tutaj wycieki danych z firm prywatnych i instytucji i razem daje to 34%, ale jak pytaliśmy o to osobno, to mamy 19% respondentów obawia się wycieku danych firm prywatnych, a 15% z

instytucji, czyli jakby większość Polaków identyfikuje te zagrożenia w takiej kolejności: wyłudzenie przez oszustwo, atak hakerów na telefon lub komputer, wycieki danych. To pokazuje, że ciągle jeszcze właśnie nie jesteśmy w stanie zrozumieć, że te nasze dane, że ochrona tych naszych danych, nie do końca jest od nas tylko i wyłącznie zależna. Bo przecież nasze dane są w wielu miejscach i nawet szczerze mówiąc pewnie wiele osób nie wie do końca w ilu tych miejscach, te dane są zgromadzone. Mam nadzieje, że ten wątek pojawi się też w dyskusji, która się po prezentacji rozpocznie. No bo każdy z nas był pewnie w przychodni, wiele osób było w szpitalu i tam te dane osobowe łącznie z PESEL-em, imieniem, nazwiskiem, adresem są dostępne. A jak te instytucje są chronione, no w różny sposób, nie zawsze prawidłowo. Czyli widać, że jest duża świadomość zagrożenia utraty danych osobowych, natomiast nie do końca mamy jeszcze zidentyfikowane no gdzie są te największe zagrożenia dla danych osobowych, i że nie zawsze od nas tylko i włącznie zależy to czy te dane będą bezpieczne i czy ktoś zrobi z nich niewłaściwy użytek albo nie zrobi, bo nie będzie miał do nich dostępu.

Kolejne pytanie, kiedy już wiemy, gdzie tkwi niebezpieczeństwo, no to co zrobić, gdy nastąpi takie zdarzenie, gdzie te dane są zagrożone. No tutaj się okazuje już przypominam Państwu, że 90% respondentów twierdziło, że potrafi zadbać o to bezpieczeństwo, natomiast gdy nastąpi już jakieś zdarzenie, okazuje się, że ten odsetek osób, które wiedzą, co zrobić w takim przypadku jest znacznie, znacznie mniejszy. Czyli widać, że tracimy już taką pewność siebie, którą wykazaliśmy wcześniej. W przypadku próby wyłudzenia danych osobowych zaledwie, no nieco więcej [niż] ponad połowa respondentów twierdzi, że wie, jak postępować. W przypadku, kiedy nastąpi wyciek danych jeszcze mniej, bo 46%, a 41% wtedy, kiedy nastąpi atak hakerski. Jak konkretnie reagujemy? Proszę zwrócić uwagę, że tutaj powiem tak naprawdę w różnej konfiguracji, w różnej kolejności dwa działania, które podejmujemy. Czyli zgłoszenie na policję i zmiana hasła. To też pokazuje, że nie do końca radzimy sobie z taką sytuacją, kiedy już wiemy, że te dane zostały przejęte przez osoby niepowołane, przez przestępców, którzy mogą z nimi coś zrobić. No zgłoszenie na policję jest niewątpliwie wskazane, tak, ale to bardziej chodzi o to, żeby mieć takie zabezpieczenie, jeżeli ktoś te dane wykorzysta w taki sposób, że np. wyłudzi na nasze dane, jakieś świadczenie, umowę, pożyczkę, no to wtedy mamy takie zaświadczenie, że to nie my, co pozwoli jakby uniknąć kłopotów. Zmiana hasła. Proszę Państwa, jeżeli to też pokazuje, jak rozumiemy pojęcie danych osobowych. Zmiana hasła w przypadku, kiedy stracimy PESEL, jest do niczego nam nieprzydatna, bo ona przed niczym nas nie chroni. Zmiana hasła oczywiście wtedy, kiedy np. blokujemy dostęp do konta bankowego albo do konta w serwisie społecznościowym. Rzeczywiście ta zmiana jest przydatna. W przypadku utraty PESEL, ona nic nie daje, bo ten sam PESEL jest tym „towarem", który jest bardzo pożądany przez przestępców i przy wykorzystaniu tego PESEL-a w

połączeniu z naszym imieniem, nazwiskiem, mogą dokonywać przestępstw. Mamy jeszcze zgłoszenie do Urzędu Ochrony Danych Osobowych. No tak, to jest też właściwe działanie i najmniej bo zaledwie 1/4 respondentów, w przypadku wycieku danych uważa, że należy sprawdzić swoje dane w Biurze Informacji Gospodarczej, czyli tam, gdzie są rejestrowane np. wszelkie zapytania z banku czy z firmy pożyczkowej o to, czy posiadacz takiego PESEL-u jest zadłużony bądź nie. To się dzieje tylko wtedy, kiedy np. posiadacz lub w jego imieniu, ktoś, kto tymi danymi dysponuje próbuje zaciągnąć kredyt lub pożyczki.

Fajne pytanie, jakie zadaliśmy to, czy respondenci, czy Polacy wiedzą, jakie są konsekwencje utraty danych osobowych. Tutaj też 2/3 ankietowanych, czyli bardzo wysoki odsetek, deklaruje, że wie, jak mogą być te konsekwencje.

Natomiast już ta lista tych konsekwencji wskazuje to, o czym przed chwilą mówiliśmy, że my chyba nie do końca jeszcze rozumiemy, co się kryje pod pojęciem tych danych osobowych, jakie to są dane. Kiedy 86% respondentów wskazuje, że mogą przestępcy zaciągnąć zobowiązania finansowe na te wyłudzone dane, no to jest to właściwe rozumienie tej definicji. Mogą założyć firmę na nasze dane, na które zaciągną kolejne zobowiązania finansowe, 64% wskazań to również jest właściwe rozumienie. Natomiast, jeżeli spora grupa respondentów, bo 2/3 mówi, że, podszywając się pod nas, mogą próbować oszukać naszych przyjaciół lub rodzinę albo mogą nas szantażować w celu uzyskania korzyści finansowych, to jest 51% wskazań. To tak naprawdę okazuje się, że spora grupa Polaków pod pojęciem, pod terminem dane osobowe rozumie tak naprawdę tożsamość, bo przecież przy wykorzystaniu numeru PESEL nie można się pod nas podszyć, próbować oszukać przyjaciół lub rodzinę. Raczej prawdopodobnie tutaj ci, którzy odpowiadali w ten sposób, mieli na myśli nie wiem, włamanie się do konta na Facebooku i próba, no bardzo popularna swego czasu wśród oszustów, namawiania na jakiś tam przekazanie pieniędzy, podszywając się pod osobę znaną tym, których próbuje się oszukiwać. Natomiast interesujące jest to wskazanie, że 68% ankietowanych, że przestępcy mogą sprzedać wyłudzone dane. Czyli to wskazuje na to, że coraz więcej Polaków ma świadomość tego, że nasze dane są towarem. Takim towarem bardzo pożądanym przez przestępców. Takim samym, jak auto, które mogą nam ukraść, biżuterię, zegarek czy cokolwiek innego. Więc to niewątpliwie jest cenna i ciekawa informacja, która pokazuje, że mamy świadomość tego, że jest to rzecz, którą warto chronić. Miejmy nadzieję na to, że z każdym rokiem ta świadomość będzie jeszcze bardziej rosła. Teraz deklaracja, a czyny. Deklarujemy, że świetnie wiemy, jak poradzić sobie z wyłudzeniem danych, a jeszcze lepiej wiemy, jak zadbać o bezpieczeństwo tych danych osobowych, ale jak zestawić deklaracje z czynami to okazuje się, że już nie jest taki jasny i klarowny obraz. Przepraszam. Bo 11,5% ankietowanych przyznało, że zdarzyło im się przekazać osobom trzecim swoje dane do logowania, oraz publikować w sieci zdjęcia swoich

dokumentów. Dokumentów, wśród których często jest numer PESEL. Chyba ta rzecz, która najbardziej jest cenna wśród wszystkich tych, które składają się na definicję danych osobowych. Co ciekawe wśród tych, którzy przyznali się do tego, że przekazało takie dane, albo opublikowało zdjęcia dokumentów największą grupę stanowią osoby najmłodsze. Czyli między 18, a 24 rokiem życia, czyli te, które najczęściej deklarowały, że są absolutnie pewne, że one potrafią chronić swoje dane osobowe. Czyli widać, że to przekonanie najmłodszych Polaków o ich wiedzy na temat sposobów zabezpieczania się przed utratą, no nie idzie w parze z rzeczywistością. No jeszcze więcej, bo prawie co czwarty, ponad co czwarty badany wskazał, że zdarzyło mu się wypełnić ankietę internetową wymagającą podania danych osobowych. Oczywiście, miejmy nadzieję, że nie były to takie strony, które pozwalały po tym te dane przejąć przestępcom. Natomiast te osoby, które deklarowały, że coś takiego zrobiły, nie weryfikowały w jakiś sposób tego, czy ta strona, na której wypełniają tą ankietę po pierwsze jest wiarygodna, a po drugie czy w ogóle podanie tych danych osobowych było celowe i wskazane. Jak poradzić sobie z konsekwencjami wycieków danych? No tu jest jeszcze gorzej, bo przypominam cały czas ten pierwszy slajd, na którym pokazywałem, że 90% Polaków uważa, że wie jak chronić dane, natomiast tylko 30%, czyli 1/3 z tej grupy wie, kto powinien się zająć przeciwdziałaniem takim negatywnym skutkom tych wycieków. No i tutaj mamy też bardzo charakterystyczne postawy, więc przede wszystkim oczekujemy od innych tego, że zadbają o to, aby krzywda nam się nie stała. Na pierwszym miejscu wskazujemy policję i inne służby wymiaru sprawiedliwości czyli np. prokuratura, która powinna się czymś takim zająć. Oczekujemy, że zrobi, to też firma lub instytucja, która jest administratorem danych. No w sumie słusznie, bo jeżeli nie dopilnowała obowiązku, no to powinna też wesprzeć nas w takich działaniach ochronnych, Urząd Ochrony Danych Osobowych, inspektorzy ochrony danych osobowych, tych instytucji i firm, w których te dane wyciekły, ale na samym końcu osoba, której dane wyciekły. Proszę Państwa, ja już mówiłem, że to jest charakterystyczne. My to często obserwujemy, że tak naprawdę, kiedy coś staje się, dzieje się na naszą szkodę, ale nie jest przez nas spowodowane, to my oczekujemy, że inni podejmą za nas trud tego, żeby zadbać o to, aby krzywda nam się nie stała, żebyśmy nie ponieśli z tego tytułu żadnych konsekwencji czy strat. Ja zawsze sobie przypominam w takiej sytuacji takie trochę inne oszustwo, którego na zasady można powiedzieć wpadłem. Otóż kiedyś dostałem wezwanie ze straży miejskiej we Wrocławiu, że parkowałem w miejscu niedozwolonym. No i na tym wezwaniu był podany numer rejestracyjny mojego samochodu. Oczywiście numer się zgadza, natomiast marka się nie zgadzała auta. No i mogłem zrobić coś takiego, co wiele osób robi, uznając, że skoro to nie jest moje auto, czyli jakaś pomyłka, to w ogóle wyrzucam to pismo do kosza i nic z tym nie robię. Oczywiście konsekwencja byłaby taka, że prawdopodobnie albo inspektor skarbowy

pobrałby mi z konta mandat albo komornik za to złe parkowanie. No ja byłem bardziej aktywny. Czyli zadzwoniłem do straży miejskiej i powiedziałem, że numer się zgadza, ale marka nie, w związku z tym prawdopodobnie jest to pomyłka. No i okazało się, że rzeczywiście mieli dużo zgłoszeń takich, że przestępcy podszywali się, że stosowali sfałszowane tablice rejestracyjne. No i w ten sposób jakby też działali na szkodę posiadaczy tych prawdziwych samochodów. Taka sama postawa występuje tutaj. To znaczy my oczekujemy, że jeżeli nie zawiniliśmy, to ktoś inny ma się tym zająć, sami nie podejmujemy żadnej aktywności, a to jest niestety teoretycznie słuszna postawa, natomiast konsekwencje tego mogą nas dotknąć. Bo mechanizm, kiedy np. na nasze dane osobowe zostanie zaciągnięta pożyczka lub kredyt jest taki, że ta pożyczka, kredyt ktoś będzie windykował. Zanim my wybronimy się z tego, trochę czasu to potrwa. Więc z tym wydaje mi się, że tutaj musimy większą wagę przywiązywać też do takiej edukacji wśród Polaków, żeby wskazywać, że jednak ich aktywna postawa też powinna być, jest wskazana w tym, żeby niwelować te skutki wycieku danych i ich negatywne konsekwencje. Ciekawy fragment badania dla administratorów baz danych. Pytaliśmy też w tym badaniu co w przypadku wycieku powinien zrobić taki administrator. Też ciekawy wynik. Przede wszystkim jesteśmy zainteresowani tym, żeby nas poinformować o tym wycieku. Poinformować jakie dane wyciekły. Wdrożyć działania, które zmniejszą ryzyko ponownego wycieku. Proszę zwrócić uwagę, że wskazuje na to 57% respondentów, a tylko 44% oczekuję, że otrzyma jakieś wskazówki, co powinni zrobić, żeby zminimalizować skutki tego wycieku. Czyli znowu taka bierna postawa, w zasadzie oczekujemy, że ktoś za nas rozwiąże problem, a my nie chcemy się w to w żaden sposób angażować. No i czego od administratora danych, bazy danych oczekują osoby, których dane wyciekły? 53% oczekiwałoby wsparcia prawnego. Czyli widać znamy już konsekwencje tego, jak to się może źle dla nas skończyć. 52% oczekiwałoby pokrycia kosztów wsparcia prawnego oraz ewentualnych konsekwencji wycieku. A 39% ankietowanych chciałoby otrzymać rekompensatę z tej firmy, z której dane wyciekły. To tyle, jeżeli chodzi o wyniki badań. Powtórzę jeszcze raz, że są dostępne na stronie serwisu ChronPESEL.pl i na stronie uodo.gov.pl. Zachęcam do ich pobrania, do zapoznania się z tymi raportami. No i mam nadzieję, że będą one teraz przedmiotem debaty i naszych ekspertów znakomitych, ale też zachęcam Państwa do zadawania pytań, udziału w tej dyskusji, w czacie, który jest dla Państwa dostępny. Dziękuję bardzo.

