## Wyniki warsztatów „Tak dla ochrony danych osobowych“

### „Migranci i ochrona konsumentów na rynkach cyfrowych“ 13.06.2014

Drugie warsztaty projektu „Migranci i ochrona konsumentów na rynkach cyfrowych“ były poświęcone tematyce ochrony danych osobowych i zostały przeprowadzone w dniu 13 czerwca 2014 r. w pomieszczeniach Centrali Konsumenckiej. W warsztatach wzięło udział 26 uczestników. Uczestnikami było 13 gości z Izby Deputowanych, administracji federalnej i krajowej. Warsztaty odwiedziło również sześciu przedstawicieli rosyjskich związków migrantów i stowarzyszeń takich jak Krajowy Związek Wypędzonych, Służba Migracji Młodzieży (Placówka Terenowa w Schöneberg), Związek Międzynarodowy (Placówka Terenowa w Marzahn-Hellersdorf), Centrum Młodzieży i Rodziny Schalach i Centrum Integracji Box 66.

Eva Bell z Zarządu Centrali Konsumenckiej otworzyła warsztaty słowem powitalnym, w którym podkreśliła ważność ochrony danych osobowych u osób z doświadczeniem migracyjnym. Wskazała na nowy projekt ustawy, która w przyszłości przyzna Centralom Konsumenckim prawo do wnoszenia powództwa związku na naruszenia prawa ochrony danych osobowych.

Sabine Toepfer-Kataw, Sekretarz Stanu do spraw ochrony konsumenta w swojej mowie powitalnej przedstawiła wyniki Monitora Konsumenta 2013, który wymienia olbrzymie deficyty kształcenia konsumentów wśród migrantów pochodzenia tureckiego i rosyjskiego. Wielu konsumentów nie jest wystarczająco poinformowanych o znaczeniu ochrony danych osobowych. Postulowała konieczność wytworzenia lepszej świadomości ochrony danych osobowych wśród konsumentów przy wykorzystaniu wysoko rozwiniętej technologii informacyjnej i komunikacyjnej. Wstępna selekcja danych użytkowników w Internecie przez firmy takie jak Google umożliwiła stworzenie profili konsumenckich i dostosowaną do nich reklamę. Tymi danymi interesują się nie tylko przedsiębiorstwa, lecz także przestępcy. Z tego względu na pierwszym planie musi się znaleźć nie tylko zagadnienie ochrony danych osobowych, ale także ochrony konsumentów. Sekretarz Stanu zakończyła swoje słowo powitalne wezwaniem Unii Europejskiej do stworzenia jednolitych i wysokich standardów i reguł dotyczących ochrony danych osobowych i zaznajomienia z nimi ludzi.

Dr. Günter Hörmann, członek Zarządu Centrali Konsumenckiej w Hamburgu, opisał różne pola działania Central Konsumenckich w ciągu ostatnich pięciu dziesięcioleci, które stopniowo dostosowywały się do potrzeb konsumentów. Podkreślił on wzrastające znaczenie danych osobowych we współczesnym społeczeństwie informacyjnym i komunikacyjnym. Zapisywanie danych telefonicznych i internetowych oraz dostęp do nich bez wiedzy osób zainteresowanych przyczyniają się do wywołania uczucia stałego obserwowania życia prywatnego. Przedsiębiorstwa są w stanie zdobyć doskonałe i monopolistyczne pozycje rynkowe w wyniku zręcznego powiązania danych i nakłonienia w ten sposób konsumenta do korzystania z ich ofert (przykładami są Google i Facebook). Odesłał do orzeczenia Europejskiego Trybunału Sprawiedliwości (ETS) na temat Dyrektywy WE w sprawie zatrzymywania generowanych lub

przetwarzanych danych. ETS obalił Dyrektywę WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w kwietniu 2014 r., ponieważ naruszała ona prawa podstawowe. Pan Hörmann podkreślił wartość ochrony danych osobowych jako nieodzowny warunek nie tylko do ochrony demokracji, ale również do ochrony konsumenta.

Dr. Çiçek Bacik, kierowniczka projektu „Migranci i ochrona konsumentów na rynkach cyfrowych“ podkreśliła szczególną rolę migrantów i działań Centrali Konsumenckiej w Berlinie na rzecz tej grupy docelowej. Oprócz porad udzielanych w języku tureckim przez honorowych prawników Centrala Konsumencka w Berlinie zatrudniła obecnie rosyjskojęzycznego prawnika, który co miesiąc udziela porad również na miejscu w Marzahn i Lichtenberg w języku rosyjskim i niemieckim. Ponadto pani Bacik poinformowała o szkoleniach multiplikatorów w ramach istniejącego od roku 2012 projektu „Szkolenie mentorów na temat ochrony konsumenta ukierunkowanej na grupę docelową“.

