OCHRONA DANYCH OSOBOWYCH W ZASOBACH LDAP – omówienie problematyki prawnej

Użyte w niniejszej opinii sformułowania oznaczają, co następuje:
Ustawa - ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. nr 101 z 2002 r., poz. 926).
UMK, uczelnia – Uniwersytet im. Mikołaja Kopernika w Toruniu

I. OCHRONA DANYCH OSOBOWYCH W UNII EUROPEJSKIEJ

Do najważniejszych obowiązujących europejskich aktów prawnych z zakresu ochrony danych osobowych należą:

1. Konwencja nr 108 rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych
2. Konwencja z Schengen, powołującą do życia specjalny system informacyjny
3. Karta Praw Podstawowych Unii Europejskiej oraz
4. dyrektywy.

Powyższe akty różnią się pomiędzy sobą zakresem i rangą, a co za tym idzie różny jest sposób w jaki ich postanowienia powinny zostać wdrożone do porządku prawnego kraju członkowskiego.

Implementacja poszczególnych rozwiązań tych aktów znajduje się obecnie na różnych poziomie zaawansowania w poszczególnych krajach członkowskich.

1. Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, podpisana w Strasburgu 28 stycznia 1981 r.

Konwencja była pierwszym aktem wysokiej rangi, który określił zasady przetwarzania danych. Weszła w życie 1 października 1985 r. i do tej pory ratyfikowała ją większość państw europejskich.

Konwencja, po wejściu w życie nie wywołuje żadnych skutków prawnych w stosunku do obywateli krajów, które ją ratyfikowały. Stanowi swego rodzaju porozumienie pomiędzy państwami. Zapewnia jednak wspólny poziom ochrony danych w skali europejskiej nie utrudniając jednocześnie wykorzystywania nowoczesnej techniki informacyjnej i telekomunikacyjnej. Konwencja wyznaczyła kierunek dalszego ustawodawstwa Unii w zakresie ochrony danych osobowych.

Celem Konwencji jest zapewnienie na obszarze państw członkowskich każdemu ochrony praw i wolności w związku z automatycznym przetwarzaniem danych. Jest to pierwszy akt, który określił czym są dane osobowe, które z nich w szczególności powinny być chronione, jakie prawa przysługują w związku z tym każdej osobie oraz jakie są obowiązki państw w tej dziedzinie. Konwencja precyzuje pojęcie

danych osobowych, określa zasady ochrony danych, a także przekazywanie danych osobowych pomiędzy krajami.

Ratyfikowanie Konwencji jest możliwe wyłącznie dla kraju, który wprowadził do swojego prawa przepisy konieczne dla realizowania zasad ochrony danych określonych w Konwencji. Polska podpisała Konwencje w 1999 r., zaś ratyfikowała ją 24 maja 2002 r., co było jednym z warunków koniecznych do spełnienia przed przystąpieniem do Unii.

2. **Konwencja z 19 czerwca 1990 r. poświecona znoszeniu kontroli granicznej pomiędzy państwami Wspólnoty Europejskiej, powołująca do życia System Informacyjny Schengen (Traktat z Schengen).**

Konwencja, w postanowieniach Tytułu IV części 3 określiła zasady funkcjonowania specjalnego systemu informacyjnego, tzw. Systemem Informacyjnym Schengen (SIS).

SIS został utworzony w celu udzielenia pomocy policji oraz organom celnym w zakresie wymiany informacji dotyczących osób przekraczających granice państw stanowiących strony porozumienia.

W istocie SIS składa się z szeregu wzajemnie zintegrowanych krajowych systemów informacyjnych. Informacje z SIS mogą być wykorzystane przez organy innego państwa niż ten, który dane wprowadził, lecz wyłącznie dla celów określonych w specjalnym raporcie.

Dane zawarte w SIS udostępniane są w sposób nieograniczony tylko określonym organom, w zakresie wykonywanych przez nie zadań. W ograniczonym natomiast zakresie prawo dostępu do danych przysługuje również organom wydającym wizy do danego kraju.
Każde udostępnienie danych jest rejestrowane w lokalnej strukturze SIS na okres sześciu miesięcy, po czym zapis dotyczący udostępnienia jest usuwany z SIS. Dane osobowe nie mogą być przetwarzane po usunięciu celu, dla którego zostały zebrane, przy zastrzeżeniu, iż cel ten powinien być weryfikowany co trzy lata.

Zasady dostępu do SIS regulują szczegółowo prawa państw-sygnatariuszy Traktatu, które ponoszą również odpowiedzialność za niezgodne z postanowieniami Traktatu udostępnienie danych osobowych oraz za ich aktualność i usunięcia z SIS.
Przestrzeganie postanowień Traktatu bada organ nadzoru, składający się z osób wyznaczonych przez sygnatariuszy traktatu.