Panie Andrzeju bardzo, bardzo serdecznie dziękuję za tą prezentację, za przypomnienie nam wyników badań i ich komentarz, także ciekawe przykłady z Pana życia również. Dziękujemy za podzielenie się tymi informacjami. Szanowni Państwo, zanim przejdziemy do drugiej części naszego spotkania, czyli debaty chciałbym serdecznie zaprosić Pana Prezesa UKE Jacka Oko, do krótkiego wystąpienia. Mam nadzieję, że Pan Prezes jest już z nami, jest gotowy dostarczyć taką informację, że zaszczyci nas swoją obecnością. Czy

jesteśmy gotowi Drodzy Państwo, to pytanie do naszych szanownych gości. Może zanim tą krótką przerwę techniczną zagospodarujemy, mam nadzieję, że z sukcesem, to ja pozwolę sobie przypomnieć drugi punkt naszego dzisiejszego spotkania, czyli debatę, którą poprowadzi Pani Ewelina Janczylik-Foryś, zastępca rzecznika prasowego Urzędu Ochrony Danych Osobowych. Pani Ewelino, może oddam Pani w tej chwili już głos. Poczekamy na połączenie z Panem Prezesem, a Ewelina może w tej chwili Państwu jeszcze raz przypomni uczestników debaty którą, poprowadzi. Oddaję głos Ewelinie Janczylik-Foryś.

Dzień dobry Państwu. Jest mi niezmiernie miło poprowadzić dla Państwa tę część dzisiejszego spotkania, czyli debatę ekspertów. Temat naszej debaty to budowanie świadomych postaw w ochronie danych osobowych i wpływ administratora na kształtowanie zachowań Polaków. Do udziału w naszej rozmowie zaprosiliśmy ekspertów, znamienitych gości: Monika Krasińska, dyrektor Departamentu Orzecznictwa i Legislacji UODO, Bartłomiej Drozd, ekspert serwisu ChronPESEL, Dorota Grudzień-Barbachowska dyrektor Departamentu Polityki Konsumenckiej UKE oraz Pan Wiesław Paluszyński, prezes Polskiego Towarzystwa Informatycznego, ale także przewodniczący Sektorowej Rady do spraw Kompetencji, Telekomunikacja i Cyberbezpieczeństwo. Widzę, że wszyscy uczestnicy naszej debaty są obecni. Zapraszam Państwa serdecznie.

Dzień dobry.

Dzień dobry. Mam nadzieję, że mnie słychać. Witam Państwa serdecznie.

Dzień dobry.

Jeszcze zapraszam Panią dyrektor, Monikę Krasińską.

Nie wiem, czy Pani dyrektor, nie ma jakiś problemów z połączeniem, to może w tym czasie, pozwolicie Państwo, że podsumujemy tą prezentację, którą oczywiście też przedstawił dla nas Pan Andrzej Kulik, z Krajowego Rejestru Długów. Powodem, dla którego się dzisiaj spotykamy, jest prezentacja wyników badania przeprowadzonego w 2022 roku w marcu „Ochrona danych osobowych w 2022 roku". Dzięki przeprowadzonemu badaniu, mogliśmy zaprezentować dla Państwa wyniki badań właśnie przedstawione w dwóch raportach. Pierwszy to jest „Wiedza na temat bezpieczeństwa danych osobowych". Drugi to z kolei "Cyberzagrożenia- czego boją się Polacy". Proszę Państwa te wyniki badań tak jak mieliśmy okazję usłyszeć, pokazały nam czy Polacy mają świadomość zagrożeń, jak sobie radzą w sytuacjach związanych z naruszeniem ochrony danych osobowych. Czy potrafią przeciwdziałać negatywnym konsekwencjom tego typu wydarzeń. Z raportu wynika dość optymistycznie, że 90% Polaków deklaruje, iż wie, jak zadbać o

bezpieczeństwo swoich danych. Dlatego zwracam się teraz do pana Bartłomieja Drozda z taką prośbą. Przypomnijmy, jak zatem obywatele mogą zadbać o swoje dane osobowe.

Dzień dobry, witam serdecznie. No raport, tak jak przedstawił pan Andrzej Kulik, pokazuje, że z jednej strony każdy deklaruje, że wie co ma zrobić. Natomiast, jeżeli zaczynaliśmy w badaniu, dopytywać o szczegóły, to okazywało się, że niestety ta świadomość już malała, co mamy zrobić. Tutaj przede wszystkim powinniśmy jako użytkownicy internetu zachować trochę zdrowy rozsądek, bo z jednej strony trochę narzekamy na to, że rzeczywiście ta cyberprzestępczość rośnie w internecie i tych cyberzagrożeń jest coraz więcej. Z drugiej zaś strony bardzo dużo benefitów mamy jako użytkownicy internetu. No bo ostatnie czasy pokazały, że rzeczywiście od zakupów, nawet chociaż dzisiaj nasze spotkanie jest też w formie elektronicznej, tak jak widać, w związku z tym korzystamy z tych benefitów, czystych korzyść. Natomiast, jeżeli chodzi o nas, to co powinniśmy zrobić? No to ten zdrowy rozsądek, o którym wspomniałem, ponieważ cyberprzestępcy nie śpią i jak pokazują ostatnie czasy i też tutaj Andrzej Kulik o tym wspominał, mamy dużo problemów związanych z podszywaniem się pod instytucje, instytucje publiczne, pod prywatne firmy tzw. phishing. Czyli trochę ten pośpiech i ta ilość informacji, o której tutaj też pan Adam Sanocki wspominał, czyli przepływ informacji i nasza głowa już jest zmęczona, powoduje, że my trochę już nie reagujemy na pewne rzeczy i trochę nieświadomie, a wystarczy, żebyśmy się zatrzymali na sekundę, przeczytali ze zrozumieniem to co do nas trafia, te informacje, te komunikaty, które do nas przychodzą i zobaczyli, że tutaj tak naprawdę ktoś się pod nas podszył. I widać to, że było dużo tak naprawdę wyłudzeń i przestępczości, kiedy były akcje związane z covidem i podszywaniem się pod instytucje medyczne, pod pielęgniarki, pod różne fundacje, które zbierały. Później były sytuacje podszywania się pod urzędy w momencie, kiedy był spis powszechny, pod rachmistrzów. Też były głośne akcje, że ktoś dzwoni, bo potrzebuje nasz PESEL, nasze dane, bo podszywa się pod rachmistrza. Później była sytuacja kiedy jest rozliczanie PIT-u i pod urząd skarbowy ktoś się podszywa. Więc też zwracajmy uwagę tutaj przede wszystkim, no ja wiem, że tutaj grono jest głównie inspektorów. Natomiast myślę, że każdy z nas jako użytkownik internetu, jako też osoba prywatna korzystająca z dobrodziejstw techniki, ma też gro ludzi wokół siebie starszych, rodziców czy dziadków, żeby też trochę edukować w tym zakresie. I teraz trochę zwrócić uwagę na to do nas kto dzwoni, że nie możemy podawać wszystkich danych wrażliwych osobie przez telefon konsultantowi. Konsultant nie może oczekiwać od nas danych do logowania się do powiedzmy bankowości elektronicznej. To samo zwracajmy uwagę na to, co przychodzi w SMS-ach, w mejlach, w linkach, kto jest nadawcą czy tam czasem nie jest jedna literka zmieniona i już faktycznie to nie jest to. My czasami, głośna była ostatnio sytuacja, kiedy pół Polski praktycznie dostało SMS-a od jednego z największych dostawców prądu i nawet ludzie

czasami klikali i nie myśleli, że oni tam prądu nie mają. Mają w ogóle w innej firmie, tak. To też pokazuje, że my w oderwaniu od czegoś, jesteśmy w pracy tak jak teraz. Dostajemy SMSa - zaraz wyłączymy ci prąd i klikamy w link, a nawet nie myślimy, że przecież nie mamy w tej firmie tego prądu. Sprawdzić tak naprawdę, czy coś się dzieje w tej sytuacji, czy rzeczywiście, jeżeli mamy wątpliwość, czy zapłaciliśmy daną fakturę, czy coś jest nieuregulowane, zadzwońmy do naszego dostawcy, do naszej firmy z którą mamy podpisaną umowę na infolinię, którą mamy wskazaną. Sprawdźmy stronę internetową, czy ona nie jest podejrzana, czy link, który może wyglądać dziwnie, ma dziwne znaczki, to nie klikajmy, wystarczy później zadzwonić do tej firmy i się dowiedzieć czy rzeczywiście są jakieś zaległości i tak naprawdę zdrowy rozsądek i trochę takiego, takiej przerwy, jak ja powiedziałem. Zatrzymać się na sekundę, przeczytać ze spokojem, nie stresować się, dlatego, że później są takie instytucje jak Państwo, jak Urząd Ochrony Danych Osobowych i wtedy rzeczywiście też możemy się zwrócić z jakimś tematem i z problemem.

Tak jak Pan powiedział, przede wszystkim brakuje nam często ostrożności, działamy pod presją czasu. Dlatego właśnie, czy ważne są też działania edukacyjne. Widzę, że jest z nami też Pan Prezes Urzędu Komunikacji Elektronicznej, pan Prezes Jacek Oko, także Panie Prezesie, oddaje też w tej chwili Panu głos. Dziękuję za przyjęcie zaproszenia i wzięcie udziału w naszym spotkaniu.

Dziękuję bardzo. Czy mnie słychać?

Tak, słychać.

Dobrze, bo ja już byłem wcześniej tylko aplikacja, trochę dziwnie to wykryła i dopiero teraz się udało włączyć dwukierunkowo, bo słyszałem całą prezentację poświęconą badaniu. Tu troszeczkę przepraszam Państwa panelistów, za chwileczkę się wyłączę, nie przeszkadzając w bardzo ciekawej niewątpliwie dyskusji, wtrącając troszeczkę swój grosz, to bardzo ciekawa ankieta. Natomiast mam wrażenie, że zresztą widać to było po tej, też widać po tej też analizie. Szczególnie na końcu, że jako obywatele, jako użytkownicy cyberprzestrzeni mamy pewne wyobrażenie. Nasza pewność, to jest zaskakujące spadła po okresie pandemicznym, gdzie mieliśmy jeszcze wyższą pewność i przekonanie, że wiemy co robić. Sądzę, że to też jest efektem pewnych zdarzeń, które się wokół nas toczą i odbywają, czyli zwiększa się liczba, cyberprzestrzeń wymuszeń, wyłudzeń i tego typu działań. Zresztą pewno jeszcze zwiększonych sytuacją międzynarodową i konfliktem, który się blisko nas toczy, ale zwróćcie Państwo uwagę, że jedna taka istotna rzecz. Rozdźwięk między teoretyczną wiedzą albo przeświadczeniem, że wiem, a umiejętnościami czy kompetencjami rzeczywistymi, kompetencjami cyfrowymi. To jest problem, z którym się my borykamy również jako Urząd. W naszych programach właśnie bardzo mocno chcemy zwracać uwagę na edukację, na

