Wzór „Karty szkolenia w zakresie ochrony danych osobowych" – formularz przeznaczony dla osób przetwarzających dane osobowe w Dziale Zatrudnienia i Kadr

1/ „Regulamin Przetwarzania i Ochrony Danych Osobowych" i „Procedury dotyczące stosowania Regulaminu Przetwarzania i Ochrony Danych Osobowych"

Na podstawie przepisów art. 24 ***Rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)***, zwanego w dalszej części ***„RODO"*** – Dyrektor Szpitala Specjalistycznego w Brzozowie Podkarpackiego Ośrodka Onkologicznego im. Ks. Bronisława Markiewicza zarządzeniem Nr 65/2018 z dnia 25 maja 2018 roku wprowadził do stosowania ***„Regulamin przetwarzania i ochrony danych osobowych"*** **wraz z procedurami dotyczącymi stosowania tego Regulaminu,** które określają zasady i procedury obowiązujące przy przetwarzaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Szpital Specjalistyczny w Brzozowie. Regulamin wraz z procedurami stanowi zbiór ogólnych i szczegółowych zasad postępowania, których przestrzeganie jest niezbędne do zapewnienia bezpiecznego przetwarzania danych osobowych. Jednocześnie regulacja ta będzie ulegać ciągłej modyfikacji, z uwagi na konieczność dostosowania zapisów w niej zawartych do stanu rzeczywistego oraz do zmieniających się przepisów prawa. Regulamin przetwarzania i ochrony danych osobowych oraz wszelka dokumentacja dotycząca przetwarzania danych osobowych w Szpitalu Specjalistycznym w Brzozowie dostępna jest dla wszystkich pracowników Szpitala – w formacie PDF – na stronie internetowej Szpitala pod adresem: http://www.szpital-brzozow.pl/ w zakładce „Strefa Pracownika".

Zawartość tej zakładki mogą przeglądać wszystkie osoby przetwarzające dane osobowe na potrzeby Szpitala po zalogowaniu się i wpisaniu odpowiedniego hasła. Zawartość tej zakładki podlega ochronie – treści tam zawarte objęte są tajemnicą przedsiębiorstwa i przeznaczone są wyłącznie dla Pracowników Szpitala Specjalistycznego w Brzozowie oraz osób wykonujących na rzecz Szpitala pracę na podstawie zawartej ze Szpitalem umowy cywilnoprawnej.

2/ Szkolenie w zakresie ochrony danych osobowych

Osoby dopuszczone do przetwarzania danych osobowych w Szpitalu Specjalistycznym w Brzozowie podlegają obowiązkowemu przeszkoleniu w tym zakresie – szkolenie obejmuje w szczególności treść obowiązujących przepisów dotyczących ochrony danych osobowych oraz wewnętrzne uregulowania. Nowo przyjmowani pracownicy, a także stażyści, studenci i wolontariusze podlegają obowiązkowemu przeszkoleniu przez Inspektora Ochrony Danych przed dopuszczeniem do przetwarzania danych osobowych. Po zakończeniu szkolenia osoby przeszkolone podpisują stosowne Oświadczenie (tzw. *„Klauzulę poufności"*) oraz potwierdzają odbycie szkolenia zgodnie z ***„Kartą szkolenia w zakresie ochrony danych osobowych".***

3/ Przetwarzanie danych

W Szpitalu Specjalistycznym w Brzozowie przetwarza się dane osobowe w następujących zbiorach danych osobowych:

- **dokumentacja dotycząca pacjentów i byłych pacjentów;**
- dokumentacja dotycząca **pracowników i byłych pracowników oraz członków ich rodzin**;
- dokumentacja dotycząca **kontrahentów** Szpitala;
- dokumentacja dotycząca **osób fizycznych będących stroną umów cywilnoprawnych** zawartych ze Szpitalem;
- dokumentacja dotycząca **kandydatów do pracy**;

- dokumentacja dotycząca **wolontariuszy, praktykantów i studentów**;
- dokumentacja dotycząca **nadawców i odbiorców korespondencji**;
- dokumentacja dotycząca **osób przyjmowanych do zakwaterowania do Hoteliku Szpitalnego (pacjenci i ich opiekunowie)**;
- dokumentacja dotycząca **osób fizycznych składających oferty w związku z postępowaniem prowadzonym w ramach zamówień publicznych**;
- dokumentacja dotycząca **wypadków przy pracy i w drodze do lub z pracy**;
- zbiór danych pochodzący z monitoringu wizyjnego;
- wykaz udostępnionej dokumentacji medycznej.

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują **Administrator Danych Osobowych**, którym jest Szpital Specjalistyczny w Brzozowie, reprezentowany przez Dyrektora Szpitala, oraz wyznaczony przez niego **Inspektor Ochrony Danych**.
W przypadku danych osobowych przetwarzanych w systemach informatycznych, za bezpieczeństwo przetwarzania tych danych odpowiada **Administrator Systemów Informatycznych** oraz podlegli mu pracownicy Sekcji Obsługi i Konserwacji Urządzeń.

4/ Główne zadania Inspektora Ochrony Danych

1) informowanie Administratora Danych oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich z tytułu przetwarzania danych osobowych i doradzanie im w tej sprawie;

2) monitorowanie przestrzegania przepisów dotyczących przetwarzania danych osobowych oraz polityk Administratora Danych w dziedzinie ochrony danych osobowych (działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty);

3) współpraca z organem nadzorczym, czyli z Prezesem Urzędu Ochrony Danych Osobowych oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

5/ Ogólne pojęcia z zakresu przetwarzania danych osobowych

Dane osobowe oznaczają wszelkie 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

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

1/ zbieranie,

2/ utrwalanie,

3/ organizowanie,

4/ porządkowanie,

5/ przechowywanie,

6/ adaptowanie lub modyfikowanie,

7/ pobieranie,

8/ przeglądanie,

9/ wykorzystywanie,

10/ ujawnianie poprzez przesłanie,

11/ rozpowszechnianie lub innego rodzaju udostępnianie,

12/ dopasowywanie lub łączenie,

13/ ograniczanie,

14/ usuwanie

15/ niszczenie.

6/ Przechowywanie zbiorów danych osobowych, dostęp do obszarów przetwarzania danych osobowych, procedura udostępniania danych oraz procedura niszczenia dokumentacji zbędnej zawierającej dane osobowe

1. **Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych muszą pozostawać zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika.** Opuszczenie pomieszczenia, w którym znajdują się dane osobowe musi być zawsze poprzedzone odpowiednim ich zabezpieczeniem przed możliwością ingerencji przez osoby nieupoważnione do przetwarzania danych osobowych. **Przy planowanej dłuższej nieobecności pracownika pomieszczenie, w którym znajdują się dane osobowe musi być zamknięte na klucz.**

2. W Szpitalu Specjalistycznym w Brzozowie zainstalowane są systemy sygnalizujące włamania i pożary – systemy te zainstalowane są na Izbie Przyjęć Szpitala, serwerowni Szpitala, serwerowni Zakładu Radioterapii, Wentylatorni, w Zakładzie Radioterapii, Archiwum Szpitalnym, Kasie, Aptece Szpitalnej oraz w Dziale Organizacji, Nadzoru, Statystyki i Analiz Medycznych.

3. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, pracownicy zobowiązani są do sprawdzenia stanu zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, dokumentacji i innego wyposażenia. **W przypadku stwierdzenia nieprawidłowości lub naruszenia stanu zabezpieczeń, pracownik, który to stwierdził, natychmiast powiadamia o tym swojego bezpośredniego przełożonego, który z kolei jest zobowiązany do niezwłocznego zawiadomienia Inspektora Ochrony Danych.**

Od momentu rozpoczęcia pracy do momentu jej zakończenia na pracownikach Szpitala spoczywa pełna odpowiedzialność za zabezpieczenie pomieszczeń Szpitala przed nieupoważnionym dostępem do tych pomieszczeń.

Po zakończeniu pracy pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy oraz wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych polegających na:

- zabezpieczeniu dokumentacji i pieczęci służbowych;
- zabezpieczeniu komputerów i nośników informacji;
- wyłączeniu wszystkich urządzeń energetycznych zasilanych energią elektryczną (czajniki, wentylatory itp.) zgodnie z zasadami bhp;
- zamknięciu okien i drzwi.

Klucze od biurek stanowiskowych i szaf biurowych są w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.

Duplikaty kluczy, będące kluczami zapasowymi do pomieszczeń administracyjnych są przechowywane w zamkniętej gablocie w gabinecie Kierownika Sekcji Gospodarczej.

Pracownik, któremu zostały powierzone klucze oraz kod cyfrowy do systemu alarmowego zobowiązany jest do:

- wykorzystywania ich zgodnie z przeznaczeniem;
- nie kopiowania oraz nie udostępniania osobom trzecim powierzonych kluczy – bez zgody Dyrektora Szpitala;
- nie udostępniania kodu cyfrowego do systemu alarmowego osobom trzecim.

4. Dokumentacja zawierająca dane osobowe winna być archiwizowana w pomieszczeniach, w których systematycznie monitoruje się temperaturę i wilgotność powietrza – **w przypadku Szpitala Specjalistycznego w Brzozowie za prowadzenie archiwum dokumentacji odpowiedzialny jest Dział Organizacji, Nadzoru, Statystyki i Analiz Medycznych.**

5. Jakiekolwiek udostępnianie danych osobowych może odbywać się wyłącznie w trybie oraz w pełnej zgodności z przepisami prawa oraz wewnętrznymi procedurami.

7/ Osoby upoważnione do przetwarzania danych osobowych i dostęp do danych osobowych w systemach informatycznych

Do przetwarzania danych osobowych w Szpitalu Specjalistycznym w Brzozowie upoważnione są jedynie osoby posiadające pisemne upoważnienie do przetwarzania danych osobowych, wydane przez Administratora Danych – upoważnienia te wydawane są zgodnie z zasadą wiedzy koniecznej.

Inspektor Ochrony Danych prowadzi elektroniczny rejestr upoważnień.

Upoważnienia do przetwarzania danych osobowych wydawane są na okres wykonywania pracy w Szpitalu Specjalistycznym w Brzozowie. W przypadku praktykantów, stażystów i wolontariuszy upoważnienia do przetwarzania danych osobowych wydawane są na okres trwania stażu, praktyki lub wolontariatu. Po zakończeniu okresu, na który zostało wydane upoważnienie, traci ono moc, co jest odnotowane w rejestrze upoważnień.
Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu **identyfikatora (loginu)** i właściwego **hasła**. **Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi, który odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora.**

Inspektor Ochrony Danych przydziela każdemu użytkownikowi systemu informatycznego indywidualne hasło dostępu oraz osobisty identyfikator. Hasło dostępu poszczególnego użytkownika podlega zmianie nie rzadziej niż raz na miesiąc. **Zmiana hasła dokonywana jest samodzielnie przez użytkownika systemu, przy czym hasło powinno zapewniać odpowiedni stopień bezpieczeństwa – winno składać się z ośmiu znaków alfanumerycznych oraz znaków specjalnych.** Identyfikator każdego użytkownika zostaje wpisany do ewidencji pracowników upoważnionych do przetwarzania danych osobowych wraz z imieniem i nazwiskiem użytkownika oraz podlega rejestracji w systemie informatycznym. Identyfikator ten nie podlega zmianie, a po wyrejestrowani użytkownika z systemu informatycznego nie może być przydzielony innej osobie.
Użytkownik systemu informatycznego nie może udostępniać innym osobom własnego hasła i identyfikatora w celu uzyskania dostępu do systemu informatycznego – podczas nadawania uprawnień do pracy w systemie informatycznym osoba, której będą nadane stosowne uprawnienia podpisuje klauzulę o następującej treści:

„Zobowiązuję się do zachowania w tajemnicy i nie udostępniania osobom trzecim kodu identyfikacyjnego (loginu) oraz hasła, a także zobowiązuję się do zmiany indywidualnego hasła startowego podczas pierwszego logowania i kolejnych zmian hasła nie rzadziej niż raz w miesiącu.
Równocześnie wyrażam zgodę na to, iż wszystkie działania w systemie informatycznym Szpitala Specjalistycznego w Brzozowie wykonane przez użytkownika o wskazanym kodzie identyfikacyjnym (loginie), będą przypisane mojej osobie ***i w przypadku stwierdzenia udostępnienia tego loginu i hasła osobom trzecim, zostanie mi cofnięte uprawnienie do przetwarzania danych osobowych."***

8/ Procedura niszczenia materiałów zawierających dane osobowe

1/ W przypadku konieczności zniszczenia materiałów zawierających dane osobowe (dokumentacja medyczna, dokumentacja pracownicza, wydruki z systemów informatycznych, wyniki badań, płyty DVD, płyty CD, dokumentacja zbiorcza etc.) każda osoba będąca w posiadaniu takich materiałów zobowiązana jest do ich przekazywania osobie wyznaczonej przez kierownika danej komórki organizacyjnej do zabezpieczania tych materiałów.

Zabrania się wynoszenia poza teren Szpitala wszelkich materiałów zawierających dane osobowe.

2/ Materiały powyższe muszą być przechowywane w obrębie danej komórki organizacyjnej oraz w odpowiedni sposób zabezpieczone.

3/ Po zebraniu odpowiedniej ilości tych materiałów (stosownie do możliwości przechowywania tych materiałów przez każdą komórkę organizacyjną Szpitala) osoba wyznaczona przez kierownika danej komórki organizacyjnej do zabezpieczania tych materiałów zawiadamia telefonicznie Inspektora Ochrony Danych w Szpitalu Specjalistycznym w Brzozowie o konieczności zniszczenia materiałów zawierających dane osobowe.

4/ Inspektor Ochrony Danych – po konsultacji z Kierownikiem Sekcji Gospodarczej w Szpitalu Specjalistycznym w Brzozowie – wyznacza termin odbioru materiałów przeznaczonych do zniszczenia.

