LISTA KONTROLNA

Czy jesteś gotowy na RODO?

UNIWERSYTET
WARSZAWSKI

Opracował: Dominik Ferenc
Administrator Bezpieczeństwa Informacji

Warszawa 2018 r.

W celu sprawdzenia czy jednostka organizacyjna Uniwersytetu Warszawskiego jest przygotowana na stosowanie przepisów ogólnego rozporządzenia o ochronie danych osobowych (RODO - Dz.U. UE L 119/1 z dnia 4 maja 2016 r.) została przygotowana lista kontrolna, która ma pomóc w dostosowaniu jednostki organizacyjnej do prawidłowego przetwarzania danych osobowych.

Lista kontrolna jest narzędziem, którego uzupełnienie pozwoli na wskazanie obszarów przetwarzania danych osobowych, które należy dostosować do stanu zgodnego z przepisami regulującymi ochronę danych osobowych, a także działań, które należy podjąć, by zgodnie z przepisami przetwarzać dane osobowe w jednostce organizacyjnej w szczególności pod kątem:

- zasad przetwarzania danych osobowych,
- przesłanek legalności przetwarzania danych osobowych,
- obowiązków informacyjnych,
- ochrony danych w fazie projektowania i domyślnej ochrony danych,
- powierzenia przetwarzania danych osobowych,
- prowadzenia rejestru czynności przetwarzania,
- zapewnienia bezpieczeństwa danych osobowych,
- oceny skutków dla ochrony danych osobowych,
- przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych.

nazwa jednostki organizacyjnej

Lista kontrolna zgodności z RODO

Zasady przetwarzania danych osobowych					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówka**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
1.	art. 5 ust. 1 lit. a	Przetwarzanie zgodnie z prawem i w sposób przejrzysty dla osoby, której dane dotyczą.	Wszystkie komunikaty dot. przetwarzania danych osobowych powinny być łatwo dostępne i zrozumiałe.	1. Czy przetwarzane w jednostce organizacyjnej dane osobowe przetwarzane są w sposób legalny?	
2.	art. 5 ust. 1 lit. b	Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane w sposób niezgodny z tymi celami. Zbieranie danych w celach archiwalnych, badań naukowych, historycznych lub statystycznych nie jest uznawane za niezgodne z celem pierwotnym.	Cele przetwarzania danych osobowych na UW określa ustawa Prawo o szkolnictwie wyższym. Jeżeli cel przetwarzania wykracza poza sferę obowiązków wynikających z przepisów, należy także zakomunikować inny cel zbierania danych.	2. Czy dane przetwarzane w jednostce organizacyjnej są przetwarzane w sposób rzetelny?	
3.	art. 5 ust. 1 lit. c	Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do realizacji celów, dla których są przetwarzane (minimalizacja danych).	Ukształtowanie zakresu przetwarzania danych, w taki sposób. by zbierane były tylko dane niezbędne, które pozwolą na osiągnięcie zamierzonego celu.	3. Czy zakres przetwarzanych danych osobowych jest adekwatny do celu ich przetwarzania?	
4.	art. 5 ust. 1 lit. d	Dane osobowe powinny być prawidłowe i w razie potrzeby uaktualniane, należy podjąć wszelkie rozsądne działania, aby dane	Dane zbierane w procesie przetwarzania powinny być zgodne z prawdą, pełne (kompletne) oraz powinny odpowiadać aktualnemu stanowi rzeczy. Należy	4. Czy zapewniono merytoryczną poprawność danych osobowych?	

		osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.	zadbać o merytoryczną poprawność zbieranych danych osobowych.		
5.	art. 5 ust. 1 lit. e	Dane należy przechowywać w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane są przetwarzane.	Zasada ograniczenia przechowywania danych zabezpiecza osobę, której dane dotyczą, przed przetwarzaniem przez nieograniczony okres. Przechowywanie w celach archiwalnych, badań naukowych, historycznych lub celów statystycznych jest dozwolone.	5. Czy dane przetwarzane są przez czas niezbędny do realizacji celu?	
6.	art. 5 ust. 1 lit. f	Dane powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych w tym ochronę danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.	Zapewnienie bezpieczeństwa polega na wdrożeniu odpowiednich środków technicznych i organizacyjnych adekwatnych do określonego poziomu ryzyka.	6. Czy dane osobowe są zabezpieczone i przechowywane w sposób adekwatny do ryzyka przetwarzania danych?	
7.	art. 5 ust. 2	Administrator danych jest odpowiedzialny za przestrzeganie przepisów dotyczących zasad przetwarzania danych, musi być w stanie wykazać ich przestrzeganie („rozliczalność”).	Przez zapewnienie rozliczalności należy rozumieć obowiązek administratora danych do przestrzegania zasad ochrony danych osobowych i umiejętność wykazania przestrzegania tych przepisów – pomocny w tym jest rejestr czynności przetwarzania.	7. Czy w jednostce organizacyjnej wykonuje się nałożone na nią obowiązki wynikające z przepisów regulujących ochronę danych osobowych?	

Przesłanki legalności przetwarzania danych osobowych					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówka**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
8.	art. 6 ust. 1 lit. a	Przetwarzanie danych osobowych jest dopuszczalne, gdy: osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych	Należy potrafić udowodnić, iż jednostka pozyskała stosowne zgody na przetwarzanie danych osobowych. Np. w przypadku procesu rekrutacji na	8. Jeżeli podstawą prawną przetwarzania danych osobowych jest zgoda osoby,	

		osobowych w jednym lub większej liczbie określonych celów.	studia zgoda pobierana jest od kandydata w systemie IRK i za pomocą formularza papierowego. Zgodę należy zbierać np. od studentów w przypadku, gdy ich dane będą przetwarzane w celu innym niż związane z tokiem studiów z wyłączeniem marketingu/ofert oferowanych przez jednostkę. Zgoda wymagana jest zawsze od osób, które chcą wziąć udział np. w konkursie, seminarium, konferencji itp. Dowodem udzielenia zgody może być np.: – podpis osoby pod klauzulą zgody, – mail z klauzulą zgody w treści, – checkbox z zaznaczeniem zgody. Klauzula zgody musi mieć wyraźnie określony cel lub cele. Zgodnie z przepisami RODO konieczne jest pozyskanie odrębnej zgody na każdy z celów. Należy zachować treść udzielonych zgód.	której dane dotyczą, to czy jest ona udokumentowana? 9. Czy klauzula zgody ma precyzyjnie określone cele? 10. Czy zachowana jest treść udzielonych zgód z przypisaniem do osoby, która udzieliła zgody?	
9.	art. 6 ust. 1 lit. b	Przetwarzanie danych jest dopuszczalne, gdy przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą.	Należy posiadać lub potrafić wskazać miejsce przechowywania zawartej umowy z osobą, której dane dotyczą.	11. Jeżeli przetwarzanie odbywa się na podstawie umowy z osobą, której dane dotyczą, to czy taka umowa jest przechowywana?	
10.	art. 6 ust. 1 lit. c	Przetwarzanie danych jest dopuszczalne, gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.	Należy umieć wykazać podstawę prawną przetwarzania danych osobowych np.: – ustawa Prawo o szkolnictwie wyższym, – ustawa Kodeks pracy.	12. Gdy przetwarzanie odbywa się na podstawie przepisu prawa, to czy wskazano podstawę prawną?	
11.	art. 6 ust. 1 lit. d	Przetwarzanie danych osobowych jest dopuszczalne, gdy przetwarzanie jest	Żywotne interesy to interesy o dużym znaczeniu dla osoby, której dane	13. Czy w jednostce organizacyjnej	

		niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.	dotyczą, lub innej osoby fizycznej, takie jak: zdrowie i życie, mogą to być także interesy majątkowe. Podstawa żywotnych interesów jest stosowana wtedy, gdy przetwarzania nie da się oprzeć na innej podstawie prawnej.	przetwarzane są dane na podstawie przesłanki żywotnych interesów osoby, której dane dotyczą?	
12.	art. 6 ust. 1 lit. e	Przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.	Dotyczy to sytuacji, gdy w przepisach prawa wskazano wprost obowiązek przetwarzania określonych danych lub też wskazano zadania, do których realizacji niezbędne jest przetwarzanie danych osobowych.	14. Czy w przypadku wykonywania zadań w interesie publicznym jest wskazywana podstawa prawna, z której wynika interes publiczny?	
13.	art. 6 ust. 1 lit. f	Przetwarzanie danych jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.	Przetwarzanie danych na potrzeby prawnie uzasadnionych celów powinny być „niezbędne". Uzasadnienie prawne nie odnosi się do uzasadnienia, interesu, który można utożsamić z uprawnieniem do przetwarzania danych, które miałoby wynikać z jakiegoś konkretnego przepisu. Podstawa prawna wskazana w art. 6 ust. 1 lit. f nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizowania swoich zadań, a więc Uniwersytet Warszawski nie może przetwarzać danych osobowych na podstawie niniejszej przesłanki.		

