BEZPIECZEŃSTWO INFORMACJI, W TYM OCHRONA DANYCH OSOBOWYCH – PODSTAWOWE POJĘCIA I INFORMACJE

UCK Uniwersyteckie Centrum Kliniczne

REGULACJE DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI

1. **Przepisy prawa powszechnie obowiązującego:**
   - dyrektywy,
   - rozporządzenia,
   - Konstytucja
   - ustawy
   - rozporządzenia
2. **Polskie normy**
3. **Decyzje administracyjne**
4. **Kodeksy postępowania**
5. **Wytyczne, poradniki**

Wykaz: Załącznik nr 11 do Księgi Jakości - WYKAZ DOKUMENTÓW ZWIĄZANYCH Z KJ - Dz-21.0 „POLITYKĄ BEZPIECZEŃSTWA INFORMACJI”.

REGULACJE DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI

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 (tzw. ogólne rozporządzenie o ochronie danych osobowych, w skrócie RODO) **(data rozpoczęcia stosowania: 25.05.2018 r.).**

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

Uchylono dotychczas obowiązującą ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

DANE OSOBOWE

Dane osobowe –
informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą).

Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak:

- imię i nazwisko,
- numer identyfikacyjny,
- dane o lokalizacji,
- identyfikator internetowy lub
- jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dane osobowe stanowią informacje w formie komunikatów (niezależnie od sposobu ich utrwalenia), np. w formie:

- słów,
- dźwięków,
- fotografii.

DANE OSOBOWE C.D.

Przykłady osób zidentyfikowanych lub możliwych do zidentyfikowania:

- Kierownik Działu Aparatury Medycznej UCK
- Inspektor Ochrony Danych UCK
- Monika, Pełnomocnik Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji UCK
- jkraszewski@uck.gda.pl
- Ordynator KOR UCK
- Dyrektor Naczelny UCK
- Aleksandra D., Prezydent Miasta Gdańska
- wokalistka zespołu „Hey”
- pisarka, autorka sagi o Fjällbace
- Dyrektor generalny Tesla Inc.
- reżyser, laureat nagrody Akademii Filmowej (Oscary) za 2021 r.
- Anna L., trenerka personalna, żona znanego polskiego piłkarza

Tożsamość tych osób znasz lub bez problemu ustalisz

DANE DOTYCZĄCE ZDROWIA

DANE DOTYCZĄCE ZDROWIA

- dane osobowe o zdrowiu fizycznym osoby fizycznej,
- dane osobowe o zdrowiu psychicznym osoby fizycznej, w tym dane o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia.

PRZYKŁADY

- informacje zbierane podczas rejestracji pacjenta do usług opieki zdrowotnej lub podczas świadczenia usług opieki zdrowotnej,
- oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej dla celów zdrowotnych (np. numer księgi głównej),
- informacje pochodzące z badań laboratoryjnych lub lekarskich,
- wszelkie informacje o przebytych lub aktualnych chorobach.

UCK Uniwersyteckie Centrum Kliniczne

„ZWYKŁE” DANE OSOBOWE (ART. 6 RODO)

Art.6 ust. 1 RODO: Przetwarzanie tzw. „zwykłych” danych osobowych jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

- osoba, której dane dotyczą **wyraziła zgodę** na przetwarzanie (…),
- przetwarzanie jest **niezbędne do wykonania umowy**, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
- przetwarzanie jest **niezbędne do wypełnienia obowiązku prawnego** ciążącego na administratorze,
- przetwarzanie jest **niezbędne do ochrony żywotnych interesów osoby**, której dane dotyczą lub innej osoby fizycznej,
- przetwarzanie jest **niezbędne do wykonania zadania realizowanego w interesie publicznym** lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
- przetwarzanie jest **niezbędne do celów wynikających z prawnie uzasadnionych interesów** realizowanych przez administratora lub przez 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.