3. **Karta Praw Podstawowych Unii Europejskiej, przyjęta i ogłoszona w Nicei, w grudniu 2000 r.**

Ten akt o bardzo ogólnym charakterze określa katalog podstawowych praw i wolności obywatela Unii. Katalog ten, poza wartościami uznawanymi powszechnie przez różne akty prawa międzynarodowego (m.in. prawo do godności osoby ludzkiej, prawo do życia, zakaz tortur i nieludzkiego traktowania, prawo do wolności, rzetelnego

procesu), zawiera też w art. 19 prawo do ochrony danych osobowych („Każdy ma prawo zdecydowania czy jego dane osobowe mogą być ujawnione i jak mogą być wykorzystane").

4. Dyrektywy Parlamentu Europejskiego oraz Rady.

Dyrektywy kierowane do państw członkowskich nie regulują bezpośrednio praw i obowiązków obywateli. Dyrektywy zobowiązują państwa, aby w swoim prawie wewnętrznym, realizowały wymagania dyrektyw, przy czym z reguły nie ma znaczenia forma implementacji postanowień danej dyrektywy. W zakresie ochrony danych osobowych wyróżniamy:

a) **Dyrektywa 95/46/WE Parlamentu Europejskiego oraz Rady** z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnym przepływie tych danych.

Zasady ochrony praw i swobód jednostek, szczególnie prawa do prywatności, które zawarte są w niniejszej dyrektywie, utrwalają i umacniają zasady wyrażone w Konwencji Rady Europy z dnia 28 stycznia 1981 w sprawie ochrony jednostek w zakresie automatycznego przetwarzania danych osobowych. Treść Dyrektywy jest interesująca głównie z uwagi na wyraźne wskazanie, iż odnosi się ona do zautomatyzowanego sposobu przetwarzania danych.
Postanowienia tej dyrektywy stanowiły podstawę dla rozwiązań polskiej ustawy o ochronie danych osobowych, szczególnie w zakresie definicji, zgodności przetwarzania z prawem oraz określenia zasad przetwarzania.

Dyrektywa zawiera najważniejsze definicje z zakresu ochrony danych osobowych, na których oparto definicje znajdujące się w polskiej ustawie, tj. danych osobowych, przetwarzania danych osobowych., Istotnie natomiast różni się od polskiej ustawy w zakresie ścisłego wyznaczenia różnicy między administratorem danych (oznacza osobę fizyczną lub prawną, urząd publiczny, agendę lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych; jeżeli cele i sposoby przetwarzania danych są określane w ustawach i innych przepisach krajowych lub przepisach Wspólnoty, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub ustawodawstwo Wspólnoty) a przetwarzającym (oznacza osobę fizyczną lub prawną, urząd publiczny, agendę lub inny organ przetwarzający dane osobowe w imieniu administratora danych).

Dane osobowe mogą być gromadzone do określonych, wyraźnych i legalnych celów oraz nie mogą być poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem. Dalsze przetwarzanie danych w celach historycznych, statystycznych lub naukowych nie będzie uważane za niezgodne z przepisami pod warunkiem stworzenia przez państwa członkowskie odpowiednich zabezpieczeń.

Administrator danych odpowiada w myśl postanowień Dyrektywy za ich przetwarzanie w zgodzie z prawem oraz w sposób rzetelny, zgodnie z celem, dla

jakiego zostały zebrane, za ich prawidłowość, aktualność, przechowywanie w formie umożliwiającej identyfikację osób oraz przy zastosowaniu odpowiednich zabezpieczeń.

Dyrektywa wymienia cele dozwolonego zbierania danych osobowych zbliżone do tych, jakie znajdują się w polskiej ustawie, przy podobnych zastrzeżeniach w zakresie szczególnych danych dotyczących np. poglądów politycznych, przekonań religijnych. Podobne rozwiązania znajdują się również w odniesieniu do informowania podmiotu danych osobowych o przetwarzaniu jego danych i prawa sprzeciwu w stosunku do przetwarzania danych.

Dyrektywa przewiduje także wprowadzenia obowiązku powiadomienia odpowiedniego organu nadzorczego o przewidywanych operacjach przetwarzania danych.

Dyrektywa w znikomym natomiast stopniu odnosi się do kwestii udostępniania danych.

b) **Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady** z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze telekomunikacyjnym.

Przedmiotem tej Dyrektywy jest harmonizacja przepisów państw członkowskich wymaganych dla zapewnienia ekwiwalentnego poziomu ochrony podstawowych praw i wolności, a w szczególności prawa do prywatności, odnośnie do przetwarzania danych osobowych w sektorze telekomunikacyjnym oraz w celu zabezpieczenia wolnego przepływu tego typu danych i sprzętu oraz usług telekomunikacyjnych we Wspólnocie.

Dyrektywa dotyczy przetwarzania danych w związku ze świadczeniem dostępnych publicznie usług telekomunikacyjnych w publicznych sieciach telekomunikacyjnych we Wspólnocie, w szczególności poprzez cyfrowe sieci usług zintegrowanych ISDN i publiczną cyfrową sieć ruchomą.

