# **Procedura ochrony danych osobowych w związku z wykonywaniem pracy w formie zdalnej**

## **Wprowadzenie**

1. Procedura ochrony danych osobowych w pracy zdalnej, zwana dalej „Procedurą”,
określa zasady bezpiecznego przetwarzania oraz skutecznej ochrony danych osobowych
w pracy zdalnej w Uniwersytecie zgodnie z RODO[[1]](#footnote-1), odrębnymi przepisami prawnymi powszechnie obowiązującymi i regulującymi przedmiotowe kwestie, Polityką ochrony danych osobowych w Uniwersytecie Ekonomicznym w Katowicach[[2]](#footnote-2), jak również
z zaleceniami wydawanymi w tym przedmiocie, z zastrzeżeniem postanowień określonych
w ust. 2.
2. Pracownik wykonujący pracę zdalną jest zobowiązany do przetwarzania i ochrony danych osobowych zgodnie z postanowieniami określonymi w ust. 1 oraz dbania o bezpieczeństwo danych osobowych, ich poufność oraz integralność mając na uwadze dbałość o dobro Uniwersytetu.
3. Pracodawca przeprowadza, w miarę potrzeby, instruktaż i szkolenie w przedmiotowym zakresie dla pracowników wykonujących pracę zdalną.
4. Pracownik wykonujący pracę zdalną potwierdza w postaci papierowej lub elektronicznej zapoznanie się z Procedurą oraz jest obowiązany do jej przestrzegania.
5. W ramach wykonywania pracy zdalnej pracownik jest zobowiązany do przetwarzania danych osobowych jedynie w celach służbowych określonych w umowie o pracę i w zakresie czynności.
6. Zabronione jest wykorzystywanie przez pracownika danych osobowych w celach niezwiązanych z wykonywaniem zadań i obowiązków służbowych.
7. Wykonywanie pracy w formie zdalnej odbywa się na służbowym lub prywatnym sprzęcie komputerowym za pisemną wiedzą i zgodą pracodawcy.
8. Przy wykonywaniu pracy zdalnej pracownik może używać narzędzi lub materiałów niezapewnionych przez pracodawcę, pod warunkiem, że umożliwia to poszanowanie
i ochronę informacji poufnych i innych tajemnic prawnie chronionych, w tym tajemnicy przedsiębiorstwa lub danych osobowych, a także informacji, których ujawnienie mogłoby narazić Uniwersytet na szkodę.
9. Pracownik jest odpowiedzialny za właściwe zabezpieczenie danych osobowych przetwarzanych przez niego w ramach pracy zdalnej oraz dbania o powierzony sprzęt
do wykonywania pracy zdalnej i wykorzystywania go wyłącznie dla celów służbowych.
10. Pracownik jest zobowiązany do zachowania poufności informacji i danych osobowych podczas wykonywania czynności służbowych, w tym rozmów telefonicznych
czy wideokonferencji.
11. W przypadku gdy pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, czy też ze względu na siłę wyższą (np. brak prądu lub Internetu),
o których mowa w niniejszej Procedurze, jest zobowiązany do niezwłocznego poinformowania pracodawcy/bezpośredniego przełożonego i oczekiwania na wytyczne
oraz polecenia w przedmiotowym zakresie.
12. Pracownik przetwarza dane osobowe w pracy zdalnej wyłącznie w tym celu, w jakim byłyby wykorzystywane w siedzibie Uniwersytetu.
13. W ramach wykonywania pracy zdalnej należy korzystać wyłącznie z dostępu do zaufanych sieci teleinformatycznych i niedozwolone jest korzystnie z otwartych sieci bezprzewodowych typu hotspot.
14. Praca zdalna jest realizowana przy wykorzystaniu oprogramowania i urządzeń niezbędnych do wykonywania przydzielonych zadań oraz umożliwiających komunikowanie się
na odległość.
15. Pracownik wykonujący pracę zdalną posługuje się służbową pocztą elektroniczną
z zachowaniem zasad bezpieczeństwa danych osobowych oraz jest zobowiązany
do aktywowania przekierowania służbowego numeru telefonu[[3]](#footnote-3).
16. Pracownik wykonujący pracę zdalną i wykorzystujący urządzenia służbowe/prywatne jest zobowiązany do zadbania o to, by były one zabezpieczone hasłem, miały zainstalowaną bieżącą aktualizację systemu operacyjnego, oprogramowania użytkowego oraz systemu antywirusowego.
17. Podczas wykonywania pracy zdalnej należy zachować szczególną ostrożność w zakresie możliwości wystąpienia ataków o charakterze socjotechnicznym i cybernetycznym.
18. W ramach wykonywania pracy zdalnej należy zadbać o skuteczne i bezpieczne archiwizowanie dokumentów – zarówno dokumentacji papierowej, jak i elektronicznej
oraz nieprzechowywania ich trwale w zasobach prywatnych, z zastrzeżeniem postanowienia określonego w ust. 19.
19. Po zakończeniu okresu pracy zdalnej zobowiązuje się pracownika do przeniesienia dokumentów do uczelnianych zasobów.
20. Pracownik zabezpiecza przed dostępem osób postronnych do urządzeń, które wykorzystuje w pracy zdalnej oraz do posiadanych dokumentów, danych i informacji. Powyższe dotyczy również zabezpieczenia przed utraceniem, uszkodzeniem lub zniszczeniem tych urządzeń
lub dokumentów.
21. Ilekroć jest mowa w Procedurze o „urządzeniu” należy przez to rozumieć komputer stacjonarny, laptop, notebook, ultrabook, tablet, smartfon, pendrive oraz każde inne urządzenie elektroniczne wykorzystywane do pracy zdalnej, w tym do komunikacji.

