

Załącznik nr 1
do Zarządzenia
Dyrektora GZOPO
nr GZOPO.0210.2.11.2023
z dnia 7 kwietnia 2023 r.

PROCEDURY BEZPIECZEŃSTWA I OCHRONY INFORMACJI PODCZAS PRACY ZDALNEJ

.....
Data

.....
Pieczęć i podpis Pracodawcy

Spis treści

I.	Wprowadzenie.....	2
II.	Definicje.....	2
III.	Warunki jakie musi spełniać miejsce świadczenia pracy zdalnej.....	3
IV.	Bezpieczeństwo pracy zdalnej.....	3
IV.I.	Dostęp do danych.....	3
IV.II.	Internet.....	3
IV.III.	Urządzenia służące do pracy zdalnej.....	4
IV.IV.	Zabezpieczanie przekazywanych informacji.....	5
IV.V.	Zasady korzystania z dokumentów w formie papierowej.....	5
IV.VI.	Przechowywanie danych i nośników.....	6
IV.VII.	Transport sprzętu i nośników danych.....	6
IV.VIII.	Szczególne sytuacje.....	6
V.	Działania niedozwolone.....	7
IX.	Szkolenia.....	7
X.	Załączniki.....	7
	Załącznik nr 1.....	8

I. Wprowadzenie.¹

1. „Procedury bezpieczeństwa i Ochrony Informacji Podczas Pracy Zdalnej”, zwane dalej Procedurą, określają zasady postępowania z informacjami, zasady ich zabezpieczenia i ochrony podczas wykonywania pracy zdalnej, zgodnie z wymogami art. 67²⁶ ustawy z dnia 26 czerwca 1974 r. Kodeks pracy.
2. W przypadku danych osobowych, mają zastosowanie również wdrożone u Pracodawcy procedury dotyczące zasad ich przetwarzania.
3. Obowiązek stosowania Procedury dotyczy każdego pracownika wykonującego pracę zdalną bez względu na tryb jej uruchomienia.
4. Jeżeli pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą (np. brak prądu lub Internetu), niezwłocznie zgłasza to pracodawcy i postępuje zgodnie z jego instrukcjami.
5. Złamanie zasad określonych w Procedurze lub niedostosowanie się do postanowień niniejszej Procedury może stanowić naruszenie obowiązków pracowniczych.

II. Definicje.

1. Pracodawca, administrator – należy przez to rozumieć pracodawcę pracownika wykonującego pracę zdalną.
2. Pracownik – należy rozumieć, zgodnie z definicją pracownika, określoną w ustawie z dnia 26 czerwca 1974 r. Kodeks pracy.
3. Informacje – należy przez to rozumieć wszelkie dane, w tym dane osobowe.
4. 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.
5. Przetwarzaniu – 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.
6. IOD – należy przez to rozumieć Inspektora Ochrony Danych, powoływanego przez Administratora zgodnie z art. 37 RODO.
7. 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.).

¹ Procedury dotyczą również ochrony danych osobowych.

III. Warunki jakie musi spełniać miejsce świadczenia pracy zdalnej.

1. O możliwości podjęcia pracy zdalnej przez pracownika decyduje pracodawca.
2. Pracownik musi zapewnić właściwe warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.
3. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, jak kawiarnie, restauracje, galerie handlowe, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.
4. Pracując w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu np. komputera, tabletu, smartfona, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający wgląd.
5. Praca zdalna powinna odbywać się zgodnie z harmonogramem ustalonym z pracodawcą, co oznacza, że pracownik jest dostępny i realizuje swoje działania w ustalonych godzinach.
6. Odchodząc od komputera lub kończąc korzystanie z tabletu, smartfona należy upewnić się, że urządzenie zostało zablokowane.
7. Prowadzenie służbowych spotkań zdalnych lub rozmów telefonicznych jest realizowane w sposób zapewniający poufność informacji przekazywanych w trakcie spotkania/rozmowy.

IV. Bezpieczeństwo pracy zdalnej.

IV.I. Dostęp do danych.

1. Pracownik wykonujący pracę zdalną, uzyskuje dostęp do informacji, w tym danych osobowych, których przetwarzanie jest niezbędne do wykonywania obowiązków pracowniczych.
2. Dostęp do danych możliwy jest po nadaniu pracownikowi upoważnienia do ich przetwarzania i trwa do momentu ustania zatrudnienia.
3. Pracownik utrzymuje w tajemnicy otrzymane od pracodawcy dane dostępowe, w tym loginy i hasła oraz zabezpiecza je przed dostępem osób nieuprawnionych, w tym domowników.
4. Pracownik jest zobowiązany do pracy w ramach przydzielonego mu konta w systemie informatycznym.
5. Dostęp do informacji odbywa się w sposób zdalny i następuje poprzez:
 - a) dostęp do skrzynki pocztowej pracownika w domenie pracodawcy;
 - b) dostęp do określonych zasobów w infrastrukturze pracodawcy przy użyciu szyfrowanego połączenia zdalnego (np.VPN).