Obowiązek informacyjny					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówki**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
14.	art. 13 ust. 1	Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych	W celu spełnienia obowiązku informacyjnego należy poinformować osobę, której dane dotyczą o:	15. Czy jednostka organizacyjna wykonuje obowiązek informacyjny?	

		podaje jej wszystkie następujące informacje: a) swoją tożsamość i dane kontaktowe oraz gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela; b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych osobowych oraz podstawę prawną przetwarzania; c) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania; d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią; e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją; f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.	– nazwie administratora danych, adresie i danych kontaktowych, – danych kontaktowych inspektora ochrony danych osobowych, – celach przetwarzania danych osobowych oraz podstawie prawnej przetwarzania (np. zgoda, przepis prawa), – jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f (do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią) – należy poinformować o prawnie uzasadnionych interesach realizowanych przez administratora, – odbiorcach danych lub kategoriach odbiorców danych, jeżeli istnieją, – gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, – okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalenia tego okresu, – prawie żądania od administratora dostępu do danych osobowych osoby, której dane dotyczą, – prawie do cofnięcia zgody w dowolnym momencie (cofnięcie zgody w przypadku studentów odbywających tok studiów cofnięcie zgody nie jest możliwe, z uwagi na	16. Czy stosowane klauzule informacyjne są zgodne z przepisami określonymi w RODO? 17. Czy obowiązek informacyjny jest spełniony przed rozpoczęciem przetwarzania danych osobowych?	
	art. 13 ust. 2	Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych			

		osobowych administrator podaje osobie, której one dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania: a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalenia tego okresu; b) informacje o prawie żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych; c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; d) informacje o prawie wniesienia skargi do organu nadzorczego; e) informacje, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jet zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych; f) informacje o zautomatyzowanym	to, że dane przetwarzane są na podstawie przepisów prawa), – prawie wniesienia skargi do organu nadzorczego, – obowiązku ustawowym lub umownym lub warunku zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ew. konsekwencje niepodania danych, – (gdy ma to zastosowanie) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu. W przypadku zbierania danych, nie od osoby, której dane dotyczą (art. 14 ust. 2 lit. f), należy poinformować tę osobę dodatkowo o: – źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych. **Obowiązek informacyjny należy spełnić przed rozpoczęciem zbierania danych osobowych.** Obowiązek informacyjny można spełnić przez wprowadzenie tzw. klauzul informacyjnych. Klauzula informacyjna może przyjąć postać informacji np.: – zamieszczonej w formularzu, – zamieszczonej w regulaminie, – zamieszczonej w mailu,		

		podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.	– zamieszczonej na stronie internetowej.		

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówki**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
15.	art. 25 ust. 1	Uwzględnianie ochrony danych w fazie projektowania.	Zgodnie z tą zasadą należy uwzględnić odpowiednie środki techniczne i organizacyjne, które pomogą w skutecznej realizacji zasad ochrony danych osobowych. Należy posłużyć się zasadą minimalizacji danych oraz wdrożyć odpowiednie ustawienia domyślne dotyczące prywatności osób, których dane dotyczą.	18. Czy przetwarzanie danych osobowych odbywa się w sposób bezpieczny?	
16.	art. 25 ust. 2	Domyślana ochrona danych.	Rezultatem domyślnej ochrony danych jest doprowadzenie do sytuacji, w której domyślnie będą przetwarzane tylko te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania.	19. Czy jednostka organizacyjna przetwarza tylko dane niezbędne do realizacji celu, w jakim zbiera dane osobowe?	