5/ W przypadku stanowisk samodzielnych lub jednoosobowych stanowisk pracy – osoby zajmujące te stanowiska osobiście przedkładają do zniszczenia zbędne materiały zawierające dane osobowe.

6/ W przypadku fizycznej likwidacji urządzeń przetwarzających dane osobowe proces kasacji zostaje przeprowadzony przez Administratora Systemów Informatycznych w obecności osoby zlecającej kasację.

9/ Wystąpienie zagrożeń bezpieczeństwa danych osobowych oraz incydentów zagrażających bezpieczeństwu danych osobowych oraz procedury zabezpieczające

Zagrożenie bezpieczeństwa danych osobowych i incydenty zagrażające bezpieczeństwu danych

- **zagrożenia bezpieczeństwa danych** oznaczają wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;
- **incydent** oznacza takie pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności;
- **naruszenie ochrony danych osobowych** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Do **typowych zagrożeń bezpieczeństwa danych** osobowych należy nieprzestrzeganie zasad ochrony danych osobowych (np. niestosowanie zasady czystego biurka, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

Do **typowych incydentów zagrażających bezpieczeństwu danych** osobowych należą:

zdarzenia losowe:
pożar, zalanie, awarie serwera, awarie komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników systemu informatycznego, utrata lub zagubienie danych;

umyślne incydenty:
włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wir usów i innego szkodliwego oprogramowania

1/ Każdy osoba biorąca udział w przetwarzaniu danych osobowych jest odpowiedzialna za bezpieczeństwo tych danych. **W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogące spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania Inspektora Ochrony Danych.**

2/ W przypadku stwierdzenia naruszenia bezpieczeństwa danych, Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające, w toku którego:

- ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
- zabezpiecza ewentualne dowody;
- ustala osoby odpowiedzialne za naruszenie;
- podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
- inicjuje działania dyscyplinarne;
- wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;
- dokumentuje czynności podjęte w prowadzonym postępowaniu.

O naruszeniu ochrony danych osobowych w systemach informatycznych Szpitala mogą świadczyć

następujące symptomy:

- brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych;
- brak możliwości zalogowania się do tej aplikacji;
- ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji;
- wygląd aplikacji inny niż normalnie;
- inny zakres danych niż normalnie dostępny dla użytkownika – dużo więcej lub dużo mniej danych;
- znaczne spowolnienie działania systemu informatycznego;
- pojawienie się niestandardowych komunikatów generowanych przez system informatyczny;
- ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe;
- ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii zapasowych;
- włamanie lub próby włamania do szafek, w których przechowywane są – w postaci elektronicznej lub papierowej – nośniki danych osobowych;
- zagubienie bądź kradzież nośnika danych osobowych;
- kradzież sprzętu informatycznego, w którym przechowywane są dane osobowe;
- informacja z systemu antywirusowego o zainfekowaniu systemu;
- fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej;
- podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

W przypadku wystąpienia powyższych symptomów, jak również innych objawów, które mogą wskazywać na zagrożenie bezpieczeństwa danych osobowych, należy natychmiast powiadomić Inspektora Ochrony Danych.

Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia. W przypadku, gdy zgłoszenie o podejrzeniu incydentu otrzyma osoba inna niż Inspektor Ochrony Danych, jest ona zobowiązana poinformować o tym fakcie Inspektora Ochrony Danych.

Zasady pracy na służbowym sprzęcie komputerowym oraz zasady dostępu do sieci internetowej zostały określone w Zarządzeniu Nr 54/2011 Dyrektora Szpitala z dnia 10 maja 2011 roku wraz z jego aktualizacją – zgodnie z postanowieniami tego zarządzenia:

1/ na stacjach komputerowych pracują tylko osoby do tego upoważnione;

2/ komputer służbowy wykorzystywany jest tylko do celów służbowych;

3/ użytkownik komputera służbowego ponosi pełną odpowiedzialność za powierzony sprzęt komputerowy i zainstalowane oprogramowanie;

4/ użytkownik komputera służbowego ma obowiązek poinformować pracownika Sekcji Obsługi i Konserwacji Urządzeń o wszystkich uszkodzeniach sprzętu systemu w momencie ich zauważenia, oraz o komunikatach informujących o obecności wirusów;

5/ użytkownikowi komputera służbowego zabrania się:

- pobierania pakietów instalacyjnych oprogramowania oraz instalowania ich na dysku komputera;
- dokonywania zmian w konfiguracji istniejącego oprogramowania;
- łamania zabezpieczeń systemu i łamania haseł;
- udostępniania loginu i hasła osobom trzecim;
- używania stanowisk komputerowych w celach zarobkowych czy komercyjnych;
- wykonywania czynności naruszających prawa autorskie twórców lub dystrybutorów oprogramowania i danych;
- wyszukiwania i prezentowania materiałów o treści obrażającej uczucia innych;
- naruszania praw autorskich i licencyjnych;
- otwierania stron dotyczących przemocy, pornografii itp.;
- korzystania z gier komputerowych, serwerów CHAT, IRC i innych komunikatorów internetowych;
- wchodzenia na strony zawierające pirackie oprogramowanie;
- pobierania plików z sieci i zapisywania ich na nośnikach przenośnych;
- podłączania do szpitalnej sieci internetowej komputerów prywatnych oraz podłączania do komputera nośników prywatnych (pendrivów, płyt CD itp.);
- kopiowania danych osobowych na jakiekolwiek nośniki informacji;
- udostępniania sprzętu komputerowego osobom nieupoważnionym.

Ponadto w obowiązującym w Szpitalu Specjalistycznym w Brzozowie ***„Regulaminie przetwarzania i ochrony danych osobowych"*** zapisano między innymi:

*„W przypadku pracowników Szpitala, oraz osób wykonujących na jego rzecz pracę w oparciu o umowy cywilnoprawne i kontraktowe, możliwy jest – **w wyjątkowych, indywidualnych przypadkach** – dostęp do sieci lokalnej LAN oraz do sieci rozległej WAN poprzez prywatny komputer przenośny. W tej sytuacji o dostępie do sieci – w przypadku pracowników Szpitala – decyduje Administrator Danych Osobowych, który, na wniosek bezpośredniego przełożonego pracownika, skierowany do Administratora, udziela – po konsultacji z Inspektorem Ochrony Danych oraz Kierownikiem Sekcji Obsługi i Konserwacji Urządzeń – indywidualnej zgody na dostęp do szpitalnej sieci internetowej. W przypadku osób zajmujących kierownicze stanowiska w Szpitalu (zastępcy dyrektora Szpitala, ordynatorzy, kierownicy komórek organizacyjnych) oraz pracowników zatrudnionych na samodzielnych stanowiskach pracowniczych wniosek do Administratora Danych Osobowych składany jest przez te osoby.*

Przed udzieleniem zgody na podłączenie komputera do sieci musi się odbyć dokładne sprawdzenie czy komputer prywatny spełnia podstawowe wymogi podłączenia do sieci informatycznej, tzn. czy posiada odpowiednie zabezpieczenia antywirusowe i inne.
Minimalne środki ochrony to: zainstalowane systemy typu firewall oraz antywirus, wdrożony system aktualizacji systemu operacyjnego oraz jego składników, wymaganie podania hasła przed uzyskaniem dostępu do pracy na komputerze, niepozostawianie niezablokowanych stacji bez nadzoru, bieżąca praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.

