RODO, czyli ochrona danych osobowych

Wprowadzenie[1]

Problematyka ochrony danych osobowych, w tym danych dotyczących zdrowia[2], zdaje się ostatnio wszechobecna w różnego rodzaju mediach[3,4], a to za sprawą rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz. Urz. UE L 119 z 5 kwietnia 2016 r.), zwanego „**RODO**" lub zamiennie „**Rozporządzeniem**".

Rozporządzenie to, stanowiąc instrument unifikacji prawa[5] na obszarze państw członkowskich, zaczęło obowiązywać tamże już 24 maja 2016 r. Unijny legislator, licząc się jednak z koniecznością posiadania niezbędnego czasu dla wdrożenia nowych rozwiązań przez jego adresatów, przyjął, że będzie ono stosowane od 25 maja 2018 r. Do tej daty zagadnienia ochrony danych osobowych w Polsce regulują, poza przepisami prawa europejskiego *sensu largo,* przede wszystkim ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (Tekst jedn. Dz. U. 2016 r., poz. 922 ze zm.), a także wydane na jej podstawie rozporządzenie Ministra Administracji i Spraw Wewnętrznych z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Niniejszy artykuł wpisuje się niejako w trwające od dłuższego czasu przygotowania GUMed do adaptacji Rozporządzenia. Przebiegające w Uczelni w pierwszym kwartale br. obligatoryjne szkolenia pracowników z tego zakresu niewątpliwie, stanowią ważny, a wręcz niezbędny, etap wdrażania ww. dokumentu, budując przede wszystkim świadomość prawną społeczności akademickiej. Zaakcentować też należy, że GUMed jako członek Konferencji Rektorów Akademickich Uczelni Medycznych (KRAUM) uczestniczy aktywnie w przygotowaniu tzw. kodeksu branżowego, zatytułowanego „Kodeks postępowania w zakresie ochrony danych osobowych dla uczelni medycznych". Nadto też jest on jednym z podmiotów wspierających powstanie innego kodeksu branżowego, a to „Kodeksu postępowania podmiotów wykonujących działalność leczniczą"[6]. Godzi się też w tym miejscu nadmienić, że Uczelnia już w 2 semestrze roku akademickiego 2017/2018 uruchomiła na kierunku studiów zdrowie publiczne (studia pierwszego stopnia), przedmiot Ochrona danych. Takie podejście do przedmiotowego zagadnienia zdaje się pozytywnie wyróżniać GUMed na tle oceny stopnia zaawansowania implementacji RODO w Polsce.

Stan przygotowań w tym zakresie, zarówno po stronie podmiotów zobowiązanych (administratorów danych[7] i pod-

[1] Wszystkie wskazane w przypisach do niniejszego artykułu linki prowadzą do materiałów dostępnych w dniu 10.03.2018 r.

[2] Do danych osobowych dotyczących zdrowia RODO (motyw 35) zalicza się wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE; numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne *in vitro*.

[3] Przykładowo tylko można wskazać teksty dostępne pod linkami: http://www.lex.pl/rodo-newsletter?utm_source=wolterskluwer.pl&utm_medium=baner&utm_campaign=WKPL_PRW_ACQ_newsletter-RODO-01-18-WKC0118003-IEM003_OTH&utm_content=160x600&_ga=2.92158547.873248798.1520600469-393562227.1520190055; http://prawo.gazetaprawna.pl/artykuly/1064902,rodo-dane-osobowe-ochrona-anych-sluzba-zdrowia.html; https://www.pwc.pl/pl/artykuly/2018/proces-wdrozenia-rodo.html; https://www.pwc.pl/pl/uslugi/rodo-rozporzadzenie-o-ochronie-danych-osobowych.html; https://giodo.gov.pl/pl/p/opinie-wytyczne-wskazowki. W Internecie można zapoznać się, i to, co ważne, bezpłatnie, z webinariami o charakterze wprowadzającym do problematyki RODO, a to np. https://www.pwc.pl/pl/wydarzenia/webinaria/wdrozenie-rodo-krok-po-kroku.html; https://www.pwc.pl/pl/wydarzenia/webinaria/2018/praktyczne-aspekty-wdrozenia-rodo.html

[4] Materiały, w tym aktualności dot. RODO można znaleźć m.in. na stronie https://www.giodo.gov.pl.