podniesienie kompetencji, na wytworzenie kompetencji. Natomiast już na końcu prezentacji wybrzmiał jeden element, na który ja bym chciał bardzo mocno zwrócić uwagę, że ta ankieta, gdyby ją podzielić na grupy wiekowe, ona byłaby rzeczywiście, średnio stochastycznie wychodzi nam to, co jest prezentowane. Jednak warto według mnie analizować również te grupy wiekowe, iż mamy co najmniej dwie szczególnie narażone. Wybrzmiało to narażenie w stosunku do młodych ludzi, tam w przedziale 18 - 24. Ja bym się bardzo mocno zastanawiał nad tym wcześniejszym wiekiem, gdzie jest pewien element badania otoczenia, odkrywania świata, który wygląda bardzo, bardzo ciekawie. Internet otworzył mnóstwo drzwi. Pytanie czy wszystkie drzwi są otwarte w sposób pozytywny. Czy ktoś za tymi drzwiami nie chce skorzystać z łatwowierności, z tych elementów takich bardzo mocno prywatnych, jak mówimy o prywatności. Ja bym tu rozmawiał nie tylko o tożsamości. Oczywiście dane osobowe, ochrona danych osobowych, to są głównie dane, które mówimy o PESEL-u, mówimy o danych identyfikacyjnych, czy np. o numerze rejestracyjnym samochodu itd. czy o tych wszystkich elementach. Zwróciłbym jednak bardzo mocny nacisk na to pokolenie wchodzące do życia i powierzanie przez nich swoich danych prywatności, obrazów w przestrzeń nie wiadomo dla kogo, a efekty tego są potem postrzegane w bardzo mocnych presjach, naciskach, wyłudzeniach itd. Czyli cały ten problem, z którego np. rodzice, co wynika również z badań UKE, mam nadzieję Pani dyrektor Grudzień-Barbachowska o tym też wspomni, wynika, jak mało rodzice wiedzą, co robią ich nastoletnie dzieci, które wychowują się praktycznie od urodzenia co najmniej ze smartfonem w ręce. To jest pokolenie, które się urodziło ze smartfonem w ręce, czyli z dostępem do internetu mobilnym. W każdym miejscu gdzie są. Zwróciłbym uwagę również jak mówimy o danych osobowych, czemu, możemy się zastanawiać, czemu ta młoda grupa ludzi tak dąży. Może mamy tą obawę przed odrzuceniem, że zjawisko, w którym nie ma nas na sieci, to nas nie ma tak, czyli te wszystkie zjawiska FOMO [ang. Fear of Missing Out- lęk przed pominięciem] itd., z którymi się spotykamy, to jest warte uwagi. Czy mamy z tego powodu się wstrzymywać w rozwoju aplikacji, budowania przestrzeni cyfrowej? Absolutnie nie. Rozwój tej przestrzeni, to jest tak naprawdę rozwój gospodarki. Zobaczcie Państwo, ile odkryliśmy jako społeczeństwo możliwości działania w okresie pandemii, kiedy zostaliśmy zmuszeni do skorzystania z narzędzi, nazwijmy to cyberpracy zdalnej, komunikowania się poprzez narzędzia komunikacji elektronicznej. Za tym rozwojem idzie rozwój zagrożeń i zawsze idzie grupa ludzi, która będzie chciała z tych zagrożeń czerpać swoje prywatne, własne korzyści, o których tu znakomicie zaprezentował Pan dyrektor we wstępie i pan Bartłomiej również zaczął na to wskazywać. Jeżeli mówimy o roli UKE, pani Dyrektor na pewno lepiej powie, ale tutaj uczestniczymy aktywnie chociażby w przygotowaniu platform pod walkę z SMS-phishingiem czy smishingiem, możemy to tak nazywać. Zastanawiamy się, jak ograniczyć spoofing czyli narzędzia komunikacji, które mogą służyć

właśnie potem w kolejnych krokach do wymuszania, do zdobywania danych. Bowiem kompetencje cyfrowe, co ta ankieta bardzo dobrze pokazała, to jest rozdźwięk między ja myślę, a ja wiem i ja potrafię. Martwi mnie natomiast bardzo to, że mało osób, stosunkowo mało, bo mniej niż połowa oczekuje rekomendacji, nie oglądamy, nie korzystamy z po pierwsze instytucji, które tu były wymienione w tej ankiecie. Mnie zmartwiło bardziej to, że w tej ankiecie nie pojawiła się żadna instytucja powoływana przez ustawy o krajowym systemie cyberbezpieczeństwa. Żaden z CIRT-ów, CERT-ów nie funkcjonuje w świadomości, ISAC-i, które funkcjonują, które budujemy. Dzisiaj ludzie nie czekają, z tego wynika, nasi respondenci, nie czekają na rekomendację, na dobre praktyki, nie czytają tego. O tym też trzeba mówić, trzeba ich uczulać. No i druga grupa, o której warto mówić to są seniorzy. Okres senioralny, powoli patrząc na siebie również gdzieś się do tego zbliżam. Ja jestem już nauczony korzystania z narzędzi komunikacji elektronicznej, ale jest jeszcze grupa, która nie jest nauczona, która to traktuje jako zło konieczne. A przecież to jest fantastyczne narzędzie do komunikacji właśnie, gdzie mamy problemy z ruchomością, z dostępem, z różną lokacją w różnych miejscach fizycznie, a z możliwością porozmawiania. Ale jednocześnie, przez to zwiększa się to zagrożenie, a świadomość w tej grupie, tego takiego klikania z głową. To jak mówimy o tych akcjach, ale tak, czyli rozumnie, rozsądnie, z refleksją. Ile razy w emocjach nam wszystkim zdarzyło się nieracjonalny link kliknąć, żeby zobaczyć, co tam jest, bo się spieszę. Mimo, że mamy świadomość, a ludzie, którzy tej świadomości nie mają będą bardziej podatni. Sądzę, że ta dyskusja bardzo mocno podkreśli, te elementy i taką ogólną refleksję, że warto edukować, warto rozmawiać, a sądzę, że Urząd Ochrony Danych Osobowych jest jednym z wiodących miejsc, który takie akcje powinien prowadzić. No bo mówimy o tożsamości, mówimy o prywatności, czyli mówimy o naszych danych, bo podejrzewam albo mam przeświadczenie, że będziemy jednak rozszerzać ten pakiet danych, które uważamy za dane osobowe. Czyli wszystkie te elementy, które umożliwiają jakby indywidualizację, a jednocześnie identyfikację nas jako podmiotów, jako podmioty niestety, przedmioty wręcz czasami działań cyberprzestępców czy cyberprzestępczości. Dziękuję bardzo.

Panie prezesie, bardzo dziękuję za podzielenie się tymi spostrzeżeniami, taką analizę naszych wyników przeprowadzonego badania. Podjął Pan faktycznie bardzo ważne kwestie, na które my także jako prelegenci dzisiejszej debaty chcemy zwrócić uwagę. Mówił o tym Pan Prezes jak ważne są kampanie edukacyjne i pomimo takiego optymistycznego przekonania, że wiemy, jak zadbać o bezpieczeństwo danych osobowych to nadal trzeba jednak edukować. Urząd Ochrony Danych Osobowych od wielu lat prowadzi taki program edukacyjny "Twoje dane - Twoja sprawa" i wspólnie również z UKE prowadziliśmy webinarium dotyczące bezpieczeństwa w sieci "Klikam z głową". Prosiłabym Panią dyrektor Grudzień-Barbachowską, aby nam coś więcej Pani powiedziała o tym programie.

Halo. Dzień dobry wszystkim jeszcze raz. Witam serdecznie i dziękuję za zaproszenie, bo temat ochrony danych osobowych, cyberprzestępczości, budowania kompetencji cyfrowych Polaków, obywateli jest dla Urzędu Komunikacji Elektronicznej szczególnie ważny. Tak proszę Państwa, my od wielu, wielu lat prowadzimy działalność edukacyjną, bo Urząd Komunikacji Elektronicznej to nie tylko regulacja i regulacja rynku telekomunikacyjnego, pocztowego czy działania operacyjne zmierzające do zabezpieczenia interesów użytkowników końcowych. Natomiast również to są właśnie działania edukacyjne, które zmierzają do zapewnienia dobrostanu konsumentów, klientów usług cyfrowych. My proszę Państwa wiele lat temu zaczęliśmy edukować seniorów, zaczęliśmy edukować młodzież. Mówiliśmy o tym, jak podpisywać właściwie umowy telekomunikacyjne, na co zwrócić uwagę w świecie realnym. Na co zwrócić uwagę, jak przychodzi do ciebie akwizytor i chce sprzedać tobie usługę tak telekomunikacyjną czy usługę innego typu. Jak się zabezpieczyć w takiej sytuacji, jak nie popadać właśnie w..., jak nie dać się zwieść tym wszystkim działaniom socjotechnicznych, które stosują właśnie przedstawiciele najróżniejszego typu firm. I proszę Państwa, z czasem, jak robiliśmy ewaluację naszych projektów, rozmawialiśmy też z uczestnikami tych naszych spotkań. Zauważyliśmy bardzo głęboką potrzebę spojrzenia też na temat cyberbezpieczeństwa, na temat edukacji cyfrowej, na temat digitalizacji procesów, uczenia właśnie o tym wszystkich grup klientów, konsumentów. Proszę Państwa, my dwa lata temu rozpoczęliśmy nową kampanię, bo te kampanie coraz ewoluują, która jest, jakby kontynuacją właśnie kampanii "Klikam z głową", czyli bądź bezpieczny w sieci de facto, zachowaj rozum, zachowaj rozsądek, zatrzymaj się. To, o czym pan Bartłomiej mówił, zatrzymaj się na chwilę. Przeczytaj, tak. Tak jak w świecie realnym, tak w świecie wirtualnym, przeczytaj, zobacz w co klikasz. Zaczęliśmy proszę Państwa działać w obszarze właśnie usług cyfrowych i rozpoczęliśmy nową kampanię "Ja online", która jest konsekwencją właśnie tych działań, wstępnie działań edukacyjnych dotyczących projektu "Klikam z głową". I my proszę Państwa z wielką przyjemnością muszę powiedzieć, podjęliśmy działalność, współpracę z Urzędem Ochrony Danych Osobowych, ponieważ każdy z nas zarówno Urząd Komunikacji Elektronicznej, jak i Urząd Ochrony Danych Osobowych ma swoich klientów. Dociera do określonej rzeszy użytkowników, więc z wielką przyjemnością podjęliśmy tą współpracę i udało nam się chyba w bardzo fajny sposób połączyć zarówno Państwa tematykę, czyli ochronę danych osobowych, właśnie z tym elementem komunikacji elektronicznej, cyfryzacji, digitalizacji procesów w jakich uczestniczą klienci, konsumenci. Myślę, że to nie jest pierwszy i ostatni raz. Zresztą dzisiejsze spotkanie, jest również wynikiem naszej współpracy w obszarze edukacyjnym i naszym dążeniem jest myślę i UKE i UODO właśnie rozwijanie tych kompetencji obywateli. My proszę Państwa, podejmujemy szereg działań i chciałam Państwu powiedzieć w kontekście edukacji, potrzeby edukacji, cyberedukacji chciałam Państwu

powiedzieć o ostatnim naszym wydarzeniu, które zrealizowaliśmy. Na początku czerwca tego roku przeprowadziliśmy serię otwartych webinarów dla szkół - dla dzieci z szóstej, ósmej klasy. I muszę Państwu powiedzieć, że tematyka była trudna, bo to była tematyka właśnie związana z cyberprzestępczością, z problemami, które dzieci spotykają w sieci, z hejtem, z dezinformacją, z phishingiem, z przestępstwami na tle seksualnym również z ochroną danych osobowych, z budowaniem bezpiecznego, bezpiecznej przestrzeni w internecie. I proszę Państwa w ciągu kilku dni, wyobraźcie Państwo sobie na cztery nasze sesje edukacyjne zgłosiło się do nas czternaście i prawie pół tysiąca dzieciaków z całej Polski. To świadczy o tym, jak wysoka jest świadomość potrzeby edukacji też wśród nauczycieli, bo to nauczyciele ze szkół podstawowych zidentyfikowali ten problem, które mają u siebie w szkołach i zidentyfikowali potrzeby edukacyjną i zgłosili się do nas z prośbą o przeprowadzanie właśnie takich zajęć. I proszę Państwa ta ilość dzieciaków, które uczestniczyły w naszych zajęciach, jest znakiem potrzeby edukacji dzieci i młodzieży, to, o czym mówił pan Prezes Oko - od najmłodszych lat, edukacji dzieci i młodzieży w zakresie bezpiecznego korzystania z sieci, bezpiecznego korzystania z internetu, dbania o swoje dane osobowe, budowania tej świadomości dobrego działania nie tylko w życiu realnym, ale również właśnie w życiu, w tym cyber naszym życiu, które de facto no stanowi lwią część naszego 24-godzinnego czasu przebywania. Wiecie Państwo tak sobie pomyślałam, że jeszcze powiem Państwu, jak przygotowywałam się do naszego spotkania, to przejrzałam sobie dane na temat czasu spędzania przez użytkowników na świecie w sieci. I proszę Państwa, wyobraźcie sobie, że wg danych, jakie wyszukałam z raportów ten czas wynosi 6 godzin 54 minuty na dobę. Powiem szczerze, że jest mi trudno sobie wyobrazić, ale jeżeli przeanalizujemy sobie naszą aktywność zawodową, prywatną, myślę, że również w naszym…, my również jesteśmy w stanie dostrzec to, że jesteśmy uzależnieni od internetu, że korzystamy z tych usług cyfrowych, że potrzebujemy również wiedzy w tym zakresie, potrzebujemy ochrony, także i ochrony informacji na temat na temat możliwości ochrony i działań. Jeszcze mam prośbę, bo chyba padło jedno pytanie, skierowane przez uczestników naszego spotkania, bo być może o tym zapomnę, a chciałbym powiedzieć. Gdzie możemy szukać informacji o incydentach? Proszę Państwa, ja zachęcam Państwa wszystkich do przejrzenia strony CERT.pl. To jest strona, która właśnie, to jest miejsce, gdzie możemy sprawdzić informacje o naruszeniach, jakie mają miejsce w sieci. CERT.PL jest prowadzony przy NASK-u i proszę Państwa możemy tam sprawdzić informacje na temat złośliwych domen. W roku 2021 do CERT Polska trafiła informacja o ponad 33 000 złych zachowań w sieci, które dają nam też informację o tym, na co mamy uważać, na co zwracać uwagę i dają nam też to poczucie bezpieczeństwa. Także zachęcam tych wszystkich z Państwa, którzy są zainteresowani wiedzą na temat zagrożeń i budowania też kompetencji cyfrowych, jak się chronić, jak się bronić do odwiedzenia właśnie strony CERT Polska, na której możemy

uzyskać szereg informacji dotyczących aktywności cyberprzestępców, obecnie w sieci. Także proszę Państwa. Ja już nie, ja jestem gadułą, więc zabieram dużo czasu, ale proszę Państwa, cieszę się ze współpracy z UODO. Prowadzimy szereg działań edukacyjnych. Zachęcam również do wejścia na naszą stronę cik.uke.gov.pl, na której jest szereg informacji na temat kampanii edukacyjnych Prezesa UKE. Jeżeli Państwo jesteście nauczycielami, rodzicami, również zachęcam do kontaktu z nami, do współpracy. Jesteśmy chętni, jeżeli chodzi o spotkania, o prowadzenie wykładów i jesteśmy w kontakcie cały czas z obywatelami.