Po pozytywnym rozpatrzeniu wniosku przez Administratora Danych Osobowych, wniosek ten przekazany zostaje Kierownikowi Sekcji Obsługi i Konserwacji Urządzeń, który kontaktuje się z osobą, której dotyczy wniosek i uzyskuje od niej niezbędny do nadania uprawnień adres fizyczny karty sieciowej, zainstalowanej w komputerze przenośnym.

Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków. Przetwarzanie tych danych może odbywać się wyłącznie za zgodą Administratora Danych Osobowych oraz za wiedzą Inspektora Ochrony Danych.

Zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzania danych ustala przełożony pracownika, za wiedzą Inspektora Ochrony Danych. W przypadku osób wykonujących pracę na rzecz Szpitala w oparciu o umowę cywilnoprawną lub umowę kontraktową, zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzania danych ustala Administrator Danych Osobowych.

Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych, zobowiązana jest do

zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.

Użytkownik komputera przenośnego zobowiązany jest do:

- *transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności: transportowania komputera w bagażu podręcznym, nie pozostawiania komputera w samochodzie, przechowalni bagażu itp.;*
- *korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego;*
- *nie zezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe;*
- *zabezpieczania komputera przenośnego hasłem;*
- *blokowania dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika;*
- *kopiowania danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych;*
- *umożliwienia, poprzez podłączenie komputera do sieci informatycznej Szpitala Specjalistycznego w Brzozowie, aktualizacji wzorców wirusów w programie antywirusowym;*
- *utrzymanie konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł;*
- *wykorzystywanie haseł o odpowiedniej jakości, zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe;*
- *zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.*

W razie zgubienia lub kradzieży komputera przenośnego pracownik zobowiązany jest do natychmiastowego powiadomienia Administratora Danych Osobowych i Inspektora Ochrony Danych, zgodnie z zasadami informowania o naruszeniu ochrony danych osobowych.

Użytkownicy systemu informatycznego są zobowiązani do bezwzględnego przestrzegania następującej procedury rozpoczęcia, prowadzenia i zakończenia pracy w systemie informatycznym*:*

- **rozpoczynając pracę przy komputerze użytkownik loguje się do systemu poprzez wprowadzenie wymaganych identyfikatorów i haseł w sposób uniemożliwiający ich ujawnienie osobom trzecim;**
- w przypadku jakiejkolwiek przerwy w pracy w systemie informatycznym i opuszczenia stanowiska pracy użytkownik jest zobowiązany do wylogowania się z systemu bądź zablokowania stacji roboczej;
- użytkownik jest zobowiązany do korzystania z systemu informatycznego w sposób uniemożliwiający osobom nieuprawnionym zapoznanie się z danymi osobowymi;
- **po zakończeniu pracy w systemie informatycznym użytkownik jest zobowiązany do zamknięcia aplikacji, wylogowania się z systemu oraz wyłączenia komputera;**

- **w celu przesłania w postaci elektronicznej (e-mail) komunikatów służbowych zawierających dane osobowe należy korzystać wyłącznie ze służbowych skrzynek pocztowych; wiadomość zawierającą dane osobowe należy przed wysłaniem zaszyfrować za pomocą programu 7-zip i zaopatrzyć w odpowiedni klucz (hasło); zaszyfrowaną wiadomość można wysłać jedynie za pomocą służbowej skrzynki pocztowej, natomiast klucz do odszyfrowania wiadomości należy przekazać adresatowi wiadomości telefonicznie; z uwagi na wysokie niebezpieczeństwo związane z tego typu operacjami zaleca się aby czynności te wykonywane były pod bezpośrednim nadzorem pracownika Sekcji Obsługi i Konserwacji Urządzeń;**

- **niedozwolone jest – bez powiadomienia o tym fakcie Administratora Danych Osobowych i Inspektora Ochrony Danych – zapisywanie czy kopiowanie na nośniki zewnętrzne informacji zawierających dane osobowe."**

Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia w Szpitalu naruszenia bezpieczeństwa danych osobowych Inspektor Ochrony Danych, we współpracy z Kierownikiem Sekcji Obsługi i Konserwacji Urządzeń, jest zobowiązany do podjęcia kroków w celu:

- wyjaśnienia zdarzenia, a w szczególności czy miało miejsce naruszenie ochrony danych osobowych;
- wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów, a w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich;
- zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia;
- usunięcia skutków incydentu i przywróceniu pierwotnego stanu systemu informatycznego (to jest stanu sprzed incydentu).

Inspektor Ochrony Danych określa w formie raportu, na podstawie zebranych informacji, przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, jest on zobowiązany do pisemnego powiadomienia Administratora Danych, który może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych.

Inspektor Ochrony Danych prowadzi ewidencję interwencji związanej z zaistniałymi incydentami w zakresie bezpieczeństwa danych osobowych. Ewidencja taka obejmuje następujące informacje:

- imię i nazwisko osoby zgłaszającej incydent;
- imię i nazwisko osoby przyjmującej zgłoszenie incydentu;
- datę zgłoszenia incydentu;
- przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu;
- wyniki przeprowadzonych działań;
- podjęte akcje naprawcze i ich skuteczność.

10/ Odpowiedzialność

1. Za przestrzeganie zasad dotyczących bezpieczeństwa przetwarzania danych osobowych, odpowiedzialni są wszyscy pracownicy Szpitala oraz osoby wykonujące na jego rzecz pracę w oparciu o umowy cywilnoprawne oraz umowy kontraktowe.

2. W przypadku pracowników Szpitala, których zakres obowiązków pracowniczych nie obejmuje konieczności przetwarzania danych osobowych, a które z racji tych obowiązków mogą mieć dostęp do pomieszczeń, w których przetwarza się dane osobowe – pracownicy Sekcji Gospodarczej, Sekcji Higieny

Szpitalnej, Sekcji Technicznej, Kuchni i Pralni – nałożono obowiązek pisemnego oświadczenia zawierającego klauzulę zobowiązującą do zachowania w tajemnicy, nieujawniania i niewykorzystywania wszelkich informacji, z którymi zapoznali się z racji wykonywanych obowiązków, w szczególności dotyczących danych osobowych.

3. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień dotyczących zasad przetwarzania danych osobowych. **Przypadki, nieuzasadnionego zaniechania obowiązków pracowniczych w powyższym zakresie potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.**

Wobec osoby, która w przypadku naruszenia bezpieczeństwa przetwarzania danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła określonego działania, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi procedurami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

Kara dyscyplinarna nie wyklucza odpowiedzialności karnej tej osoby zgodnie z odpowiednimi przepisami, oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

Podstawa prawna przetwarzania danych osobowych przez pracowników Działu Zatrudnienia i Kadr – Spis aktów prawnych i regulacji wewnętrznych:

1/ *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – Dziennik Urzędowy Unii Europejskiej L 119/1;*

2/ *Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych – Tekst jednolity: Dziennik Ustaw z dnia 19 września 2019 roku pozycja 1781;*

3/ *Ustawa z dnia 26 czerwca 1974 roku Kodeks pracy – Tekst jednolity: Dziennik Ustaw z dnia 5 czerwca 2019 roku pozycja 1040;*

4/ *Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 roku w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika – Tekst jednolity: Dziennik Ustaw z dnia 8 maja 2017 roku pozycja 894;*

5/ *Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 roku w sprawie dokumentacji pracowniczej – Dziennik Ustaw z dnia 19 grudnia 2018 roku pozycja 2369;*

6/ *Ustawa ustawy z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne – Tekst jednolity: Dziennik Ustaw z dnia 16 kwietnia 2019 roku pozycja 700;*

7/ *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych – Tekst jednolity: Dziennik Ustaw z dnia 5 grudnia 2017 roku pozycja 2247;*

8/ *Regulamin Pracy Szpitala Specjalistycznego w Brzozowie Podkarpackiego Ośrodka Onkologicznego im. Ks. Bronisława Markiewicza z dnia 31 stycznia 2014 roku.*

Obowiązujący stan prawny – ogólna charakterystyka

Podstawa Prawna przetwarzania danych osobowych w procesie rekrutacji oraz w zatrudnieniu – stan obowiązujący:

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - RODO)

Zgodnie z Rozporządzenia „RODO":

1) ***dane osobowe oznaczają*** *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;*

2) ***przetwarzanie oznacza*** *operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;*

3) ***zbiór danych oznacza*** *uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;*

4) ***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;

*5) **podmiot przetwarzający oznacza** osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;*

*6) **odbiorca oznacza** osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;*

*7) **zgoda osoby, której dane dotyczą oznacza** dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;*

*8) **naruszenie ochrony danych osobowych oznacza** naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.*

Zasady dotyczące przetwarzania danych osobowych – art. 5 „RODO"

1. Dane osobowe muszą być:

*a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą **(„zgodność z prawem, rzetelność i przejrzystość");***

*b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami **(„ograniczenie celu");***

*c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane **(„minimalizacja danych");***

*d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane **(„prawidłowość");***

e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane

*wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą **(„ograniczenie przechowywania");***

f) 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").

*2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie **(„rozliczalność").***

Obowiązki administratora – art. 24 „RODO"

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Bezpieczeństwo przetwarzania – art. 32 „RODO"

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) pseudonimizację i szyfrowanie danych osobowych;

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

4. 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.

KODEKS PRACY

Jakie dane pracodawca może pozyskiwać

Zgodnie z wydanym w miesiącu październiku 2018 roku przez Urząd Ochrony Danych Osobowych poradnikiem pt. „Ochrona Danych Osobowych w Miejscu Pracy – Poradnik dla Pracodawców": *„pracodawca powinien przetwarzać tylko takie dane, które są niezbędne ze względu na cel ich zbierania, jakim jest podjęcie przez niego decyzji o zatrudnieniu nowego pracownika; oznacza to, że pracodawca nie może żądać od kandydata* ***danych nadmiarowych****, które nie są niezbędne do przeprowadzenia rekrutacji – dane osobowe nie mogą być zbierane na zapas, „na wszelki wypadek", tj. bez wykazania zgodnego z prawem celu ich pozyskania i wykazania ich niezbędności dla realizacji tego celu przez administratora. Ponadto, żądanie przez pracodawcę od kandydatów do pracy informacji wykraczających poza to, co przede wszystkim przewidują przepisy prawa pracy może naruszać zarówno postanowienia RODO, jak i przepisy prawa pracy rodząc np. zarzut dyskryminacji."*

Zgodnie z „Poradnikiem": *„Zdarza się, że osoby kandydujące do pracy przekazują z własnej inicjatywy więcej danych, niż wskazane w Kodeksie pracy. W takiej sytuacji dane osobowe kandydata, o ile nie należą do szczególnej kategorii danych, są przetwarzane przez potencjalnego pracodawcę na podstawie zgody, która może polegać na oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Aplikacja kandydata stanowi zazwyczaj odpowiedź na ogłoszenie o pracę pracodawcy, kandydat jest świadomy, do jakiego podmiotu składa aplikację oraz w jakim celu jego dane mają być przetwarzane. Kandydat zna jednocześnie zakres danych, jaki przekazuje pracodawcy. Oznacza to, że zwykłe dane osobowe, które wykraczają poza zakres uregulowany przepisami prawa pracy, są przetwarzane przez pracodawcę na podstawie zgody kandydata, która przejawia się przez działanie, polegające np. na przesłaniu pracodawcy życiorysu i listu motywacyjnego."*

W Dzienniku Ustaw z dnia 19 kwietnia 2019 roku – w pozycji 730 – ukazała się Ustawa z dnia 21 lutego 2019 roku ***o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia***

27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – **z mocą obowiązującą od dnia 4 maja 2019 roku.**

W art. 4 tej ustawy wprowadzono zmiany mające na celu dostosowanie brzmienia obowiązujących przepisów prawa pracy do **art. 6 ust. 1 lit. c.** rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, **który wprowadził przesłankę istnienia „obowiązku prawnego" jako podstawy pobierania danych osobowych.** Przepisy rozporządzenia (UE) 2016/679, przyznają państwom członkowskim swobodę w określeniu zasad przetwarzania przez pracodawców danych osobowych pracowników, jednocześnie wskazując na konieczność uzależnienia gromadzenia niektórych danych od wyrażenia zgody osoby ubiegającej się o zatrudnienie bądź pracownika.