Powierzenie przetwarzania danych osobowych					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówki**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
17.	art. 28	Przetwarzanie danych osobowych odbywa się w imieniu administratora z wykorzystaniem usług podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych.	W przypadku powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu należy z tym podmiotem zawrzeć stosowną umowę powierzenia przetwarzania lub gdy przetwarzanie odbywa się na podstawie już zawartej umowy powierzenia należy dokonać sprawdzenia treści pod kątem nowych przepisów. Dowodem na spełnienie obowiązku wynikającego z art. 28 jest posiadanie umów powierzenia przetwarzania danych lub aneksów. Umowa powierzenia przetwarzania danych osobowych w szczególności powinna obejmować następujące elementy: – przedmiot i czas trwania przetwarzania, – charakter i cel przetwarzania, – rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, – obowiązki i prawa administratora danych, – wskazanie, że przetwarzanie odbywa się wyłącznie na udokumentowane polecenie administratora, – zapewnienie, że osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania uzyskanych danych w tajemnicy,	20. Czy w jednostce organizacyjnej zidentyfikowano podmioty zewnętrzne, z którymi podpisano lub należy podpisać umowę powierzenia przetwarzania danych osobowych? 21. Czy powierzenie przetwarzania danych osobowych ma formę pisemną? 22. Czy umowa powierzenia przetwarzania zawiera wszystkie obligatoryjne elementy wynikające z RODO?	

			– informacje o podjętych środkach bezpieczeństwa danych, – zobowiązanie podmiotu przetwarzającego do przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego, – pomoc administratorowi danych poprzez odpowiednie środki techniczne i organizacyjne w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, – pomoc administratorowi danych w wywiązaniu się z obowiązku zapewnienia bezpieczeństwa danych, zgłaszania naruszeń ochrony danych organowi nadzorczemu, zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, oceny skutków przetwarzania danych osobowych, – zobowiązanie do usunięcia lub zwrotu administratorowi danych wszelkich danych osobowych oraz usunięcia wszelkich ich istniejących kopii, – zobowiązanie do udostępnienia administratorowi danych wszelkich informacji niezbędnych do spełnienia obowiązków określonych w art. 28 RODO oraz umożliwienie administratorowi danych lub upoważnionemu przez administratora danych audytorowi przeprowadzenia audytów czy inspekcji.		

Rejestrowanie czynności przetwarzania					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówki**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
18.	art. 30	Prowadzenie rejestru czynności przetwarzania danych osobowych. Rejestr może być prowadzony w wersji elektronicznej lub papierowej.	Rejestr czynności przetwarzania jest narzędziem niezbędnym przy obowiązku wykazania rozliczalności przetwarzania danych osobowych. Rejestr taki obowiązkowo powinien uwzględniać informacje takie jak: – dane administratora w tym adres, – cel przetwarzania, – opis kategorii osób, których dane są przetwarzane, oraz kategorii danych osobowych – kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, – gdy ma to zastosowanie, informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, – jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych, – ogólny opis technicznych i organizacyjnych środków bezpieczeństwa. Rejestr czynności przetwarzania będzie także pomocny przy spełnieniu obowiązku dotyczącego dokonania oceny skutków dla ochrony danych osobowych.	23. Czy w jednostce organizacyjnej zidentyfikowano procesy przetwarzania danych osobowych? 24. Czy w jednostce organizacyjnej ustalono kategorie osób, których dane dotyczą? 25. Czy w jednostce organizacyjnej ustalono kategorie podmiotów, którym dane będą przekazywane?	