[5] Warto może przypomnieć, że rozporządzenia wydawane przez organy UE stanowią instrumenty unifikacji prawa (tj. zapewniają jednolitość regulacji we wszystkich państwach członkowskich tej organizacji). Cechuje je nie tylko abstrakcyjny charakter (normują nieokreśloną liczbę sytuacji, które mogą mieć miejsce w przyszłości) i ogólny zasięg (ich adresatami są zarówno państwa członkowskie, jak i osoby fizyczne i prawne), w czym przypominają krajowe ustawy), ale także bezpośrednią skuteczność (stanowią podstawę prawną dochodzenia przez osoby fizyczne i prawne praw nimi przyznanych przed sądami krajowymi) i bezpośrednią stosowalność (są stosowane w państwach członkowskich bez wprowadzania ich/implementacji za pomocą środków krajowych).

[6] Zob. np. https://www.csioz.gov.pl/pl/aktualnosci/szczegoly/spotkanie-dotyczace-kodeksu-branzowego-dla-sektora-ochrony-zdrowia/; http://gazetalekarska.pl/?p=38278;http://www.lex.pl/czytaj/-/artykul/giodo-zacheca-do-tworzenia-branzowych-kodeksow-postepowania?refererPlid=5259215.

[7] W świetle RODO „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania; status administra-

miotów przetwarzających[8])[9], jak i administracji publicznej jest wysoce niezadawalający[10]. Ministerstwo Cyfryzacji nie uporało się na czas, choć intensywne pracę zdają się trwać, z przygotowaniem projektu nowej ustawy o ochronie danych osobowych, który – w świetle RODO – winien mieć charakter quasi komplementarny do zawartych tam przepisów. Przepisy tej ustawy powinny w zakresie określonym w samym RODO doprecyzować jego postanowienia oraz dostosować polski porządek prawny do zawartych w nim regulacji (chodzi przy tym nie tylko o kwestie czysto techniczne czy proceduralne, choć w znacznej mierze tak, ale także np. o status organu nadzorczego/polskiego organu ochrony danych osobowych, ochronę prywatności dzieci; ew. obniżenie kar administracyjnych przewidzianych w RODO wobec określonej kategorii podmiotów; możliwe zróżnicowanie obowiązków „mniejszych" i „większych podmiotów"). Z prawdopodobieństwem graniczącym z pewnością ustawa taka nie zostanie uchwalona, a w tym samym nie wejdzie w życie, przed 25 maja 2018 r., pogłębiając stan niepewności prawnej[11]. Podkreślić przy tym należy, że zwłoka w jej przygotowaniu nie zwalnia nikogo z obowiązku stosowania RODO od 25 maja 2018 r. i nie stwarza, takie przynajmniej głosy pobrzmiewają ze strony administracji rządowej, „taryfy ulgowej" dla tych, którzy nie rozpoczęli tego procesu lub rozpoczęli go za późno.

Z niepokojem należy przyjąć dość dramatyczne wystąpienie Generalnego Inspektora Ochrony Danych Osobowych (GIODO) do Ministra Finansów podkreślające wpływ opóźnień i niepewności na przygotowanie samego organu ochrony danych osobowych do nowych regulacji prawnych. Edyta Bielak-Jomaa, piastująca ten urząd, alarmuje m.in., że *Nałożenie na organ nadzorczy nowych obowiązków (jak np. przyjmowanie naruszeń ochrony danych czy też nakładanie administracyjnych kar pieniężnych) determinuje wzrost zatrudnienia zarówno w związku z realizacją nowych zadań ale również w związku z koniecznością właściwego przygotowania GIODO do prawidłowego wdrożenia nowych obowiązków, tj. reorganizacji Biura GIODO, zaplanowania i implementacji systemów niezbędnych do realizacji zadań, określenia szeregu różnych procedur, jak również wdrożenia systemów informatycznych*[12].