Zwracamy uwagę cały czas jednak na tą potrzebę edukowania i wydaje się, że można podejmować szereg różnych działań, a i tak no nieustannie należy jednak informować i budować taką świadomość w społeczeństwie, jeżeli chodzi o prawo do ochrony danych osobowych, prawo do prywatności. Zwróciliśmy też uwagę na to, że biorąc pod uwagę liczbę osób, które wiedzą, jak zadbać o swoje dane osobowe, najpewniej czują się młodzi ludzie i tak jak mówimy o tych kompetencjach cyfrowych, to pewnie oni mają, no najszerzej zbudowane te kompetencje cyfrowe. Gorzej troszeczkę wypadają osoby starsze, dlatego że z przeprowadzonych przez nas badań wynika, że niespełna 9% twierdzi, że wie, jak właśnie zadbać o swoje dane osobowe. Tak więc też część tych kampanii powinna się odnosić, jak już zaznaczyliśmy do osób starszych, prawda? Bo one są często niejednokrotnie jeszcze bardziej narażone na działania przestępców. Panie prezesie, zwracam się do pana Paluszyńskiego. W jaki sposób w takim razie zachęcić też osoby starsze, którym te technologie cyfrowe być może nie są tak bliskie, żeby zwrócili większą uwagę na to, jak w ogóle posługują się swoimi danymi, komu te dane udostępniają?

Znaczy ja chcę powiedzieć, że pojęcie osób starszych i wykluczonych cyfrowo, które funkcjonuje u nas wcale nie ma wielkiego związku z rzeczywistymi kompetencjami tych grup zawodowych posługiwania się w internecie. Były takie badania zrobione na temat rzeczywistych umiejętności dzieci w wieku szkolnym i z tego wynika, że większość tych dzieci komputerem posługuje się raz w tygodniu. W związku z tym ich kompetencje komputerowe są bardzo niewielkie. Oni w większości posługują się smartfonami i są użytkownikami tych rozwiązań, które są im dostępne i swoje dane osobowe umieszczają w dowolny sposób, w dużych ilościach na blogach, w dyskusjach, w sieci, pod postacią zdjęć, czasami głupich wypowiedzi, które do końca życia ich później będą prześladowały, bo internet niestety nie zapomina, pomimo prawa do zapomnienia, które zostało w prawie zapisane. W związku z czym ja twierdzę, że edukować trzeba wszystkie grupy społeczne. W tym też te grupy najstarsze. One się najchętniej dają edukować. Natomiast przez tą edukację my bardzo często zwalniany regulatorów i rządzących od obowiązku racjonalnego myślenia o usługach, które udostępniają tym grupom, które korzystają, użytkownikom. Tutaj w tle toczy się dyskusja o PESEL-u i ona ma już brodę w dyskusji. Wydaje się, że wreszcie najwyższy czas przerwać chocholi taniec,

że PESEL czy posiadanie PESEL-a w połączeniu z danymi osobowymi do czegokolwiek, kogokolwiek uprawnia. To jest to po prostu straszliwe uproszczenie i zwalamy później na użytkownika konsekwencje tego typu działania, gdzie wystarczy to do zaciągnięcia kupna telefonu komórkowego od operatora, karty SIM, kredytu czy innych tego typu rzeczy. Kiedy tak naprawdę nie powinno to upoważniać do niczego, ponieważ PESEL nie jest poufnym identyfikatorem znanym tylko osobie, na którą są zaciągane tego typu zobowiązania. To od dawna powinno być już dawno załatwione, że nic takiego nie może się dziać. A się dzieje. Druga sprawa: dlaczego ci, którzy świadczą usługi, nie mają dostępu do unieważnionych dowodów osobistych, do rejestru dowodów osobistych w momencie zawierania tych umów. Ja pamiętam, że wielokrotnie myśmy wnioskowali do ministra ówczesnego spraw wewnętrznych i administracji, o udzielenie takich uprawnień do weryfikacji online w oparciu o rejestry publiczne, państwowe tym, którzy są zobowiązani do świadczenia usługi. Nie można się tego doprosić, żeby ten system domknąć. Bezpieczeństwo nie jest tylko po stronie użytkownika, wręcz odwrotnie. Systemy, które są dostarczane użytkownikowi muszą być logiczne i muszą uwzględniać rzeczywiste uwarunkowania, które funkcjonują na rynku. Ostatnio wyczytałam w prasie, że coś się zmienia, bo ma być publiczny rejestr unieważnionych dowodów osobistych. Więc dlaczego jest z tym problem, bo o ile wiem, to jeżeli zastrzegam dowód osobisty, za chwilę jest w rejestr wprowadzony, jako rejestr państwowy, ale on jest poufny. Nie ma do niego dostępu. No to są jakieś absurdalne rzeczy w systemie świadczenia usług drogą elektroniczną. Najwyższy czas by było, żeby te absurdy polikwidować. Jeżeli można było wprowadzić w sektorze bankowym dwuskładnikowe uwierzytelnienie, to na pewno można zastosować też bezpieczne rozwiązanie. Tutaj nie będę mówił jakie. Fachowcy wiedzą, jak je można zastosować, żeby oparte częściowo na kryptografii. Mamy elektroniczny dowód osobisty, który mógłby być wykorzystany. Proszę Państwa, kto w banku jak popatrzy na dowód osobisty, jest w stanie patrząc na ten dokument rozpoznać, czy ta osoba na dowodzie to jest ta osoba, która stoi przed okienkiem? Przecież to jest w większości wypadków fikcyjne. Ludzie nie umieją, nie są szkoleni. Pracownicy nie są szkoleni z tego, jak mogą rozpoznać tą osobę. Trzeba wspierać ich narzędziami informatycznymi, rozpoznawania twarzy w tym celu, porównywania. Jeżeli mówimy o biometryce to ona nie jest tylko istotna z punktu widzenia użytkownika. Ona jest też istotna z punktu widzenia świadczącego usługę. My w wielu momentach publicznie zamieszczamy kontekst danych osobowych w sposób legalny, bo prawo to dopuszcza - w księgach wieczystych, w innych tego typu rejestrach, tam jest imię, nazwisko, numer PESEL. Przecież nie chodzi o to, żeby zabronić dostępu do tych ksiąg, bo istotą tych ksiąg jest właśnie zapewnienie rękojmi własności, tak? Czyli jednoznaczności, przynależności tego kawałka ziemi, której one dotyczą do określonej osoby. Tylko budowanie systemów z uwzględnieniem tego, że takie fakty mają

miejsce. Jeśli chodzi natomiast o CERT. To wszystko jest fajnie. Tylko nie wiem, co mógłby zrobić potencjalny użytkownik przeczytając, jakie są groźne domeny. Czyli już jakby, wiedział nawet, że może tam wejść do tego rejestru ostrzeżeń. On nic nie zrobi. To są ostrzeżenia, które powinni wykorzystywać dostawcy usług i firmy zajmujące się czy przetwarzające czy to dane osobowe, czy świadczący usługi elektroniczne. Potencjalny użytkownik będzie miał z tym poważny problem. U nas poziom tego co ja nazywam cyberhigieną, czyli podstawową informacją o tym, jak się posługiwać, jak się znajdować w internecie jest niski. I smutne jest, że on jest niski też w biznesie i w administracji i w firmach usługowych. On nie jest tam wyższy niż w przypadku ludzi korzystających z usług służby zdrowia czy innych tego typu powszechnych usług, które funkcjonują. No, przecież jeżeli ja idę do hotelu, to podaję numer PESEL, bo tego ode mnie żądają. Teraz już nie żądają skanu mojego dowodu osobistego, więc poprawiło się. Przez długie lata walczyłem z tym skanem dowodu osobistego, żeby go nie było. A na czym polega główny problem? Główny problem polega na socjotechniczne, która jest stosowana przez oszustów. Te scenariusze, publikowanie tych scenariuszy, przed czym się strzec, nie technicznych, ale socjotechnicznych, to jest największe zagrożenie. W tym tygodniu ja sam dostałem jedną propozycję, że moja rodzina zginęła w Stanach Zjednoczonych i bardzo proszą, żebym się kontaktował, podał dane, bo duży spadek na mnie czeka. To akurat wiem, że nie mam rodziny w Stanach Zjednoczonych, więc wyrzuciłem to od razu do kosza. A drugi to oczywiście standardowy numer. Zbliża się termin płatności za prąd, w związku z czym mam zapłacić 2,5 za rachunek, co też wylądowało w koszu. No dobrze, ale to są całe kampanie, które to robią. I w związku z czym powinny być też kampanie publiczne, społeczne, nie tylko w szkoleniach, które no rozbijają te scenariusze, które ludzi dobrej woli no oszukują, tak? Zbieranie pieniędzy na pomoc dla Ukrainy, zbieranie pieniędzy na dla osób chorych - to są wszystko scenariusze żerujące na dobrej, na emocjach [wtrącenie], na życzliwości i na emocjach naszych. No i niestety trzeba to w jakiś sposób zacząć odróżniać, a tu najczęściej ludzie starsi padają ofiarą tego typu scenariuszy, bo atak na wnuczka i na policjanta, pomimo że wielokrotnie o tym się mówi, no to jest. Ja myślę, że w tej edukacji duża część w tej chwili działania powinna też przypaść temu nowo powołanemu Biuru do Spraw Przeciwdziałania Cyberprzestępczości Komendy Głównej Policji, które zostało powołane. Tam ma być docelowo prawie kilka tysięcy policjantów zajmujących się tą działalnością, więc zakładając, że prewencja jest najlepszym elementem przeciwdziałania i ci fachowcy są bardzo dobrze opłacani, bo tam są bardzo wysokie wynagrodzenia w tej jednostce z funduszu m.in. wypracowywanego przez NASK PIB. To połączenie tego systemu, żeby te nowe scenariusze szybko były publikowane, ale jednocześnie, żeby zmienić te reguły gry świadczenia usług, żeby one były bezpieczniejsze, żeby nie tylko użytkownik odpowiadał za nierozsądne zbudowanie scenariusza usługowego od strony świadczącego usługę.

To są chyba rzeczy niezbędne, żeby cokolwiek się dało zrobić. No i edukować, edukować z cyberhigieny i edukować na wyższym poziomie, dla tych, którzy pracują w instytucjach publicznych, firmach, żeby oni wiedzieli jak się powinni zachować, żeby wiedzieli, co mają zrobić, żeby wiedzieli jak zdefiniować ryzyka, które są związane z ich biznesem.

Dziękuję, panie Prezesie. Powiedział Pan bardzo wiele ciekawych rzeczy. Ja pozwoli Pan wynotowałam trzy i chciałbym się teraz trochę zatrzymać przy tych trzech punktach, które sobie wynotowałam: PESEL, rejestry i biometria. Mówiliśmy już o tym, jak sami powinniśmy zadbać o swoje dane osobowe. I teraz poproszę o zabranie głosu panią Monikę Krasińską, dyrektor Departamentu Orzecznictwa i Legislacji w UODO. Zastanawiam się w kontekście też tych doniesień medialnych sprzed ostatnich kilku dni, właśnie czy nie potrzebujemy takiej systemowej pomocy, pomocy konkretnej instytucji, konkretnej organizacji w przypadku, gdy dojdzie np. do naruszenia naszych danych osobowych i do wycieku numeru PESEL. To jest jedno pytanie, które chciałabym skierować do pani Dyrektor. I drugie też pytanie, które także dotyka tego numeru PESEL, to często właśnie administratorzy mogą mieć wpływ na kształtowanie tych zachowań użytkowników na społeczeństwa. Dlaczego? Dlatego, że administratorzy często przy logowaniu potrzebują od nas takich informacji, jak imię, nazwisko, adres zamieszkania, adres e-mail, numer telefonu, numer PESEL. No i czy tego typu, taki szereg w ogóle danych osobowych jest potrzebny administratorowi do tego, żeby np. zweryfikować naszą tożsamość. Czy administrator potrzebuje aż tylu danych osobowych? Pani dyrektor, bardzo proszę.