DANE OSOBOWE SZCZEGÓLNEJ KATEGORII (ART. 9 RODO)

Art. 9 ust. 2 RODO:
Art.9 ust. 1 RODO [mówiący o zakazie przetwarzania danych szczególnej kategorii] nie ma zastosowania, jeśli:

- osoba, której dane dotyczą wyraziła wyraźną zgodę (…), chyba że prawo Unii lub państwa członkowskiego przewidują, iż (…) nie może uchylić zakazu (…),
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonania szczególnych praw (…) w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej (…),
- przetwarzanie jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
- przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami (…),
- przetwarzanie dotyczy danych osobowych upublicznionych przez osobę, której dane dotyczą,
- przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy,
- przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

DANE OSOBOWE SZCZEGÓLNEJ KATEGORII (ART. 9 RODO)

Art. 9 ust. 2 RODO:
Art.9 ust. 1 RODO [mówiący o zakazie przetwarzania danych szczególnej kategorii] nie ma zastosowania, jeśli:

- przetwarzanie jest **niezbędne dla celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego** na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3 RODO,

- przetwarzanie jest niezbędne **ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego,** takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową,

- przetwarzanie jest **niezbędne do celów archiwalnych w interesie publicznym,** do celów badań naukowych lub historycznych lub do celów statystycznych (…).

PRZETWARZANIE DANYCH OSOBOWYCH (ART. 4 PKT 2 RODO)

Przetwarzanie – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak:

Przetwarzanie	**Zbieranie**	**Utrwalanie**	**Organizowanie**
Porządkowanie	**Przechowywanie**	**Adaptowanie lub modyfikowanie**	**Pobieranie**
Przeglądanie	**Wykorzystywanie**	**Ujawnianie poprzez przesłanie**	**Rozpowszechnianie lub innego rodzaju udostępnianie**
Dopasowywanie lub łączenie	**Ograniczanie**	**Usuwanie**	**Niszczenie**

UCK Uniwersyteckie Centrum Kliniczne

CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH. RCP I RKCP

Czynność przetwarzania danych osobowych – zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane.

Rejestr Czynności Przetwarzania (RCP) - prowadzony przez Administratora danych wykaz czynności przetwarzania danych osobowych.

Rejestr Kategorii Czynności Przetwarzania (RKCP) – prowadzony przez Podmiot przetwarzający wykaz kategorii czynności przetwarzania.

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH (ART. 5 RODO)

Dane osobowe winny być:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (**„zgodność z prawem, rzetelność i przejrzystość”**),
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (…) (**„ograniczenie celu”**),
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (**„minimalizacja danych”**),
- prawidłowe i w razie potrzeby uaktualniane (…) (**„prawidłowość”**),
- przechowywane w formie umożliwiającej identyfikujące osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (**„ograniczenie przechowywania”**),
- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (**„integralność i poufność”**).

Administrator jest odpowiedzialny za przestrzeganie ww. przepisów i musi być w stanie wykazać ich przestrzeganie (**„rozliczalność”**).

ZGODNOŚĆ Z PRAWEM PRZETWARZANIA. PODSTAWY PRZETWARZANIA DANYCH OSOBOWYCH

Kiedy przetwarzanie danych jest dozwolone?

1. **Art. 6 RODO**
   Dotyczy "zwykłych" danych osobowych.

2. **Art. 9 RODO**
   Dotyczy danych osobowych szczególnej kategorii.

3. **Art. 10 RODO**
   Dotyczy danych odnoszących się do wyroków skazujących oraz czynów zabronionych.