Analiza zmian:
1. Nowe brzmienie przepisów Kodeksu pracy w **art. 22(1) § 1–3** wskazuje na kategorie danych osobowych, które są niezbędne do pozyskania przez pracodawcę, w związku z podejmowaniem przez niego działań przed zawarciem umowy o pracę oraz po jej zawarciu. Po wprowadzeniu zmian pracodawca nie może żądać od kandydata na pracownika i od pracownika **imion rodziców**, będzie natomiast mógł żądać danych kontaktowych i danych dotyczących kwalifikacji zawodowych.
2. Zmienione przepisy nie zwalniają pracodawców od konieczności oceny, czy wszystkie z gromadzonych danych konieczne są do realizacji celu, jakim jest zatrudnienie określonej osoby. Pracodawca gromadzi informacje o wykształceniu, kwalifikacjach zawodowych i przebiegu dotychczasowego zatrudnienia osoby ubiegającej się o zatrudnienie **tylko gdy uzna że jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku.**
Powyższa norma służy pełnej realizacji przewidzianej w art. 5 ust. 1 lit. c rozporządzenia (UE) 2016/679 - zasady minimalizmu przetwarzania danych.
3. Pracodawca może żądać od pracowników dodatkowo danych dzieci i innych członków rodziny, numeru PESEL pracownika, miejsca zamieszania pracownika oraz wykształcenia jeśli informacji tych nie uzyskał przed zatrudnieniem pracownika.
4. Inne dane osobowe pracownika, będą mogły być pobierane m.in. gdy będzie to niezbędne do wypełniania obowiązku pracodawcy nałożonego przepisem prawa - obowiązek taki wynikać może zarówno z przepisów Kodeksu pracy, jak i odrębnych przepisów prawnych.
5. Tak jak przed zmianą przepisów dane będą udostępniane pracodawcy na podstawie oświadczenia przy czym pracodawca będzie mógł żądać udokumentowania danych osobowych w niezbędnym zakresie.
6. Gromadzenie innych danych osobowych osoby ubiegającej się o zatrudnienie lub pracownika przekazywanych zarówno z inicjatywy pracodawcy jak i na wniosek pracownika, możliwe będzie również na podstawie zgody pracownika.
Zasada ta nie będzie dotyczyła danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o których mowa w art. 10 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679. **Tego rodzaju dane osobowe będą mogły być przetwarzane wyłącznie w przypadku gdy przepis prawa będzie przewidywać**

obowiązek ich żądania przez pracodawcę lub obowiązek ich udostępnienia przez osobę ubiegającą się o zatrudnienie lub pracownika.

7. Zgoda osoby ubiegającej się o zatrudnienie lub pracownika będzie mogła stanowić podstawę przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby o których mowa w art. 9 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679. Brak udzielenia zgody lub jej wycofanie nie będzie mogło powodować negatywnych konsekwencji dla pracownika.

8. Dane biometryczne będą mogły być pobierane od pracownika i przetwarzane w sytuacjach, w których podanie takich danych będzie niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę lub dostępu do pomieszczeń wymagających szczególnej ochrony.

9. W przepisach wyraźnie określono, że do przetwarzania danych osobowych mogą być dopuszczone osoby mające odpowiednie upoważnienie wydane przez pracodawcę. Osoby takie mają obowiązek do zachowania tajemnicy.

10. Doprecyzowano zasady stosowania monitoringu w zakładzie pracy. Na podstawie zmienionych przepisów monitoring nie obejmuje;

- pomieszczeń udostępnianych zakładowej organizacji związkowej,
- pomieszczeń sanitarnych, szatni, stołówek oraz palarni - chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne dla zapewnienia bezpieczeństwa, ochrony mienia lub zachowania tajemnicy informacji i nie naruszy to godności oraz innych dóbr osobistych pracownika; dodatkowo instalacja monitoringu wizyjnego w pomieszczeniach sanitarnych wymaga uzyskania przez pracodawcę uprzedniej zgody zakładowej organizacji związkowej lub przedstawicieli pracowników.

11. Wprowadzono zmiany redakcyjne oraz doprecyzowujące zakres orzeczeń lekarskich, których może żądać pracodawca, tryb przechowywania i zwrotu orzeczeń lekarskich – **art. 229 Kodeksu Pracy.**

Dane osobowe pracownika

Zgodnie z § 1 art. 22[1] Kodeksu pracy pracodawca żąda **od osoby ubiegającej się o zatrudnienie** podania danych osobowych obejmujących:

1) imię (imiona) i nazwisko;
2) datę urodzenia;
3) dane kontaktowe wskazane przez taką osobę;
4) wykształcenie;
5) kwalifikacje zawodowe;
6) przebieg dotychczasowego zatrudnienia.

Zgodnie z § 2 tego artykułu: pracodawca żąda podania danych osobowych, o których mowa w § 1 pkt 4-6, gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku.

Zgodnie z § 3 tego artykułu: pracodawca żąda **od pracownika** podania dodatkowo danych osobowych obejmujących:

1) adres zamieszkania;

2) numer PESEL, a w przypadku jego braku - rodzaj i numer dokumentu potwierdzającego tożsamość;

3) inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy;

4) wykształcenie i przebieg dotychczasowego zatrudnienia, jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie;

5) numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych.

Zgodnie z § 4 tego artykułu: Pracodawca żąda podania innych danych osobowych niż określone w § 1 i 3, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Zgodnie z § 5 tego artykułu: Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której dane dotyczą. Pracodawca może żądać udokumentowania danych osobowych osób, o których mowa w § 1 i 3, w zakresie niezbędnym do ich potwierdzenia.

Zgoda osoby ubiegającej się o zatrudnienie lub pracownika na przetwarzanie przez pracodawcę innych danych osobowych

Zgodnie z art. 22^{1a} Kodeksu Pracy:

§ 1. Zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez pracodawcę innych danych osobowych niż wymienione w art. 22^1 § 1 i 3, z wyjątkiem danych osobowych, o których mowa w art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), zwanego dalej "rozporządzeniem 2016/679".

§ 2. Brak zgody, o której mowa w § 1, lub jej wycofanie, nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę.

§ 3. Przetwarzanie, o którym mowa w § 1, dotyczy danych osobowych udostępnianych przez osobę ubiegającą się o zatrudnienie lub pracownika na wniosek pracodawcy lub danych osobowych przekazanych pracodawcy z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika.

Zgodnie z art. 22^{1b} Kodeksu Pracy:

§ 1. Zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez pracodawcę danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, wyłącznie w przypadku, gdy przekazanie tych danych osobowych następuje z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika. Przepis art. 22^{1a} § 2 stosuje się odpowiednio.

§ 2. Przetwarzanie danych biometrycznych pracownika jest dopuszczalne także wtedy, gdy podanie takich danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony.

§ 3. Do przetwarzania danych osobowych, o których mowa w § 1, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy.

Monitoring w zakładzie pracy

Zgodnie z art. 22^{2} Kodeksu Pracy:

§ 1. Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring).

§ 1^{1}. Monitoring nie obejmuje pomieszczeń udostępnianych zakładowej organizacji związkowej.

§ 2. Monitoring nie obejmuje pomieszczeń sanitarnych, szatni, stołówek oraz palarni, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu określonego w § 1 i nie naruszy to godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Monitoring pomieszczeń sanitarnych wymaga uzyskania uprzedniej zgody zakładowej organizacji związkowej, a jeżeli u pracodawcy nie działa zakładowa organizacja związkowa - uprzedniej zgody przedstawicieli pracowników wybranych w trybie przyjętym u danego pracodawcy.

§ 3. Nagrania obrazu pracodawca przetwarza wyłącznie do celów, dla których zostały zebrane, i przechowuje przez okres nieprzekraczający 3 miesięcy od dnia nagrania.

§ 4. W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin określony w § 3 ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.

§ 5. Po upływie okresów, o których mowa w § 3 lub 4, uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej.

§ 6. Cele, zakres oraz sposób zastosowania monitoringu ustala się w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy.