IV.II. Internet.

1. Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy.
2. Jeżeli pracodawca udostępnia pracownikowi modem Internetowy lub telefon służbowy z dostępem do Internetu, który może pełnić funkcję HotSpot, pracownik powinien korzystać w pierwszej kolejności z tych urządzeń.

3. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:
 - a) Korzystanie z Internetu powinno wymagać uwierzytelnienia, np. poprzez hasło,
 - b) Hasło dostępu powinno składać się z co najmniej 8 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych.
 - c) Jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny.
 - d) Dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej.
 - e) Został zmieniony domyślny adres routera (najczęściej 192.168.1.1.) na inny.
4. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela Administrator Systemu Informatycznego.

IV.III. Urządzenia służące do pracy zdalnej.

1. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.
2. Praca zdalna powinna być realizowana z wykorzystaniem służbowego sprzętu, jak komputera stacjonarny, laptop, smartfon, tablet, itp.
3. Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą pracodawcy.
4. Pracownik jest uprawniony także do zabrania komputera stacjonarnego do miejsca wykonywania pracy zdalnej, na czas wykonywania tej pracy.
5. Jeżeli z jakichś względów pracownik nie może wykonywać pracy zdalnej z wykorzystaniem służbowego sprzętu, zgłasza to pracodawcy, który może wydać zgodę na pracę z wykorzystaniem prywatnych urządzeń.
6. Urządzenie służbowe jest wydawane pracownikowi za protokołem.
7. Po otrzymaniu zgody na pracę zdalną i uzgodnieniu z pracodawcą z jakich urządzeń będzie korzystał pracownik w celu jej zrealizowania, pracownik niezwłocznie zgłasza ten fakt ASI.
8. ASI odnotowuje, które urządzenia są wykorzystywane przez pracownika do pracy zdalnej, jeżeli to niezbędne, przeprowadza ich przegląd.
9. W przypadku, gdy przegląd jest niemożliwy, pracownik na żądanie ASI udostępnia urządzenie zdalnie (z wykorzystaniem zaproponowanego przez ASI narzędzia), w celu dokonania jego zdalnego przeglądu.
10. Przegląd urządzeń prywatnych jest obowiązkowy.
11. Minimalne wymagania w zakresie bezpieczeństwa:
 - a) Zaszyfrowany dysk;
 - b) Na urządzeniu zainstalowane jest legalne i aktualne oprogramowanie;
 - c) Zostały włączone automatyczne aktualizacje;
 - d) Została włączona zapora systemowa;
 - e) Został zainstalowany i działa w tle program antywirusowy;
 - f) Zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token;
 - g) Wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej;
 - h) Został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip);
 - i) Zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności;
 - j) Jeżeli urządzenie daje taką możliwość, praca jest wykonywana na koncie z ograniczonymi uprawnieniami;

12. Pracodawca może dodatkowo wymagać, aby urządzenie wykorzystywane do pracy zdalnej zawierało inne zabezpieczenia, jak:
 - a) Wyłączone porty pamięci zewnętrznych;
 - b) Oprogramowanie służące monitorowaniu wykonywania pracy przez pracownika, wykorzystywane zgodnie z wymaganiami przepisów prawa pracy;

IV.IV. Zabezpieczanie przekazywanych informacji.

1. Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę.
2. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, powinny zostać one zabezpieczone hasłem.
3. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, powinny zostać udostępnione w załączniku zabezpieczonym hasłem.
4. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, nawet jeżeli są to jedynie imiona, nazwiska, czy adresy e-mail.
5. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji.
6. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.
7. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
8. Rekomendowane metody zabezpieczania hasłem:
 - a) Nadanie hasła do pliku, w którym są dane osobowe;
 - b) Zabezpieczenie pliku lub plików poprzez kompresję z zabezpieczeniem archiwum wynikowego hasłem.
9. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
10. 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.
11. Szczegółowe zasady korzystania z poczty e-mail określają wewnętrzne procedury ochrony informacji.
12. Masowe wysyłki wiadomości e-mail należy realizować poprzez specjalne oprogramowanie udostępnione w tym celu przez pracodawcę.
13. Pracownik może także przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez pracodawcę serwerów sieciowych lub plików FTP.
14. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (weTransfer, Google Drive, DropBoX) może odbywać się tylko za zgodą pracodawcy, po wcześniejszym zabezpieczeniu hasłem plików.

