OCHRONA DANYCH OSOBOWYCH W PRAKTYCE UNIWERSYTETU WARSZAWSKIEGO

– pytania i odpowiedzi

UNIWERSYTET WARSZAWSKI

Opracował: Dominik Ferenc
Administrator Bezpieczeństwa Informacji

Warszawa 2018 r.

Spis treści

1. **Czy zgodne z prawem jest umieszczanie imion i nazwisk kandydatów na I rok studiów, bez ich zgody, na listach wyników egzaminów wstępnych?**

TAK, zgodnie z art. 169 ust. 16 ustawy Prawo o szkolnictwie wyższym wyniki postępowania rekrutacyjnego są jawne.

2. **Czy uprawnione jest publikowanie list zawierających dane osobowe studentów wraz z wynikami z egzaminów w ramach realizowanego toku studiów?**

NIE, jedyną podstawą prawną uprawniającą do publikowania (np. zamieszczania na stronach internetowych) list zawierających dane osobowe studentów (np.: nr PESEL, imię i nazwisko, nr indeksu) wyników z egzaminów jest zgoda osoby, której dane dotyczą. Ustawa Prawo o szkolnictwie wyższym nie przewiduje takiej formy upublicznienia wyników z egzaminów cząstkowych. Aby jawnie publikować wyniki z egzaminów, należy posiadać zgodę osoby, której dane dotyczą.

3. **Czy dane studenta przetwarzane są na podstawie zgody na przetwarzanie danych??**

NIE, dane osobowe studentów przetwarzane są na podstawie przesłanki wynikającej z art. 6 ust. 1 lit. c GDPR*, a więc w celu wypełnienia obowiązku prawnego wynikającego z ustawy Prawo o szkolnictwie wyższym.

4. **Czy zgodna z prawem jest praktyka zatrzymywania dokumentów tożsamości przez biblioteki czy domy studenta?**

NIE, takie postępowanie jest sprzeczne z przepisami ogólnego rozporządzenia o ochronie danych osobowych. Zatrzymywanie dokumentu może odbywać się tylko na podstawie konkretnego przepisu prawa. Zgodnie z ustawą o ewidencji ludności i dowodach osobistych, zatrzymanie dowodu osobistego może odbywać się tylko w określonych w ustawie przypadkach. Mimo iż nie ma uregulowanego prawem zakazu pozostawiania legitymacji studenckich, przetrzymywanie ww. dokumentu jest zabronione. Dozwolone natomiast jest przedstawienie dokumentów tożsamości do wglądu i ewentualnego spisania danych.

5. **Do UW zwraca się pracodawca z prośbą o potwierdzenie wykształcenia (dyplomu) studenta, co robić?**

Uniwersytet Warszawski przetwarza dane osobowe w celu realizacji obowiązków wynikających z ustawy Prawo o szkolnictwie wyższym, aby udostępnić dane (czyt. potwierdzić wykształcenie) podmiot zwracający się z wnioskiem o udostępnienie danych osobowych powinien wskazać podstawę prawną udostępnienia – spełnić choć jedną przesłankę z art. 6 GDPR.

Pracodawca zgodnie z ustawą Kodeks pracy ma prawo żądać od pracownika udokumentowania danych przez dostarczenie dowodu osobistego, świadectwa pracy czy dyplomu. Natomiast prowadzenie tzw. background screening (weryfikacji przedstawionych

* Rozporządzenie 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) – General Data Protection Regulation)

przez pracownika danych) wymaga wyraźnej zgody pracownika. Pracodawca powinien uzyskać zgodę pracownika na ew. sprawdzenie podanych przez niego informacji – zgoda taka powinna być udzielona na jasno określony cel i zakres. Jeżeli natomiast została nam przesłana kopia dyplomu, powinniśmy zweryfikować jego autentyczność, w przypadku weryfikacji negatywnej, należy zgłosić ten fakt na policję.

