Kontakt dla mediów:
Luiza Nowicka, PARP
e-mail: luiza_nowicka@parp.gov.pl
tel.: 880 524 959

Informacja prasowa
Warszawa, 14.06.2022 r.

Projektowanie prywatności. Jak chronić dane osobowe i bezpiecznie korzystać z nowych technologii?

Rozwój nowoczesnych technologii otwiera wiele możliwości, ale wiąże się także z licznymi zagrożeniami. Użytkownicy często nie zdają sobie sprawy z tego, jak niebezpieczne może być dzielenie się swoimi danymi osobowymi. Niezwykle istotne jest, by działania mające na celu zapewnienie ochrony prywatności i bezpieczeństwa danych, były podejmowane już w fazie projektowania nowych rozwiązań technologicznych.

Kilka słów na temat rewolucji nowych technologii

Wpływ nowoczesnych technologii na rozwój społeczny i gospodarczy jest nie do przecenienia. Szczególnie można się było o tym przekonać przez ostatnie lata pandemii COVID-19, kiedy to dzięki powszechnemu wykorzystaniu technologii informacyjno-komunikacyjnych, możliwa była praca, edukacja, czy podtrzymywanie więzi społecznych. Rozwój technologii cyfrowych jest faktem, to nie tylko ostatnie 2 lata, ale od przełomu XX i XXI wieku obserwowana jest intensyfikacja cyfryzacji w wielu obszarach życia. W gospodarce, w sektorze publicznym, w usługach, we wspomnianej już edukacji. Z roku na rok nowe technologie odgrywają coraz większą rolę. O skali zmian, świadczy fakt, że na co dzień używamy wielu urządzeń z przedrostkiem – smart, których moce obliczeniowe znacznie przekraczają moc komputera wykorzystanego w 1969 roku do lotu na Księżyc. Obecnie mówi się o czwartej rewolucji technologicznej (po wynalezieniu maszyny parowej, elektryczności i automatyzacji oraz komputeryzacji). Rewolucji, która niesie ze sobą szansę na rozwój społeczno-gospodarczy.

Jednocześnie, niejako na żywym organizmie, doświadczamy też negatywnych konsekwencji zachodzących przemian. Pojawiają się nawet głosy, mówiące o tyranii technologii, kiedy to sztuczna inteligencja, czy Internet rzeczy niosą ze sobą zagrożenia dla prywatności informacyjnej, czyli sprawowania kontroli nad informacjami dotyczącymi osób korzystających z tych nowoczesnych rozwiązań.

Jak zatem zadbać o własne bezpieczeństwo i ochronę prywatności, kiedy korzystamy ze smartfonów, komputerów, sieci Internet, smart TV etc.? Na co zwracać uwagę przy projektowaniu nowych rozwiązań technologicznych, aby potencjalne zagrożenia nie zniweczyły szans na rozwój?

Czym jest projektowanie prywatności?

Korzystanie z nowoczesnych technologii ma swoją cenę, nie tylko tę wyrażoną wprost w walucie za zakup danego urządzenia, czy usługi. Aby móc używać urządzenia typu smart, musimy podać swoje dane osobowe. Co prawda, założenie konta użytkownika wymaga podania ograniczonego zakresu tych danych (imię, nazwisko, adres e-mail). Jednak to nie koniec. W trakcie użytkowania tego typu urządzeń, zbierają one szereg dodatkowych danych (m.in.: dane lokalizacyjne, identyfikator internetowy, logi, informacje dotyczące naszych zachowań – np. czy śpimy, biegamy, chodzimy, etc.). Tym samym jakiekolwiek zdarzenie skutkujące utratą poufności, dostępności, czy integralności danych osobowych może skutkować negatywnymi konsekwencjami dla osób, których te dane dotyczą (może prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych).

Urząd Ochrony Danych Osobowych – w poradniku dla nauczycieli i uczniów, pt. „Warto wiedzieć... Nowe technologie a prywatność. Jak zadbać o bezpieczeństwo w internecie?", wydanym z okazji Dnia Nowych Technologii w Edukacji – wskazuje na zagrożenia, jakie mogą być skutkiem nieświadomego korzystania z nowych technologii. Są to: utrata dostępu do kont internetowych, uzyskanie dostępu do nieodpowiednich do wieku nielegalnych treści, doświadczenie hejtu, fake news, deepfake, infekowanie sprzętu złośliwym oprogramowaniem, czy atak socjotechniczny.

Dla lepszego uzmysłowienia wagi potencjalnych zagrożeń, należy przywołać sens słów wypowiedzianych przez wiceprezesa jednej z dużych firm motoryzacyjnych. Otóż producenci nowych technologii wiedzą o użytkownikach wszystko – co i kiedy robimy, kto łamie prawo.

