PRACA ZDALNA
ZAPEWNIENIE ZGODNOŚCI Z PRZEPISAMI OCHRONY DANYCH OSOBOWYCH

W toku działania w trybie pracy zdalnej, będzie dochodziło do przetwarzania danych osobowych poza terenem Uniwersytetu. Pojawiają się nowe ryzyka i zagrożenia, które nie występują w przypadku pracy w pomieszczeniach biurowych Uczelni.

Dane osobowe, to nie jedyna wartościowa informacja znajdująca się w dokumentach i systemach informatycznych użytkowanych w Uczelni, w tym na służbowych laptopach czy smartfonach. Równie wartościowe mogą być informacje dotyczące działalności wewnętrznej Uczelni dokumenty stanowiące tajemnicę służbowa, skarbową, telekomunikacyjną czy też inne informacje prawnie chronione - nie wspominając o dokumentacji prowadzonych prac naukowych.

Przepisy dotyczące ochrony danych osobowych (RODO) nie zabraniają nikomu pracy zdalnej. Rozporządzenie nie zawiera szczegółowych instrukcji lub obostrzeń z tym związanych.
Nie znaczy to jednak, że przy podejmowaniu pracy zdalnej nie powinniśmy brać pod uwagę przepisów RODO. Niezależnie od miejsca , w którym odbywa się praca należy stosować adekwatne środki zabezpieczeń technicznych i organizacyjnych minimalizujące możliwość powstania incydentów związanych z naruszeniem ochrony danych osobowych (art. 32 RODO). Kierownicy jednostek organizacyjnych (Lokalni administratorzy danych osobowych - LADO) organizując pracę zdalną pracowników powinni również mieć na uwadze ogólne zasady RODO a zwłaszcza:

- **integralność i poufność** (art. 5 ust. 1 lit. f RODO) - w szczególności przetwarzanie powinno odbywać się w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, a Administrator (LADO) powinien zagwarantować ochronę przed ich niedozwolonym lub niezgodnym z prawem użyciem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem,

- **rozliczalność** (art. 5 ust. 2 RODO) – **Administrator (LADO) powinien być w stanie wykazać, że przestrzega podstawowych zasad RODO**, w tym tej wskazanej powyżej, co oznacza, że powinien on dysponować dowodem na to, że przyjęte środki są faktycznie adekwatne i zostały odpowiednio wdrożone.

Zapewnienie tego aby pracownicy mogli respektować powyższe zasady wymaga odpowiedniego poziomu świadomości. Stosowanie proponowanych poniżej środków zabezpieczających nie pomoże w niczym , jeżeli pracownik udostępni włączony komputer (dokumenty) osobie trzeciej (w tym członkom rodziny), czy też pozostawi komputer w samochodzie na przednim fotelu auta robiąc zakupy. Stosowanie poniżej wskazanych środków w mojej ocenie zapewni adekwatny poziom bezpieczeństwa, kiedy pracujemy w trybie „Home office".

Ponieważ na administratorze (LADO) ciąży obowiązek rozliczalności, w zaistniałej sytuacji, w której organizowanie szkoleń jest zawieszone, najlepszym wyjściem jest wysłanie przez LADO (kierowników jednostek organizacyjnych Uczelni) maila do wszystkich pracowników o obowiązujących podczas pracy zdalnej zasadach, zobowiązanie ich do wypełnienia i przesłania podpisanego oświadczenia zgodnie z załączonym wzorem.

ŚRODKI TECHNICZNE I ORGANIZACYJNE ZAPEWNIAJĄCE BEZPIECZEŃSTWO PRZETWARZANYCH DANYCH

Dane osobowe przetwarzane są tylko na polecenie Administratora (LADO) przez pracowników posiadających odpowiednie upoważnienia.

Podczas pracy zdalnej obowiązują wszystkie dotychczas obowiązujące środki bezpieczeństwa, streszczenie powyższych zawiera „Mini poradnik IOD – Jak uniknąć naruszenie ochrony danych osobowych" – rozesłany do pracowników Uczelni na początku kwietnia 2019 r.

Zabrania się pracy zdalnej z dokumentami zawierającymi szczególne kategorie danych osobowych (dawniej – dane wrażliwe).

I. DOKUMENTY PAPIEROWE

Należy unikać wynoszenia dokumentów papierowych poza teren Uczelni. W większości przypadków możemy pracować na skanach, zdjęciach czy wyciągach z bazach danych.
Jeśli nie ma innej możliwości, na wyniesienie dokumentów zgodę może wyrazić kierownik jednostki organizacyjnej. Pracownik jest odpowiedzialny za uniemożliwienie dostęp do dokumentów osobom nieupoważnionym (w tym domownikom!), oraz ich ochronę w trakcie przenoszenia. Nie wolno wyrzucać dokumentów zawierających dane osobowe do kosza w domu. Po zakończeniu pracy zdalnej należy zwrócić je do do biura, wykorzystane zbędne dokumenty należy zniszczyć w niszczarce.