6. **Czy na stronie Uniwersytetu Warszawskiego można publikować wizerunek sprawcy czynu zabronionego (zdjęcia, nagrania wideo)?**

NIE. W świetle ustawy o ochronie danych osobowych – nikt nie może udostępniać danych osobowych, osoby, której dane dotyczą, jeżeli nie została spełniona jedna z przesłanek wynikających z art. 6 GDPR – stanowisko to dotyczy także upubliczniania zapisu z monitoringu wizyjnego. Z art. 23 ustawy Kodeks cywilny (tekst jednolity: Dz. U. z 2018 r. poz. 650) wynika wprost, że wizerunek jest dobrem osobistym człowieka i nie ma przy tym znaczenia, że osoba może zostać uznana za sprawcę czynu zabronionego. Warto jednak zwrócić uwagę na art. 13 ust. 3 ustawy Prawo prasowe, który wskazuje, iż: właściwy prokurator lub sąd może zezwolić, ze względu na ważny interes społeczny, na ujawnienie danych osobowych i wizerunku osób, przeciwko którym toczy się postępowanie przygotowawcze lub sądowe. policja natomiast publikuje wizerunki i dane osób, wobec których organy - prokuratury lub sądy wydały zgodę na publikację listu gończego. Uprawnienie to wynika z art. 21 ustawy o policji. Pobieranie danych i wizerunków osób poszukiwanych i zaginionych ze stron serwisu policji, a następnie umieszczanie na innych niż policyjne stronach internetowych jest dozwolone.

7. **Czy zgodne z prawem jest publikowanie zdjęć studentów bez ich zgody?**

NIE. Wizerunek jest traktowany jako dobro osobiste człowieka w rozumieniu art. 23 ustawy Kodeks cywilny, aby publikować zdjęcia studentów na stronach należy posiadać zgodę osoby, której dane dotyczą.
Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej (art. 81 ustawy o prawie autorskim i prawach pokrewnych).
Zezwolenia nie wymaga rozpowszechnianie wizerunku:

- osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych,
- osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

8. **Czy dane osobowe na żądanie studentów UW mogą być przesyłane do innych administratorów danych?**

NIE, aby żądanie takie było zasadne przetwarzanie musiałoby odbywać się na podstawie zgody osoby, której dane dotyczą oraz odbywać się w sposób zautomatyzowany.
Jedyną prawnie dopuszczalną formą przesyłania danych osobowych studentów UW jest podstawa wynikająca z art. 165 ustawy Prawo o szkolnictwie wyższym w przypadku przeniesienia studenta z uczelni macierzystej do innej uczelni.

9. **Czy zgodne z prawem jest udostępnianie informacji zawierających dane osobowe przez telefon?**

NIE. Jeżeli nie mamy pewności co do osoby, z którą prowadzimy rozmowę, przekazywanie informacji zawierających dane osobowe jest zabronione.

10. **Czy dopuszczalne jest publikowanie w Internecie informacji o studentach wykreślonych z listy studentów?**

NIE, gdyż obowiązujące przepisy prawa nie kształtują takich obowiązków lub uprawnień uczelni, których realizacja wymagałaby publikacji danych o skreśleniu z listy studentów w Internecie.

11. **Czy członkowie komisji rekrutacyjnych/stypendialnych/konkursowych powinni posiadać upoważnienie do przetwarzania danych osobowych?**

TAK, członkowie komisji posiadają dostęp do danych osobowych, tym samym przetwarzają dane osobowe.
Procedura wydawania upoważnień została opisana w Rozdziale 10 Polityki ochrony danych osobowych załączonej do Zarządzenia nr 51 Rektora UW z dnia 15 maja 2018 r. w sprawie ochrony danych osobowych na Uniwersytecie Warszawskim.

