Załącznik do Zarządzenia nr 595/23
Burmistrza Śmigla
z dnia 17.05.2023 r.

Regulamin ochrony danych osobowych w pracy zdalnej

I. Wprowadzenie

1. Niniejszy regulamin określa zasady ochrony danych osobowych podczas pracy zdalnej i jest wprowadzany w związku z przepisami rozporządzenia PEiR (UE) nr 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 (Dz.Urz. UE L z 2016 r. 119, s. 1 ze zm.) – dalej RODO oraz ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2022 r. poz. 1510 z późn. zm.).
2. W Regulaminie pod określeniem "pracownik" należy rozumieć zarówno osoby zatrudnione w ramach stosunku pracy, jak i współpracowników, na stale wykonujących zadania w ramach umów cywilnoprawnych wymagające dostępu do zasobów sprzętowych i informacyjnych organizacji. Pod określeniem "pracodawca" należy rozumieć zarówno pracodawcę, jak i zlecającego usługi.

II. Warunki podjęcia pracy zdalnej

1. O możliwości podjęcia pracy zdalnej przez pracownika decyduje pracodawca.
2. Pracownik może zgłosić pracodawcy chęć podjęcia pracy zdalnej.
3. Warunki i zasady pracy zdalnej, w tym zakres i harmonogram wykonywanej pracy określa pracodawca w odrębnym regulaminie i/lub porozumieniu z pracownikiem.
4. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady ochrony danych osobowych podczas pracy zdalnej określone w niniejszym Regulaminie.
5. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodnie z niniejszym Regulaminem, warunki techniczne oraz lokalowe, ochrony danych osobowych w miejscu wykonywania pracy zdalnej.
6. 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.
7. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych. W przypadku osób realizujących zadania w oparciu o umowy cywilnoprawne postępowanie niezgodnie z niniejszym Regulaminem może oznaczać wykonanie zadania niezgodnie z przedmiotem umowy i z wymaganą przez pracodawcę starannością i zawodowym profesjonalizmem i skutkować rozwiązaniem umowy, a także przewidzianymi w umowie karami umownymi.

III. Miejsce świadczenia pracy zdalnej

1. Pracownik musi zapewnić właściwe warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.
2. Pracownik wykonuje pracę zdalną pod adresem, który wskazał pracodawcy. 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.

3. Pracując w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera oraz smartfona, a także zapewnienie swobodnej pracy.
4. Praca zdalna powinna odbywać się zgodnie z harmonogramem ustalonym z pracodawcą, co oznacza, że pracownik jest dostępny i realizuje swoje działania w ustalonych godzinach.
5. Odchodząc od komputera lub kończąc korzystanie ze służbowego smartfona należy upewnić się, że urządzenie zostało zablokowane.
6. Prowadzenie służbowych spotkań zdalnych lub rozmów telefonicznych jest realizowane w sposób zapewniający poufność informacji przekazywanych w trakcie spotkania/rozmowy.

IV. Bezpieczeństwo pracy zdalnej

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 korzysta z tych urządzeń do połączeń z Internetem.
3. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:
    1. Korzystanie z Internetu 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. Jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny.
    4. Dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej.
4. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela dział IT.
5. Zasady przeprowadzania bezpiecznej wideokonferencji określa załącznik numer 1 *(źródło: https://uodo.gov.pl/pl/138/1525).*

Urządzenia służące do pracy zdalnej

1. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.
2. Praca zdalna jest 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 jakiś 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 do działu IT.
8. Dział IT odnotowuje, które urządzania są wykorzystywane przez pracownika do pracy zdalnej, jeżeli to niezbędne, przeprowadza ich przegląd.
9. W przypadku, gdy przegląd jest niemożliwy, pracownik na żądanie pracownika działu IT udostępnia urządzenie zdalnie (z wykorzystaniem zaproponowanego przez dział IT narzędzia), w celu dokonania jego zdalnego przeglądu.
10. Przegląd urządzeń prywatnych, na których wykorzystanie pracodawca wyraził zgodę, jest obowiązkowy.
11. Minimalne wymagania w zakresie bezpieczeństwa:
    - Na urządzeniu jest legalne i aktualne oprogramowanie;
    - Zostały włączone automatyczne aktualizacje;
    - Została włączona zapora systemowa;
    - Został zainstalowany i działa w tle program antywirusowy;
    - Zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token;
    - Wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej;
    - Został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych;
    - Zostało ustawione automatyczne blokowanie urządzenia po 10 minutach przy braku aktywności;
    - 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:
    - Zaszyfrowany dysk
    - Wyłączone porty pamięci zewnętrznych
    - Oprogramowanie służące monitorowaniu wykonywania pracy przez pracownika, wykorzystywane zgodnie z wymaganiami przepisów prawa pracy.