W szczególności Dyrektywa nakazuje dostawcom publicznie dostępnych usług telekomunikacyjnych podjęcie odpowiednich technicznych i organizacyjnych środków w celu zapewnienia bezpieczeństwa oferowanych przez nich usług, odnośnie do bezpieczeństwa sieci. W przypadku szczególnego ryzyka naruszenia bezpieczeństwa sieci, dostawca publicznie dostępnych usług telekomunikacyjnych musi poinformować abonentów o zaistniałym ryzyku i o możliwych środkach zaradczych, włącznie ze związanymi z tym kosztami.

Jednocześnie Dyrektywa zezwala jednak na udostępnianie danych osobowych w drukowanych, elektronicznych lub telefonicznie dostępnych książkach telefonicznych, przy czym w takich przypadkach publikowane dane powinny być ograniczone do minimum niezbędnego do rozpoznania określonego abonenta,

chyba, że w sposób wyraźny zezwoli on na publikację większej liczby informacji o swojej osobie. Abonent powinien być również uprawniony do bezpłatnego zastrzeżenia swoich danych.

c) **Dyrektywa 2000/31/WE Parlamentu i Rady WE** z dnia 8 czerwca 2000r. w sprawie niektórych aspektów prawnych usług w społeczeństwie informacyjnym, a w szczególności handlu elektronicznego w obrębie wolnego rynku ("Dyrektywa dotycząca handlu elektronicznego").

Dyrektywa określa prawa i obowiązki adresatów i świadczących tzw. usługi społeczeństwa informacyjnego, tj. świadczone drogą elektroniczną, z którymi wiąże się wykorzystanie danych osobowych niezbędnych dla skutecznego zawierania umów, a także komunikacji pomiędzy stronami takich umów.

Z uwagi na zdalną i elektroniczną formę udostępniania i przekazywania danych osobowych przyjęto w omawianej Dyrektywie zasadę przejrzystości działań świadczącego usługi oraz ochrony prywatności adresata usługi.

Dane osobowe powinny być przetwarzane przede wszystkim za zgodą usługobiorcy, a nadto usługobiorca ma obowiązek sprawdzania czy adresat świadczonej przez niego usługi nie zażądał zaprzestania korzystania z jego danych osobowych – tzw. „opt-out".

Dane zbierane od usługobiorcy powinny być ograniczone do niezbędnego minimum, koniecznego do wywiązania się z umowy o świadczenie usługi.

d) **Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady** z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (Dyrektywa o ochronie prywatności i komunikacji elektronicznej).

Przepisy niniejszej dyrektywy rozwijają i uzupełniają postanowienia omówionej powyżej Dyrektywy 95/46/WE w zakresie korzystania przez osoby fizyczne z publicznie dostępnych usług w komunikacji elektronicznej w publicznych sieciach komunikacyjnych we Wspólnocie w celach prywatnych lub gospodarczych, nawet w przypadkach, gdy nie są abonentem danej usługi.

Przepisy Dyrektywy określają sposoby przekazywania danych osobowych, włączając w to np. prezentację numeru, ujawnianie danych w spisach abonentów, bilingach.

Artykuły 4 i 5 mówią wprost o bezpieczeństwie sieci oraz o obowiązku informowania przez dostawcę usług o zagrożeniu bezpieczeństwa sieci, za której pomocą przetwarzane są dane osobowe.

Dyrektywa łączy z bezpieczeństwem również zagadnienie poufności danych przesyłanych w sieciach, tj. zakaz m. in. kopiowania tych danych.

Istotne wydaje się, iż Dyrektywa nakłada na dostawcę usług obowiązek poinformowania abonenta usługi o celach przetwarzania oraz prawie sprzeciwu wobec tego rodzaju przetwarzania przez administratora danych w przypadku dostępu za pomocą sieci do danych przechowywanych w terminalu abonenta.

Dyrektywa 2002/58/WE uchyla Dyrektywę 97/66/WE z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze telekomunikacyjnym. Uchylenie to nastąpi z dniem 31 października 2003 r.. Do tego czasu państwa członkowskie zobowiązane są wprowadzić w życie postanowienia Dyrektywy 2002/58/WE.

Pozostałymi europejskimi aktami prawnymi niższej rangi są rekomendacje i rezolucje Rady Europy oraz rezolucje wydawane przez Parlament Europejski.

II. ZBIERANIE, ADMINISTROWANIE I UDOSTĘPNIANIE DANYCH OSOBOWYCH NA PODSTAWIE USTAWY O OCHRONIE DANYCH OSOBOWYCH Z DNIA 29 SIERPNIA 1997 R.