12. **Czy dla pracownika, który posiada dostęp do danych osobowych powinno zostać wydane upoważnienie do przetwarzania danych osobowych?**

TAK, dla każdego pracownika posiadającego dostęp do danych osobowych powinno zostać wydane (przez Administratora lub kierownika jednostki organizacyjnej) upoważnienie do przetwarzania danych osobowych.
Procedura wydawania upoważnień została opisana w Rozdziale 10 Polityki ochrony danych osobowych załączonej do Zarządzenia nr 51 Rektora UW z dnia 15 maja 2018 r. w sprawie ochrony danych osobowych na Uniwersytecie Warszawskim.

13. **Czy każda osoba upoważniona do przetwarzania danych osobowych powinna przejść szkolenie z ochrony danych osobowych?**

TAK, każdy uprawniony do przetwarzania danych osobowych i innych informacji chronionych, musi być odpowiednio przeszkolony z zasad i przepisów dotyczących przetwarzania i ochrony danych osobowych.

14. **Czy podczas mojej nieobecności mogę przekazać osobie, która mnie zastępuje mój login oraz hasło do systemu?**

NIE, udostępnianie danych uwierzytelniających jest zabronione. W przypadku, gdy osoba zastępująca potrzebuje uzyskać dostęp o szerszym zakresie uprawnień, powinna zawnioskować zgodnie z przyjętą na UW procedurą o zwiększenie zakresu uprawnień.

15. Czy Uniwersytet Warszawski ma prawo publikować na swoich stronach internetowych dane osobowe pracowników?

TAK, informacje o pracowniku, takie jak jego imię i nazwisko, służbowy: numer telefonu, adres e-mail, są ściśle związane z wykonywaną przez niego pracą. Informacje takie mogą zostać podane do publicznej informacji bez zgody pracownika.

16. Co powinienem zrobić w przypadku czasowego opuszczenia stanowiska pracy?

W przypadku opuszczenia obszaru przetwarzania danych osobowych, gdy pozostaje on bez nadzoru osób upoważnionych, należy zamknąć pomieszczenie na klucz. Klucze do pomieszczeń powinny pozostawać pod nadzorem osób upoważnionych.
Czasowo opuszczając stanowisko pracy należy wylogować się z systemu lub uruchomić wygaszacz ekranu chroniony hasłem. Nie należy pozostawiać dokumentów zawierających dane osobowe w miejscu widocznym.
Po zakończonej pracy należy wylogować się ze wszystkich systemów, z których korzystaliśmy podczas pracy, zamknąć w szafach dokumenty zawierające dane osobowe lub inne tajemnice ustawowo chronione.

17. Jak długie powinno być hasło do systemu informatycznego?

Zaleca się stosowanie haseł o długości minimum 8 znaków, składających się z dużych i małych liter, cyfr oraz znaków specjalnych. Mile widziane są hasła o długości co najmniej 15 znaków.
Nie należy stosować haseł składających się z imion i nazwisk, dat urodzenia, haseł domyślnych takich jak: admin, hasło, password itp.
W przypadku konieczności zmiany hasła nie należy dokonywać „lekkiej" modyfikacji hasła starego.