Zabezpieczanie przekazywanych informacji

1. Do pracy zdalnej pracownik wykorzystuje tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę.
2. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, uprzednio należy je zabezpieczyć hasłem.
3. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, należy przesyłać je 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, o ile nie będzie wykorzystywane do zabezpieczania plików w komunikacji z innymi odbiorcami.
8. Rekomendowane metody zabezpieczania hasłem:

1. Nadanie hasła do pliku, w którym są dane osobowe
2. 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.
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.

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. Pracownik zapewnia zabezpieczenie dokumentów w miejscu wykonywania pracy zdalnej, poprzez przechowywanie w szafie zamykanej na klucz, do której tylko on ma dostęp.

V. Szczególne sytuacje

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do działu IT.

2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy, działu IT, *a także* inspektorowi ochrony danych.

VI. Działania niedozwolone

1. Niedozwolone jest:
   - Udostępnianie innym osobom danych służących do uwierzytelnienia do systemów i/lub usług;
   - Przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail;
   - Przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
   - Korzystanie z urządzeń, które nie zostały zatwierdzone przez pracodawcę;
   - Odmówienie pracownikowi działu IT przeglądu urządzenia;
   - Niszczenie dokumentów w domu;
   - Udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
   - Dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami;
   - Samodzielne zniszczenie dokumentów w domu;
   - Logowanie się na konto innego użytkownika;
   - Zabranie dokumentów bez pisemnej lub elektronicznej zgody pracodawcy;
   - Zabranie oryginałów dokumentów;
   - Niezwrócenie dokumentów;
   - Niepotwierdzenie z pracodawcą zakresu zwróconych danych.

VII. Informacje końcowe

1. Służbowy sprzęt IT wydany pracownikowi w celu realizacji pracy zdalnej podlega kontroli przez komórkę IT.
2. Zasady przetwarzania danych osobowych w trakcie realizacji pracy zdalnej podlegają kontroli przez inspektora ochrony danych.
3. Pracownik w sytuacji incydentu lub naruszenia przepisów prawa w zakresie przetwarzania danych osobowych niezwłocznie zgłasza je telefonicznie lub e-mailowo inspektorowi ochrony danych.
4. Wszelkie nieprawidłowości związane z realizacją pracy zdalnej pracownik zgłasza swojego przełożonemu.

Załącznik nr 1
do regulamin ochrony danych osobowych w pracy zdalnej

ZASADY BEZPIECZNEGO PROWADZENIA WIDEOKONFERENCJI	
Etapy wideokonferencji	**WYTYCZNE**
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 używana 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 telekonferencji korzystaj z kodów dostępu/PIN-ów. 12. Przeskanuj program do telekonferencji systemem antywirusowym.
W trakcie korzystania z wideokonferencji	1. Ogranicz ilość podawania danych osobowych - użyj służbowego adresu e-mail. 2. Użyj innego hasła, niż używane przez Ciebie w innych usługach. 3. Nie udostępniaj linków do organizowanych konferencji poprzez media społecznościowych. 4. Włącz, jeśli to możliwe, domyślną ochronę hasłem spotkania on-line. 5. Zarządzaj opcjami udostępniania ekranu. 6. Nie udostępniaj dokumentów służbowych za pomocą czatu, który może być publiczny. 7. Jeżeli to możliwe, korzystaj z opcji zamazywania tła *(tak żeby rozmówcy nie widzieli Twojego otoczenia).* 8. Korzystaj z opcji „poczekalnia", tak abyś mógł kontrolować osoby uczestniczące w telekonferencji; unikniesz przypadkowych lub niechcianych osób. 9. Logując się do telekonferencji, 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 telekonferencji nie działa w tle.