Podkreśliła ona, że według Monitora Konsumenta Berlin 2013 migranci stanowią szczególnie wrażliwą grupę konsumentów i mają dużą potrzebę uświadomienia w zakresie Internetu i telekomunikacji. Według tego badania większość z nich (56 % pochodzenia tureckiego i 47 % pochodzenia rosyjskiego) wykorzystuje Internet do zdobycia informacji. Jak większość ludności niemieckiej również migranci wykorzystują Internet do robienia zakupów i wykonywania operacji bankowych. Ponad jedna trzecia tureckojęzycznych i rosyjskojęzycznych konsumentów została już skonfrontowana z problemami e-commerce i miała dwa razy wyższe rachunki za smartfony niż konsumenci niemieccy. Z tych powodów pani Bacik podkreśliła szczególne znaczenie tego projektu. Podczas gdy według Monitora Konsumenta Berlin 2013 85% Niemców świadomie decyduje, do jakich danych (osobowych) mogą mieć dostęp programy i aplikacje, z których korzystają, to tylko 45% osób pochodzenia tureckiego i 37% osób rosyjskojęzycznych zwraca uwagę na ochronę swoich danych osobowych.

Omawiając cele projektu pani Bacik wyjaśniła różne działania zaplanowane w celu uświadomienia turecko- i rosyjskojęzycznych konsumentów w zakresie rynków cyfrowych: uświadomienie grupy docelowej w zakresie praw konsumenta, ofert rynkowych i doradczych na rynkach cyfrowych, badanie sytuacji rynkowej na rynku telekomunikacyjnym przy pomocy badań rynku i warsztatów, sporządzanie informacji w zakresie telekomunikacji i Internetu, rejestrowanie skarg grupy docelowej i pośredniczenie w przekazywaniu informacji na temat kompetentnego obchodzenia się z usługami telekomunikacyjnymi, Internetem i ochroną danych. Planowane dwa badania rynku koncentrują się na taryfach telefonicznych do Turcji i taryfach do Federacji Rosyjskiej, przy czym ich głównym tematem jest badanie i ocena cen, serwisu i sposobu prowadzenia spraw handlowych operatorów telefonicznych. Centralny moduł projektu stanowi następujące po nim udostępnienie odpowiednich dla grup docelowych informacji na temat rynków cyfrowych. Pani Bacik wspomniała, że informacje dla grup docelowych są udostępniane po niemiecku oraz w wersjach skróconych/polach informacyjnych w języku tureckim lub rosyjskim. Na koniec poinformowała o wyniku warsztatów wprowadzających.

Christian Dahler, referent do spraw informatyki z Biura Pełnomocnika Berlina ds. Ochrony Danych Osobowych i Bezpieczeństwa Informacyjnego wygłosił referat na temat podstaw bezpiecznego korzystania z sieci WLAN i smartfonów i objaśnił uczestnikom ślady danych, które konsumenci pozostawiają w Internecie. Najpierw wyjaśnił, dlaczego jest ważne, aby podczas surfowania w Internecie używać zawsze zaszyfrowanych sieci WLAN. Ponieważ instytucje publiczne, kawiarnie czy sklepy nie zawsze zapewniają szyfrowane połączenie internetowe, to należy unikać takich połączeń. W szczególności podczas nieszyfrowanych połączeń internetowych należy zaniechać korzystania z usług e-commerce. Wyjątkami są VPN (Virtual Private Network) i IPsec (Internet Protocol Security). W miarę możliwości należy używać szyfrowania WPA- i WPA2 (Wi-Fi Protected Access) ze względu na ich bezpieczeństwo. Zbudowanie sieci z WPS (Wi-Fi Protected Setup) jest wprawdzie komfortowe, ale częściowo niebezpieczne. Podczas gdy po włączeniu komputera w ciągu 1-2 minut nawiązywane jest automatyczne połączenie internetowe, może dojść do przechwycenia numerów PIN.

Kolejnym warunkiem bezpiecznego surfowania w Internecie jest używanie bezpiecznych, trudnych do odgadnięcia i możliwie nie ustawionych wstępnie haseł do sieci WLAN, które w razie potrzeby można też konfigurować również przy pomocy specjalnego oprogramowania. Również deaktywacja zdalnej konfiguracji routera po zbudowaniu sieci przyczyni się do zabezpieczonej transmisji danych.