18. Czy mam obowiązek posiadać służbowy adres e-mail??

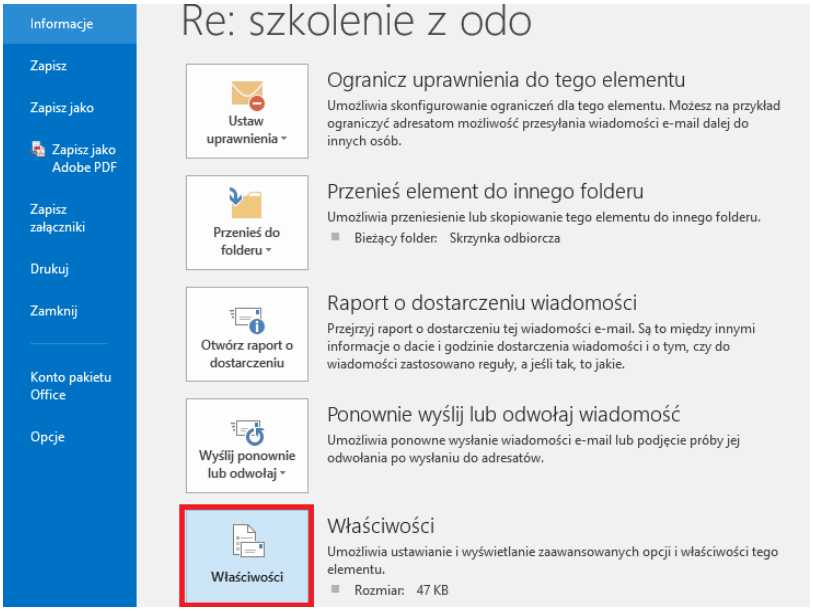
TAK, każda osoba realizująca zadania o charakterze służbowym powinna posługiwać się adresem mailowym założonym w domenie Uniwersytetu Warszawskiego. Korzystanie w celach służbowych z prywatnych adresów mailowych jest zabronione.

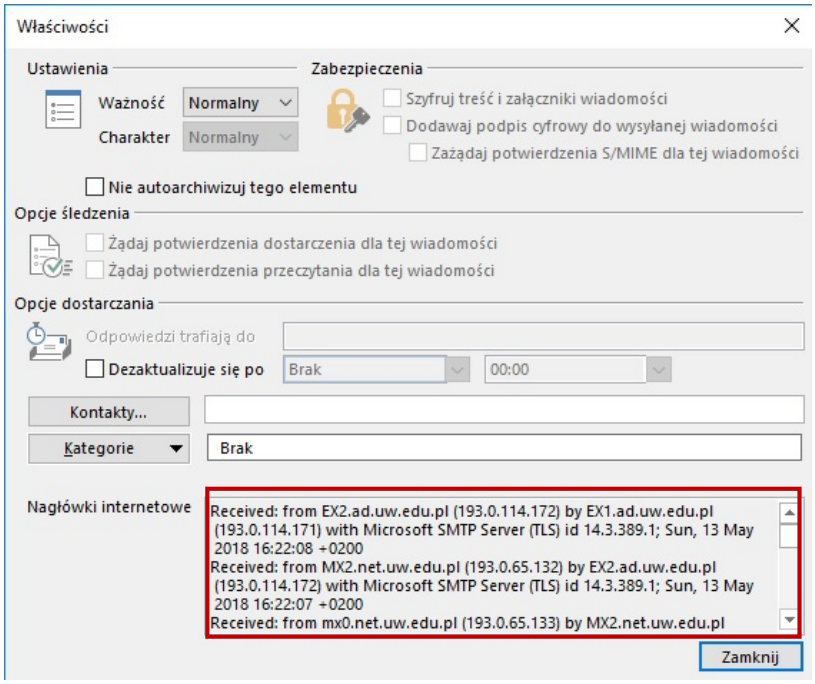
19. Co zrobić, jeżeli podejrzewam, że otrzymana przeze mnie wiadomość mailowa jest fałszywa i może zawierać szkodliwe oprogramowanie?

Użytkownicy poczty elektronicznej zobowiązani są do zwracania szczególnej uwagi na otrzymywane wiadomości elektroniczne:

- należy przeczytać uważnie wiadomość, w przypadku wątpliwości porównać ją z innymi mailami od tego samego nadawcy,
- zawsze sprawdzać adres mailowy nadawcy (czy nadawca czasem nie posłużył się tylko aliasem, a adres mailowy przypisany jest do innej domeny mailowej),
- nie należy otwierać załączników lub linków do stron internetowych, które budzą wątpliwość,
- należy sprawdzać co najmniej adres z linii Return-Path: tworzonej podczas przesyłania poczty, więc trudniejszej do zafałszowania, zaleca się także sprawdzenie linii Received: opisujące całą drogę maila.