Witam Państwa bardzo serdecznie. Przepraszam za problemy techniczne, ale słyszałam wszystko, a nie byłam widziana i słyszana. No właśnie, to jest ta komunikacja za pośrednictwem wyłącznie tego środowiska wirtualnego. Ta komunikacja niestety doznaje bardzo wielu ograniczeń i ryzyk. Dzisiaj mówimy o cyberzagrożeniach. Zechcę za chwilę powiedzieć, dlaczego tak bardzo my nie powinniśmy koncentrować się wyłącznie na PESEL-u jako takim, tylko w ogóle przyjrzeć się całemu modelowi funkcjonowania u nas gwarancji, które mają być zapewnione podmiotom danych, czyli osobom w rezultacie poszkodowanym bardzo często, stojącym na tej linii frontu, na z góry skazanej pozycji. Bardzo często osobom, które muszą udowadniać, że nie są przysłowiowym wielbłądem, że to nie one są dłużnikiem, że to nie one działały w jakiejś złej wierze. Bardzo często to te osoby są pozostawione same sobie na tym odcinku dalszych działań. Oczywiście istnieją pewne rekomendację, programy edukacyjne, ale mam takie wrażenie i analiza tego raportu, który jest przedmiotem dzisiejszego, naszego spotkania pokazuje, że jednak nie wszyscy jesteśmy wystarczająco świadomi konsekwencji funkcjonowania w świecie wirtualnym. Bo no oczywiście weszliśmy z takim rozpędem, z impetem w świat wirtualny, w internet, w zarządzanie cyfrowe, funkcjonowanie

cyfrowe z powodów głównie wynikających z pandemii. To przyspieszenie tak naprawdę uskuteczniła pandemia. Funkcjonujemy w tym świecie coraz bardziej intensywnie i są tego, oczywiście i pozytywy, ale też i są tego negatywy. Dzisiaj Państwo mówicie o tym, w jaki sposób jednak wciąż jest za mała ta edukacja. I zresztą czytam tutaj słowa na czacie poszczególnych uczestników naszego spotkania. Mówimy o tym zbyt wciąż niskim poziomie edukacji. O tym wciąż niskim poziomie wiedzy. No ja miałam okazję ostatnio przez kilka dni być nad polskim morzem i muszę Państwu powiedzieć, że widziałam tam masę dzieci. Większość tych dzieci siedziała w smartfonach, zamiast bawić się w piasku. Większość tych dzieci po prostu korzystała z określonych usług, zamiast rozmawiać z innymi dziećmi. Nawet wakacje nie stały się czasem odpoczynku. Oczywiście przede wszystkim jest to kwestia też tej wiedzy i edukacji, która powinna cały czas przyświecać rodzicom. To oni tutaj bardzo często też tkwią w głębokiej niewiedzy, bo stoją obok tych dzieci i też w tych smartfonach namiętnie wystukują różne komunikaty, robią zdjęcia, zamiast oglądać rzeczywistość i przesyłają je kolegom, koleżankom, rodzinie. Cały czas, w związku z tym pozostawiają swoje ślady, pokazują swoją aktywność, pokazują swoje życie. Ludzie młodzi bardzo często w ten sposób funkcjonują, bo są nauczeni właśnie takiej interakcji, interakcji cyfrowej, takiej komunikacji. Co zresztą jest przedmiotem coraz większej ilości także opracowywanych komentarzy dedykowanych uzależnieniom cyfrowym, właśnie ludzi starszych, dzieci, ludzi młodych, bo tych uzależnień od chociażby smartfonów sukcesywnie przybywa i ten problem narasta. Tutaj musi być zachowany pewien balans i o tym balansie warto zawsze także pamiętać, jeżeli mówimy o ochronie danych osobowych. To znaczy z jednej strony rzeczywiście będąc gospodarzami własnych danych, musimy mieć świadomość odpowiedzialności za te dane, które w końcu są też naszą własnością, naszym mieniem, naszym potencjałem, naszą wizytówką. Z drugiej strony oczekujemy i mamy prawo oczekiwać po stronie instytucji publicznych większego zaangażowania, większego zainteresowania, większego wsparcia i pomocy. Proszę Państwa realizujemy jako Urząd Ochrony Danych Osobowych, wespół przecież i z Panem i z innymi instytucjami, szereg różnego rodzaju programów. Podejmujemy szereg inicjatyw. Ale wciąż wydaje się, że bez takiej jeszcze większej współpracy, także międzyresortowej nie jesteśmy w stanie osiągnąć oczekiwanego rezultatu. Mówię tutaj o chociażby i programach edukacyjnych, które powinny być wpisane, również w kwestie związane z cyberzagrożeniami. Programach dedykowanych i przedszkolakom i dzieciakom w szkołach podstawowych i w szkołach średnich, studentom. Bardzo wiele osób, pomimo przecież coraz większej ilości informacji funkcjonującej w sieci, tak naprawdę dowiaduje się o zagrożeniach dopiero podejmując pracę, dopiero podejmując aktywność zawodową. Oczywiście instytucje publiczne nie zastąpią nas w rozwadze nad podjęciem ostatecznej decyzji co do danych osobowych, niemniej jednak nie zgodzę się tutaj ze stwierdzeniem, iż należy przyjrzeć się całemu modelowi funkcjonującego w

Polsce prawa, żeby dostrzec jednak pewne mankamenty. Chodzi o to proszę Państwa, żeby nie tylko tworzyć przepisy, które mają leczyć przysłowiową chorobę, ale, żeby przede wszystkim zapobiegać tej chorobie. I tutaj obawiam się, że tworzenie kolejnych wyłącznie rejestrów, gdzie mają być kolejne dane osobowe, które mają być umiejscawiane przez osoby zainteresowane, poszkodowane, nie wiem, czy spełni tak do końca zakładany rezultat. Tutaj należałoby się przyjrzeć całemu funkcjonującemu w Polsce właśnie modelowi gwarancji dla osób, których dane dotyczą, pokrzywdzonych bardzo często działaniami, zaniechaniami administratorów odpowiedzialnych za te dane osobowe. Oczywiście Urząd Ochrony Danych Osobowych będzie cały czas weryfikował i sprawdzał zgodność działań tych administratorów, tych przetwarzających z przepisami rozporządzenia o ochronie danych osobowych, ale tutaj wydaje się, że tylko i wyłącznie ta działalność na niwie ochrony danych osobowych bez zwiększenia edukacji, która w ogóle dotyczy ochrony prywatności w sieci jako takiej, ochrony godności, naszej godności także przez nas samych w sieci może przez niektórych być postrzegana jako niestety, ale tylko takie działanie nie do końca zaspokajające potrzeby społeczne. Natomiast niewątpliwie organ nadzorczy, organ do spraw ochrony danych osobowych daje wyraz, proszę Państwa, swojemu podejściu bardzo konsekwentnemu od wielu lat do tematu ochrony danych osobowych w swoich licznych decyzjach. Tutaj Państwo wskazujecie na różne wyroki. Tak są bardzo różne wyroki, które zapadają w sprawach, w których my jednak jako priorytet stawiamy sobie ochronę tej słabszej strony, czyli osoby fizycznej, dotkniętej naruszeniem. Ale prawem sądów jest rozstrzyganie w zróżnicowany sposób. My podejmujemy także działania związane z kasacjami wielu wyroków, ale też są wydawane rozstrzygnięcia, które w pełni popierają stanowisko organu nadzorczego. I teraz jeśli mówimy o takim systemowym podejściu w ogóle do ochrony danych, do zarządzania prywatnością w sieci to proszę Państwa, rzeczywiście cały czas przez wiele, wiele lat zabrakło nam takiej poważnej, międzyresortowej i interdyscyplinarnej debaty nad tym, jak mają w ogóle wyglądać dane w rejestrach publicznych. Jak mają w ogóle wyglądać konsekwencje ujawnienia tych danych. Jak tak naprawdę, dlaczego pewne dane w tych rejestrach publicznych funkcjonują. My tutaj mówimy o tym PESEL-u, proszę Państwa. I zgodzę się tutaj z uczestnikami naszego spotkania, którzy na czacie wskazują pewne delikatnie ujmując niekonsekwencje ustawodawcy, że z jednej strony ta informacja jest powszechnie dostępna w różnego rodzaju bazach i rejestrach, jak zresztą też wiele innych informacji, a z drugiej strony za ujawnienie tożsamych danych nakładane są kary. Bo jednak te dane nakazuje rozporządzenie o ochronie danych osobowych chronić. Ja mam takie wrażenie, że przy dyskusjach dotyczących dostosowania przepisów prawa polskiego do rozporządzenia o ochronie danych osobowych zabrakło takiego holistycznego spojrzenia właśnie na zarządzanie informacją w rejestrach publicznych, w systemach teleinformatycznych. I mamy dzisiaj takie

bardzo rozdrobnione i takie bardzo i nie zawsze kompatybilne rozwiązanie. Czyli coś, co jest szczególnie chronione w jednym rejestrze, w zasadzie nie podlega ochronie w innym, bo jest jawny i wykorzystywany bez żadnych reguł, bez żadnych warunków wstępnych. Tutaj zostało też wcześniej powiedziane, że tak naprawdę nie jest problemem posługiwanie się PESEL-em dla zidentyfikowania osoby. Bo rzeczywiście jest to identyfikacja za pomocą identyfikatora, który no w sposób jednoznaczny może przesądzić o tym, że Kowalski jest Kowalski. Ale problemem jest tak naprawdę uwierzytelnianie osób podających się za Kowalskich. Problemem jest to, że jednak istnieje duża łatwość pozyskania takiego zakresu informacji, który będzie bardzo łatwy w obróbce dla przestępców sieciowych i wykorzystają ten zasób dla wyciągnięcia określonych korzyści z naruszeniem praw podmiotów danych. Czyli tu trzeba się po prostu zastanowić i cały czas organ nadzorczy zachęca do takiej dyskusji, włącza się do tej dyskusji, chociażby w toku postępowań legislacyjnych. Bo przecież nie tylko organ nadzorczy zwraca ciągle uwagę na pewne niedoskonałości tworzonych rozwiązań prawnych. Ale my też rekomendujemy pewne kwestie, pokazując brak przemyślenia konstrukcji określonych przepisów, o których pewnie jeszcze będziemy mówić. Na dzień dzisiejszy mogę powiedzieć, że taka poważna debata dotycząca właśnie tego, jak ma wyglądać podejście do PESEL-a w Polsce przeprowadzona nie została. Ponieważ my, jeszcze raz mówię, my dzisiaj de facto zastanawiamy się jak uleczyć pewien stan chorobowy. Ale cały czas nie są podejmowane działania, które mają pokazać, jak zapobiec pewnym rozwiązaniom. Oczywiście rozporządzenie o ochronie danych osobowych daje pewne wytyczne. Ono mówi, że, aby zapobiec pewnym rozwiązaniom, przeprowadź analizę ryzyka, dokonaj oceny skutków dla ochrony danych, jeżeli będzie to potrzebne, przeprowadź test prywatności, zwróć uwagę, czy pewne dane są potrzebne, niezbędne. Rozporządzenie daje pewne wytyczne, ale ostateczna decyzja jest pozostawiona w zasadzie administratorom. I mamy do czynienia z bardzo zróżnicowanymi praktykami administratorów, chociażby w sektorze prywatnym, gdzie jedni dla zawarcia umowy potrzebują szeregu danych osobowych włącznie prawie, że z imieniem ojca i matki osoby posługującej się określonym PESEL-em i mamy do czynienia z takimi, którzy wymagają dosyć wąskiego zakresu danych osobowych, gdzie jest imię, nazwisko, PESEL czy adres. Adres, który umówmy się, ale przecież nie występuje na dowodzie osobistym. I tu wydaje mi się, że jednak należałoby zwrócić szczególną uwagę na to za pomocą jakich mechanizmów edukacyjnych, ale też nadzorczych z punktu widzenia właśnie organów, regulatorów należałoby podnosić te standardy ochrony danych osobowych u samych administratorów. Bo mówię samo karanie to jeszcze przecież nie jest ten element, który będzie wpływał na podniesienie wiedzy, poziomu kompetencji, czy też świadomości administratorów. Proszę Państwa, ja ostatnio na wykładzie na jednej z uczelni uzyskałam pytanie od inspektora ochrony danych, który powiedział: „Proszę Panią, przecież my jako