Na koniec pan Dahler objaśnił niektóre podstawowe ustawienia bezpieczeństwa w smartfonach, na przykład używanie hasła w celu uniknięcia nieuprawnionego dostępu do urządzenia i zapisanych w nim danych, kontrolę podczas pobierania i używania bezpłatnych aplikacji i kontrolę podczas przyznawania praw dostępu do własnych danych. Nadto należy ostrożniej obchodzić się z funkcją lokalizacyjną niektórych aplikacji, ponieważ umożliwia ona np. tworzenie profili przemieszczania się użytkowników. W przypadku nieznanych aplikacji jest ważne, aby zebrać o nich informacje. Aktualnie sprawdzone aplikacje w sklepach producentów prezentują się nieco bezpieczniej. W szczególności aplikacje do androida często nie są sprawdzone. Za pomocą pobranych aplikacji można uzyskać dostęp do wrażliwych danych użytkownika. Często nie jest jasne, kto otrzyma dane użytkownika i do czego zostaną one wykorzystane. Na przykład podczas grania przechwycone dane mogą być używane do celów reklamowych. Z tego względu lepiej jest wyłączać WLAN podczas grania.

W drugiej fazie swojego referatu pan Dahler wyjaśnił, jakie dane użytkownika są przekazywane podczas wywoływania stron internetowych. Na podstawie przekazanych danych na temat typu przeglądarki internetowej, systemu operacyjnego, informacji o rozdzielczości ekranu i głębi kolorów można na przykład ustalić, z jakiego urządzenia następuje dostęp do danej strony internetowej. O związanych z urządzeniami cenach dla konsumentów media donosiły już w związku z urządzeniami firmy Apple.

Kolejną możliwością korzystania ze stron internetowych do personalizacji i rozpoznawania danych są cookies. Cookies to małe pliki tekstowe z informacjami o odwiedzonych stronach internetowych, które są zapisywane przez te strony internetowe na komputerze użytkownika,

aby móc go potem zidentyfikować. Ponadto za pomocą tak zwanych tracking-cookie wyszukiwarki mogą śledzić zachowanie poszczególnych użytkowników podczas surfowania w Internecie i sprzedawać te informacje współpracującym stronom internetowym w celu sporządzenia ukierunkowanej oferty. Ponadto sklepy internetowe zapisują dotychczasowe zamówienia i zaznaczone wcześniej produkty użytkownika, aby móc mu celowo zaoferować dodatkowe pasujące artykuły. Taki dostęp do danych można zminimalizować przez wyłączenie poszczególnych funkcji przeglądarki internetowej, takich jak np. JavaScript i Add-Ons (małe rozszerzenia przeglądarki internetowej), jak NoScript i AddBlock-Plus. Pan Dahler podkreślił podwyższone bezpieczeństwo surfowania w trybie incognito i zademonstrował jego ustawienie w przeglądarce internetowej.

Ponadto poinformował on o prawie do określenia prawa do informacji zgodnie z §§33-35 Federalnej Ustawy o ochronie danych osobowych (Bundesdatenschutzgesetz - BDSG), w ramach której osoby zainteresowane mogą żądać zarówno powiadomienia i informacji na temat zapisanych danych jak również ich poprawienia, zablokowania i usunięcia. Na koniec opowiedział o tak zwanej Liście Robinsona (www.robinsonliste.de), która obiecuje ochronę przed niepożądanymi przesyłkami reklamowymi i telefonami.

Dr. Kei Ishii i Polina Roggendorf z projektu Konsumenci bezpieczni online prowadzonego przez Uniwersytet Techniczny w Berlinie poinformowali uczestników o bezpiecznym surfowaniu w Internecie. Na przykładzie trójwymiarowej struktury konstrukcyjnej rosyjskojęzycznej informacyjnej strony internetowej państwo Roggendorf i Ishii zademonstrowali niewidoczne powiązania Internetu. Wspomnieli, że wiele zdarzeń w Internecie odbywa się automatycznie i w sposób niewidoczny dla użytkownika. Celem niewidzialnego Internetu jest zbieranie danych. Istnieją jednak aplikacje, które pomagają w wykryciu, jakie przedsiębiorstwa śledzą zachowanie użytkownika podczas surfowania w sieci. Na przykładzie programu Ghostery dr Ishii pokazał, ile i które przedsiębiorstwa obserwują odwiedziny otwartej przez niego strony internetowej. Oznacza to, że te przedsiębiorstwa mają dostęp do danych użytkownika i używają ich we współpracy z cookies do celów reklamowych. Liczba takich działających w sposób niewidzialny stron internetowych podczas przeciętnego surfowania w sieci może wynosić ponad 100. Właściwym zagrożeniem zbierania danych nie jest reklama, ale niepożądane zapisywanie danych. Trend łączenia danych, które są zbierane z różnych źródeł, wciąż przybiera. Statystycznym ujmowaniem i wyjaśnianiem zgromadzonych danych zajmuje się na przykład Piwik-Analytics[1]. Dalej dr Ishii wyjaśnił, że operatorzy stron internetowych sami decydują, do jakiego zbioru danych z ich stron internetowych mogą mieć dostęp specjalistyczne przedsiębiorstwa. Poprzez zapytania w wyszukiwarkach, wywołanie stron internetowych itp. na przykład Google uzyskuje określone specyficzne informacje o użytkowniku, które w ciągu dziesiątych części sekundy za pomocą cookie-matching tzn. porównania cookie zostają przyporządkowane do oceny zachowania w Internecie i są sprzedawane przez Google w formie aukcji firmom reklamowym. Na koniec dr Ishii udzielił kilku rad na temat ochrony własnych danych podczas surfowania w Internecie: zabezpieczenie