UCK Uniwersyteckie Centrum Kliniczne

OBOWIĄZEK INFORMACYJNY ADO (ART. 13 I 14 RODO)

ART. 13 RODO: Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:

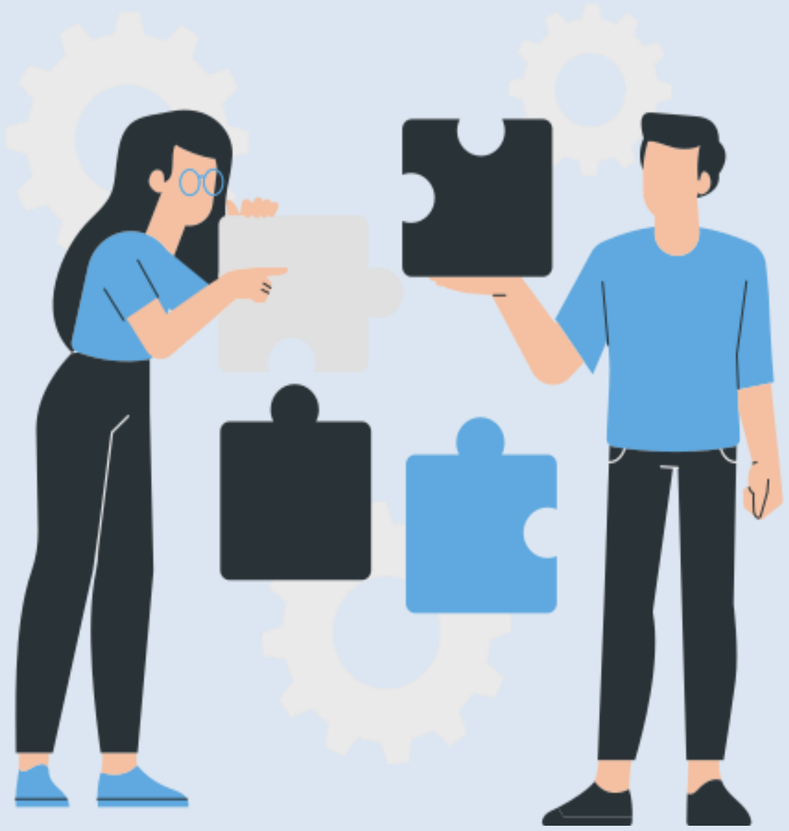
- swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela,
- gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych,
- cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania,
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią,
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej (…)

Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:

- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
- informacje o prawie do 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;
- 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,
- informacje o prawie wniesienia skargi do organu nadzorczego,
- informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (…).

Więcej: https://uck.pl/polityka-prywatnosci/przetwarzanie-danych-osobowych.html

BEZPIECZEŃSTWO INFORMACJI



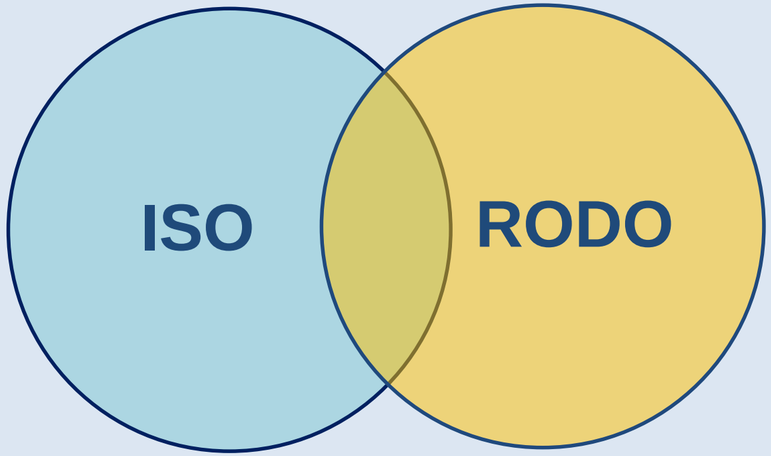
BEZPIECZEŃSTWO INFORMACJI

- zachowanie poufności, integralności i dostępności informacji. Dodatkowo mogą być brane pod uwagę inne właściwości (atrybuty) informacji, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI. OBSZARY DZIAŁAŃ