Przypomnijmy zatem, że RODO wprowadza dotkliwe kary administracyjne za nieprzestrzeganie jego postanowień, w tym brak wdrożenia. Podmioty zobowiązane mogą zostać ukarane karą pieniężną od 10 do 20 mln euro lub od 2% do 4% wartości rocznego światowego obrotu przedsiębiorstwa, w zależności od tego, jakiego naruszenia się dopuściły i która z ww. wartości jest wyższa. Kary mają być nakładane proporcjonalnie, w zależności od skali naruszenia przepisów, z uwzględnieniem kryteriów określonych w art. 83 RODO.

Co do administracji publicznej, Ministerstwo Cyfryzacji podjęło próby przeforsowania obniżenia wysokości ww. administracyjnych kar pieniężnych do poziomu 100.000 zł. Takie „ulgowe traktowanie" zostało potraktowane jako dyskryminujące przez tych, którzy pod ową ulgę nie podpadaliby.

Istota RODO

Objętość niniejszego artykułu pozwala wyłącznie na sygnalizację czy raczej przypomnienie wybranych wątków omawianej problematyki. Warto powtórzyć zatem, że RODO jest odpowiedzią na nowe lub zmodyfikowane, nieobjęte/za słabo zidentyfikowane, dotychczasowymi regulacjami prawnymi, zjawiska/zmiany/przeobrażenia społeczne, kulturowe, techniczne, technologiczne i inne, w tym takie, jak: szybki postęp w różnych obszarach życia, globalizacja, wzrastająca aktywność cyfrowa/internetowa społeczeństw, coraz bardziej wyrafinowane techniki analizowania danych (w tym big data), profilowanie, cyberataki, wzrost wartości komercyjnej danych i wielkości „obrotu" nimi.

RODO poprzez swoją elastyczność stwarza bazę dla wykładni dynamicznej, idącej z duchem czasu, miękko dostosowującej się do wyzwań przyszłości. Stąd też np. nie wskazuje wymaganych środków technicznych ochrony danych osobowych, pozostawiając ten problem administratorom danych/podmiotom przetwarzającym. RODO niejako usamodzielnia te podmioty, zmusza do autodiagnozy statusu danych przez nie przetwarzanych i procesów, którym są poddawane, (samo)naprawy luk w ich ochronie/procesach, określania odpowiednich (i ich aktualizowania wobec wielu zmiennych) środków mitygowania naruszeń. Pamiętać należy, że Rozporządzenie nie podaje konkretnych przykładów najlepszych rozwiązań; nie określa też choćby minimalnych standardów technicznych mających na celu zabezpieczenie danych. Czasami sugeruje/zachęca, np. do skorzystania z narzędzi pseudonimizacji[13] i czy szyfrowania danych.

tora ma ww. okolicznościach np. GUMed, podmiot leczniczy, indywidualna/grupowa praktyka lekarska etc.

[8] W świetle RODO „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora; status taki ma np. podmiot świadczący usługi serwisu oprogramowania, obsługującego bazę danych osobowych, np. pacjentów/studentów/pracowników, któremu administrator (tych danych) (patrz przypis 8) zleca usunięcie wady, przekazując nośnik zawierający, który je zawiera.

[9] Patrz https://giodo.gov.pl/pl/1520281/10353.

[10] GIODO wysoce negatywnie odniósł się do jednej z wersji projektu ustawy o ochronie danych osobowych przygotowanej przez Ministerstwo Cyfryzacji, wskazując m.in., w jakim zakresie jest on niezgodny.

