Zarządzenie nr 24/23
Rektora Collegium Witelona Uczelnia Państwowa
z dnia 05 kwietnia 2023 r.

w sprawie wprowadzenia Procedury ochrony danych osobowych w ramach pracy zdalnej

Na podstawie art. 23 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2022 r. poz. 574 ze zm.) i art. 67^{26} § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2022 r. poz. 1510 ze zm.), zarządzam co następuje:

§ 1.

Wprowadzam Procedurę ochrony danych osobowych w ramach pracy zdalnej, stanowiącą załącznik do niniejszego zarządzenia.

§ 2.

Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązującą od 07 kwietnia 2023 r.

REKTOR
prof. dr hab. Andrzej Panasiuk

RADCA PRAWNY
mgr Ewa Kozłowska

Załącznik do zarządzenia nr 24/23 Rektora Collegium
Witelona Uczelnia Państwowa z dnia 05 kwietnia 2023 r.

Procedura ochrony danych osobowych w ramach pracy zdalnej

§ 1.
Zakres i cel procedury

1. Niniejsza Procedura określa zasady bezpieczeństwa informacji i danych osobowych w trakcie pracy zdalnej.
2. Inspektor Ochrony Danych dalej IOD, powołany w Uczelni przeprowadza, w miarę potrzeb, instruktaż i szkolenie w tym zakresie dla pracowników wykonujących pracę zdalną.
3. Pracownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
4. Pracownik w trakcie pracy zdalnej zobowiązany jest dbać o bezpieczeństwo danych, ich poufność oraz integralność.

§ 2.
Wyjaśnienie pojęć

1. Pracodawca, administrator – należy przez to rozumieć pracodawcę pracownika wykonującego pracę zdalną.
2. Dane osobowe – należy przez to rozumieć dane osobowe w rozumieniu art. 4 pkt 1) RODO, czyli wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, czyli takiej osobie, 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.
3. IOD – należy przez to rozumieć Inspektora Ochrony Danych, powoływanego przez Administratora zgodnie z art. 37 RODO.
4. Przetwarzanie – należy przez to rozumieć operację lub zestaw operacji określonych w art. 4 pkt 2) RODO, takie 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; w szczególności, w odniesieniu do niniejszego regulaminu: rejestrowanie, przechowywanie, udostępnianie.
5. RODO – należy przez to rozumieć rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.U. UE. L. Nr 119, s. 1 ze zm.).

§ 3.
Dokumentacja ochrony danych osobowych

1. Dokumentację ochrony danych osobowych Uczelni stanowi Polityka ochrony danych osobowych oraz niniejsza procedura.
2. Załącznik nr 1 do niniejszej procedury stanowi oświadczenie o zapoznaniu się z obowiązującymi zasadami ochrony danych podczas pracy zdalnej.
3. Wykonywanie pracy zdalnej nie zwalnia z obowiązku przestrzegania przepisów dotyczących ochrony danych osobowych przyjętych w Uczelni.
4. W przypadku wątpliwości co do dopuszczalnego postępowania z danymi osobowymi, pracownik, po sprawdzeniu, czy dokumentacja ochrony danych osobowych nie reguluje takiego obszaru, kontaktuje się z IOD Uczelni.

§ 4.
Praca z danymi w obiegu elektronicznym

1. Dostęp do danych osobowych odbywa się w sposób zdalny i następuje poprzez:
   1) dostęp do skrzynki pocztowej pracownika w domenie Uczelni;
   2) dostęp do systemu informatycznego przetwarzającego dane osobowe, niezbędny do wykonywania obowiązków służbowych;
   3) dostęp do określonych zasobów w infrastrukturze pracodawcy przy użyciu szyfrowanego połączenia zdalnego (np. VPN).
2. Jeżeli pracownik przesyła załączniki zawierające dane osobowe muszą być one zaszyfrowane odpowiednim programem (np. 7-zip).
3. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji np. SMS-em.
4. Hasło powinno być silne i zawierać minimum 6 znaków w tym duża litera, cyfra oraz znak specjalny.

5. Przy wysłaniu wiadomości należy dochować należytej staranności, w szczególności sprawdzić, czy jest kierowana do odpowiedniego odbiorcy.
6. W przypadku wysyłania informacji do kilku odbiorców, którzy nie znają się wzajemnie i/lub ich adresy e-mail są adresami prywatnymi, należy skorzystać z opcji Ukrytej kopii (UDW/BCC), tzn. adresy wpisać w to pole.
7. Nie należy przesyłać plików z danymi osobowymi (np. w celu pracy z danymi osobowymi), jeżeli możliwy jest dostęp do danych w systemie informatycznym.
8. Zasady bezpiecznego prowadzenia wideokonferencji określa załącznik nr 2.