inspektorzy ochrony danych osobowych i tak cały czas jesteśmy zmuszani do pisania polityk ochrony danych osobowych, które później musimy sprawdzać, ponieważ robimy kontrole i audyty. Bo administratorzy cały czas uważają, że ochrona danych jest czymś formalnym, formalnym." Czyli z punktu widzenia formalnego, wystarczy określona dokumentacja. No tak nie jest, jeżeli my nie uzmysłowimy sobie, że ochrona danych, ochrona prywatności to nie jest tylko formalizm, ale to jest pewien styl bycia, pewien styl funkcjonowania firmy, pewien styl myślenia zarządu, pewien styl myślenia pracowników, nie-zastraszonych ochroną danych, ale realizujących konsekwentnie pewne programy, no to jako administratorzy jesteśmy w stanie wtedy zdziałać więcej wspólnie. A jako osoby, których dane dotyczą jesteśmy w stanie więcej, bardziej konsekwentnie od tych administratorów oczekiwać określonych zachowań. Oczywiście, dzisiaj dostrzegamy to, że administratorzy de facto oczywiście spełniają obowiązek informacyjny. Informują o naruszeniu. Ale w zasadzie osoba poszkodowana określonym naruszeniem ochrony danych osobowych sama musi borykać się z określonymi konsekwencjami działań i podejmować ten trud i wysiłek cały czas ochrony swych praw. Oczywiście jest w tym czynnie wspierana, przecież może złożyć wniosek o odszkodowanie za naruszenie przepisów o ochronie danych osobowych do sądu. Może złożyć skargę do Urzędu Ochrony Danych Osobowych, może złożyć tutaj wniosek do innych organów o zbadanie działalności określonych podmiotów. Natomiast wydaje się, że bez przeprowadzenia takiej naprawdę poważnej dyskusji czy coś możemy więcej jako państwo także zaproponować takim osobom, czy nie wprowadzić jeszcze jakiś dodatkowych mechanizmów, chociażby w przepisach branżowych. A takie mechanizmy przecież są wprowadzane w niektórych krajach Unii Europejskiej. No bez wprowadzenia tego wszystkiego, bez tej dyskusji dzisiaj możemy tak jak powiedziałam na samym początku, jedynie zastanawiać się jak zminimalizować stratę i to po stronie administratora, jeszcze bardziej po stronie samej osoby, której dane dotyczą. A ta minimalizacja strat proszę Państwa ma głównie polegać na tym, że administrator no na przyszłość musi być bardziej ostrożny, podejmować szereg działań, żeby nie dopuścić do podobnych wydarzeń. A w przypadku osób, których dane dotyczą, no proszę Państwa, to jest często strach: utrata wizerunku, utrata prestiżu, to jest utrata poczucia bezpieczeństwa. Tutaj zostało zadane na czacie takie pytanie: „No w zasadzie ile zostało udowodnionych takich wydarzeń, zdarzeń, gdzie na skutek wycieku PESEL-a nastąpiło jakieś zdarzenie negatywne dla osoby?" Proszę Państwa ja myślę, że do końca nikt tego nie wie, ponieważ tak naprawdę to dopiero organy ścigania mogłyby ustalić źródła pozyskania informacji, jak i same podmioty, które dopuściły się określonych zdarzeń negatywnych. Tutaj cały czas wydaje mi się, że osoby, których dane dotyczą, no muszą mieć zagwarantowane w sposób jeszcze bardziej optymalny swoje prawa. Muszą czuć się po prostu bezpieczne. No i temu też służą decyzje organu nadzorczego, bo przecież organ nadzorczy w takich sytuacjach, nawet

jeżeli zdarzenie miało miejsce i nawet jeżeli takie wydarzenie nie pociągnęło realnie dla tej osoby żadnych negatywnych dla niej konsekwencji i tak nakłada kary i tak upomina i tak zwraca uwagę na pewne rozwiązania, które muszą być wdrożone. Bo dzisiaj być może tej osobie nie zdarzyła się krzywda, ale jutro może się zdarzyć.

Jest ryzyko, prawda? Istnieje ryzyko. Pani dyrektor, pozwoli też Pani, że przedstawię kilka takich statystyk dotyczących właśnie tego ryzyka. Z takiego ostatniego raportu Infodoc, który jest przygotowywany w ramach prowadzenia społecznej kampanii informacyjnej, systemu Dokumenty Zastrzeżone, wynika, że w pierwszym kwartale 2022 roku odnotowano 1915 prób wyłudzeń kredytów i pożyczek. I to oznacza, że średnio jest to 21 prób wyłudzeń dziennie i każdego dnia próbowano na cudze dane ukraść łącznie 575 000 zł, a w ogóle cały rok 2020 to, przepraszam cały rok 2021, to jest wzrost o 17% liczby wyłudzeń oraz 32% łącznych kwot w porównaniu do roku poprzedniego, czyli do roku 2020. Tak więc być może trudno na dzisiaj określić tak, że dzisiaj doszło do szkody, do naruszenia, ale cały czas istnieje to ryzyko, że być może w przyszłości ktoś te nasze dane wykorzysta. A mówiąc o właśnie o naszych danych osobowych, o bazach danych zwracam się do pana Bartłomieja Drozda, czy my w ogóle jesteśmy w stanie określić, w ilu miejscach się znajdują nasze dane osobowe?

No niestety, nie jesteśmy, myślę, że zwykły obywatel nie jest w stanie wiedzieć, ponieważ dla niego w perspektywie głowy dalej wydaje mu się, że dane osobowe są w urzędzie czy w banku. Zapomina, że jego dane osobowe są dzisiaj wszędzie, w każdej aplikacji, w każdej stronie gdzie klika "wyrażam zgodę" i tak naprawdę nie czyta tego, co tam jest napisane, kto przetwarza dane osobowe, kto się tym zajmuje, w jaki sposób są przetwarzane. Tylko po prostu klika i jesteśmy w aplikacji. Myślę, że to jest dzisiaj no, bardzo, bardzo dobrzy przedmówcy pan Wiesław, pani Monika, pani Dorota powiedzieli bardzo dużo fajnych, interesujących rzeczy na ten temat. Ponieważ mamy kilka grup. Ja bym się na tym skupił. Mamy grupę młodzieży, która tak naprawdę, jak też wskazywał pan Wiesław i pani Monika, dzisiaj żyją i tylko żyją w czasach kiedy jest internet, kiedy żyją ze smartfonem w ręce, tabletem. I to jest ich świat. Nie ma ich w internecie, to tak naprawdę jakby nie istnieli. W związku z tym myślę, że ta grupa klika i swoje dane osobowe od małego przekazuje wszędzie. Nie ma takiej higieny do tego, żeby zachować swoje dane czy osobowe, czy no może jeszcze powiedzmy ta młodzież do 18-stki to nie ma dowodu osobistego, to powiedzmy z niego nie korzysta. Natomiast powyżej 18 roku życia, jak pokazują badania do 26 [r.ż.] też robią zdjęcia mandatu, zdjęcia dokumentu tożsamości. "O! Już mam dowód osobisty, mogę kupić sobie piwo". Wrzuca go do sieci internetowej. To jest jakieś po prostu kuriozum, że ludzie tak postępują. I to już o tym mówi ta grupa nasza, kiedy my pamiętamy, powiedzmy czasy jeszcze bez tej takiej cyfryzacji. Kiedy to

nie było tak popularne i dopiero się internet powiedzmy rodził. Znowu, higiena zupełnie inna jest u ludzi starszych, którzy bardzo sceptycznie podchodzą do internetu. Dzisiaj trochę mniej o nich mówimy. Natomiast uważam, że edukować [niewyraźnie] powinniśmy też ludzi starszych. Bo jak pani Monika i pan Wiesław też wspominali o tych akcjach na wnuczka, kiedy rzeczywiście ktoś przychodził - domokrążca i próbował wyłudzić od osób starszych pieniądze, to dzisiaj on to samo robi tylko poprzez internet, poprzez telefon, poprzez nagabywanie ludzi starszych. I nawet dzisiaj rano widziałem informację, że ktoś też, tak jak pan Wiesław wspominał o tej rodzinie w Stanach, która gdzieś tam rzekomo zginęła. To dzisiaj jest news w faktach gdzie ktoś wyłudził 100 000, bo powiedział, że osoba bliska, syn miał wypadek. I dalej to samo się dzieje. Czyli dalej po prostu trochę ta inna technologia, inne możliwości. Teraz te nasze dane osobowe są wszędzie, bo dzisiaj one tak jak wspomniałem: to jest w szpitalu, w urzędzie, w banku. Przetwarzane są dosłownie wszędzie: są sklepy internetowe, my robimy zakupy, czasami nieświadomie, czasami są aplikacje kiedy choćby nawet my jako rodzice powinniśmy zwracać uwagę dzieciom, kiedy dzieci wymuszają na nas różne aplikacje, instalują na naszych smartfonach, klikają i nawet my nie wiemy kiedy później mamy różne podpięte aplikacje, wyrażone zgody z naszego smartfona. Często też mamy podpiętą kartę do jakiś drobnych płatności i nawet nie wiemy kto jest po drugiej stronie administratorem, kto jest właścicielem. Była taka, nie wiem czy Państwo oglądają, taka aplikacja, która się pojawiła, pokazując nasze twarze jak będą wyglądać za naście, dziesiąt lat starzej. Później się okazało, że wszyscy się z tego wypisywali, bo niby to było śmieszne, klikaliśmy zgodę, wpisywaliśmy swoje dane. Okazało się, że administratorem jest jakaś firma ze Wschodu i kompletnie nie wiedzieliśmy, o co tu chodzi. Więc to jest jakby jedna bardzo ważna grupa. I myślę, że tutaj powinniśmy się też przede wszystkim na tej edukacji, tak jak wspominamy, skupić. Bo myślę, to młode społeczeństwo, które nie szanuje swoich danych w sieci, które traktuje sieć jako byt i zapomina i nie ma kontaktu czasem z rzeczywistością, to ich edukacja jest bardzo istotna. Z drugiej strony myślę, że my też powinniśmy mieć świadomość tego, że dzisiaj, tak jak pokazują też badania, to nie tylko wyciek, czy ktoś włamie się do danej instytucji, czy ktoś włamie się na serwer banku, czy wycieką dane z jakiejś uczelni, czy z jakiejś innej instytucji. To jest jedna sprawa. Druga sprawa to jest to co też pani Ewelina powiedziała. Dzisiaj są wyłudzenia w każdej minucie, w każdym dniu są próby wyłudzenia finansowania na nasze dane. I to jest też przestrzeganie przez nas i to, w jaki sposób my podchodzimy do tego gdzie udostępniamy dane i w jaki sposób my nimi zarządzamy my sami prywatnie, jakie mamy hasła do naszych mediów społecznościowych, do bankowości elektronicznej. Jak do tego podchodzimy, co z tym robimy, czy traktujemy wszystkie maile przychodzące w sposób, tak jak powiedziałem to dzisiaj, na początku wypowiedzi. Mamy trochę taką refleksję, że staramy się czytać z uwagą, z rozsądkiem to co do nas

przychodzi i nie klikać we wszystko w to co przyszło, czy poprzez maila, czy poprzez SMS-a. Tutaj też telefony, które do nas przychodzą, to nie zniknie. Tutaj choćby Urząd Ochrony Danych Osobowych, że tak powiem kolokwialnie „stanął na głowie", żeby tutaj zadbać o to wszystko, to przestępcy też będą cały czas dbać o to wszystko, bo oni z tego żyją. Będą robić różne, przeróżne akcje na to, żeby tą naszą uśpioną czujność, to kiedy my mamy dobre serce, próbujemy pomóc, tak jak pan Wiesław wspominał na Ukrainę. Wcześniej ja mówiłem o tych rachmistrzach, o tych różnych akcjach. No to powoduje, że my niestety nie myślimy, klikamy i w ten sposób też działamy. Też ja przestrzegam zawsze też w wypowiedziach i też w różnych artykułach, żebyśmy zwracali uwagę na to, jeżeli robimy zakupy przez internet, które dzisiaj są bardzo modne i ten procent bardzo mocno podskoczył. Tutaj pandemia się jakby przysłużyła temu i to myślę że idzie w dobrym kierunku. Natomiast sklep internetowy chce od nas, to powinien podstawowe dane, czyli imię nazwisko, adres dostawy, telefon, żeby ten towar wysłać. Natomiast są sklepy, które chcą od nas nasz numer PESEL. Po co ten numer PESEL? Do tego, żeby ten towar wysłać. Nie patrzymy, nie czytamy regulaminu. Powinniśmy mieć zawsze taką refleksję, żeby zobaczyć czy jest regulamin, regulamin danego sklepu internetowego. Czy tam jest ktoś, kto przetwarza dane osobowe, czy ten sklep ma numer telefonu, żeby się z nim skontaktować w razie co. Po co te dane? Jeżeli mamy możliwość też nie dawajmy numeru karty w takim sklepie internetowym jeżeli go nie znamy.` Płaćmy innymi, płaćmy szybkim przelewem, płaćmy BLIK-iem. Płaćmy takimi metodami gdzie ktoś nie będzie miał możliwości pobierania stałego pieniędzy z naszego konta. Ilu ludzi się do nas zgłasza, mówi, że okazało się, że gdzieś tam kiedyś coś zapłacili, a ktoś małe kwoty pobierał, oni nie zwrócili uwagi, że co miesiąc tam jest 10, 15 zł pobierane, aż w końcu ktoś już widział, że jest ta nasza czujność uśpiona i wziął 150 zł albo "wyczyścił" naszą kartę i my całkowicie na to nie zwracamy uwagi. Gdzieś dziecko pobrało aplikację, kliknęło, pomyśleliśmy że to jest darmowe, a później są jakieś pieniądze, konsekwencje. A później się okazuje, że mamy jakąś płatność w dolarach czy w euro, bo z jakiejś instytucji powiedzmy z Los Angeles. I tu się zastanawiamy co z tym zrobić. Później przychodzi do nas wezwanie do zapłaty. I mówimy jak to się stało, że musimy dzisiaj zapłacić jakieś zobowiązanie, gdzie oprocentowanie jest, nie wiem, 500, 600%. Co my mamy teraz z tym zrobić?