Bezpieczeństwo informacji - obszary działań:

- Klasyfikacja informacji
- Bezpieczeństwo fizyczne i środowiskowe
- Bezpieczeństwo teleinformatyczne (w tym cyberbezpieczeństwo UCK)
- Bezpieczeństwo informacji w zarządzaniu zasobami ludzkimi (bezpieczeństwo osobowe)
- Zarządzanie incydentami i słabościami SZBI
- Zarządzanie ryzykiem
- Zarządzanie ciągłością działania
- Zapewnienie zgodności z prawem przetwarzania



ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI.
STRUKTURA SZBI. STRUKTURA SYSTEMU OCHRONY DANYCH OSOBOWYCH

STRUKTURA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI)

- Najwyższe Kierownictwo
- Pełnomocnik Dyrektora Naczelnego ds. SZBI
- Właściciele zasobów/aktywów
  (są jednocześnie Właścicielami ryzyk) (np. kierownicy KO, osoby sprawujące samodzielne stanowiska)
- Administratorzy zasobów/aktywów
- Pozostali pracownicy

Zespół ds. Bezpieczeństwa Informacji

Norma ISO/IEC 27001

STRUKTURA SYSTEMU OCHRONY DANYCH OSOBOWYCH

- Administrator Danych Osobowych (ADO)
- Inspektor Ochrony Danych
- Upoważnieni pracownicy
  Przetwarzają dane osobowe zgodnie z nadanym przez Administratora Danych upoważnieniem (w zakresie uzasadnionym wykonywanymi obowiązkami)

RODO

UCK Uniwersyteckie Centrum Kliniczne

ZASOBY/AKTYWA INFORMACYJNE

Ogół informacji będących w posiadaniu UCK niezależnie od ich klasyfikacji i stopnia ochrony.

Zasoby informacyjne stanowią zarówno informacje przetwarzane w systemach informatycznych, jak i w formie tradycyjnej.

Aktywa informacyjne stanowią np.:

- dokumenty systemowe (np. zapisy, instrukcje i procedury),
- informacje będące efektem procesu (np. reklama, spisy, bazy danych, formularze itp.),
- informacje uzyskiwane na wejściu (np. od klientów, od firm zewnętrznych, od innych działów),
- informacje przekazywane do innych procesów (na wyjściu).

Prowadzony jest wykaz aktywów informacyjnych UCK.

BEZPIECZEŃSTWO OSOBOWE

I

Czynności przed zatrudnieniem bądź podjęciem współpracy

II

Czynności związanie z podjęciem zatrudnienia bądź współpracy

III

Czynności związane z modyfikacją zatrudnienia bądź współpracy

IV

Czynności związane z zakończeniem zatrudnienia bądź współpracy

PZ-ZI-06 – „Bezpieczeństwo informacji w zarządzaniu zasobami ludzkimi”

WYMAGANIA BEZPIECZEŃSTWA INFORMACJI ZWIĄZANE Z ZATRUDNIENIEM / PODJĘCIEM WSPÓŁPRACY

- Oświadczenie o zachowaniu poufności
- Przeszkolenie z zakresu bezpieczeństwa informacji
- Upoważnienie do przetwarzania danych osobowych

- Powierzenie przetwarzania danych osobowych, umowa powierzenia danych osobowych
- Umowa o poufności
- Lista kontrolna – wymogi bezpieczeństwa
- Wykaz przykładowych klauzul umownych
- Informator bezpieczeństwa informacji (dla kontrahenta)

- Oddanie do korzystania aktywów
- Nadanie uprawnień dostępowych

UPOWAŻNIENI PRACOWNICY

Oświadczenie

o znajomości i przestrzeganiu przepisów i zasad odnoszących się do ochrony informacji, w tym danych osobowych oraz o zachowaniu w tajemnicy tych informacji.

