PREZES URZĘDU
OCHRONY DANYCH
OSOBOWYCH
dr Edyta Bielak-Jomaa

Warszawa, dnia stycznia 2019 r.

ZSPR.027.417.2018

Pan
Adam Bodnar
Rzecznik Praw Obywatelskich
Al. Solidarności 77
00-090 Warszawa

W związku z Pańskim wystąpieniem z dnia 9 grudnia 2018 r., (sygn. VII.520.76.2018.KŁ), dotyczącym wątpliwości związanych z wykorzystywaniem urządzeń rejestrujących tzw. odręczny podpis biometryczny, uprzejmie wyjaśniam co następuje.

Zgodnie z art. 4 pkt. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[1], zwanego dalej rozporządzeniem 2016/679 danymi biometrycznymi są dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

Rozstrzygając wątpliwości wokół kwalifikacji danych biometrycznych jako danych osobowych, wskazała Grupa Robocza Artykułu 29 ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, która jest niezależnym organem doradczym w sprawach ochrony danych i prywatności, powołanym na mocy artykułu 29 Dyrektywy o ochronie danych 95/46/WE. W

[1] Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm. - Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

skład tego organu wchodzą przedstawiciele krajowych organów ochrony danych z państw członkowskich UE, Europejskiego Inspektora Ochrony Danych oraz Komisji Europejskiej. Jego zadania opisane zostały w artykule 30 Dyrektywy 95/46/WE i artykule 15 Dyrektywy 2002/58/WE. Do kompetencji Grupy Roboczej Artykułu 29 należy badanie kwestii dotyczących zastosowania dyrektyw o ochronie danych w celu przyczynienia się do jednolitego stosowania dyrektyw. Grupa Robocza realizuje to zadanie wydając rekomendacje, opinie i dokumenty robocze.

W związku z powyższym Grupa Robocza Art. 29[2] podnosiła, iż w większości przypadków przetwarzane informacje stanowić będą dane osobowe w rozumieniu art. 2 lit. a dyrektywy 95/46. Są to bowiem dane związane z określoną osobą fizyczną, pozwalające na ustalenie lub potwierdzenie czyjejś tożsamości. Ostatecznie natomiast jest to uzależnione od tego, czy podmiot stosujący narzędzia kontroli biometrycznej posiada dostęp do innych informacji odnoszących się do osoby kontrolowanej, tak aby możliwa była jej identyfikacja. Zgodnie z art. 4 pkt 14 rozporządzenia ogólnego dane biometryczne to dane osobowe, które dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

Urząd Ochrony Danych Osobowych (ani uprzednio Generalny Inspektor Ochrony Danych Osobowych) nie przeprowadzał dotąd badań w zakresie przepływu danych elektronicznych wygenerowanych podczas składania własnoręcznego podpisu na urządzeniu elektronicznym, sposobu ich powiązania z informacją, której mają dotyczyć oraz sposobu zapisu tych informacji, zwłaszcza zaś ustalenie, czy zapis ten zawiera informację dotyczącą dynamiki składania podpisu.

W związku z tym Urząd Ochrony Danych Osobowych może odnieść się do interesującej Pana kwestii jedynie teoretycznie podkreślając, że zgodnie z zasadą integralności i poufności (art. 5 ust. 1 lit. f rozporządzenia 2016/679) dane są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Powszechnie przyjmuje się, że integralność danych oznacza właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany. Poufność danych to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom, zaś rozliczalność to właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Omawiana zasada została skonkretyzowana w dalszej części rozporządzenia. Zgodnie z art. 32 ust. 1 rozporządzenia 2016/679, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot

[2] Grupa Robocza Art. 29 przyjęła Opinię 3/2012 w sprawie sytuacji w dziedzinie technologii biometrycznych (WP 193)

przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym m.in. w stosownym przypadku:

1)pseudonimizację i szyfrowanie danych osobowych;

2)zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

3)zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

4)regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Jednocześnie informuję, że problemem żądania składania przez klienta firm własnoręcznego podpisu elektronicznego na urządzeniu elektronicznym jest analizowany przez organy ochrony danych zrzeszone w ramach Międzynarodowej Grupy Roboczej ds. Ochrony Danych w Telekomunikacji (tzw. Grupy Berlińskiej, której UODO jest członkiem) i budzi wiele wątpliwości. Dotyczą one m.in. faktu, że w przypadku aplikacji stosowanych przez niektóre banki czy operatorów telefonicznych po złożeniu własnoręcznego podpisu, klient nie ma już nad nim kontroli. Zastrzeżenia odnoszą się również do tego, że tylko od firmy stosującej tego tupu rozwiązania zależy to, do jakiego dokumentu podpis będzie dołączony. Niektóre podmioty, zauważając niedostatki istniejących rozwiązań, podpisują porozumienia z organem certyfikacyjnym, w rezultacie których organ certyfikacyjny używa klucza do odszyfrowania danych dostarczonych przez klienta, a odszyfrowane dane przekazywane są na podstawie warunków umowy (np. do danego eksperta sądowego). Niemniej warunki te mogą być kształtowane dowolnie, a klient nie ma na to żadnego wpływu. Grupa Berlińska zaniepokojona jest również faktem, że stosowane obecnie rozwiązania dotyczące własnoręcznego podpisu składanego na urządzeniu elektronicznym (podpisu biometrycznego) nie spełniają wymogów dla zaawansowanych podpisów elektronicznych i tym samym także wymogów dla kwalifikowanego podpisu elektronicznego przewidzianych w *Rozporządzeniu Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającym dyrektywę 1999/93/WE.*

Podobne praktyki stosowane również przez inne podmioty, jako potwierdzenie określonych działań, jak np. faktu wyrażenia woli przez składającego taki podpis, mogą być coraz powszechniejsze.

Biorąc powyższe pod uwagę, w celu zajęcia wiążącego stanowiska w omawianej sprawie, konieczne jest przeprowadzenie badań w zakresie przepływu danych elektronicznych wygenerowanych podczas składania własnoręcznego podpisu na urządzeniu elektronicznym, sposobu ich powiązania z informacją, której mają dotyczyć, oraz sposobu zapisu tych informacji, zwłaszcza zaś ustalenie, czy zapis ten zawiera informację dotyczącą dynamiki składania podpisu

(szybkości ruchu i nacisku rysika na urządzenie itp.) Niezbędne jest również zbadanie tej technologii pod kątem stosowania rozwiązań związanych z ochroną prywatności, takich jak zasada wbudowywania elementów wspierających prywatność na każdym etapie realizacji projektu (tzw. Privacy By Design) oraz przeprowadzenia szacunkowej oceny wpływu zastosowanej technologii na ochronę prywatności (czyli wykonanie tzw. Privacy Impact Assessment).

Ponadto zgodnie z przepisami rozporządzenia 2016/679, administrator zobowiązany jest do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych. W toku procesu szacowania ryzyka oraz wdrażania zabezpieczeń, administrator powinien uwzględnić m.in. charakter, zakres, kontekst i cele przetwarzania danych osobowych, a także prawdopodobieństwo wystąpienia i wagę potencjalnych zagrożeń. Należy uznać, że ewentualny wyciek danych biometrycznych generalnie zawsze skutkował będzie stosunkowo dużym ryzykiem naruszenia praw i wolności osób fizycznych. Ponadto, z uwagi na konieczność uwzględnienia kontekstu przetwarzania dane biometryczne, jako dane szczególnej kategorii, zawsze muszą być zabezpieczone w szczególny sposób. Innymi słowy, wymagania w odniesieniu do danych biometrycznych są zawsze wyższe niż w stosunku do zwykłych danych.