Bezpieczeństwo danych osobowych					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówki**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
19.	art. 32	Administrator i podmiot przetwarzający zobowiązani są do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cel przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.	**Zabezpieczenia osobowe:** – świadomość odpowiedzialności karnej za naruszenie ochrony danych osobowych, – zachowanie ostrożności przy udzielaniu informacji przez telefon poza UW, – zachowanie ostrożności przy udzielaniu informacji osobom nieuprawnionym, – zgłaszanie incydentów naruszenia ochrony danych osobowych, – zakaz przekazywania haseł dostępu do systemu, – blokowanie dostępu do systemu podczas opuszczenia stanowiska pracy, – ustawienie monitorów w sposób uniemożliwiający odczyt wyświetlania danych, – zamykanie pomieszczeń po zakończeniu pracy, – niepozostawianie dokumentów zawierających dane osobowe po zakończeniu pracy, – niszczenie dokumentów przy pomocy niszczarki.	26. Czy pracownicy zostali zapoznani z polityką bezpieczeństwa ochrony danych osobowych? 27. Czy pracownicy posiadają upoważnienia do przetwarzania danych osobowych? 28. Czy pracownicy zachowują ostrożność przy przekazywaniu danych osobowych przez telefon poza Uniwersytet Warszawski? 29. Czy pracownicy pozwalają na przebywanie w obszarze przetwarzania danych osób nieuprawnionych bez nadzoru? 30. Czy pracownicy niszczą dokumenty papierowe zawierające dane osobowe przy użyciu niszczarki dokumentów? 31. Czy pracownik posiada dostęp do programów przetwarzających dane osobowe jedynie przez zalogowanie się przy użyciu identyfikatora oraz hasła? 32. Czy pracownicy są świadomi konieczności zgłaszania incydentów	

				naruszenia ochrony danych osobowych? 33. Czy pracownicy mają świadomość, iż dokumenty papierowe należy przenosić w sposób uniemożliwiający ich widoczność? 34. Czy pracownicy, przenosząc dane na nośnikach danych, szyfrują ich zawartość?	
			Zabezpieczenia organizacyjne: – sprawdzenie zgodności przetwarzania danych osobowych z przepisami RODO, – wdrożenie dokumentacji ochrony danych osobowych w jednostce, – wydanie upoważnień dla pracowników posiadających dostęp do danych osobowych, – zapewnienie szkoleń z ochrony danych osobowych, – prowadzenie ewidencji osób upoważnionych, – prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych, – oświadczenia o zachowaniu poufności dla osób sprzątających, wolontariuszy itp., – określenie obszarów przetwarzania danych osobowych,	35. Czy na Uniwersytecie Warszawskim powołano Administratora Bezpieczeństwa Informacji? 36. Czy jednostka organizacyjna prowadzi ewidencję osób upoważnionych? 37. Czy pracownicy zostali zapoznani z przepisami regulującymi ochronę danych osobowych? 38. Czy w jednostce organizacyjnej określono obszary przetwarzania danych osobowych? 39. Czy w jednostce organizacyjnej wdrożono procedurę przyznawania pracownikom uprawnień do przetwarzania danych osobowych w systemach informatycznych?	

			– wdrożenie procedury przyznawania uprawnień użytkownikom systemów informatycznych, – sprawdzenie czy dokumenty przechowywane są w sposób uniemożliwiający podgląd przez osoby nieuprawnione.		
			Zabezpieczenia fizyczne: – szafy zamykane na klucz, – drzwi do pomieszczeń zamykane na klucz zwykłe lub wzmocnione lub ognioodporne, – sejfy, kasy pancerne, – zabezpieczenia okien, – system alarmowy, – system kontroli dostępu, – nadzór służby ochrony, – system przeciwpożarowy i/lub gaśnice wolnostojące.	40. Czy dane osobowe zabezpieczone są w sposób fizyczny? 41. Czy kopie zapasowe/archiwalne, na których umieszczone są dane osobowe przechowywane są w odrębnym pomieszczeniu? 42. Czy obszar przetwarzania danych osobowych zabezpieczony jest przed dostępem osób nieuprawnionych?	
			Zabezpieczenia informatyczne: – sprawdzenie, czy w systemie możliwe jest odnotowanie źródła pochodzenia danych osobowych, daty i zakresu udostępnienia danych osobowych, sprzeciwu osoby, której dane dotyczą, – sprawdzenie, czy system pozwala na tworzenie i drukowanie raportów zawierających odnotowane informacje o osobie, której dane dotyczą,	43. Czy programy przetwarzające dane osobowe automatycznie odnotowują: datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu? 44. Czy system umożliwia tworzenie raportów zawierających informacje o	