Przeszkolenie

Upoważnienie do przetwarzania danych osobowych

Administrator oraz Podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia Administratora lub Podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je **wyłącznie na polecenie Administratora**, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

UCK Uniwersyteckie Centrum Kliniczne

UŚWIADAMIANIE, KSZTAŁCENIE I SZKOLENIA Z ZAKRESU BEZPIECZEŃSTWA INFORMACJI

Osoby/podmioty, które – w związku z wykonywanymi zadaniami – uzyskują dostęp do aktywów informacyjnych UCK:

- posiadają odpowiednią wiedzę z zakresu bezpieczeństwa informacji (tj. posiadają poziom świadomości bezpieczeństwa informacji odpowiedni do zajmowanego stanowiska / wykonywanych zadań),
- znają zalecenia i metody właściwego użytkowania i ochrony systemów informacyjnych.

Przyznanie dostępu do aktywów informacyjnych UCK, w tym zwłaszcza informacji i środków przetwarzania informacji odbywa się wyłącznie po udokumentowanym przekazaniu odpowiednich, obowiązujących w UCK, zasad bezpieczeństwa informacji.

SZKOLENIA PODSTAWOWE

SZKOLENIA DODATKOWE (dostosowane pod kątem powierzonych do wykonania zadań), których odbycie jest warunkiem uzyskania dostępu do: poszczególnych zasobów informacyjnych UCK, w tym systemów teleinformatycznych przetwarzających dane, do zaawansowanych funkcjonalności systemów teleinformatycznych UCK).

SZKOLENIA WSTĘPNE

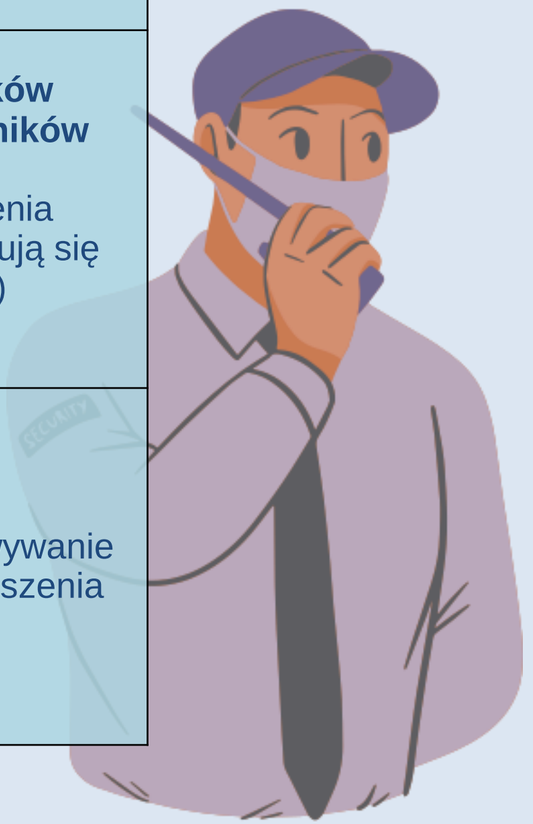
SZKOLENIA OKRESOWE

SZKOLENIA DOSZKALAJĄCE

UCK Uniwersyteckie Centrum Kliniczne

BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

Fizyczne zabezpieczenie wejść (zabezpieczenie wejść do budynków i pomieszczeń)	**Kontrola dostępu**	**Ochrona przed zagrożeniami zewnętrznymi** (ochrona przed siłami natury i działaniem osób trzecich, np. mury, przegrody, odpowiednie usytuowanie mebli biurowych)
Zabezpieczanie pomieszczeń przez pracowników (obowiązek zabezpieczenia pomieszczeń, w których znajdują się informacje chronione)	**Obszar bezpieczny** (wyznaczony obszar przetwarzania informacji / danych osobowych, strefy bezpieczeństwa, praca w obszarze bezpiecznym)	**Zabezpieczanie nośników informacji przez pracowników** (obowiązek zabezpieczenia nośników, na których znajdują się informacje chronione)
Polityka czystego biurka, polityka czystej tablicy (zasady dotyczące zachowania polityki czystego biurka i czystej tablicy podczas pracy i po jej zakończeniu)	**Nadzór nad osobami trzecimi** (nadzór nad osobami nieuprawnionymi do przetwarzania informacji, np. pacjentami, kontrahentami)	**Polityka kluczy** (zdawanie klucza, przechowywanie pod nadzorem, zakaz wynoszenia klucza do domu)