A. Zbieranie i administrowanie danymi.

1. Status administratora danych.

Nie istnieje odrębna procedura „mianowania" administratora. W przypadku spełnienia przez dany podmiot warunków określonych ustawą – staje się on administratorem i jest zobowiązany do przestrzegania obowiązków określonych w ustawie.
Definicja administratora, zawarta w art. 7 ust. 1 pkt 4) Ustawy zawiera dwa elementy:

a) Przynależność danego podmiotu do określonego w art. 3 Ustawy zakresu podmiotowego. Wymienione są tu dwie kategorie podmiotów, do których stosuje się przepisy Ustawy: podmioty prywatne i podmioty publiczne.
   Do podmiotów publicznych, oprócz organów państwowych oraz samorządu terytorialnego należą także inne państwowe i komunalne jednostki organizacyjne, a także podmioty niepaństwowe realizujące zadania publiczne.
   Szkoła wyższa, będąca państwową jednostką organizacyjną, działająca w oparciu o ustawę z 12 września 1990 r. o szkolnictwie wyższym, realizująca zadania publiczne z zakresu edukacji narodowej - należy do kategorii podmiotów publicznych.

b) Spełnienie pierwszego warunku nie wystarcza jednak do uznania tego podmiotu za administratora danych. Drugim elementem definicji administratora danych jest posiadanie przez dany podmiot kompetencji decyzyjnych w stosunku do danych podlegających przetworzeniu („decydowanie o celach i środkach przetwarzania danych").

Nie każdy zatem organ dysponujący danymi osobowymi będzie administratorem danych w rozumieniu ustawy. Będzie nim tylko ten organ, który podejmuje decyzję co do celu w jakim dane są przetwarzane oraz środków, czyli metody ich przetwarzania.

Spełnienie obu przesłanek opisanych powyżej klasyfikuje dany podmiot jako administratora danych w rozumieniu Ustawy.

Pojęcie administratora danych nie jest jednak tożsame z pojęciem administrującego zbiorem danych, który to termin został zawarty w przepisach karnych Ustawy (art. 51). Analizując powyższe występujące w Ustawie zwroty należy przyjąć, że podmiotem administrującym danymi jest podmiot, który zarządza, zawiaduje zbiorem danych lub danymi w procesie ich przetwarzania. Nie musi być to zatem administrator danych. Warto zwrócić uwagę, że odpowiedzialność karna z tytułu udostępnienia danych lub umożliwienia do nich dostępu osobom nieupoważnionym obejmuje każdy podmiot, który czyni to administrując zbiorem danych, nawet nie będąc jego administratorem.

2. Obowiązki administratora w zakresie zbierania (gromadzenia) danych.

Podstawowym terminem występującym w ustawie jest pojęcie „przetwarzania danych". Definicja tego pojęcia została zawarta w art. 7 ust. 1 pkt 2). Przetwarzanie danych obejmuje różnego typu operacje dokonywane na danych osobowych, w tym ich zbieranie oraz udostępnianie. Zbieranie danych może mieć charakter pierwotny (polega na ich pozyskaniu od osoby, której te dane dotyczą) albo wtórny (pozyskanie danych od z innego źródła, niż osoba, której dotyczą dane).

Baza katalogowa systemu LDAP obejmuje dane pozyskiwane z bazy kadrowej pracowników uczelni (w tym pracowników uczelni wykonujących pracę w filii). Należy tu rozgraniczyć dwie sytuacje. W sytuacji wykorzystywania danych pracowników uczelni dla realizacji obowiązków wynikających z umowy o pracę (a taką realizacją jest udostępnienie danych pracowników studentom) mamy do czynienia z pierwotnym gromadzeniem danych osobowych. W przypadku wykorzystywania już uzyskanych danych dla celów badawczych – mamy do czynienia z wtórnym pozyskaniem danych.

Przetwarzanie danych, a w tym ich gromadzenie, jest dopuszczalne wyłącznie w sytuacjach wymienionych w art. 23 Ustawy. Podstawowym warunkiem jest uzyskanie zgody osoby, której dane dotyczą. Przetwarzanie danych bez zgody jest możliwe tylko, gdy przewidują to przepisy prawa, jest to konieczne do realizacji umowy, jest niezbędne do wypełnienia prawnie usprawiedliwionych celów statutowych administratora danych albo jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.

Baza LDAP zamierza objąć już istniejący zbiór danych osobowych pracowników, powstały w celu realizacji obowiązków pracodawcy, jakim jest uczelnia, a wynikający z przepisów prawa pracy.

Biorąc pod uwagę powyższe, gromadzenie danych dla celów użycia ich w systemach kadrowych uczelni nie wymaga zgody osób, których one dotyczą, gdyż na ich gromadzenie zezwalają przepisy prawa.

Umieszczenie natomiast tych danych w bazie katalogowej dostępnej zarówno wewnątrz uczelni dla innych pracowników, w celu ułatwienia komunikacji oraz przepływu informacji, jak i na zewnątrz w sieci Internet, stanowi realizację zadań uczelni jako części systemu edukacji narodowej. Można zatem uznać, że przetwarzanie tych danych jest niezbędne do wykonywania określonych prawem zadań realizowanych dla dobra publicznego, a w związku z tym jest dopuszczalne. Nie dotyczy to oczywiście danych prywatnych (adres, prywatny telefon).