§ 7. Pracodawca informuje pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy, nie później niż 2 tygodnie przed jego uruchomieniem.
§ 8. Pracodawca przed dopuszczeniem pracownika do pracy przekazuje mu na piśmie informacje, o których mowa w § 6.
§ 9. W przypadku wprowadzenia monitoringu pracodawca oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem.
§ 10. Przepis § 9 nie narusza przepisów art. 12 i art. 13 rozporządzenia 2016/679.

W dniu 1 stycznia 2019 roku weszło w życie **ROZPORZĄDZENIE MINISTRA RODZINY, PRACY I POLITYKI SPOŁECZNEJ** z dnia 10 grudnia 2018 roku **w sprawie dokumentacji pracowniczej** – zastępujące **ROZPORZĄDZENIE MINISTRA PRACY I POLITYKI SOCJALNEJ** z dnia 28 maja 1996 roku **w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika.**

Zgodnie z nowym rozporządzeniem:

§ 3. *Akta osobowe pracownika składają się z 4 części i obejmują:*
1) ***w części A*** *-* ***oświadczenia lub dokumenty dotyczące danych osobowych,*** *zgromadzone w związku z ubieganiem się o zatrudnienie, a także skierowania na badania lekarskie i orzeczenia lekarskie dotyczące wstępnych, okresowych i kontrolnych badań lekarskich (art. 229 § 1 pkt 1, § 1^1 i 1^2 Kodeksu pracy);*

2) ***w części B*** *- oświadczenia lub dokumenty dotyczące nawiązania stosunku pracy oraz przebiegu zatrudnienia pracownika, w tym:*

a) ***oświadczenia lub dokumenty dotyczące danych osobowych,*** *gromadzone w związku z nawiązaniem stosunku pracy,*

b) ***umowę o pracę,*** *a jeżeli umowa nie została zawarta z zachowaniem formy pisemnej - potwierdzenie ustaleń co do stron umowy, rodzaju umowy oraz jej warunków (art. 29 § 2 Kodeksu pracy),*

c) ***zakres czynności (zakres obowiązków),*** *jeżeli pracodawca dodatkowo w tej formie określił zadania pracownika wynikające z rodzaju pracy, określonego w umowie o pracę,*

d) ***dokumenty dotyczące wykonywania przez pracownika pracy w szczególnych warunkach lub o szczególnym charakterze*** *w rozumieniu przepisów ustawy z dnia 19 grudnia 2008 r. o emeryturach pomostowych (Dz. U. z 2018 r. poz. 1924),*

e) ***potwierdzenie zapoznania się przez pracownika:***
– ***z treścią regulaminu pracy*** *(art. 104^3 § 2 Kodeksu pracy) albo obwieszczenia (art. 150 § 7 Kodeksu pracy),*
– ***z przepisami oraz zasadami bezpieczeństwa i higieny pracy*** *(art. 237^4 § 3 Kodeksu pracy),*

*– **z zakresem informacji objętych tajemnicą** określoną w odrębnych przepisach dla danego rodzaju pracy, zajmowanego stanowiska lub pełnionej funkcji,*

*f) **potwierdzenie poinformowania pracownika:***
*– **o warunkach zatrudnienia** (art. 29 § 3 i art. 29^1 § 2 Kodeksu pracy) oraz o zmianie warunków zatrudnienia (art. 29 § 3^2 i art. 29^1 § 4 Kodeksu pracy),*
*– **o celu, zakresie oraz sposobie zastosowania monitoringu** (art. 22^2 § 8 Kodeksu pracy),*
*– **o ryzyku zawodowym,** które wiąże się z wykonywaną pracą, oraz o zasadach ochrony przed zagrożeniami (art. 226 pkt 2 Kodeksu pracy),*

g) potwierdzenie otrzymania przez pracownika młodocianego oraz jego przedstawiciela ustawowego informacji o ryzyku zawodowym, które wiąże się z pracą wykonywaną przez młodocianego, oraz o zasadach ochrony przed zagrożeniami (art. 201 § 3 Kodeksu pracy),

*h) **dokumenty potwierdzające ukończenie wymaganego szkolenia w zakresie bezpieczeństwa i higieny pracy,***

*i) **oświadczenia dotyczące wypowiedzenia warunków pracy lub płacy lub zmiany tych warunków w innym trybie,***

*j) **dokumenty dotyczące powierzenia pracownikowi mienia** z obowiązkiem zwrotu albo do wyliczenia się, dokumenty dotyczące przyjęcia przez pracownika wspólnej odpowiedzialności materialnej za mienie powierzone łącznie z obowiązkiem wyliczenia się (art. 124 i art. 125 Kodeksu pracy),*

*k) **dokumenty związane z podnoszeniem kwalifikacji zawodowych** przez pracownika lub związane ze zdobywaniem lub uzupełnianiem wiedzy i umiejętności na zasadach innych niż dotyczące podnoszenia kwalifikacji zawodowych,*

*l) **dokumenty związane z przyznaniem pracownikowi nagrody lub wyróżnienia** (art. 105 Kodeksu pracy),*
*m) **dokumenty związane z ubieganiem się i korzystaniem przez pracownika z urlopu macierzyńskiego, urlopu na warunkach urlopu macierzyńskiego, urlopu rodzicielskiego, urlopu ojcowskiego lub urlopu wychowawczego**,*

*n) **dokumenty związane z łączeniem korzystania z urlopu rodzicielskiego z wykonywaniem pracy u pracodawcy udzielającego tego urlopu** (art. 182^{1e} Kodeksu pracy),*

*o) **dokumenty związane z obniżeniem wymiaru czasu pracy, w przypadku pracownika uprawnionego do urlopu wychowawczego** (art. 186^7 Kodeksu pracy),*

*p) **oświadczenie pracownika będącego rodzicem lub opiekunem dziecka o zamiarze lub o braku zamiaru korzystania z uprawnień związanych z rodzicielstwem** (art. 189^1 Kodeksu pracy),*

*q) **dokumenty związane z udzielaniem urlopu bezpłatnego** (art. 174 i art. 174[1] Kodeksu pracy),*

*r) **skierowania na badania lekarskie i orzeczenia lekarskie** dotyczące:*
– wstępnych badań lekarskich (art. 229 § 1 pkt 2 Kodeksu pracy),
– okresowych i kontrolnych badań lekarskich (art. 229 § 2 i 5 Kodeksu pracy),

*s) **umowę o zakazie konkurencji,** jeżeli strony zawarły taką umowę w okresie pozostawania w stosunku pracy (art. 101[1] § 1 Kodeksu pracy),*

*t) **wniosek pracownika o poinformowanie właściwego okręgowego inspektora pracy o zatrudnianiu pracowników pracujących w nocy oraz kopię informacji w tej sprawie skierowanej do właściwego inspektora pracy** (art. 151[7] § 6 Kodeksu pracy),*

*u) **dokumenty związane ze współdziałaniem pracodawcy z reprezentującą pracownika zakładową organizacją związkową lub innymi podmiotami w sprawach ze stosunku pracy wymagających takiego współdziałania,***