Wspomniane zagrożenia, coraz częściej z kolei wpływają na budowanie świadomości użytkowników. Z przeprowadzonych przez Fortinet badań nt. rozwiązań typu smart wynika, że użytkownicy mają obawy związane z naruszeniem ich prywatności, oczekują większej kontroli nad swoimi danymi osobowymi oraz wskazują na producentów, jako odpowiedzialnych za bezpieczne przetwarzanie danych osobowych.

– Tym samym projektowanie prywatności będzie w głównej mierze sprowadzało się do uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych – privacy by design/default – podkreśla **Jacek Przygoda** z Polskiej Agencji Rozwoju Przedsiębiorczości.

Wymagania te zostały wprost wyrażone w obowiązujących przepisach o ochronie danych osobowych (RODO) oraz standardach z rodziny ISO (m.in.: seria 2700).

Jakie są zasady (dobre praktyki) projektowania prywatności?

– Projektowanie prywatności w praktyce polega przede wszystkim na całościowej analizie procesu przetwarzania danych (od początku do końca cyklu), analizie potencjalnych ryzyk dla ochrony

danych osobowych i doborze adekwatnych zabezpieczeń, zastosowaniu odpowiednich rozwiązań technicznych i organizacyjnych – dodaje **Jacek Przygoda**.

Co ważne – należy pamiętać, aby ww. działania miały miejsce jeszcze przed rozpoczęciem procesu przetwarzania danych (stąd „w fazie projektowania"). Powszechnym błędem jest zajmowanie się ochroną danych osobowych i prywatności osób, których te dane dotyczą, w momencie, kiedy przetwarzanie danych już trwa, a nawet dopiero w momencie materializacji jakiegoś zagrożenia (np. wycieku danych). Dobrze zaprojektowany pod względem prywatności proces przetwarzania danych będzie zapewniał osobie, której dane dotyczą, wiedzę na temat wykorzystania jej danych – w jakim celu będą gromadzone, w jakim zakresie i kto będzie miał do nich dostęp, w jaki sposób może sprawować kontrolę nad swoimi danymi. Należy pamiętać o minimalizacji przetwarzanych danych, pseudonimizacji, przejrzystości co do funkcji i przetwarzania danych osobowych (np. niestosowanie tzw. domyślnych zgód, czyli checkboxów lub suwaków ustawionych w pozycji na „tak", kiedy to brak podjęcia działania przez użytkownika oznacza de facto zgodę na przetwarzanie jego danych w jednym lub kilku celach), umożliwieniu osobie – której dane dotyczą – monitorowania i przetwarzania danych.

Bardzo ważne jest także budowanie świadomości bezpiecznego korzystania z nowych technologii wśród użytkowników. Wdrożenie zabezpieczeń przez producentów nie będzie wystarczająco skuteczne, jeśli zostanie pominięty tzw. ludzki aspekt w projektowaniu prywatności. We wspomnianym poradniku Urzędu Ochrony Danych Osobowych przedstawione zostały podstawowe zasady dbania o bezpieczeństwo swoich danych i prywatności. Należy pamiętać o korzystaniu tylko z zaufanego łącza, używać silnych i zróżnicowanych haseł, kontrolować – co i komu udostępniamy poprzez zarządzanie uprawnieniami w aplikacji, zwracać uwagę na to – kto i jak zamierza korzystać z twoich danych osobowych (zapoznać się z polityką prywatności i klauzulą informacyjną), ograniczać ujawniane o sobie informacje. Stosując się na co dzień do tych zasad minimalizujemy ryzyko wystąpienia zagrożeń dla naszej prywatności.

Jaki jest wpływ nowych technologii na podnoszenie konkurencyjności firm – wyzwania i rekomendacje

O szansach, jakie niesie ze sobą wykorzystanie nowoczesnych technologii, można było się przekonać podczas kolejnych fal pandemii wirusa SARS-CoV-2. Firmy, które wdrożyły narzędzia służące do pracy zdalnej lub zdalnej obsługi klienta, zyskiwały na konkurencyjności. Nowe technologie w biznesie to przede wszystkim możliwości dostosowania procesów biznesowych do zmiennych warunków otoczenia biznesowego. Zastosowanie innowacyjnych rozwiązań to szansa na poprawę konkurencyjności i rozwoju firmy. Zapewnienie przy tym bezpieczeństwa danych osobowych i ochrony prywatności użytkowników (pracowników, klientów) – może stanowić wartość dodaną dla przedsiębiorstwa.