II. ZEWNĘTRZNE NOŚNIKI DANYCH

Należy wykorzystywać (za zgodą przełożonego) służbowe **szyfrowane** zewnętrzne nośniki danych (np. pendrive, zewnętrzny dysk twardy, karty pamięci). Procedury szyfrowania należy uzgodnić z administratorem systemu informatycznego. Do szyfrowania danych należy wykorzystywać oprogramowanie przeznaczone do użytku komercyjnego.
Na urządzeniach przenośnych zabrania się przenoszenia całych baz danych czy też szerokich wyciągów z baz danych osobowych.

III. PRZESYŁANIE DOKUMENTÓW POCZTĄ EKEKTRONICZNĄ

Dokument zawierające dane osobowe mogą być przesyłane jako załączniki **wyłącznie w formie zaszyfrowanej.** Hasło do pliku należy przekazywać z wykorzystaniem innych kanałów komunikacji.

IV. SŁUŻBOWY KOMPUTER , SMARTFON

Do pracy zdalnej można wykorzystać służbowe komputery przenośne (laptopy) wyłącznie za zgodą Administratora – LADO.
Służbowy komputer przeznaczony do pracy w trybie home office powinien spełniać poniższe kryteria:

1) Indywidualny login oraz hasło dostępu do systemu.
2) Obowiązkowo - zaszyfrowany dysk twardy.
3) Aktualny program antywirusowy z firewallem.
4) Wygaszacz ekranu włączający się po kilku minutach bezczynności (1- 4 min.) z opcją konieczności ponownego logowania się do systemu.
5) Możliwość automatycznego backupu danych lub ręczna procedura backupowa.

Zalecane jest stosowanie nakładki prywatyzujące na ekran minimalizujące ryzyko wglądu w ekran monitora osobom postronnym.

Smartfon to też komputer

Smartfony dorównują powoli laptopom. Zarówno jeśli chodzi o ich moc obliczeniową, pamięć (a więc i możliwość przechowywania danych osobowych) oraz funkcjonalność.
Służbowe smartfony są często podstawowym narzędziem do sprawdzania poczty e-mail, a nawet obsługi przeglądarkowych systemów informatycznych zawierających bardzo duże ilości danych osobowych.
Podobnie jak w przypadku służbowego komputera, smartfon powinien spełniać większość z poniższych kryteriów:

1) Obowiązkowo – blokada ekranu. Sama blokada karty SIM PIN-em to zdecydowanie za mało.
2) Szyfrowanie danych.

3) Możliwość automatycznego backupu danych.

V. DOSTĘP ZDALNY DO SYSTEMÓW INFORMATYCZNYCH UCZELNI

Zgodnie z postanowieniem Kanclerza Uniwersytetu Opolskiego nr 4/2020 z dnia 18 marca 2020 r. zabrania się udzielania zdalnego dostępu do systemów informatycznych Uczelni w których gromadzone są dane osobowe i inne informacje ważne dla funkcjonowania uniwersytetu.

Postanowienie nie anuluje wcześniej wydanych zezwoleń wydanych przez ASI dla administratorów systemów – pracowników Centrum Informatycznego.
Łączenie z uczelnianymi systemami realizowane może być wyłącznie za pośrednictwem bezpiecznego łącza VPN.

Praca zdalna z dostępem do systemów informatycznych ważnych dla funkcjonowania Uczelni może być realizowana wyłącznie z komputerów służbowych podłączonych do domeny uniwersyteckiej oraz po uzyskaniu zgody Kanclerza i Administratora Systemów Informatycznych (ASI).

VI. WYKORZYSTYWANIE KOMPUTERÓW PRYWATNYCH

Administrator – LADO może zezwolić pracownikom na pracę zdalną na własnym sprzęcie komputerowym i zastosować coraz popularniejsze rozwiązanie BYOD (Bring Your Own Device). Taka praktyka nie jest zabroniona przez RODO. **Zezwolenie takie nie może dotyczyć systemów ważnych dla funkcjonowania Uczelni o których mowa w pkt. V.**
Może się to odbyć wyłącznie za dobrowolną zgodą pracownika.
Aby dopuścić prywatny sprzęt do użytku, informatyk jednostki organizacyjnej lub pracownik Centrum Informatycznego powinien wcześniej zadbać o jego odpowiednie zabezpieczenie i sprawdzenie. Przy tej okazji możemy wejść w obszar prywatności pracownika, który powinien mieć tego świadomość zgłaszając wniosek - wyrażając zgodę na wykorzystanie prywatnego sprzętu.