			– podłączenia serwera do UPS, – klimatyzacja w serwerowni, – systemy operacyjne lub programy zapewniają rejestrację dostępu do danych osobowych, – zapewnienie szyfrowania połączenia przez Internet (SSL, VPN), – stosowanie oprogramowania antywirusowego, – firewall do ochrony dostępu do sieci komputerowej, – aktualizacja oprogramowania, – określenie praw dostępu do danych przechowywanych w systemach informatycznych, – odrębny identyfikator dla każdego użytkownika, – wykonywanie kopii bezpieczeństwa.	osobie, której dane dotyczą, w przystępnej formie? 45. Czy systemy informatyczne zapewniają rejestrację dostępu do danych osobowych? 46. Czy użyto Firewall do ochrony dostępu do sieci komputerowej? 47. Czy serwerownia wyposażona jest w klimatyzację? 48. Czy użyto systemu IDS/IPS do wykrywania i blokowania ataków do sieci komputerowej? 49. Czy stosowany jest NAT? 50. Czy systemy operacyjne i przeglądarki mają instalowane aktualizacje? 51. Czy zainstalowano wygaszacze ekranów chronione hasłem na stacjach roboczych? 52. Czy nośniki informacji podłączone do stacji roboczej sprawdzane są oprogramowaniem antywirusowym? 53. Czy pracownik, czasowo opuszczając stanowisko pracy, wylogowuje się z systemu? 54. Czy ekrany monitorów zostały ustawione w sposób uniemożliwiający	

				wgląd przez osoby nieupoważnione?	

Ocena skutków dla ochrony danych					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówki**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
20.	art. 35	Dokonanie oceny skutków dla ochrony danych osobowych. Przed rozpoczęciem przetwarzania danych dokonuje się oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, gdy przetwarzanie danych może powodować wysokie ryzyko naruszenia praw lub wolności osób, której dane dotyczą.	Dokonanie oceny skutków dla ochrony danych osobowych jest niezbędne w celu ustalenia procesu przetwarzania danych osobowych oraz podjęcia określonych środków ochrony danych adekwatnych do poziomu ryzyka. Ocena skutków dla ochrony danych powinna polegać na: – ustaleniu procesu/ów przetwarzania danych (np. proces rekrutacji), – ustaleniu odpowiedzialności za proces, – podjęciu decyzji o konieczności wykonania oceny skutków, – uzasadnieniu decyzji, – wskazaniu interesariuszy (np. pracownicy, studenci itp.), – podjęciu konsultacji z Inspektorem Ochrony Danych, – określeniu planowanego terminu i sposobu realizacji praw i obowiązków osób, których dane dotyczą, – identyfikacji i opisie aktywów, – opracowaniu przepływu danych, – określeniu wymagań w zakresie ochrony prywatności,	55. Czy w jednostce organizacyjnej ustalono procesy przetwarzania danych osobowych? 56. Czy w jednostce organizacyjnej dokonano analizy ryzyka procesów przetwarzania danych osobowych? 57. Czy w jednostce organizacyjnej wykonano ocenę skutków dla ochrony danych osobowych?	

			– określeniu wymogów ogólnych w zakresie bezpieczeństwa danych, – wybraniu odpowiedniej metody szacowania ryzyka, – dokonaniu klasyfikacji danych, – określeniu zasad postępowania z danymi, – identyfikacji zagrożeń, – wyznaczeniu wartości ryzyka, – opracowaniu planu postępowania z ryzykiem, – określeniu poziomu ryzyka szczątkowego, – ustaleniu sposobu przeglądu i monitorowania ryzyka, – opracowaniu raportu z oceny skutków dla ochrony danych.		

Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówki**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
21.	Rozdział V RODO	Przekazanie danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, następuje, gdy administrator i podmiot przetwarzający spełnią warunki określone w Rozdziale V.	Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić tylko, gdy spełnione zostaną warunki i unormowania wynikające z RODO przy zapewnieniu, że nie został naruszony stopień ochrony osób fizycznych wyrażony w RODO. Podstawowym warunkiem przekazania danych osobowych do państwa trzeciego jest stwierdzenie przez Komisję Europejską, że państwo trzecie lub dana organizacja międzynarodowa zapewniają	58. Czy przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej odbywa się w sposób legalny?	

			odpowiedni stopień ochrony danych osobowych. Stwierdzenie odpowiedniego stopnia ochrony następuje w postaci aktu wykonawczego zawierającego decyzję Komisji Europejskiej. Przekazanie danych osobowych do państw trzecich lub organizacji międzynarodowych, w odniesieniu do których podjęta została decyzja o zapewnieniu odpowiedniego stopnia ochrony danych nie wymaga specjalnego zezwolenia		