## **Warunki dotyczące miejsca świadczenia pracy zdalnej**

1. Pracownik wykonuje pracę zdalną pod adresem, który wskazał pracodawcy i z nim uzgodnił.
2. Pracując w ustalonym miejscu z pracodawcą, pracownik zapewnia, aby domownicy/osoby postronne nie miały wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranów urządzeń, a także poprzez zapewnienie pracy z dokumentami w sposób uniemożliwiający im wgląd do ich zawartości czy zapoznawania się z nimi, zachowując należytą ochronę przed osobami nieuprawnionymi.
3. W ramach świadczenia pracy zdalnej należy korzystać tylko i wyłącznie z ustalonego stanowiska pracy.
4. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, takich jak kawiarnie, restauracje, galerie handlowe oraz inne miejsca, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.
5. Zabronione jest wykorzystywanie publicznego dostępu do sieci Internet czy otwartych sieci WiFi (np. WiFi hotelowe, w galeriach handlowych lub hotspot w kawiarniach).
6. Po zakończeniu pracy zdalnej bądź w sytuacji czasowego zaprzestania jej wykonywania należy każdorazowo wyłączyć urządzenia wykorzystywane do pracy zdalnej oraz system
lub je zablokować/wylogować się, a także schować wszystkie elektroniczne i papierowe nośniki informacji w bezpiecznych miejscach, w miarę możliwości do szafek/szuflad zamykanych na klucz w taki sposób, by uniemożliwić uruchomienie czy korzystanie z nich przez osoby postronne.