[1] Piwik-Analytics jest alternatywą do Google Analytics. Ten program open-source służy do zbierania i analizy danych osób odwiedzających strony internetowe. (Źródło: http://www.piwik-analytics.com/)

komputera poprzez aktualizację oprogramowania i programu antywirusowego oraz poprzez używanie bezpiecznych haseł. Do ochrony danych niezwykle ważne są odpowiednie ustawienia i funkcje przeglądarki internetowej, na przykład usuwanie historii przeglądania i cookies oraz stosowanie rozszerzeń przeglądarki, np. Ghostery. Dalsze porady dotyczące zabezpieczenia komputera i danych osobowych użytkownicy znajdą w projektach Bezpieczni konsumenci online (https://www.verbraucher-sicher-online.de/) oraz Surfujący mają prawa (https://www.surfer-haben-rechte.de/). Ponadto konsumenci powinni w miarę możliwości obchodzić się oszczędnie ze swoimi danymi i nie przekazywać żadnych danych.

W dyskusji panelowej uczestniczyli Dr. Kei Ishii i Christian Dahler. Moderatorem dyskusji był Ünal Zeran, kierownik projektu z Hamburga. Dr. Turgut Altuğ, rzecznik do spraw ochrony środowiska i ochrony konsumentów Sojuszu 90/Zieloni w Izbie Deputowanych w Berlinie opowiedział się za tym, aby takie imprezy informacyjne przeprowadzać na miejscu w organizacjach migrantów, aby te informacje mogły również dotrzeć do tej grupy docelowej. Heike Ansorena, referentka do spraw ekonomicznej ochrony konsumenta w Administracji Senackiej do spraw Sprawiedliwości i Ochrony Konsumentów w odniesieniu do „Prawa do bycia zapomnianym“ (wyrok ETS) postawiła pytanie, dlaczego Google przy składaniu wniosku o skasowanie danych osobowych wymaga kopii dowodu osobistego. Pan Dahler odpowiedział, że żądanie kopii dowodu osobistego wprawdzie nie jest wymagane prawnie, także przy zawieraniu umów o telefony komórkowe, w rzeczywistości jednak te wytyczne nie są przestrzegane. Google lub inne firmy chcą w ten sposób zidentyfikować wnioskodawcę na podstawie jego dowodu osobistego. Nadto usunięcie danych przez Google nie oznacza całkowitego usunięcia z World Wide Web.

## Wniosek

Brak świadomości migrantów na temat ochrony danych, który ujawnił się już w Monitorze Konsumenta Berlin 2013, potwierdził się zarówno na warsztatach otwierających projekt dnia 14 marca 2014 r. jak również na tych drugich warsztatach. Informacje zwrotne od uczestników pokazały, jak ważne są konkretne wskazówki działań służących samodzielnej ochronie danych i ustawieniom bezpieczeństwa komputera. Uświadomienie migrantów w sprawie ochrony danych i wzmocnienie ich kompetencji medialnych muszą odgrywać ważniejszą rolę. Ponieważ Internet stanowi nieodzowne medium w codziennym życiu migrantów, którzy w sieci napotykają na większą ilość pułapek specyficznych dla tej grupy docelowej, Centrala Konsumencka w Berlinie planuje wydanie informacji na temat ochrony danych dla rosyjsko- i tureckojęzycznych migrantów we współpracy z Berlińskim Pełnomocnikiem ds. Ochrony Danych. W tej informacji dla konsumentów mają być wymienione rady w sprawie ochrony danych. Grupa docelowa ma zostać m.in. poinformowana o tym, dlaczego ważne są ustawienia bezpieczeństwa komputera i smartfona i dlaczego zalecana jest wstrzemięźliwość przy podawaniu danych osobowych w sieciach społecznościowych lub podczas korzystania z usług e-commerce. Treści te powinny być również dostępne na stronie internetowej Centrali Konsumenckiej. Planowane na listopad interaktywne forum projektowe ma zająć się przynajmniej jednym tematem związanym z ochroną danych.

## Informacje zwrotne od uczestników warsztatów

*„Dziękuję za dobre warsztaty!“*

*„Pragnę podziękować za zaproszenie na warsztaty w sprawie ochrony danych. Były one bardzo wzbogacające.“*

*„Dziękuję za zaproszenie! Zaraz ustawię zabezpieczenia w moim komputerze!“*