ODPOWIEDZIALNOŚĆ ZA ZASOBY/AKTYWA

- Każdy pracownik **odpowiada za powierzone mu zasoby/aktywa** (sprzęt informatyczny, oprogramowanie, dokumentację papierową itp.).

- Każdy pracownik zobowiązany jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieuprawnionych oraz przed ich zniszczeniem. Zobowiązany jest do zachowania szczególnej ostrożności podczas **transportu, przechowywania i użytkowania** nośnika informacji.

- Zasoby/aktywa te przeznaczone są – co do zasady – wyłącznie do realizacji **celów służbowych**. Wykorzystanie ich do celów prywatnych możliwe jest jedynie w przypadkach określonych regulacjami wewnętrznymi UCK.

ZARZĄDZANIE INCYDENTAMI I SŁABOŚCIAMI SZBI.
ZDARZENIA ZWIĄZANE Z BEZPIECZEŃSTWEM INFORMACJI

Zdarzenia związane z bezpieczeństwem informacji
stanowią:
- naruszenia bezpieczeństwa informacji,
- pozostałe zdarzenia niemające cech naruszenia bezpieczeństwa informacji (słabości SZBI).

Słabości SZBI
mogą doprowadzić do naruszenia bezpieczeństwa informacji.

UCK Uniwersyteckie Centrum Kliniczne

ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA

Plany ciągłości działania (PCD)

Ciągłość działania - strategiczna i taktyczna zdolność organizacji do przewidywania i reagowania na sytuacje kryzysowe, umożliwiająca kontynuację procesów biznesowych na akceptowalnym, predefiniowanym poziomie w akceptowalnym czasie.

Zarządzanie ciągłością działania - proces zarządzania, który ma na celu zapewnienie niezakłóconej realizacji usług organizacji na założonym poziomie (obejmuje identyfikację zdarzeń, które mogą prowadzić do sytuacji kryzysowej lub zakłócenia dla ciągłości działania i ich wpływu na procesy biznesowe oraz wdrażanie odpowiednich środków potrzebnych do zapewnienia ciągłości działania UCK). Proces ten zapewnia strukturę, na której buduje się odporność instytucji ze zdolnością do skutecznej reakcji, i która zabezpiecza interesy kluczowych interesariuszy, jak też reputację, markę i działania kreujące wartość instytucji. Zarządzanie ciągłością działania ma na celu zapewnianie (na drodze ustanowienia procesu i organizacji działania), że pewien uznawany za minimalny, niezbędny poziom działania operacyjnego zostanie zachowany nawet w warunkach krytycznego zakłócenia.

Przeglądanie, testowanie i ocenianie Planów ciągłości działania (PCD)

STATUS IOD (ART. 38 RODO)

Administrator danych osobowych i Podmiot przetwarzający
zapewniają, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych
(IOD winien być informowany o wszelkich kwestiach dotyczących przetwarzania danych osobowych na możliwie najwcześniejszym etapie).

Administrator danych osobowych i Podmiot przetwarzający **wspierają IOD w wypełnianiu przez niego zadań,** o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej (w tym odpowiednie wsparcie finansowe, infrastrukturalne i kadrowe, a także zapewnienie udziału w szkoleniach, warsztatach, forach oraz innych spotkaniach dotyczących tematyki ochrony danych osobowych, a także wyposażenie w odpowiednią – aktualizującą jego wiedzę - literaturę fachową, w tym w czasopisma branżowe).