## **Dane osobowe w obiegu elektronicznym**

1. Instalowanie jakiegokolwiek oprogramowania na urządzeniach służbowych jest możliwe tylko przez pracowników Centrum Informatycznego Uniwersytetu lub za ich zgodą i zgodnie z ich wytycznymi.
2. W przypadku identyfikacji wirusa lub nieaktualności oprogramowania antywirusowego konieczne jest natychmiastowe skontaktowanie się z Centrum Informatycznym Uniwersytetu.
3. Pracownik nie może instalować na urządzeniach służbowych prywatnych aplikacji
lub oprogramowania.
4. Na urządzeniu służbowym nie może być instalowane żadne nielegalne oprogramowanie.
5. Pracownik odpowiada za zabezpieczenie urządzenia służbowego przed dostępem osób trzecich.
6. Pracownik nie może przechowywać żadnych służbowych danych osobowych ani informacji na innych urządzeniach niż udostępnione mu przez pracodawcę, poza urządzeniami,
o których pracodawca ma wiedzę i wyraził na nie zgodę.
7. Pracownik nie może przechowywać na urządzeniach służbowych plików niezwiązanych
z wykonywaną pracą lub jakichkolwiek innych plików lub programów, które nie posiadają stosownej licencji.
8. Zabronione jest używanie prywatnych kont pocztowych do przetwarzania służbowych danych osobowych.
9. Pracownik wykorzystuje do celów służbowych jedynie służbowy adres e-mail.
10. Pracownik odpowiada za ochronę powierzonych mu urządzeń służbowych i nie może korzystać z nich w miejscach publicznych.
11. Urządzenia służbowe są chronione hasłem a dyski oraz nośniki danych szyfrowane.
12. Pracownik nie może łączyć się ze służbowymi systemami i dyskami sieciowymi z innego sprzętu niż sprzęt służbowy, poza urządzeniami, o których pracodawca ma wiedzę i wyraził na nie zgodę.
13. Pracownik łącząc się z zasobami sieciowymi niezbędnymi do świadczenia pracy w trybie zdalnym jest zobowiązany korzystać z bezpiecznego połączenia za pomocą sieci VPN zapewnianego przez pracodawcę.
14. Hasła do poczty elektronicznej oraz systemów nie powinny być zapisywane przez przeglądarkę internetową ani przechowywane w miejscu dostępnym dla osób postronnych (np. na kartkach przy komputerze).
15. Pracownik nie może przesyłać/korzystać z treści podejrzanych, naruszających prawa własności intelektualnej czy prawnie zabronionych.

## **IV. Urządzenia służące do pracy zdalnej**

1. Praca zdalna może być wykonywana przy wykorzystaniu urządzeń służbowych wydawanych za protokołem lub po uprzedniej zgodzie pracodawcy przy wykorzystaniu urządzeń prywatnych.
2. Urządzenia prywatne wykorzystywane do pracy zdalnej muszą w zakresie ich zabezpieczeń wypełniać wymogi takie same, jak urządzenia służbowe.
3. Urządzenie prywatne wykorzystywane do celów służbowych powinno mieć wydzielone odrębne konto użytkownika (ponadto zahasłowane) celem wykonywania na nim przedmiotowych czynności służbowych w ramach pracy zdalnej.
4. Odrębne konto użytkownika, o którym mowa w ust. 3, musi posiadać ograniczone uprawnienia bez praw administratora i być chronione silnym hasłem oraz nieudostępniane osobom trzecim.
5. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej osobom trzecim.
6. Do pracy zdalnej pracownik powinien wykorzystywać służbowe programy i systemy udostępnione mu przez pracodawcę, z wyjątkiem przypadków, gdy pracownik wykonuje pracę zdalną z wykorzystaniem prywatnego urządzenia zgodnie z postanowieniami Procedury.
7. Wykorzystywanie innych urządzeń do przesyłania i udostępniania plików może odbywać się tylko za zgodą pracodawcy, po wcześniejszym zabezpieczeniu ich hasłem.
8. Pracownik jest zobowiązany do wykonywania kopii bezpieczeństwa, którą winien przechowywać na odrębnym nośniku danych, za którego zabezpieczenie odpowiada.
9. Minimalne wymagania w zakresie bezpieczeństwa stanowią m.in.:
10. aktualne i legalne oprogramowanie na urządzeniu;
11. włączone automatyczne aktualizacje;
12. włączona zapora systemowa;
13. zainstalowane i poprawnie działający w tle program antywirusowy;
14. logowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN czy token;
15. wyłączone zapamiętywanie i autouzupełnianie hasła w przeglądarce internetowej;
16. zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip);
17. ustawione automatyczne lub ręczne blokowanie urządzenia po dłuższym braku aktywności;
18. praca jest wykonywana na koncie z ograniczonymi uprawnieniami.
19. Pracodawca może dodatkowo wymagać, aby urządzenie wykorzystywane do pracy zdalnej zawierało inne zabezpieczenia, takie jak m.in.:
20. zaszyfrowany dysk;
21. wyłączone porty pamięci zewnętrznych.
22. Zabrania się samodzielnej lub z wykorzystaniem wsparcia podmiotów zewnętrznych naprawy urządzeń służbowych wykorzystywanych do pracy zdalnej. W celu naprawy uszkodzonych urządzeń służbowych należy bezzwłocznie zwrócić je pracodawcy.
23. Zabrania się drukowania dokumentów służbowych w punktach ksero lub z pomocą innych podmiotów czy osób trzecich.
24. Za legalność oprogramowania na prywatnych urządzeniach, w tym programu antywirusowego odpowiada właściciel sprzętu.
25. Pracownik jest zobowiązany do stosowania zasady czystego ekranu, tj. blokowania sprzętu komputerowego w razie oddalenia się od miejsca pracy/zakończenia pracy.