*v) **dokumenty dotyczące wykonywania pracy w formie telepracy;***

*3) **w części C** - oświadczenia lub dokumenty związane z rozwiązaniem albo wygaśnięciem stosunku pracy, w tym:*

a) oświadczenia związane z rozwiązaniem umowy o pracę,

b) wnioski dotyczące wydania, sprostowania lub uzupełnienia świadectwa pracy,

c) dokumenty dotyczące niewypłacenia pracownikowi ekwiwalentu pieniężnego za urlop wypoczynkowy (art. 171 § 3 Kodeksu pracy),

d) kopię wydanego świadectwa pracy,

e) potwierdzenie dokonania czynności związanych z zajęciem wynagrodzenia za pracę w związku z prowadzonym postępowaniem egzekucyjnym,

f) umowę o zakazie konkurencji po ustaniu stosunku pracy, jeżeli strony zawarły taką umowę (art. 101[2] § 1 Kodeksu pracy),

g) skierowania na badania lekarskie i orzeczenia lekarskie związane z okresowymi badaniami lekarskimi w związku z wykonywaniem pracy w warunkach narażenia na działanie substancji i czynników rakotwórczych lub pyłów zwłókniających (art. 229 § 5 pkt 2 Kodeksu pracy);

*4) **w części D** - odpis zawiadomienia o ukaraniu oraz inne dokumenty związane z ponoszeniem przez pracownika odpowiedzialności porządkowej lub odpowiedzialności określonej w odrębnych przepisach, które przewidują zatarcie kary po upływie określonego czasu.*

§ 8. *Pracodawca zapewnia odpowiednie warunki zabezpieczające dokumentację pracowniczą prowadzoną i przechowywaną w postaci papierowej przed zniszczeniem, uszkodzeniem lub utratą i dostępem osób nieupoważnionych, w szczególności przez zapewnienie w pomieszczeniu, w którym przechowywana jest dokumentacja pracownicza, odpowiedniej wilgotności, temperatury i zabezpieczenie tego pomieszczenia przed dostępem osób nieupoważnionych.*

Szczególne wymagania dotyczące prowadzenia i przechowywania dokumentacji w postaci elektronicznej

§ 9.
Dokumentacja pracownicza w postaci elektronicznej jest prowadzona i przechowywana w systemie teleinformatycznym zapewniającym:

1) zabezpieczenie jej przed uszkodzeniem, utratą oraz nieuprawnionym dostępem;

2) integralność treści dokumentacji i metadanych polegającą na zabezpieczeniu przed wprowadzaniem zmian, z wyjątkiem zmian wprowadzanych w ramach ustalonych i udokumentowanych procedur;

3) stały dostęp do dokumentacji osobom do tego upoważnionym;

4) identyfikację osób mających dostęp do dokumentacji oraz rejestrowanie dokonywanych przez te osoby zmian w dokumentacji i metadanych;

5) skuteczne wyszukiwanie dokumentacji na podstawie metadanych, o których mowa w § 13 ust. 3;

6) wydawanie, w tym przez eksport w postaci elektronicznej, dokumentacji albo części dokumentacji w sposób określony w rozdziale 4;

7) funkcjonalność wydruku dokumentacji.

§ 10.
1. Dokumentację pracowniczą prowadzoną i przechowywaną w postaci elektronicznej uważa się za zabezpieczoną w zakresie, o którym mowa w § 9 pkt 1, jeżeli w sposób ciągły są spełnione łącznie następujące warunki:

1) jest zapewniona jej dostępność wyłącznie osobom upoważnionym;

2) jest chroniona przed przypadkowym lub nieuprawnionym zniszczeniem;

3) jej prowadzenie i przechowywanie odbywa się z zastosowaniem metod i środków ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.

2. Zabezpieczenie dokumentacji pracowniczej prowadzonej i przechowywanej w postaci elektronicznej polega w szczególności na:

1) systematycznym dokonywaniu analizy zagrożeń;
2) opracowaniu i stosowaniu procedur zabezpieczania dokumentacji i systemów ich przetwarzania, w tym procedur dostępu, tworzenia kopii zapasowych oraz przechowywania;

3) stosowaniu środków bezpieczeństwa adekwatnych do zagrożeń;

4) bieżącym kontrolowaniu funkcjonowania wszystkich organizacyjnych i techniczno-informatycznych sposobów zabezpieczenia, a także okresowym dokonywaniu oceny skuteczności tych sposobów;

5) przygotowaniu i realizacji planów przechowywania dokumentacji w długim czasie, w tym jej przenoszenia na nowe informatyczne nośniki danych i do nowych formatów danych, jeżeli tego wymaga zapewnienie ciągłości dostępu do dokumentacji.
***§ 12.** Prowadząc i przechowując dokumentację pracowniczą w postaci elektronicznej, pracodawca stosuje odpowiednie, w odniesieniu do ilości danych i zastosowanej technologii, rozwiązania techniczne zapewniające dostępność, używalność i wiarygodność dokumentacji, co najmniej do upływu okresu przechowywania dokumentacji.*

***§ 19.** Przepisy niniejszego rozporządzenia stosuje się do dokumentacji pracowniczej pracowników, których stosunek pracy został nawiązany począwszy od dnia 1 stycznia 2019 r.*

§ 20.
1. Do dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracowników, pozostających w dniu wejścia w życie niniejszego rozporządzenia w stosunku pracy, zgromadzonych przed tym dniem, stosuje się przepisy niniejszego rozporządzenia, z wyjątkiem § 2-6; w tym zakresie stosuje się przepisy obowiązujące przed dniem wejścia w życie niniejszego rozporządzenia.

2. Do dokumentacji pracowniczej pracowników, o których mowa w ust. 1, gromadzonej od dnia wejścia w życie niniejszego rozporządzenia stosuje się przepisy tego rozporządzenia.

3. Do zakresu kart ewidencji czasu pracy pracowników, o których mowa w ust. 1, prowadzonych w dniu wejścia w życie niniejszego rozporządzenia, stosuje się przepisy obowiązujące przed tym dniem.

***§ 21.** Pracodawcy mogą dostosować dokumentację w sprawach związanych ze stosunkiem pracy oraz akta osobowe pracowników, pozostających w dniu wejścia w życie niniejszego rozporządzenia w stosunku pracy, zgromadzone przed tym dniem, do § 2-6 niniejszego rozporządzenia.*

§ 22.

1. Do dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracowników, których stosunek pracy ustał przed dniem wejścia w życie niniejszego rozporządzenia, stosuje się przepisy tego rozporządzenia, z wyjątkiem § 2-6; w tym zakresie stosuje się przepisy obowiązujące przed dniem wejścia w życie niniejszego rozporządzenia.
2. W przypadku, o którym mowa w ust. 1, pracodawcy dostosują warunki przechowywania dotychczasowej dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracowników do warunków określonych w § 8 niniejszego rozporządzenia w okresie 12 miesięcy od dnia wejścia w życie tego rozporządzenia.

3. Przepis § 21 stosuje się odpowiednio.

§ 23. *Rozporządzenie wchodzi w życie z dniem 1 stycznia 2019 r.*