Administrator danych osobowych i podmiot przetwarzający zapewniają, by IOD **nie otrzymywał instrukcji** dotyczących wykonywania tych zadań (np. nie należy wydawać IOD instrukcji dotyczących sposobu wykładni przepisów i/lub dotyczących formułowania przez niego zaleceń i opinii); nie jest on odwoływany ani karany za wypełnianie swoich zadań; winien bezpośrednio podlegać Najwyższemu Kierownictwu (niezależność IOD).

Osoby, których dane dotyczą, **mogą kontaktować się z IOD** we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

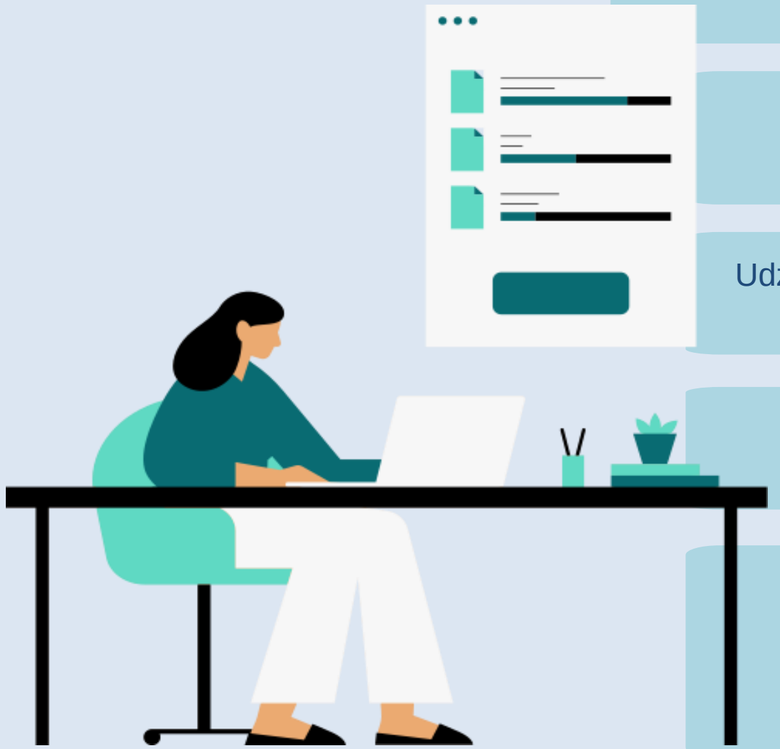
IOD jest zobowiązany do **zachowania tajemnicy lub poufności co do wykonywania swoich zadań** – zgodnie z prawem Unii lub prawem krajowym.

IOD może wykonywać inne zadania i obowiązki;
Administrator danych osobowych i podmiot przetwarzający
zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

UCK Uniwersyteckie Centrum Kliniczne

OBOWIĄZKI IOD (ART. 39 RODO)

Rola konsultacyjno-uświadamiająco-doradczo-kontrolna



Informowanie Administratora danych osobowych, Podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów (…) i doradzanie im w tej sprawie (…).

Monitorowanie przestrzegania RODO, innych przepisów (…) oraz polityk Administratora danych osobowych lub Podmiotu przetwarzającego w dziedzinie ochrony danych osobowych (…).

Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO (…).

Współpraca z Organem Nadzorczym (PUODO), w tym również uczestniczenie w kontrolach dotyczących przetwarzania danych osobowych.

Pełnienie funkcji punktu kontaktowego dla Organu Nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,

UCK Uniwersyteckie Centrum Kliniczne

KONTAKT Z INSPEKTOREM OCHRONY DANYCH

INSPEKTOR OCHRONY DANYCH
MONIKA GOLUBSKA

tel. (58) 349 21 73

iod@uck.gda.pl