## **V. Zabezpieczanie przekazywanych informacji**

1. Zabezpieczeniu podlegają wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, również imiona, nazwiska czy adresy e-mail.
2. Przy wysyłaniu wiadomości e-mail pracownik kieruje się należytą starannością, polegającą
w szczególności na sprawdzeniu, czy jest ona kierowana do odpowiedniego odbiorcy.
3. Zasada, o której mowa w ust. 2, dotyczy również wysyłania odpowiednich załączników.
4. Wszelkie informacje poufne, w szczególności dane osobowe, jeśli są przekazywane
z wykorzystaniem służbowej poczty e-mail, są udostępniane w formie załącznika, który jest zabezpieczony hasłem.
5. Hasło, o którym jest mowa w ust. 4, jest przekazywane odbiorcy inną drogą komunikacji
(np. telefonicznie).
6. Hasło, o którym mowa w ust. 4, powinno być odpowiednio skomplikowane i niesłownikowe.
7. Możliwe jest ustalenie stałego hasła na komunikację z jednym odbiorcą, o ile nie będzie wykorzystywane do zabezpieczania plików w komunikacji z innymi odbiorcami.
8. Pracownik jest zobowiązany do weryfikowania nadawców wiadomości e-mail. W przypadku wątpliwości co do tożsamości nadawcy zabronione jest otwieranie załączników
do wiadomości e-mail oraz hiperłączy znajdujących się w tekście.
9. W przypadku wysyłania informacji do kilku odbiorców, zwłaszcza na zewnątrz Uniwersytetu, którzy nie znają się wzajemnie i/lub ich adresy e-mail są adresami prywatnymi, należy każdorazowo skorzystać z opcji ukrytej kopii (UDW/BCC), tzn. adresy wpisać w to pole, chyba że osoby zainteresowane wzajemnie wobec siebie, świadomie i za zgodą udostępniły wskazane adresy e-mail.
10. Zabronione jest przesyłanie służbowych wiadomości e-mail na prywatne konta e-mail odbiorców, z wyjątkiem wysyłania ich do zainteresowanych spoza Uniwersytetu.
11. Zaleca się niekorzystanie z opcji autouzupełniania formularzy w opcjach przeglądarki internetowej.
12. W przypadku korzystania z przeglądarki internetowej należy sprawdzić informacje
o jej zabezpieczeniach. W tym celu należy kliknąć na symbol stanu bezpieczeństwa na lewo od adresu internetowego ( Bezpieczna, Informacje lub Niezabezpieczona, Niezabezpieczona lub Niebezpieczna), gdzie wyświetli się informacja o stopniu prywatności połączenia. Należy korzystać jedynie z bezpiecznych przeglądarek internetowych.
13. Masowe wysyłanie wiadomości e-mail należy realizować poprzez oprogramowanie udostępnione w tym celu przez pracodawcę.
14. Pracownik może przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez pracodawcę do tego celu serwerów plikowych.
15. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (np. weTransfer, Googe Dirve czy DropBoX) może odbywać się tylko za zgodą pracodawcy, po wcześniejszym zabezpieczeniu plików hasłem.
16. Zabrania się udostępniania dokumentów służbowych za pomocą otwartych komunikatorów internetowych.
17. Zabrania się udostępniania w mediach społecznościowych linków i innych aktywności realizowanych w ramach pracy zdalnej, przy czym dopuszczając możliwość ich wykonywania poprzez służbowe narzędzia do komunikacji zdalnej.
18. Należy weryfikować uczestników telekonferencji w celu uniknięcia przypadkowych
lub niechcianych osób w niej uczestniczących.