Istotnym obowiązkiem nałożonym na administratora gromadzącego dane osobowe jest obowiązek udzielenia określonych informacji osobom, których dane zbiera. Taki informacyjny obowiązek dotyczy także administratorów, których bazy danych powstały przed dniem wejścia w życie ustawy, a więc przed dniem 30 kwietnia 1998 r.
Gromadzenie danych osobowych w ramach projektu LDAP wymaga spełnienia przez administratora, a wiec uczelnię wyżej wymienionego obowiązku.
Poinformowanie powinno nastąpić w chwili zbierania danych, np. w momencie wypełniania ankiety przez osobę, której dane dotyczą.
W przypadku czerpania z zasobów już istniejących, poinformowanie powinno nastąpić w formie osobnego komunikatu obejmującego:

- informację o zmianie celu zbierania danych (baza LDAP), a szczególności o przewidywanych odbiorcach lub kategoriach odbiorców danych;
- źródle z jakiego dane są pobierane;
- prawie wglądu osoby, której dane dotyczą do swoich danych oraz ich poprawiania
- uprawnieniu osoby, której dane dotyczą do wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na szczególna sytuację;

Podmiot zbierający dane powinien ponadto podać swoją pełną nazwę i adres siedziby (chyba, że nastąpiło to już wcześniej).

Przepis regulujący obowiązek informacji (art. 25 ust. 2 pkt 3) przewiduje zwolnienie z tego obowiązku w sytuacji, gdy dane te są niezbędne do badań naukowych. Wydaje się jednak, że przepis ten należy rozpatrywać łącznie z przepisem art. 26 ust. 2 określającym dopuszczalność przetwarzania danych w celu innym niż ten, dla którego zostały zebrane. Nakłada on na administratora obowiązek informacji pomimo tego, że dane są przetwarzane w celach badań naukowych.

3. Obowiązki administratora w zakresie czynności administrowania danymi.

Ustawa nakłada na administratora precyzyjnie określone obowiązki. Z uwagi na to, iż opinia ta dotyczy konkretnej sytuacji, uwzględnione zostały te obowiązki, które dotyczą uczelni jako administratora danych bazy LDAP.

a) Administrator powinien zadbać, aby dane były zbierane wyłącznie dla oznaczonych celów, poprawne merytorycznie i przechowywane tylko tak długo jak jest to konieczne dla osiągnięcia celu ich przetwarzania.

Należy zauważyć, że cel wykorzystywania danych może być zmieniony tylko na ściśle określony ustawą inny cel, a przy tym wyłącznie przy spełnieniu przesłanek, do których należy: nienaruszanie praw i wolności osób, których te dane dotyczą, spełnienia obowiązku informacji (patrz wyżej – pkt 2) i oczywiście spełnienia co najmniej jednego z warunków dopuszczalności przetwarzania danych.

b) Osobie, której dane dotyczą, został przyznany w art. 32 katalog praw. Z ich realizacją wiążą się określone obowiązki po stronie administratora. Jest on zobowiązany zatem do:
   - udzielenia na żądanie takiej osoby wyczerpującej informacji na temat przetwarzanego zbioru danych. W skład takiej informacji wchodzi rodzaj zbieranych danych, sposób zbierania, cel i zakres przetwarzania oraz zakres udostępniania;
   - uzupełnienia, uaktualnienia lub sprostowania danych na żądanie osoby, której dotyczą;
   - wstrzymania przetwarzania danych lub nawet usunięcia, gdy ich zebranie nastąpiło z naruszeniem przepisów ustawy lub nie są już potrzebne do realizacji celu, dla którego zostały zebrane;
   - przyjęcia wniosku dotyczącego żądania zaprzestania przetwarzania danych osoby, której te dane dotyczą ze względu na jej szczególną sytuację.

c) Administrator jest zobowiązany do zastosowania odpowiednich środków technicznych i organizacyjnych, które zapewnią pełną ochronę przetwarzanych danych. Jest zobowiązany zapewnić pełną kontrolę nad wprowadzaniem danych do systemu informatycznego (jakie dane podlegają wprowadzeniu, kiedy i przez kogo) oraz ich udostępnianiem.
d) Ponadto, może on dopuszczać do obsługi systemu informatycznego i urządzeń służących do przetwarzania danych wyłącznie upoważnione osoby. Jest on zobowiązany prowadzić ewidencję wszystkich osób zatrudnionych przy przetwarzaniu danych.

Z racji tego, że baza LDAP będzie zawierała dane dotyczące pracowników uczelni, uczelnia jest zwolniona, na podstawie art. 43 ust. 1 pkt 4) Ustawy z obowiązku rejestracji zbioru danych przez Generalnego Inspektora Danych Osobowych.

4. Obowiązki administratora wynikające z Rozporządzenia.

Warto zwrócić uwagę na inny, poza Ustawą, akt prawny nakładający obowiązki na administratora danych. Jest to *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz. U. Nr 80, poz. 522)

Poza obowiązkami o charakterze organizacyjnym (odpowiednio zabezpieczone pomieszczenie), personalnym (wyznaczenie administratora bezpieczeństwa informacji) oraz technicznym (zapewnienie odpowiednich systemów zabezpieczających przed utratą danych w wyniku awarii, czy uwierzytelniających użytkowników) administrator powinien opracować instrukcje:

- postępowania w sytuacji naruszenia ochrony danych oraz
- określającą sposób zarządzania systemem informatycznym używanym do przetwarzania danych.