[11] Generalny Inspektor Ochrony Danych Osobowych wysoce negatywnie odniósł się do jednej z wersji projektu ustawy o ochronie danych osobowych przygotowanej przez Ministerstwo Cyfryzacji, podkreślając m.in. swoje wątpliwości co do zgodności z prawem niektórych zawartych tam propozycji. Zob. https://giodo.gov.pl/pl/1520280/10202.

[12] Patrz Pismo Generalnego Inspektora Ochrony Danych Osobowych dr Edyty Bielak-Jomaa do Ministra Finansów https://www.giodo.gov.pl/pl/1520281/10380; odpowiedź Ministra Finansów na ww. pismo: https://www.giodo.gov.pl/pl/file/13164.

[13] W świetle art. 4 pkt 5 RODO „pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Przestrzeganie RODO w organizacji wymaga wprzęgnięcia w nią w szczególności:

- ciągłych, nieustających procesów monitorowania przepływu danych/reakcji na naruszenia (choćby wobec obowiązku terminowego zgłaszania naruszeń ochrony danych organowi nadzorczemu czy przekazania informacji o nich podmiotom, których danych naruszenie dotyczy; prowadzenia rejestru przetwarzania danych, podejścia opartego na ryzyku i zasady rozliczalności),
- ich odpowiedniej aktualizacji/dostosowania do zmiennych,
- zbudowania stałego, odpowiedzialnego („czynnego"/współpracującego z jego członkami i innymi jednostkami w organizacji) interdyscyplinarnego zespołu (członek władz, prawnik/przedstawiciel IT/kierownicy projektów/ kierownicy działów przetwarzających dane, w tym działów HR, itp.), sprawującego pieczę nad ochroną danych osobowych w organizacji.

RODO bowiem nastawia w swej istocie na czujność.

Wobec powyższego często można usłyszeć od ekspertów z tej dziedziny, bardzo plastyczne, stwierdzenie, że ochrona danych osobowych od 25 maja br. ma być po prostu „wszyta" w DNA" każdej organizacji.

Dość powszechne jeszcze podejście, sprowadzające się do wdrożenia przepisów o ochronie danych osobowych poprzez „jednorazowy" akt przygotowania wielu dokumentów (np. polityki bezpieczeństwa informatycznego/ewidencji upoważnień do dostępu do danych osobowych/regulaminów itp.) i procedur odchodzi od lamusa. Zastępuje je podejście oparte na ryzyku (z ang. *risk based approach*). Pomocne w tych wszystkich procesach mogą być: tzw. kodeksy postępowania (branżowe), mechanizm certyfikacji, wytyczne Europejskiej Rady Ochrony Danych (która zastąpi już wkrótce Grupę Roboczą 29), normy ISO (w zakresie budowy i zarządzania środkami bezpieczeństwa).

Administrator/podmiot przetwarzający będzie musiał wykazać, że przestrzega prawa (zasada rozliczalności), np. poprzez udokumentowanie wdrożenia instrumentów prawnych wymaganych przez RODO, takich jak. przeprowadzenie oceny skutków dla ochrony danych (PIA), wdrożenie zasad *privacy by design* (ochrona danych w fazie projektowania) i *privacy by default* (domyślna ochrona danych). Te ostatnie zaś zasady stanowią wyraz podejścia mającego na celu na celu ochronę prywatności podmiotów danych. Ochrona ta musi być uwzględniania i stosowana w praktyce przy prowadzeniu wszelkich projektów i działań. *Privacy by design* ma stać się koniecznym elementem każdego podejmowanego projektu, niezależnie od tego, jaki jest jego charakter czy cel. W przypadku systemów teleinformatycznych oznacza to przede wszystkim wbudowanie ochrony prywatności zarówno w architekturę systemu, jak i w procesy, które system obsługuje, np. poprzez jak najszybszą pseudonimizację danych czy też umożliwienie osobie, której dane dotyczą, monitorowania przetwarzania danych. Domyślna ochrona to zaś taka, która funkcjonuje bez konieczności jakiejkolwiek aktywności podmiotów danych. Przy tym wszystkim należy jeszcze rozważyć, czy konieczne jest powołanie w organizacji inspektora ochrony danych osobowych.