§ 5.
Praca z dokumentami papierowymi

1. Wynoszenie dokumentacji papierowej z siedziby Uczelni powinno być ograniczone do niezbędnego minimum. Pracodawca może zezwolić pracownikom na korzystanie z dokumentacji papierowej zawierającej dane osobowe w trakcie pracy zdalnej tylko w wyjątkowych sytuacjach. Generalną zasadą jest praca w obiegu elektronicznym.
2. W przypadku konieczności korzystania z dokumentacji papierowej poza siedzibą Uczelni w pierwszej kolejności należy rozważyć wykonanie kopii dokumentacji, na której pracownik będzie pracował. Kopie dokumentów z danymi osobowymi podlegają takiej samej ochronie jak oryginały.
3. Po uzyskaniu zgody na korzystanie z dokumentów papierowych poza siedzibą Uczelni, pracownik jest zobowiązany sporządzić ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane. Zestawienie jest przekazywane swojemu przełożonemu.
4. Wynoszenie dokumentów lub ich kopii powinno mieć miejsce w zabezpieczonej aktówce i w taki sposób, aby były niewidoczne dla osób trzecich.
5. Pracownik zobowiązany jest do odpowiedniego zabezpieczenia danych w miejscu wykonywania pracy zdalnej - dokumenty i ich kopie powinny być przechowywane w zamykanych na klucz szufladach biurka lub szafach, należy zabezpieczyć dostęp do nich osób nieuprawnionych, w tym dzieci i domowników.
6. Po zakończeniu okresu pracy zdalnej, wszystkie oryginały dokumentów należy zwrócić, a kopie zniszczyć.

§ 6.
Wymogi bezpieczeństwa dotyczące sprzętu

1. Praca zdalna powinna być wykonywana przede wszystkim z wykorzystaniem urządzeń służbowych, takich jak komputer stacjonarny, laptop, smartfon, tablet itp. Dopuszcza się używanie urządzeń prywatnych, z zachowaniem wymagań w zakresie bezpieczeństwa, określonych w niniejszej procedurze.
2. W przypadku udostępnienia przez Uczelnię modemu Internetowego lub telefonu służbowego z dostępem do Internetu, który może pełnić funkcję Hotspot, to osoba świadcząca pracę zdalną zobowiązana jest korzystać w pierwszej kolejności z tych urządzeń. Przekazany sprzęt należy wykorzystywać jedynie do celów służbowych.
3. W przypadku korzystania z domowej sieci Wi-Fi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:
   1) połączenie z domową siecią Wi-Fi powinno wymagać uwierzytelnienia, np. poprzez hasło;
   2) hasło dostępu powinno składać się z co najmniej 8 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych;
   3) jeżeli jest to możliwe, należy zmienić login do panelu administracyjnego routera na własny;
   4) dostęp do panelu administracyjnego routera powinien być możliwy wyłącznie z urządzeń znajdujących się w sieci domowej;
   5) gdy został zmieniony domyślny adres routera (najczęściej 192.168.1.1.) na inny.
4. Pomocy w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia, na potrzeby pracy zdalnej, udziela Sekcja ds. Informatyzacji.
5. Instalowanie jakiegokolwiek oprogramowania na urządzeniu służbowym jest możliwe tylko przez pracowników Sekcji ds. Informatyzacji lub za ich zgodą i zgodnie z ich wytycznymi.
6. Na urządzeniach wykorzystywanych do pracy zdalnej nie może być instalowane żadne nielegalne oprogramowanie.
7. Pracownik odpowiada za zabezpieczenie sprzętu przed dostępem osób trzecich, a w szczególności domowników i dzieci.
8. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom. Jeśli do pracy zdalnej wykorzystywane jest urządzenie prywatne, z którego korzystają inne osoby, należy założyć osobne konto w systemie operacyjnym, zabezpieczone hasłem.
9. Pracownik odpowiada za bezpieczeństwo powierzonego mu sprzętu, nośników i dokumentacji podczas ich transportu. W szczególności nie jest dozwolone pozostawianie ich bez nadzoru (np. w środku transportu – samochodzie, komunikacji publicznej).
10. Wymagania w zakresie bezpieczeństwa sprzętu:
    1) urządzenie posiada legalne i aktualne oprogramowanie;
    2) zostały włączone automatyczne aktualizacje i zapora systemowa;
    3) zainstalowany jest i działa w tle program antywirusowy;
    4) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token;

5) wyłączono autouzupełnianie i zapamiętywanie haseł w przeglądarce internetowej;
6) zainstalowano program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip);
7) ustawione zostało automatyczne blokowanie urządzenia po dłuższym braku aktywności;
8) jeżeli urządzenie daje taką możliwość, praca może być wykonywana na koncie z ograniczonymi uprawnieniami.