Panie Bartłomieju pełna zgoda. Natomiast mówi pan o takich zachowaniach, no, które dotyczą nas. A ja też z kolei zastanawiam się jak administratorzy, jakie mogą administratorzy podjąć działania, żeby właśnie wpływać na tę postawę użytkowników, na postawy konsumentów. Zwracam się z pytaniem do pana Wiesława Paluszyńskiego, czy właśnie Pan zauważył, aby przedsiębiorcy, aby administratorzy zwiększali bezpieczeństwo swoich systemów teleinformatycznych?

Znaczy zależy jacy administratorzy. Znaczy bardzo często, to tak jak powiedziała pani Dyrektor, RODO jest

traktowane jako niechciany obowiązek. W związku z czym wypełnia się wszystko to, co wynika z formalnych rzeczy RODO, nie do końca zresztą jeszcze sprawnie. Dlatego, że jest bardzo wiele takich firm, które biegają po rynku i robią tą całą dokumentację pod RODO, taką samą dla wszystkich firm, które świadczą usługi. Jest to bardzo znany objaw, za 2000 zł dam ci dokumentację RODO łącznie z opisem twoich procesów. Pomimo, że te procesy są w każdej firmie inne i przy każdej usłudze inne, to przechodzi i po prostu jest to tzw. fikcja RODO. Ona jest dosyć powszechna w Polsce przy świadczeniu usługi zarządzania danymi osobowymi. W związku z czym to jest jedna grupa. I dopóki się ich nie złapie na tym, ktoś nie wykaże, że po prostu te procesy to są zupełnie inne procesy, najczęściej nie ma właśnie tego, o czym pani Dyrektor powiedziała, że powinno być, czyli analiz ryzyka przetwarzania danych osobowych w kontekście procesu i zaplanowania takich działań i środków technicznych, które powinny być odpowiednie do ryzyka, a nie jakieś, kto komuś się wydaje, że jest potrzebne. Największym niebezpieczeństwem bezpieczeństwa jest to, że stosujemy mnóstwo rozwiązań technicznych, które nie do końca w ogóle są potrzebne w danym miejscu, czy w danym rozwiązaniu. Natomiast uciekają nam poważne luki w naszym systemie. I to jest dosyć powszechna sprawa. Przy poważniejszych graczach usług świadczonych drogą elektroniczną jest inaczej. Oni zdają sobie sprawę z konsekwencji i wiele robią w kierunku zapewnienia bezpieczeństwa tych usług. Ale tak jak powiedziałem, u nas pokutuje i pani Dyrektor to niejako potwierdziła, pokutuje magia PESEL-a i jakieś takie podejście do zbierania tych danych, które wydaje się, że powinni usługodawcy zapewnić bezpieczeństwo. I to zaczyna być problem, który jest problemem szerokim, no bo często się porównuje do administracji publicznej. I mówi się tak, jeżeli administracja publiczna świadczy usługę i do świadczenia tej usługi wystarcza to i tamto, dlaczego my w firmie mamy włożyć większe pieniądze i robić to usługę inaczej niż to robi administracja publiczna? Jeżeli uważa się, że administracja publiczna robi to dobrze i to jest wystarczające, to my będziemy robili dokładnie tak samo. No i mamy takie koło zamachowe, które się toczy przez te usługi. Natomiast rzeczywiście wydaje się, że jest po prostu bardzo różnie. Tak samo jak i te usługi administracyjne są bardzo różne, bo to też nie jest taka prawda, że każda usługa jest taka sama, na takim samym poziomie bezpieczeństwa, to tak samo jest z tymi przedsiębiorcami. Oni w zależności od tego, czy tych przedsiębiorców jest kilkaset tysięcy, jeżeli byśmy popatrzyli na tych, którzy świadczą różne rodzaje usług elektronicznych, więc to się po prostu tak toczy. Dobre przykłady, ja myślę, że dla przedsiębiorców są potrzebne dobre przykłady i to jest klucz do wszystkiego.

Mówimy o tych zabezpieczeniach, o takich działaniach zwiększających bezpieczeństwo, a też ostatnio wyczytałam, że 97% polskich dużych przedsiębiorców posiada tzw. cyberpolisę, czyli ubezpieczenie od ataków cyberprzestępców. I co ciekawe, to z takiej cyberpolisy korzystają ci, którzy już kiedyś przeżyli, czy

wyciek danych, czy właśnie ataki ransomware. Prawie 89% zaatakowanych w przeszłości firm tego typu cyberpolisę wykupuje. Pan Prezes też mówił o lukach w różnych rozwiązaniach, zwracam się z pytaniem do pani Dyrektor Krasińskiej, jakie są tendencje legislacyjne w takim razie w obszarze cyberbezpieczeństwa i na co UODO wskazuje w swoich opiniach?

Tak jak już zwrócili uwagę moi znakomici przedmówcy, trudno jest proszę Państwa zbudować dom, jeśli nie wiemy, co w nim ma się znajdować. Jeśli nie wiemy z jakich ma się składać pomieszczeń i jakim celom ma służyć. I trudno jest zbudować system ochrony danych osobowych u administratorów, jeśli nie przeprowadzą analizy ryzyka. A jeszcze trudniej jest zbudować właściwe, dostosowane z jednej strony do potrzeb obywateli, z drugiej strony potrzeb całego rynku rozwiązania prawne, jeśli nie będzie przeprowadzona ocena skutków dla ochrony danych. Proszę Państwa, brak takiej oceny powoduje, iż działający nawet w najlepszej wierze projektodawca nie przewidzi wszystkich okoliczności, które mogą rzutować na cały zbudowany przez niego system teleinformatyczny, informatyczny, czy w ogóle cały system zarządzania informacją. Niestety w wielu aktach prawa, które są budowane i które podlegają opiniowaniu przez organ nadzorczy, brak jest takiej oceny skutków. Mówiąc krótko, projektodawca nie bardzo wie, jakie zaistnieją ryzyka. Nie przewiduje poprzez brak oceny skutków określonych scenariuszy i dopiero użytkownik tego przepisu, czyli stosujący go w praktyce, spotyka się z sytuacjami, no a teraz wobec tego zaraz, to jak ja mam teraz długo te dane przetwarzać, ponieważ w tych przepisach nie ma nic o retencji danych. Jak ja je mam przetwarzać w sposób bezpieczny, bo te przepisy w bardzo blankietowy sposób tę kwestię regulują, komu mam udostępniać, bo jest katalog podmiotów otwarty. Pod jakimi warunkami, bo w zasadzie to też nie wynika z tych przepisów. I niestety tutaj brak tej oceny skutków i brak przeprowadzenia testu prywatności, brak właśnie zastosowania tego mechanizmu privacy by design, by default powoduje, że w przepisach nie są uwzględniane te rozwiązania, które powinny tam się znaleźć, żeby całe budowane rozwiązanie, cała koncepcja po prostu była spójna. Bardzo często proszę Państwa, organ nadzorczy w swoich wystąpieniach, wskazuje na ten brak spójności w przepisach. Na brak podjęcia ostatecznej decyzji jak ten projektodawca wobec tego widzi dalsze losy tych danych. Tu chciałabym zwrócić uwagę, że sam projektodawca, bardzo często, kiedy dostaje uwagi Urzędu Ochrony Danych Osobowych prosi o spotkanie, bo nie wie, o co chodzi, bo nie rozumie, co ma zrobić. Prosi o napisanie przepisu przez organ nadzorczy, który przecież nie znając całego systemu i całej koncepcji w oparciu, o którą budowany jest dany system, nie jest w stanie, zresztą nie ma inicjatywy legislacyjnej, niczego takiego zaproponować. Tutaj brakuje takich głębszych analiz i obawiam się, że sami legislatorzy tworzący prawo nie są w stanie ich wyłącznie dokonać. To musi być szersza dyskusja, także pod kątem ochrony danych osobowych. Co widzimy, budowane są systemy, one funkcjonują w taki, a nie w inny

sposób. Słyszymy, że są bezpieczne, ale dopiero potem tworzone są przepisy prawa, które mają zalegalizować owo przetwarzanie albo słyszymy, że w zasadzie te przepisy nie różnią się od innych. Tyle, że te inne nie były zweryfikowane pod kątem dostosowania do RODO i ustawodawca uzyskuje w ten sposób informację, że jeszcze te przepisy, na które powołuje się jako wzorcowe, no też powinny być jednak zmienione. Czego brakuje oprócz tej oceny skutków, oprócz przeprowadzenia tego testu prywatności? No przede wszystkim zastanowienia się, kto za co odpowiada. Tutaj proszę Państwa, niestety w wielu aktach prawnych tak są stworzone, takie są stworzone rozwiązania, że konia z rzędem temu, kto powie mi, kto tu jest administratorem, a kto jest [podmiotem] przetwarzającym. Projektodawca boi się proszę Państwa, konstrukcji powierzenia jako instrumentu prawnego. W związku z tym, bardzo często próbuje tak stać jedną nogą przy powierzeniu, a drugą nogą przy współadministrowaniu albo wyłącznym administrowaniu. Co zazwyczaj kończy się niestety w sposób bardzo niedobry dla stosujących już później przepisy prawa, bo one te podmioty wskazują, no przecież faktycznie realizujemy cele i sposoby przetwarzania danych, realizujemy zadania, ale kto inny został nazwany wprost administratorem. Takie nazywanie administratora wprost bez doprecyzowania celów przetwarzania danych bardzo często kończy się tak naprawdę przypisaniem ról albo nie temu, co trzeba administratorowi albo nie tylko temu administratorowi, bo są jeszcze w tym układzie inni. Także tutaj brakuje, a to ma znaczenie ogromne z perspektywy chociażby podjęcia tej odpowiedzialności za co kto odpowiada, kto powinien zgłosić naruszenia. Proszę Państwa ostatnio obserwowany jest taki trend, że za przetwarzanie danych w systemach publicznych mają być odpowiedzialni także w pewien sposób użytkownicy tych systemów jako osoby prywatne. To jest też niebezpieczne, ponieważ za ich zgodą są oni tak naprawdę włączani w system zarządzania informacją. Gdy tymczasem są wyłącznie użytkownikami, którzy powinni, co najwyżej jasne, przejrzyste komunikaty jak w tym systemie się poruszać, jakie rozwiązania stosować, żeby nie narażać się na określone ryzyka jako jego eksploatańci. Także tutaj rzeczywiście mamy do czynienia z takimi sytuacjami prawnymi, z budowaniem przepisów, które nie zawsze po pierwsze, będą odpowiadać zasadom ochrony danych osobowych, czyli tej zasadzie adekwatności, proporcjonalności, celowości, integralności, bezpieczeństwa, legalności nawet. Jak również nie zawsze mamy do czynienia z takim przewidzeniem skutków, bo tutaj projektodawca musi troszkę być jak ten, który musi przewidywać konsekwencje wprowadzenia takich, a nie innych rozwiązań. Bardzo często w przepisach są wskazywane systemy odpowiedzialne za przetwarzanie danych. To nie system ma decydować o przetwarzaniu danych. To nie system ma zapewniać. Z perspektywy ochrony danych zapewniać ochronę danych i bezpieczeństwo ma administrator z jasno przypisanymi zadaniami, celami, zakresami danych, okresami retencji danych. A tymczasem bardzo często okazuje się, że nagle nam wskakuje system jako jakiś

szczególny administrator. Na co zresztą zwracamy uwagę projektodawcy, nieświadomemu, że takie rozwiązanie po prostu no zaburza pewne systemowe podejście w ogóle wynikające z rozporządzenia o ochronie danych osobowych i z wytycznych Europejskiej Rady Ochrony Danych Osobowych. Również obserwujemy w projektowanych przepisach, bardzo często takie niezrozumienie pojęcia administratora z perspektywy wskazywania administratora systemu. Okazuje się, że administrator systemu, on nie jest odpowiedzialny w zasadzie za dane, bo on jest administratorem systemu, a nie administratorem danych osobowych w tym systemie. Nie ma takiego pojęcia "administrator systemu" w rozumieniu rozporządzenia o ochronie danych osobowych. My mówimy o administratorze. I nawet jeżeli nie musimy go wprost nazywać, musimy bardzo dokładnie określać zakres jego odpowiedzialności, zakres jego zadań, jego prerogatyw, jego procesów decyzyjnych. I to ustawodawca, to projektodawca powinien przewidzieć w takich, a nie innych przepisach. Bardzo często w przepisach dotyczących również budowania tej odmiennej przestrzeni cyberbezpieczeństwa brakuje jasnych i bardzo precyzyjnie wskazanych celów przetwarzania. Co ma znaczenie, chociażby później z perspektywy szacowania to, kto jest odpowiedzialny, na jakim etapie przetwarzania za jaki proces, za jaki proces. Oczywiście rozporządzenie o ochronie danych osobowych zawsze będzie miało zastosowanie bezpośrednie i będzie stosowane nawet jeżeli polski ustawodawca zapomniał, albo zapisał pewne rozwiązanie w sposób mało klarowny. Natomiast chodzi tutaj przede wszystkim o zapewnienie przejrzystości, bo to o czym Państwo powiedzieliście wcześniej i też, o czym czytam tutaj na czacie: za długie regulaminy, nieczytelne informacje, za dużo wszystkiego w jednym miejscu i brak odesłań przejrzystych, gdzie więcej można dla zainteresowanych uzyskać informacji. Tak, cały czas nam kuleje ta zasada przejrzystości. A proszę zwrócić uwagę, że dzisiaj nie tylko młode pokolenie bazuje na szybkości przepływu informacji, oczekuje szybko informacji zwrotnej, oczekuje szybkiej informacji, to wobec tego, z jakimi zagrożeniami wiąże się takie, a nie inne rozwiązanie, które będzie stosować. Tu ta przejrzystość, niestety kuleje. A dlaczego? Bo bardzo często, jeszcze raz powtórzę, podchodzimy w bardzo formalny sposób do ochrony danych, a nie do jak do pewnego zjawiska, które powinno się stać częścią naszego po prostu codziennego życia. Bo dzisiaj proszę Państwa bez danych osobowych świat nie jest w stanie funkcjonować ani w sferze publicznej, ani w sferze prywatnej.