## **VI. Bezpieczne logowanie**

1. Dostęp do sprzętu lub programu wykorzystywanego do pracy zdalnej jest możliwy wyłącznie z wykorzystaniem indywidualnego identyfikatora oraz hasła.
2. Zabronione jest udostępnianie osobom trzecim haseł oraz przechowywanie ich w miejscach nie gwarantujących ich poufności.
3. Zabronione jest domyślne zapamiętywanie hasła dostępu do konta użytkownika systemu
na urządzeniach oraz programach wykorzystywanych w pracy zdalnej.
4. W przypadku korzystania z programów wideokonferencyjnych z funkcją rejestracji zabrania się opcji nagrywania i przechowywania nagrań bez wiedzy i zgody osób w nich uczestniczących.
5. W trakcie korzystania z programów lub platform do pracy zdalnej należy ograniczyć ilość podawanych danych osobowych zgodnie z zasadą minimalizacji danych osobowych.

## **VII. Bezpieczne przechowywanie danych**

1. Urządzenia wykorzystywane w celach służbowych powinny być zabezpieczone przed dostępem osób trzecich.
2. Zabronione jest umieszczanie danych, w tym danych osobowych w miejscach innych
niż dopuszczone przez pracodawcę.
3. Po zakończeniu okresu pracy poza miejscem jej stałego wykonywania pracownik
jest zobowiązany bezzwłocznie przekazać pracodawcy wszystkie dane związane
z wykonywanymi zadaniami służbowymi zapisane na prywatnych urządzeniach
(np. dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki
oraz inne posiadane informacje), a następnie usunąć je w sposób trwały.

## **VIII. Ochrona przed cyberatakami**

1. Do pracy zdalnej dopuszczalne jest wykorzystywanie urządzeń z zainstalowanym systemem operacyjnym w ostatniej wydanej lub jednej wcześniejszej głównej wersji. Dodatkowo jest wymagana stała aktualizacja systemu operacyjnego.
2. Urządzenia wykorzystywane do pracy zdalnej muszą mieć zainstalowane, uruchomione
i zaktualizowane oprogramowanie antywirusowe.
3. Systemy operacyjne zainstalowane na urządzeniach wykorzystywanych do pracy zdalnej mają mieć uruchomioną zaporę sieciową.

## **IX. Korzystanie z Internetu**

1. Urządzenie wykorzystywane do pracy zdalnej musi być podłączone do sieci Internet stabilnym łączem o parametrach, o których jest mowa w Zasadach wykonywania pracy
w formie zdalnej w Uniwersytecie, oraz ponadto:
2. jeśli to możliwe, należy zmienić sposób logowania do panelu administracyjnego routera z domyślnego na własny;
3. oprogramowanie urządzenia sieciowego powinno być regularnie aktualizowane.
4. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:
5. komunikacja w sieci WiFi wykorzystuje najnowsze standardy protokołów szyfrowania;
6. połączenie z siecią WiFi wymaga uwierzytelnienia poprzez silne hasło, które nie jest hasłem domyślnym w konfiguracji urządzenia.