Kontynuując, w pewnym zakresie Rozporządzenie powtarza, z reguły z lekka modyfikując, niektóre znane już na gruncie obowiązujących przepisów prawa rozwiązania. W szczególności zatem nie ulegają modyfikacji w istotny sposób, np. podstawy prawne czy zasady przetwarzania. Obowiązek informacyjny wobec podmiotów danych, zarówno w sytuacji pozyskania ich bezpośrednio od nich, jak i od osób trzecich, również pozostaje, z tym, że w dalece rozszerzonym zakresie.

Dotychczasowy administrator bezpieczeństwa informacji (ABI) zostanie zastąpiony, o ile administrator danych/podmiot przetwarzający będzie musiał go powołać, nowym podmiotem, tj. inspektorem ochrony danych osobowych (nb. GIODO jest zdania, że ABI wpisani do prowadzonego przez niego rejestru, winni od 25 maja br. „wejść w buty" tego nowego podmiotu).

Przykładowe naruszenia w sektorze medycznym

Godzi się zauważyć, że zarówno obowiązujący porządek prawny, jak i ten, z którym zostaniemy skonfrontowani począwszy od 25 maja br. traktuje i traktować jako naruszające prawa podmiotów danych osobowych (a przy tym i prawa pacjenta) będzie takie przykładowe, a zgłaszane już obecnie GIODO i Rzecznikowi Praw Pacjenta przez pacjentów, sytuacje jak:

- organizacja rejestracji w podmiocie leczniczym w taki sposób, że znajdujące się w pobliżu osoby (np. inni pacjenci, personel sprzątający) mogą usłyszeć informacje dot. rejestrowanego/ przyjmowanego pacjenta;
- brak ochrony informacji dot. pacjenta wyświetlanych na monitorach komputerów, powodujący możliwość zapoznania się z nimi przez osoby nieuprawnione[14];
- głośna „korytarzowa" konsultacja stanu zdrowia pacjenta przez lekarzy/personel medyczny w obecności osób trzecich, a także wydawanie poleceń przez lekarza odnośnie konkretnego/zidentyfikowanego pacjenta personelowi pomocniczemu w takich okolicznościach;
- kończenie przez lekarzy wpisów do dokumentacji medycznej pacjenta w obecności innego pacjenta, przy braku gwarancji ich nieujawnienia;
- wykonywanie przez lekarza telefonów dot. właśnie co obsłużonego pacjenta w obecności kolejnego pacjenta;
- przeprowadzanie wywiadu z pacjentem przy drzwiach otwartych/półotwartych, w obecności, osób niepowołanych;
- witanie przez lekarza znanego sobie pacjenta wśród innych pacjentów czekających na wizytę u niego, podczas którego padają pytania, o zmiany stanu zdrowia/

[14] Zob. A. Pochrzęst-Motyczyńska, *Dane medyczne Europejczyków warte bilion euro*, https://www.zdrowie.abc.com.pl/artykuly/dane-medyczne-europejczykow-sa-warte-bilion-euro,118999.html?utm_medium=email&utm_source=WKPL_MSG_NSL_NPOZ-09-03-18-WKC0117018_EML&utm_campaign=WKPL_MSG_NSL_NPOZ-09-03-18-WKC0117018_OTH.

samopoczucie/oceny *prima facie* jego sytuacji zdrowotnej;

- pozostawianie dokumentacji medycznej pacjentów już obsłużonych lub tych, których wizyty mają mieć miejsce w innym terminie na biurka lekarza, tak, że osoby niepowołane (np. pacjent obsługiwany właśnie), może się z nią zapoznać;
- pozostawianie dokumentacji medycznej po pracy na biurku/ w miejscu dostępnym dla osób nieupoważnionych, np. personelu sprzątającego, wbrew zasadzie „czystego biurka";
- wywoływanie pacjentów w poradni z imienia i nazwiska na wizytę[15].