Jak można sprawdzić linię Received?





Spreparowana wiadomość mailowa może zawierać załącznik ze szkodliwym oprogramowaniem, którego otworzenie może spowodować zainfekowanie komputera, czego wynikiem może być: wyłudzenie danych uwierzytelniających, zaszyfrowanie zawartości komputera lub serwera. Wiadomości o ww. treści należy zgłaszać do Help Desku poczty elektronicznej na adres: helpdesk@uw.edu.pl.

20. Czy przy masowej wysyłce maili należy posługiwać się polem ukryte do wiadomość?

TAK, podczas wysyłania wiadomości mailowej do wielu adresatów zalecane jest umieszczanie adresów mailowych w polu **ukryte do wiadomości (UDW)**, adres mailowy może stanowić informację, która pozwala na zidentyfikowanie konkretnej osoby fizycznej.

21. Co powinienem zrobić wysyłając wiadomość mailową zawierającą dokumenty z danymi osobowymi?

Wysyłając maile zawierające pliki z danymi osobowymi, plik należy co najmniej zabezpieczyć za pomocą hasła, które należy przekazać adresatowi w innej formie np. telefonicznie czy za pomocą smsa.

22. Przechowuję dane osobowe w chmurze co powinienem zrobić?

Pliki przechowywane w tzw. chmurze obliczeniowej, jeżeli zawierają dane osobowe lub inne informacje wymagające ochrony, powinny być zaszyfrowane, a dostęp do chmury powinny mieć tylko te osoby, którym dostęp do danych jest niezbędny w celu wykonywania obowiązków służbowych.

23. Jak postępować z danymi osobowymi przetwarzanymi w wersji papierowej?

- dokumenty i wydruki zawierające dane osobowe należy przechowywać w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych,
- użytkownicy są zobowiązani do stosowania „polityki czystego biurka", polega ona na zabezpieczeniu dokumentów zawierających dane osobowe w szafach, biurkach, pomieszczeniach zamykanych na klucz, ograniczając wgląd przez osoby nieupoważnione,
- dokumenty należy przenosić w sposób zapobiegający ich kradzieży, zgubieniu lub utracie,
- zalecane jest niszczenie dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

24. Jak postępować z elektronicznymi nośnikami danych osobowych?

- dane przechowywane są na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane. Po ustaniu czasu przechowywania zawartość nośnika danych podlega skasowaniu,
- dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane. Po upływie tego celu dane podlegają archiwizacji, skasowaniu lub anonimizacji,
- przenośne elektroniczne nośniki danych są przechowywane przez użytkowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach i meblach biurowych,
- w przypadku konieczności wyniesienia nośników danych poza jednostkę organizacyjną, użytkownik zobowiązany jest do zachowania szczególnej ostrożności i zabezpieczenia

nośnika, konieczne jest użycie środków ochrony kryptograficznej (szyfrowanie danych),

- w przypadku wykorzystywania elektronicznych urządzeń mobilnych (m.in. smartphone, tablet) wymaga się zastosowania następujących środków bezpieczeństwa: blokada ekranu (pin/hasło/symbol graficzny), szyfrowanie pamięci/karty pamięci, program antywirusowy, wyłączenie nieużywanych usług (np. wi-fi, bluetooth, nfc), instalowanie oprogramowania z zaufanych źródeł, używanie szyfrowania lub VPN podczas korzystania z publicznych hotspot-ów,
- w przypadku korzystania z komputerów przenośnych poza obszarem przetwarzania danych jednostki organizacyjnej, należy używać ich w sposób uniemożliwiający odczyt danych z ekranu przez osoby nieuprawnione i stosować środki ochrony kryptograficznej,
- za bezpieczeństwo komputerów przenośnych, urządzeń mobilnych, nośników danych odpowiadają ich użytkownicy. Zabrania się pozostawiania nośników danych bez nadzoru osoby upoważnionej.