IV.V. Zasady korzystania z dokumentów w formie papierowej.

1. Zgodnie z obowiązującym u pracodawcy zasadami wszystkie dokumenty zawierające informacje poufne, w tym dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w siedzibie pracodawcy.
2. Obowiązuje ogólny zakaz zabierania dokumentów lub ich kopii poza siedzibę pracodawcy.
3. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik zgłasza do pracodawcy prośbę o możliwość ich skopiowania oraz zabrania do domu na czas wykonywania pracy zdalnej.

4. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów.
5. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.
6. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane.
7. Informacja jest przekazywana pracodawcy.
8. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić.
9. Praca z dokumentami nie może być wykonywana w miejscu publicznym (kawiarnia, restauracja, galeria handlowa, itp.)
10. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić pracodawcy, który weryfikuje ich kompletność.
11. Niszczenie kopii pobranych dokumentów następuje w siedzibie pracodawcy.

IV.VI. Przechowywanie danych i nośników.

1. Pracownik odpowiada za bezpieczne przechowywanie danych, sprzętu i nośników służących do ich przetwarzania.
2. Nośniki oraz dokumentacja zawierająca dane nie powinna być pozostawiana bez nadzoru. Po zakończeniu pracy nośniki i dokumentacja powinny być schowane w miejscu zabezpieczonym (zamykanym na klucz) przed osobami nieuprawnionymi (np. w szafce, szufladzie).

IV.VII. Transport sprzętu i nośników danych.

1. 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).
2. Przewożenie dokumentacji zawierającej dane osobowe powinno odbywać się w sposób zabezpieczający ją przed dostępem osób nieuprawnionych. W tym celu pracownik umieszcza dokumentację w teczce lub skoroszycie uniemożliwiającym zapoznanie się z treścią danych osobowych, a następnie w plecaku lub torbie.
3. Dozwolony jest transport (wynoszenie poza siedzibę pracodawcy) tylko sprzętu i nośników, które wcześniej zostały zaszyfrowane.

IV.VIII. Szczególne sytuacje.

1. Problemy w działaniu udostępnionego/prywatnego sprzętu lub oprogramowania należy niezwłocznie zgłaszać ASI.
2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, ASI, a także inspektora ochrony danych (IOD)².

² W przypadku, gdy informacje zawierały dane osobowe, lub inne informacje prawnie chronione.

V. Działania niedozwolone.

1. Niedozwolone jest:

- a) Udostępnianie innym osobom danych służących do uwierzytelnienia do systemów i/lub usług;
- b) wykorzystywanie informacji przetwarzanych w ramach pracy zdalnej w innym celu niż wykonywanie obowiązków służbowych;
- c) Przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail;
- d) Przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
- e) Korzystanie z urządzeń, które nie zostały zatwierdzone przez pracodawcę;
- f) Odmówienie pracownikowi działu IT przeglądu urządzenia;
- g) Niszczenie dokumentów w domu;
- h) Udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
- i) Dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami;
- j) Logowanie się na konto innego użytkownika;
- k) Zabranie dokumentów bez pisemnej lub elektronicznej zgody pracodawcy;
- l) Zabranie oryginałów dokumentów;
- m) Niezwrócenie dokumentów;
- n) Niepotwierdzenie z pracodawcą zakresu zwróconych danych;
- o) Pozostawianie bez nadzoru wszelkiego rodzaju nośników danych.

IX. Szkolenia.

- 1. W ramach pracy zdalnej pracownik uczestniczy we wszystkich szkoleniach, warsztatach, instruktażach dotyczących bezpieczeństwa informacji, ochrony danych osobowych.
- 2. Udział pracownika w wyżej wskazanych formach doskonalenia ma charakter obowiązkowy oraz aktywny.

X. Załączniki.

- 1. Oświadczenie o zapoznaniu się z procedurami bezpieczeństwa i ochrony informacji podczas pracy zdalnej.

Data:

.....

Imię/imiona:

.....

Nazwisko:

.....

Stanowisko służbowe:

.....

OŚWIADCZENIE

Na podstawie art. 67²⁶ ustawy z dnia z dnia 26 czerwca 1974 r Kodeks Pracy, oświadczam, iż zostałem zapoznany z obowiązującymi u Pracodawcy „Procedurami bezpieczeństwa i ochrony informacji podczas pracy zdalnej” i zobowiązuję się do ich przestrzegania i respektowania wszelkich zasad z nich wynikających.

.....

(Podpis Pracownika)