## **X. Korzystanie z dokumentów w formie papierowej**

1. Dokumenty zawierające informacje poufne, w tym dane osobowe, powinny być przechowywane w szafach/szufladach zamykanych na klucz w siedzibie pracodawcy.
2. Obowiązuje ogólny zakaz zabierania oryginałów dokumentów lub ich kopii poza siedzibę pracodawcy, z zastrzeżeniem postanowienia określonego w ust. 5.
3. Co do zasady praca zdalna jest wykonywana w obiegu elektronicznym.
4. W przypadku konieczności pracy z dokumentami papierowymi, należy stosować wobec zawartych w nich informacji najwyższe standardy ochrony, w szczególności zapewnić, aby nie były udostępniane (np. pozostawione bez opieki czy w sposób umożliwiający zapoznanie się z ich treścią) osobom postronnym. Te same standardy dotyczą wszelkich kopii dokumentów.
5. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik zgłasza do bezpośredniego przełożonego prośbę o możliwość ich skopiowania oraz zabrania do domu na czas wykonywania pracy zdalnej, ale powinno być to ograniczone
do niezbędnego minimum oraz tylko w wyjątkowych sytuacjach, proporcjonalnie do celu przetwarzania danych osobowych.
6. Po otrzymaniu zgody na piśmie lub w formie wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów.
7. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty i w jakiej liczbie zostały skopiowane, a informacja jest przekazywana pracodawcy.
8. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić oraz by były niewidoczne dla osób trzecich,
na przykład w zabezpieczonej aktówce wykonanej z nieprzezroczystego materiału, ponadto nie można pozostawiać urządzeń i dokumentów w pojazdach pod nieobecność pracownika.
9. Podczas pracy zdalnej pracownik jest zobowiązany przechowywać udostępnione kopie dokumentów papierowych tylko przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej (zasada ograniczenia przetwarzania). Po tym czasie jest zobowiązany niezwłocznie zwrócić je pracodawcy, który weryfikuje ich kompletność.
10. Praca z dokumentami papierowymi nie może być wykonywana w miejscu publicznym
(np. świetlica w szkole, kawiarnia, restauracja, galeria handlowa, itp.).
11. Pracownik zapewnia zabezpieczenie dokumentów papierowych w miejscu wykonywania pracy zdalnej poprzez ich przechowywanie w miarę możliwości w szafie/szufladzie zamykanych na klucz, do której tylko on ma dostęp lub w miejscu, do którego nie mają dostępu osoby trzecie.
12. Po zakończeniu pracy z dokumentem lub jego kopią, która już nie jest potrzebna i nie wymaga dalszego przechowywania, należy dokument niezwłocznie zniszczyć z wykorzystaniem niszczarki.
13. Nie można wyrzucać dokumentów do kosza. Jeżeli pracownik nie posiada w domu niszczarki, powinien dokumenty przechowywać w bezpieczny sposób, a po zakończeniu pracy zdalnej zniszczyć je w Uniwersytecie.
14. Drukowanie dokumentów na potrzeby pracy zdalnej należy ograniczyć do niezbędnego minimum. W przypadku dokumentów zawierających dane osobowe należy w miarę możliwości dokonać anonimizacji danych osobowych.
15. Wszystkie wydruki, skanowane lub kopiowane dokumenty powinny być niezwłocznie usuwane z urządzeń, w celu uniemożliwienia zapoznania się z nimi osobom postronnym.
16. W przypadku chwilowego opuszczania stanowiska pracy należy zabezpieczać dokumenty papierowe.
17. W przerwie pracy/po jej zakończeniu pracownik powinien bezwzględnie przestrzegać zasady czystego biurka, dbając o niepozostawianie żadnych danych osobowych w jego obrębie.