Jako co najmniej wątpliwe prawnie należy także traktować wystawianie np. przez lekarzy psychiatrów zwolnień lekarskich/wypisów szpitalnych z danymi dot. ich specjalizacji czy też nazwą szpitala/oddziału wskazującymi na związek z ochroną zdrowia psychicznego/leczeniem nałogów/nerwic etc.

Można by mnożyć takie przykłady.

Podsumowanie

Jak podaje GIODO *Dane medyczne są niezwykle interesujące dla ubezpieczalni. Od nich zależy wysokość składki. Są przedmiotem handlu. Szacuje się, że dane Europejczyków będą warte bilion euro*[16].

RODO, choć traktowane przez niektórych jako dopust boży, pozwala ponownie, z większym jednak pietyzmem, pochylić się nad wszechobecnymi złymi nawykami/zwyczajami/niefrasobliwością naruszającymi szeroko pojętą prywatność podmiotów danych. Traktując je tak, możemy z jednej strony mitygować ryzyko nałożenia administracyjnej kary pieniężnej na naszą organizację/ryzyko procesów o ochronę danych/dóbr osobistych/praw pacjenta, z drugiej zaś ulepszyć procesy ochrony danych medycznych/praw pacjenta budując przy tym dobry wizerunek. Warto pamiętać także, co wybrzmiewa, na wielu szkoleniach/warsztatach/konferencjach dot. RODO, iż najsłabszym ogniwem wszelkich możliwych modeli ochrony jest człowiek. Uświadamianie personelu/osób współpracujących na pewno warte jest zatem poniesienia kosztów i czasu.

dr Lubomira Wengler, radca prawny,
Centrum Zintegrowanej Opieki i E-Zdrowia,
dr Ewa Bandurska, dr Piotr Popowski,
Zakład Zdrowia Publicznego i Medycyny Społecznej

[15] W przeprowadzonym wywiadzie przez Agnieszkę Pochrzęst-Motyczyńską z Pawłem Kaźmierczykiem z kancelarii Domański Zakrzewski Palinka *Gdy wejdzie RODO lekarz nie wywoła pacjenta po nazwisku*, https://www.zdrowie.abc.com.pl/artykuly/gdy-rodo-zacznie-obowiazywac--lekarz-nie-powinien-wywolac-pacjenta-do-gabinetu-po-nazwisku,119012.html.

[16] Zob. A. Pochrzęst-Motyczyńska, *Dane medyczne…*, *op. cit.*

Delegacja studentów w Warszawie

Członkowie SKN przy Zakładzie Anatomii i Neurobiologii w składzie: **Małgorzata Pytlik**, **Weronika Spodnik** oraz **Damian Palus** wzięli udział w Ogólnopolskiej Studenckiej Konferencji Naukowej *Odmiany anatomiczne w praktyce klinicznej* zorganizowanej przez Koło Anatomiczne Warszawskiego Uniwersytetu Medycznego oraz SKN przy Katedrze i Klinice Chirurgii Ogólnej, Transplantacyjnej i Wątroby WUMW. Odbyła się ona w dniach 7-8 kwietnia br. w Warszawie. Studenci zaprezentowali przypadki zaobserwowane w czasie preparatyki anatomicznej obejmujące nietypowe unaczynienie tarczycy, zmienność odejścia poszczególnych mięśni karku i kończyny górnej oraz badania dotyczące zmienności otworów podstawy czaszki. Wystąpienie Damiana Palusa *Wyrostek* śródowalny *i jego rola w patomechanizmie neuralgii trójdzielnej* zostało nagrodzone II miejscem w sesji *Anatomia głowy i szyi oraz OUN*. ■