W dzisiejszych czasach, dzięki ewolucji technik analitycznych, przetwarzamy w czasie rzeczywistym ogromne ilości danych, przy czym umiejętność gromadzenia i przetwarzania danych staje się coraz bardziej istotnym czynnikiem w gospodarce, przede wszystkim w branży finansowej i

ubezpieczeniowej, telekomunikacji, ale także różnego rodzaju branżach z sektora produkcji czy handlu.

Możliwości zastosowania tzw. Big Data przez przedsiębiorców to przede wszystkim monitorowanie procesów i działalności, prognozowanie trendów, zdarzeń i wyników biznesowych, personalizowanie komunikacji w obszarach marketingu i sprzedaży czy ocena ryzyka, a w konsekwencji przewaga nad konkurencją, potencjalne oszczędności i nowe obszary biznesowe poprzez bezpośrednią, zindywidualizowaną obsługę klienta.

Duże nadzieje wiąże się także z użyciem sztucznej inteligencji (AI) i przetwarzaniem danych w systemach AI – obszarem, którego przynajmniej częściową regulacją planuje zająć się Komisja Europejska. Stosując podejście oparte na ryzyku, zaproponowano w projekcie Rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) cztery obszary zastosowania AI, stwarzające ryzyko niedopuszczalne. Jeden z nich to systemy AI stosujące techniki podprogowe, wykorzystujące dowolne słabości określonej grupy osób ze względu na ich wiek, niepełnosprawność ruchową lub zaburzenie psychiczne. Kolejny to systemy na potrzeby oceny lub klasyfikacji wiarygodności osób fizycznych prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych bądź przewidywanych cech osobistych lub cech osobowości (social scoring), prowadzące do krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych. Zakazane jest także wykorzystywanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa.

W sytuacji, kiedy istnieją już algorytmy AI skutecznie naśladujące działanie ludzkiego mózgu (w szczególności technologia głębokich sieci neuronowych), stworzenie listy zakazanych praktyk i ram regulacyjnych dotyczących AI wydaje się nieuniknione.

Wysokie koszty związane z wdrażaniem nowych technologii, brak wiedzy w tym obszarze, brak wykształconej kultury organizacji w obszarze projektowania prywatności stanowią niewątpliwie przeszkody, a nawet i zagrożenia dla wspomnianych szans.

– Dlatego jednym z głównych wyzwań dla firm chcących rozwijać się z wykorzystaniem nowych technologii jest budowanie świadomości zarządzania prywatnością, w tym kultury ochrony danych osobowych. Nie ma bowiem sprzeczności w rozwoju firmy poprzez otwarcie się na nowe technologie, a zadbaniem o ochronę danych osobowych i prywatności. Brak nowych technologii lub nieumiejętne ich wykorzystanie będzie zawsze zagrożeniem dla organizacji. Projektowanie prywatności jest zatem inwestycją w rozwój firmy – zaznacza **Miłosław Madziar** z PARP.

Na szczęście, niektóre firmy zdają już sobie sprawę z tego, jak ważne jest odpowiednie zarządzanie prywatnością. Polskie startupy, które oferują ciekawe rozwiązania w zakresie ochrony danych osobowych, otrzymały wsparcie z Funduszy Europejskich w ramach organizowanych przez PARP Programów Akceleracyjnych finansowanych z Programu Inteligentny Rozwój (PO IR).

Jedną z firm, która otrzymała dotację, jest Octagon sp. z o.o. Startup opracował projekt Dataphora, który ma umożliwić skalowalny, efektywny i bezpieczny transfer wrażliwych danych osobowych klientów pomiędzy różnymi centrami biznesowymi banku. Główną ideą jest użycie blockchainowego paradygmatu Suwerennej Tożsamości, w którym klient banku w pełni kontroluje przepływ swoich danych. W rezultacie użytkownik końcowy staje się łącznikiem między jednostkami banku, więc bez jego zgody nie może dojść do żadnego transferu danych. Odbiorcą technologii jest Santander Bank Polska.

Wsparcie z Funduszy Europejskich otrzymała także firma Privacy Optimization sp. z o.o. Projekt zakładał stworzenie oprogramowania umożliwiającego zoptymalizowane zarządzanie naruszeniami danych osobowych. To pionierskie narzędzie reagowania na naruszenia prywatności, pomagające organizacjom w analizie incydentów związanych z danymi osobowymi, ocenie ryzyka i terminowym zgłaszaniu naruszeń danych osobowych odpowiednim organom ochrony danych. Odbiorcą technologii również jest Santander Bank Polska.