## **XI. Naruszenie ochrony danych osobowych podczas pracy zdalnej**

1. Pracownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych/ incydentu dotyczącego bezpieczeństwa danych osobowych w systemie informatycznym
lub w systemie tradycyjnym, jest zobowiązany do niezwłocznego poinformowania o tym pracodawcy oraz inspektora ochrony danych, zgodnie z odrębną instrukcją postępowania
z incydentami[[4]](#footnote-4).
2. W przypadku powzięcia informacji o naruszeniu/incydencie ochrony danych osobowych,
o którym mowa w ust. 1, jest prowadzone postępowanie wyjaśniające, podczas którego
m.in.:
3. ustalany jest zakres i przyczyny naruszenia/incydentu ochrony danych osobowych
oraz jego ewentualne skutki;
4. prowadzona jest konsultacja i ustalany jest tok postępowania z inspektorem ochrony danych;
5. podejmowane są działania prewencyjne zmierzające do eliminacji podobnych naruszeń/ incydentów w przyszłości i/lub zmniejszenia strat w momencie ich zaistnienia.

## **XII. Szczególne sytuacje**

1. Problemy w działaniu oraz nieprawidłowości udostępnionych urządzeń lub oprogramowania należy niezwłocznie zgłaszać do Centrum Informatycznego Uniwersytetu.
2. W przypadku zgubienia lub kradzieży urządzeń, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, Centrum Informatycznego, a także inspektora ochrony danych*.*

## **XIII. Działania niedozwolone**

Działania niedozwolone stanowią m.in.:

1. udostępnianie innym osobom danych służących do uwierzytelnienia do systemów
i/lub usług;
2. korzystanie z urządzeń, które nie zostały zatwierdzone przez pracodawcę;
3. przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail;
4. przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji,
którą przekazywany jest zabezpieczony hasłem plik lub pliki;
5. niezabezpieczenie dokumentów w miejscu świadczenia pracy zdalnej;
6. odmówienie pracownikowi Centrum Informatycznego Uniwersytetu przeglądu urządzeń i narzędzi wykorzystywanych w pracy zdalnej;
7. udostępnianie służbowych urządzeń wykorzystywanych do realizowania zadań służbowych innym osobom;
8. dzielenie się informacjami poufnymi z innymi osobami;
9. logowanie się na konto innego użytkownika;
10. zabranie dokumentów poza siedzibę pracodawcy bez uprzedniej pisemnej
lub elektronicznej zgody pracodawcy;
11. niezwrócenie dokumentów.

## **XIV. Postanowienia końcowe**

1. Złamanie zasad określonych w Procedurze czy niedostosowanie się do jej postanowień, stanowią naruszenie obowiązków pracowniczych i/lub naruszenie zasad współpracy.
2. Postanowienia wynikające z RODO, odrębnych przepisów prawnych powszechnie obowiązujących i regulujących przedmiotowe kwestie, Polityki ochrony danych osobowych w Uniwersytecie Ekonomicznym w Katowicach, jak również z zaleceń wydawanych w tym przedmiocie, stosuje się odpowiednio, również w sprawach nieuregulowanych niniejszą Procedurą.
3. Zmiana trybu i sposobu pracy nie zwalnia z obowiązku zapewnienia ciągłej ochrony danych osobowych w Uniwersytecie i nie może wpływać na zmniejszenie lub ograniczenie wcześniej obowiązujących zabezpieczeń w przedmiotowym zakresie.
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 (Dz. U. UE. L.
z 2016 r. Nr 119, poz. 1, z późn. sprost.) [↑](#footnote-ref-1)
2. zarządzenie nr 27/19 z dnia 28 marca 2019 roku w sprawie przetwarzania i ochrony danych osobowych
w Uniwersytecie Ekonomicznym w Katowicach (z późn. zm.) [↑](#footnote-ref-2)
3. dotyczy pracowników niebędących nauczycielami akademickimi [↑](#footnote-ref-3)
4. Polityka ochrony danych osobowych w Uniwersytecie Ekonomicznym w Katowicach [↑](#footnote-ref-4)