B. Udostępnianie danych osobowych.

Jedną z form przetwarzania danych osobowych, zgodnie z treścią art. 7 pkt 2 Ustawy, stanowi ich udostępnianie, a zwłaszcza poprzez systemy informatyczne, do których należy zaliczyć również udostępnianie za pośrednictwem Internetu, rozumianego dla potrzeb Ustawy jako zespół połączonych systemów informatycznych. Pomimo, iż Ustawa nie precyzuje typu nośnika, na którym czy za którego pomocą dane mogą zostać przekazane, nie ulega jednak wątpliwości, iż również udostępnianie za pośrednictwem Internetu, podlega jej przepisom. Udostępnienie danych osobowych, w tym również objętych projektem LDAP, oznacza nie tylko dopuszczenie każdej osoby do urządzeń zawierających dane (drogą zdalną), ale także pozostawienie tych urządzeń bez żadnego realnego zabezpieczenia, uniemożliwiającego dostęp do nich (B. Kurzępa Prok.i Pr. 1999/6/44 - t.2), przy czym zakres udostępnienia może być różny.

Zakres udostępnionych danych zależy od celu ich przetwarzania. Biorąc pod uwagę potrzeby UMK, opisane w Państwa piśmie, należy wskazać na dwa możliwe cele przetwarzania danych: zawarcie i wykonywanie umowy o pracę oraz realizacja przez UMK zadań określonych w Ustawie z dnia 12 września 1990 r. o szkolnictwie wyższym. W pierwszym przypadku udostępnianie danych osobowych nie stanowi udostępnienia w rozumieniu Ustawy, odpowiada natomiast ustawowemu przechowywaniu, opracowywaniu i zmienianiu danych osobowych, z uwagi jednak na treść Państwa pytań uznaliśmy za wskazane posługiwać się pojęciem udostępnienia również w stosunku do danych osobowych pracowników uczelni przetwarzanych w celu zawarcia i wykonywania umowy o pracę.

Osiągnięcie pierwszego celu wymaga zgromadzenia pełnych danych osobowych dotyczących pracownika uczelni, a w szczególności: imienia i nazwiska, adresu zamieszkania, numeru PESEL, numeru telefonu. Wyłączeniu podlegają tutaj dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, z wyjątkami określonymi w treści art. 27 Ustawy. Dane niezbędne do zawarcia i wykonywania umowy o pracę mogę być udostępniane wyłącznie pracownikom obsługującym systemy kadrowe uczelni, a także władzom UMK, na ich

żądanie, co oznacza, iż mogą być one udostępniane wyłącznie określonych osobom wewnątrz struktury organizacyjnej administratora danych – uczelni. Udostępnienie w znaczeniu ustawowym tych danych, w takim zakresie osobom trzecim, a zatem znajdującym się poza strukturą wewnętrzną administratora, wymagałoby uzyskania pisemnej zgody pracowników, których one dotyczą z uwagi na zmianę celu przetwarzania.

Podstawowym przepisem dla określenia warunków udostępnienia (w rozumieniu Ustawy) danych osobowych jest art. 23 ust. 1 pkt 4 Ustawy, zgodnie, z którym przetwarzanie (a zatem również udostępnianie) jest dopuszczalne między innymi wtedy, gdy wymaga tego wykonanie określonych prawem zadań realizowanych dla dobra publicznego. Zadaniami uczelni, określonymi w wyżej wymienionej Ustawie o szkolnictwie wyższym, zgodnie z art. 3 ust. 2 tej Ustawy są w szczególności: kształcenie studentów w zakresie danej gałęzi wiedzy oraz ich przygotowanie do wykonywania określonych zawodów, prowadzenie badań naukowych lub twórczej pracy artystycznej, przygotowanie kandydatów do samodzielnej pracy naukowej, dydaktycznej lub działalności artystycznej, kształcenie w celu uzupełnienia wiedzy ogólnej i specjalistycznej osób, które posiadają tytuły zawodowe i wykonują zawody praktyczne, rozwijanie i upowszechnianie kultury narodowej oraz postępu technicznego, a także współdziałanie w szerzeniu wiedzy w społeczeństwie oraz dbanie o zdrowie i rozwój fizyczny studentów. Wykonanie tych zadań, niewątpliwie realizowanych dla dobra publicznego, wymaga jednak udostępnienia niektórych danych osobowych pracowników uczelni, a w szczególności, zgodnie z art. 75 Ustawy o szkolnictwie wyższym, nauczycieli akademickich (pracownicy naukowo-dydaktyczni, dydaktyczni, część pracowników naukowych). Kontakt z nauczycielami akademickimi wymaga udostępnienia ich danych przede wszystkim w zakresie imienia i nazwiska, tytułu czy też stopnia naukowego, stanowiska, numeru telefonu służbowego, numeru konta poczty elektronicznej (o ile został przydzielony pracownikowi przez uczelnię) oraz ewentualnie pokoju, w którym dany nauczyciel akademicki dyżuruje. Dane takie stają się zatem danymi osobowymi, z uwagi na ich skojarzenie z imieniem i nazwiskiem nauczyciela akademickiego. Trudno natomiast wskazać, odpowiednio do Państwa pytania, na dane, które dotyczyłyby pracownika uczelni, nie stanowiąc jednocześnie danych osobowych. Z pewnością można wymienić tutaj adres poczty elektronicznej, który nie jest wystarczający do identyfikacji danej osoby. Wszystkie natomiast dane umożliwiające taką identyfikację należy uznać za dane osobowe. Udostępnienie danych pracownika uczelni – nauczyciela akademickiego, w omawianym zakresie, możliwe jest również za pośrednictwem Internetu, Ustawa nie precyzuje bowiem, jak zostało to wyżej wspomniane, sposobu udostępniania danych osobowych. Decyzję o udostępnieniu danych osobowych pracowników uczelni poprzez Internet podejmują władze uczelni, będącej administratorem danych, przy czym poszczególne czynności w ramach przetwarzania danych osobowych mogą zostać przekazane określonym jednostkom organizacyjnym uczelni, jako administrującym takimi danymi.