Wcześniej wskazane wymagania dotyczące sprzętu służbowego odnoszą się również (a wręcz – przede wszystkim) do komputerów prywatnych).

VII. WSKAZÓWKI DOTYCZĄCE OCHRONY PRZED WIRUSAMI I SZKODLIWYM OPROGRAMOWANIEM

Aby chronić urządzenie przed szkodliwym oprogramowaniem i wirusami, należy stosować się do następujących wskazówek.

- Nie pobierać nieznanych plików i aplikacji.
- Na sprzęcie służbowym instalować oprogramowanie tylko za zgodą Administratora Systemów Informatycznych (Dyrektora Ci) i swojego przełożonego pod nadzorem informatyka z uczelni
- Nie odwiedzać niezaufanych stron internetowych.
- Usuwać podejrzane wiadomości e-mail i wiadomości od nieznanych nadawców.
- Hasło logowania zmieniać nie rzadziej niż co 30 dni, przestrzegając uczelnianych wymogów odnośnie jego złożoności.
- Dezaktywować funkcje komunikacji bezprzewodowej, jak Bluetooth, WiFi w czasie, gdy nie są używane.

- Jeśli urządzenie dziwnie się zachowuje, sprawdzić za pomocą programu antywirusowego, czy nie jest zainfekowane.
- Przed uruchomieniem nowo pobranych plików (programów, aplikacji), uruchamiać na urządzeniu program antywirusowy.
- Włączyć automatyczną aktualizację systemu operacyjnego lub systematycznie dokonywać jego ręcznej aktualizacji. (obowiązkowo instalując aktualizacje - poprawki zalecane przez producenta systemu, sprzętu).
- Zainstalowany program antywirusowy z opcją pracy w tle, regularnie uruchamiać, w celu sprawdzenia całego urządzenia, aby sprawdzać, czy nie doszło do infekcji.
- Samodzielnie nie edytować ustawień rejestru ani nie modyfikować systemu operacyjnego urządzenia.

Wzór oświadczenia pracownika w związku z pracą zdalną:

Oświadczenie

W związku z podjęciem pracy zdalnej, oświadczam, że:

1. Jestem świadomy/a, że do przetwarzania danych osobowych w Uniwersytecie Opolskim są upoważnieni wyłącznie pracownicy i współpracownicy.
2. Nie dopuszczę do komputera, telefonu(smartfonu) i innych nośników wykorzystywanych podczas pracy zdalnej, oraz informacji w nich zawartych - w tym danych osobowych, domowników oraz innych osób trzecich.
3. Zachowam dane Uczelni w poufności. Wszelkie notatki będę przechowywał/a zabezpieczone, tak by osoby trzecie nie miały do nich dostępu.
4. Zapiszę wszystkie dane na komputerze w szyfrowanym katalogu „Praca_zdalna”_ lub na odpowiednio zabezpieczonym nośniku zewnętrznym udostępnionym przez Pracodawcę.
5. Nie będę kopiować/zapisywać danych służbowych na niezabezpieczone/prywatne pendrive’y i inne nośniki zewnętrzne.
6. Mam świadomość, że komputer, telefon i inne nośniki przekazane mi przez Pracodawcę służą wyłącznie do pracy służbowej – nie zainstaluję dodatkowego oprogramowania bez zgody Administratora Systemów Informatycznych – Dyrektora CI, pod nadzorem lokalnego administratora systemu informatycznego.
7. Nie będę korzystać ze służbowego sprzętu w innych celach niż te związane z pracą.
8. Komputer oraz nośniki udostępnione przez Pracodawcę zabezpieczę w odpowiedni sposób przed dostępem osób nieupoważnionych, zgodnie z przekazanymi mi w tym zakresie wytycznymi.
9. Będę przestrzegać zasad korzystania z komputera, telefonu i innych nośników przekazanych mi przez Pracodawcę zgodnie z obowiązującymi w tym zakresie procedurami, w tym w szczególności zgodnie z wytycznymi i regulaminami IT.
10. Zobowiązuję się zwrócić powierzone mi nośniki wraz z kompletnymi danymi na każde żądanie przełożonego.

…….
Czytelny podpis

Opracował:
Jacek Najgebauer
Inspektor Ochrony Danych

tel. 774527099 (wew. 7099)

45-052 Opole ul. Oleska 48 p.114