Dziękuję, pani Dyrektor, rzeczywiście mówimy o klauzulach informacyjnych, o przejrzystości, o tym jasnym języku, a przecież są to rzeczy, o których mówimy od dawna. Sama ochrona danych osobowych, to nie jest temat nowy, który wprowadziło ogólne rozporządzenie o ochronie danych osobowych, tylko ochrona danych osobowych ma w naszym kraju już swoją długoletnią historię. Natomiast na szczęście są też tacy administratorzy, którzy sami wykazują proaktywną postawę i zwracamy na to uwagę np. w takich

dodatkowych usługach, jak cybertarcza. Zauważamy, że coraz częściej operatorzy telekomunikacyjni proponują tego typu usługę właśnie dla swoich użytkowników, dla swoich klientów, tym samym, uświadamiając ich jak ważne jest właśnie odpowiednie dbanie o swoje dane osobowe i zachowanie tego cyberbezpieczeństwa. Zwracam się z pytaniem do pani Doroty Grudzień-Barbachowskiej. To jest właśnie taki przykład tego, jak administratorzy mogą mieć pozytywny wpływ na zachowania użytkowników?

Dziękuję, za oddanie głosu. Szanowni Państwo, ja z wielką uwagą, zanim odpowiem na pytanie, chciałam się odnieść w trzech zdaniach dosłownie do tego co Państwo powiedzieliście. Z wielką uwagą wysłuchałam moich szacownych przedmówców. Muszę Państwu powiedzieć tak: procesów cyfryzacji my już nie zahamujemy i digitalizacja stosunków społeczno-gospodarczych jest faktem i będzie postępować. Musimy nauczyć się żyć w tej przestrzeni digitalnej. Musimy nauczyć sobie radzić z problemami. To, co Państwo mówiliście na temat roli administratorów, na temat roli właśnie przedsiębiorców, na temat roli administracji państwowej, działań regulacyjnych, legislacyjnych na temat roli też klientów. My nie żyjemy, każdy z nas nie żyje w bańce. My żyjemy w systemie naczyń połączonych. Czyli wszystkie nasze działania - moje, Państwa, regulatorów, legislatorów, jak również przedsiębiorców połączą się w jedną całość zmierzającą ku temu, że zapewnimy sobie wzajemnie, sobie wzajemnie bezpieczeństwo w obszarze cyfrowym. Bez tego się, bez tej współpracy, nie tylko w zakresie, nie wiem ścigania przestępstw, nakładania nowych obowiązków, ale wypełniania taką dobrą praktyką, dobrą wiedzą naszego tego cyfrowego obszaru działania. To jest chyba jedyna droga do tego, żebyśmy osiągnęli po prostu sukces. Ja proszę Państwa, wielokrotnie brałam udział w kształtowaniu przepisów prawa i są takie obszary, które można bardzo ściśle regulować, ale w przypadku digitalizacji usług, w przypadku np. cyberzagrożeń, które nam w tym obszarze zagrażają. Proszę państwa, jak ta legislacja musi być mądra, jaka ona musi być przemyślana, jaka ona musi być pojemna, żeby zabezpieczyć nasze interesy nie dzisiaj tu i teraz, ale, żeby zabezpieczyć nasze interesy jako klientów też i administratorów, również myślę tu o administracji publicznej, która świadczy coraz szerszy zakres usług cyfrowych. Także my proszę Państwa, musimy patrzeć całościowo na tematy i musimy po prostu uczyć się tej odpowiedzialności, odpowiedzialnego działania. Nie wiem, czy Państwo wiecie, że na CERT Polska jest możliwość zgłoszenia drogą SMS-ową informacji na temat fałszywych SMS-ów, które otrzymujemy de facto każdego dnia. Ja proszę Państwa wczoraj otrzymałam wczoraj takie 2 SMS-y. Temat jest znany, bo dotyczy to jednego z operatorów energetycznych. Ale proszę Państwa, każdy z nas, naszym działaniem, jest w stanie zabezpieczać nie tylko swoje interesy, ale interesy innych i nawet taka mała rzecz, jak umożliwienie obywatelom zgłaszania nadużyć za pomocą środków komunikacji elektronicznej, wysłania informacji do ekspertów z CERT-u na temat podejrzanego SMS-a, który może prowadzić nas do utraty naszych danych, do

utraty naszych dóbr. A mało tego, my mamy tą świadomość, ale są inni w sieci, którzy tej świadomości wcale nie muszą mieć albo nawet jak mają świadomość, działają w takim pędzie i w takim, ta szybkość wymiany informacji, o której Państwo mówiliście, jest tak duża, że mogą po prostu pozwolić sobie na chwilę nieuwagi, która może ich kosztować bardzo, bardzo wiele. A co do proszę Państwa pytania na temat właśnie roli administratorów czy roli też przedsiębiorców, którzy świadczą usługi komunikacji elektronicznej, ta rola na pewno jest nie do opisania i tutaj muszą oni przykładać szczególną uwagę też po to, by budować taką dobrą swoją markę. To nie tylko jest kwestia stosowania przepisów, ale to jest kwestia budowania dobrej marki, solidnego partnera dla klienta, który korzysta z moich usług. Nie będę tutaj rekomendować rozwiązań, bo każdy z nas, każdy klient powinien sam ocenić, co jest mu potrzebne, tak naprawdę. I po to też jest potrzebna ta edukacja właśnie. Powinien mieć świadomość tego, w jaki sposób korzysta z telefonu. Proszę Państwa z naszych badań wynika np. że tylko 40%, a może aż 40% , nie wiem, to w zależności od tego, czy widzimy szklankę pustą do połowy, czy pełną, ale 40% osób korzysta z zabezpieczeń, deklaruje, że korzysta z zabezpieczeń smartfona. Co to oznacza, że 60% osób z takich zabezpieczeń nie korzysta. Czyli zobaczcie Państwo, jak wiele jest tutaj do zrobienia. Ile osób korzysta z zabezpieczeń komputera swojego. Również proszę Państwa tutaj pozostawia to nasze działanie, faktyczne działanie, o którym też mówicie Państwo w swoim raporcie wiele do życzenia. Więc myślę, że każdy z nas i administratorzy w zakresie usług czy bezpłatnych, czy usług płatnych, które zmierzają do niwelowania tych cyberzagrożeń, mają swoją rolę. My jako organy administracji, o czym mówiła pani Dyrektor Monika Krasińska, mamy ogromną rolę swoją w wykonywaniu takich działań, ale też i my klienci mamy ogromną rolę w tym, żeby uchronić się przed negatywnymi skutkami działania cyberprzestępców w sieci. I to powinno być naszym żywotnym interesem i powinniśmy zmierzać do tego, żeby wiedzieć jak najwięcej, żeby podążać też za tą zmieniającą się rzeczywistością. Ta edukacja będzie trwała zawsze, każdego dnia, słuchajcie do końca naszego życia, ponieważ to otoczenie zmienia się z każdym dniem i cały czas niestety musimy gonić tego królika.

Dziękuję pani Dyrektor, też wydaje mi się, że bardzo często już jesteśmy przyzwyczajeni do tego, że jest u nas takie prawo nakazane. To znaczy cały czas ktoś nam nakazuje, wskazuje nam model, za którym mamy podążać. Zaświadczenie, formularz, który należy wypełnić i my się tego bardzo mocno trzymamy. Chcemy uzyskać taki jeden kierunek i wiedzieć, w którą stronę mamy właśnie podążać. Z kolei RODO, to właśnie takie rozporządzenie, które jednak stanowi, że to administrator jest tak naprawdę tym architektem procesu przetwarzania danych, o którym często mówi pani Dyrektor Monika Krasińska i to administrator, znając wszystkie procesy w swojej firmie, powinien zwracać uwagę na to, jakie dane osobowe przetwarza, ale też w jaki sposób być może kształtować zachowania i swoich pracowników, którzy też przecież są konsumentami,

ale i także użytkowników. Myślę, że podczas naszej dzisiejszej dyskusji nie jesteśmy w stanie podjąć tych wszystkich wątków, które są bardzo ciekawe. Ja już w tej chwili Państwu dziękuję za udział w naszej rozmowie pani Dyrektor Monika Krasińska, pan Wiesław Paluszyński, pani Dorota Grudzień-Barbachowska, pan Bartłomiej Drozd. Proszę jednak Państwa o pozostanie, ponieważ w tej chwili oddaje głos rzecznikowi prasowemu Urzędu Ochrony Danych Osobowych, Adamowi Sanockiemu, na zadanie pytań i odpowiedzi.

Dziękuję Państwu bardzo serdecznie. Dziękuję Ewelinie za przeprowadzenie tej bardzo ciekawej dyskusji. To, że ta dyskusja była ciekawa, no też świadczy fakt, że od początku naszego dzisiejszego spotkania, w zasadzie do końca praktycznie mamy niezmienną, wysoką ilość uczestników, więc chciałem Państwu bardzo serdecznie za to uczestnictwo podziękować. No a Państwu, naszym ekspertom, podziękować za przyjęcie zaproszenia i udział w debacie. Myślę, że też chciałem podziękować za to, że Państwo na bieżąco śledzili nasz czat i bezpośrednio odnosili się do tych pytań, które nam się pojawiały. Myślę, że najważniejsze wątki zostały już przez Państwa w czasie rzeczywistym omówione. No pojawiało się dużo pytań związanych z użyciem dowodów osobistych, kserowaniem tych dowodów osobistych, z dowodami kolekcjonerskimi, z rolą administratorów w szkołach, w administracji publicznej, więc myślę, że nasz czas powoli dobiega końca, więc pozwólcie Państwo, że ten temat już pominiemy na tym etapie. Zachęcałbym Państwa także do bezpośredniego kontaktu z wszystkimi uczestnikami tego spotkania. Mam tutaj na myśli Urząd Ochrony Danych Osobowych, KRD, ChronPESEL, a także pewnie UKE. Myślę, że wszystkie te instytucje, organizacje są otwarte na współpracę. Mi pozostaje mieć nadzieję, że wnioski, które płyną z tegorocznego badania, a przypominam była to druga edycja badania, w jeszcze większym stopniu ułatwią administratorom dbanie o bezpieczeństwo, bezpieczne przetwarzanie danych osobowych swoich klientów na każdym etapie tego procesu. Wierzymy, że też dzisiejsze spotkanie było wartościowym źródłem informacji dla inspektorów ochrony danych osobowych i ,że mamy informację o postawach Polaków, o ich podejściu do tematu cyberzagrożeń. Wierzymy i ufamy także, że dzięki takim inicjatywom świadomość Polaków na temat zagrożeń dla ochrony danych osobowych będzie wzrastać, co zaowocuje także większą uważnością oraz umiejętnością szybkiej i skutecznej reakcji w odniesieniu do zagrożeń, na jakie w cyberprzestrzeni wszyscy jesteśmy narażeni. Na profilaktykę cyberzagrożeń składają się m.in. właśnie upowszechnienie wśród obywateli wiedzy o ochronie danych osobowych, dużo na ten temat dzisiaj, mówiliśmy, o roli edukacji, o bezpieczeństwie naszych danych, o przysługujących nam prawach. Mam nadzieję, że te webinarium i lektura też raportów, do których zachęcamy wzmocni tą praktykę. Muszę też wspomnieć o tym, co mocno wybrzmiało w tych rozwiązaniach systemowych, o których Państwo mówili. No faktycznie, trochę mam poczucie, że współpraca między regulatorami, współpraca też przy takich inicjatywach edukacyjnych, przy

tego typu badaniach, raportach jaką Urząd Ochrony Danych Osobowych od lat prowadzi jest czasami takim elementem w grze, że wycieramy mam wrażenie wodę z kapiącego kranu, a wystarczyłoby ten kram pewnie zakręcić i byłoby prościej. Natomiast tutaj potrzebujemy tak jak nieraz na tym spotkaniu padło rozwiązań systemowych. Mam nadzieję, że dzięki tej dyskusji przynajmniej mały kroczek w tym kierunku zrobiliśmy. Bardzo Państwu wszystkim dziękuję za poświęcony czas i za udział w dzisiejszym spotkaniu. Jeszcze raz dziękuję KRD, ChronPESEL za już kolejną współpracę w bardzo ciekawym raporcie z badań. Dziękuję UKE za naszą współpracę, która jest już też długa. I myślę, że będzie jeszcze bardziej się rozwijać, bo widzimy, że mamy wiele obszarów w tym celu i celów do zrealizowania. Bardzo Państwu jeszcze raz serdecznie dziękuję i do zobaczenia przy kolejnym tego typu [niewyraźnie].

Dziękujemy. Do zobaczenia.