Wątpliwości może budzić udostępnienie danych osobowych innych pracowników uczelni (naukowo-technicznych, pracowników bibliotecznych oraz dokumentacji i

informacji naukowej oraz pozostałych), jeżeli nie jest niezbędne dla wykonywania zadań ustawowych uczelni, realizowanych dla dobra publicznego. Udostępnienie danych osobowych w omawianym zakresie jest zatem możliwe osobom trzecim (przede wszystkim studentom), dla wykonania zadań ustawowych uczelni między innymi przy pomocy projektu LDAP. Projekt LDAP, jako zadanie o charakterze badań naukowych, realizowane dla dobra publicznego, może być pojmowany nie jako środek udostępnienia danych osobowych pracowników, ale również jako odrębna podstawa dopuszczalności udostępnienia, na podstawie art. 26 ust. 2 pkt 1, jeżeli pierwotny cel zbierania danych był inny niż badania naukowe (np. zawarcie i wykonywanie umowy o pracę).

Udostępnienie danych osobowych pracowników osobom trzecim, a w szczególności studentom, w opisanym tutaj zakresie może zostać dokonane również na podstawie art. 23 ust. 1 pkt 3, jako czynność niezbędna dla wykonywania umowy o pracę – udostępnienie danych osobowych nauczyciela akademickiego w zakresie umożliwiającym skontaktowanie się każdego studenta z tym nauczycielem. Wątpliwości budzi jednak dopuszczalność udostępnienia danych osobowych osobom, w stosunku, do których pracownik uczelni (nauczyciel akademicki) nie ma jakichkolwiek obowiązków określonych jego stosunkiem pracy, stąd skorzystanie z tej podstawy prawnej dla udostępnienia danych pracowników uczelni poprzez Internet, ma ograniczony zakres i nie powinno być stosowane w stosunku do projektu LDAP.

Jawność danych osobowych z uwagi na konieczność wykonywania obowiązków wynikających ze stosunku pracy, jak i określonych prawem zadań realizowanych dla dobra publicznego, w tym projekt LDAP, powoduje, iż nie będzie miał zastosowania w stosunku do UMK (w zakresie wyżej opisanych danych osobowych) przepis art. 29 ust. 3 Ustawy, który dla udostępnienia danych osobowych wymaga pisemnego i umotywowanego wniosku. Sposób udostępnienia danych uniemożliwia zastosowanie wymienionego przepisu. W przypadku natomiast danych innych niż niezbędne do kontaktów służbowych z pracownikami uczelni, wymieniony przepis powinien mieć zastosowanie, przy czym dla realizacji projektu LDAP wydaje się, iż przetwarzanie takich danych nie będzie konieczne. Warto nadto podkreślić, iż biorąc pod uwagę treść art. 30 Ustawy, administrator danych ma obowiązek odmówić udostępnienia danych, co do których konieczne jest złożenie wniosku o udostępnienie. Katalog sytuacji, w których administrator odmawia udostępnienia danych jest zamknięty i obejmuje: ujawnienie wiadomości stanowiących tajemnicę państwową, zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego, zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa, istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

Korzystanie z udostępnionych danych osobowych może mieć charakter jednorazowego odpytania bazy danych osobowych, np. w poszukiwaniu danego pracownika uczelni, bądź przekazania przez administratora części lub całości bazy danych osobie trzeciej, np. innej uczelni wyższej. Z chwilą uzyskania danych osobowych, udostępnionych przez administratora (tutaj UMK) osoba, która uzyskała