§ 7.
Działania niedozwolone

Zakazane jest:
1) pozostawianie niezablokowanego komputera, laptopa, smartfona, tabletu bez nadzoru;
2) udostępnianie osobom postronnym danych służących do uwierzytelnienia do systemów;
3) przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w treści wiadomości e-mail;
4) korzystanie z urządzeń prywatnych, które nie spełniają wymagań wymienionych w §6 pkt 8;
5) udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
6) dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami;
7) samodzielne niszczenie dokumentów służbowych w domu;
8) logowanie się na konto innego użytkownika;
9) podejmowanie pracy zdalnej w miejscach publicznych typu: kawiarnie, restauracje, galerie handlowe.

§ 8.
Postanowienia końcowe

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do Sekcji ds. Informatyzacji.
2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w tym samym dniu zgłosić zdarzenie pracodawcy, Sekcji ds. Informatyzacji, a także IOD.
3. W przypadku zauważania nieprawidłowości w funkcjonowaniu systemów informatycznych pracownik podejmuje możliwe działania zabezpieczające jednocześnie z powiadomieniem właściwych osób, zgodnie z pkt. 2.
4. Postanowienia niniejszej procedury mają zastosowanie również do osób prowadzących zajęcia na innej podstawie niż umowa o pracę.
5. W sprawach nieuregulowanych, zastosowanie mają wewnętrzne procedury obowiązujące w Uczelni oraz przepisy prawa powszechnie obowiązującego.

Załącznik nr 1 do Procedury ochrony
danych osobowych w ramach pracy zdalnej

.....
imię i nazwisko Pracownika

OŚWIADCZENIE

Oświadczam, że zapoznałam/em się z Procedurą ochrony danych osobowych w ramach pracy zdalnej, oraz znam zasady i procedury zawarte w obowiązującej Polityce ochrony danych osobowych i zobowiązuję się do ich przestrzegania.

.....
data i podpis Pracownika

Załącznik nr 2 do Procedury ochrony
danych osobowych w ramach pracy zdalnej

Zasady bezpiecznego prowadzenia wideokonferencji

Przed rozpoczęciem wideokonferencji:

1. Zapoznaj się z ogólnymi warunkami użytkowania lub polityką prywatności programu, z którego chcesz skorzystać.
2. Sprawdź, czy Twoje rozmowy będą nagrywane i przechowywane.
3. Zweryfikuj, do jakich celów będą wykorzystywane Twoje dane osobowe.
4. Sprawdź, o jakie uprawnienia do danych jesteś proszony - lista kontaktów, lokalizacja itp.
5. Do zainstalowania aplikacji na komputerze użyj oficjalnej strony aplikacji, z której chcesz korzystać; w przypadku urządzeń mobilnych wybierz oficjalny sklep - Google Play lub App Store.
6. Upewnij się, że osoby postronne nie mają dostępu do Twojego ekranu.
7. Sprawdź, czy aplikacja dysponuje niezbędnymi środkami bezpieczeństwa, takimi jak szyfrowanie.
8. Korzystaj z aplikacji webowych, nie desktopowych.
9. Zabezpiecz sieć Wi-Fi silnym hasłem.
10. Przed udostępnieniem swojego ekranu podczas rozmowy zamknij wszystkie okna, tak aby inni uczestnicy konferencji ich nie zobaczyli.
11. Przy podłączeniu się do wideokonferencji korzystaj z kodów dostępu/PIN-ów.
12. Przeskanuj program do wideokonferencji systemem antywirusowym.

W trakcie korzystania z wideokonferencji:

1. Ogranicz ilość podawania danych osobowych - użyj pseudonimu i służbowego adresu e-mail.
2. Użyj innego hasła, niż używane przez Ciebie w innych usługach.
3. Nie udostępniaj linków do konferencji w mediach społecznościowych.
4. Włącz, jeśli to możliwe, domyślną ochronę hasłem spotkania on-line.
5. Zarządzaj opcjami udostępniania ekranu.
6. W celu wykonywania rozmów służbowych wykorzystuj dostęp do sieci za pomocą szyfrowanego połączenia VPN.
7. Nie udostępniaj dokumentów służbowych za pomocą czatu, który może być publiczny.
8. Jeżeli to możliwe, korzystaj z opcji zamazywania tła (tak żeby rozmówcy nie widzieli Twojego otoczenia).
9. Korzystaj z opcji "poczekalnia", tak abyś mógł kontrolować osoby uczestniczące w wideokonferencji; unikniesz przypadkowych lub niechcianych osób.
10. Logując się do wideokonferencji, wyłącz mikrofon i kamerę (włączysz je, jak będzie to potrzebne).

Po skorzystaniu z wideokonferencji:

1. Wyłącz mikrofon i kamerę.
2. Upewnij się, że zakończyłeś spotkanie on-line i zamknąłeś aplikację.
3. Sprawdź, czy program do wideokonferencji nie działa w tle.