te dane staje się administratorem danych w rozumieniu ustawy, ciążą więc na niej, niezależnie od podmiotu udostępniającego, obowiązki wynikające z ustawy. W przypadku udostępnienia części lub całości bazy danych osobowych na podstawie umowy, nabywca danych osobowych powinien złożyć oświadczenie, iż dane będą przetwarzane w tym samym celu, w jakim przetwarzał je udostępniający. Podobnie należy traktować udostępnienie jednorazowe, cel przetwarzania danych, uzyskanych w sposób jednorazowy powinien być zgodny z celem przetwarzania określonym przez udostępniającego. Przetwarzanie uzyskanych danych zgodnie z celem określonym przez udostępniającego ma znaczenie z punktu widzenia odpowiedzialności uzyskującego dane osobowe, bowiem wykorzystanie danych osobowych w celu innym niż określony przez udostępniającego naraża wykorzystującego w taki sposób dane osobowe na odpowiedzialność karną. Udostępnieniu danych osobowych poprzez witrynę internetową, co ma zasadnicze znaczenie dla projektu LDAP, powinna towarzyszyć zatem wyraźna informacja o celu udostępnienia tych danych.

Należy wspomnieć o odrębnej instytucji powierzenia przez administratora danych ich przetwarzania innemu podmiotowi. Takie powierzenie nie zwalnia jednak samego administratora od odpowiedzialności za przestrzeganie przepisów Ustawy (art. 31 Ustawy). Udostępniający ma nawet obowiązek sprawdzenia, dla jakiego celu nabywca będzie przetwarzał dane. Udostępnienie bazy danych dla innego celu niż ten, dla którego zebrał je podmiot zbywający jest możliwe wyłącznie na warunkach przewidzianych w art. 26 ust. 2 Ustawy. Należy zatem podkreślić, iż udostępniający powinien zadbać, aby w umowie przekazania bazy danych osobowych nabywca oświadczył, dla jakich celów bazę nabywa.

Obowiązkiem administratora danych, ustanowionym w art. 32 ust. 1 pkt 5 oraz art. 33 ust. 1 pkt 4 jest również informowanie osoby, której dane dotyczą o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane. Osoba, której dane dotyczą może żądać udzielenia w formie pisemnej informacji dotyczących udostępnionych danych. Należy również zaznaczyć, iż osoba, której dane dotyczą ma prawo wniesienia, na podstawie art. 33 ust. 1 pkt 7 i 8 w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5 (dane przetwarzane w celu wykonania określonych prawem zadań realizowanych dla dobra publicznego albo wypełnienia prawnie usprawiedliwionych celów administratorów danych), pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, albo wniesienia sprzeciwu wobec przekazywania jej danych osobowych innemu administratorowi danych. W stosunku do danych udostępnionych w ramach projektu LDAP nie wydaje się jednak, aby przepis ten miał zastosowanie, bowiem dane te dotyczą wyłącznie danych niezbędnych nie tylko dla samego projektu, ale również niezbędnych dla wykonywania obowiązków wynikających ze stosunku pracy pracowników uczelni.

Wprowadzenie dodatkowych ograniczeń dotyczących dostępu do danych osobowych umieszczonych w bazie danych stworzonej na potrzeby projektu LDAP, a także wyszukiwania danych umieszczonych w tej bazie nie mają wpływu na jej status prawny. Istotne jest bowiem przetwarzanie danych w zgodzie z przepisami Ustawy, a

zatem zakres udostępnionych danych powinien odpowiadać, zgodnie z tym, co zostało podkreślone powyżej, celowi przetwarzania danych osobowych. Przetwarzanie danych w celu zawarcia i wykonania umowy o pracę wymaga udostępnienia danych pracownika w szerokim zakresie, ale wąskiemu gronu osób, co oznacza, iż baza takich danych powinna zostać zabezpieczona przed dostępem jakichkolwiek osób trzecich. Natomiast przetwarzanie zadań w celach naukowych, dla dobra publicznego nie wymaga w przypadku projektu LDAP udostępnienia szerokiego zakresu danych osobowych, ale z uwagi na cele udostępnienia nie jest konieczne tworzenie jakichkolwiek ograniczeń, a zatem nie tylko dopuszczenie osoby nieupoważnionej do urządzeń zawierających dane, ale także pozostawienie tych urządzeń bez żadnego realnego zabezpieczenia, uniemożliwiającego dostęp do nich (B. Kurzępa Prok.i Pr. 1999/6/44 - t.2), jak zostało to wskazane powyżej.

Udostępnienie danych osobowych poprzez Internet oznacza dostęp do nich również spoza granic Polski. Nie wydaje się, aby udostępnianie poprzez Internet danych w sposób umożliwiający ich odbiór za granicą różniło się od udostępnienia danych na terytorium Polski, przy zachowaniu jednak wcześniej opisanych warunków. Należy przy tym wyraźnie odróżnić udostępnienie danych od ich przekazywania za granicę, o którym stanowi art. 47 Ustawy. Ostatnia z instytucji zakłada bowiem celowe przemieszczenie danych poza granice, natomiast w przypadku udostępnienia danych osobowych poprzez Internet dostęp do nich za granicą możliwy jest z uwagi na sposób publikacji tych danych. Stąd art. 47 Ustawy nie będzie miał zastosowania w przypadku udostępniania danych, które nie stanowi ich przekazywania.

Anna Piechocka, Artur Piechocki