

ZARZĄDZENIE NR 28/2023
STAROSTY NOWOTOMYSKIEGO

z dnia 1 sierpnia 2023 r.

**w sprawie wprowadzenia procedury ochrony danych osobowych w wykonywaniu pracy
zdalnej w Starostwie Powiatowym w Nowym Tomysłu.**

Na podstawie art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz.U. z 2022 r. poz. 1526 ze zm.) oraz art. 67²⁶ ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. z 2023 r. poz. 1465t.j.) zarządzam, co następuje:

§ 1. Wprowadza się do stosowania w Starostwie Powiatowym w Nowym Tomysłu procedurę ochrony danych osobowych w wykonywaniu pracy zdalnej, stanowiący załącznik do niniejszego Zarządzenia.

§ 2. Zobowiązuje się wszystkich pracowników Starostwa Powiatowego w Nowym Tomysłu do ścisłego przestrzegania procedury.

§ 3. Wykonanie Zarządzenia powierza się pracownikom Starostwa Powiatowego w Nowym Tomysłu.

§ 4. Nadzór nad przestrzeganiem zarządzenia powierza się Sekretarzowi Powiatu.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA

Andrzej Wilkoński

Zatwierdzam pod względem
formalnoprawnym

radca prawny Wojciech Lignowski

Procedura ochrony danych osobowych w wykonywaniu pracy zdalnej

§ 1. Zakres podmiotowy procedury.

1. Procedura określa zasady ochrony danych osobowych w związku z wykonywaniem pracy zdalnej.
2. Zakresem procedury objęci są pracownicy wykonujący pracę zdalną na podstawie:
 - 1) art. 67¹⁹ § 3 Kodeksu pracy (obligatoryjna praca wykonywana na polecenie pracodawcy),
 - 2) art. 67¹⁹ § 6 Kodeksu pracy (obligatoryjna praca zdalna na wniosek pracownika).
 - 3) art. 67³³ § 1 Kodeksu pracy (praca zdalna wykonywana okazjonalnie).

§ 2. Podstawowe pojęcia.

1. Dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, np. imię i nazwisko, numer identyfikacyjny (PESEL), adres zamieszkania, adres e-mail,
2. Naruszenie ochrony danych osobowych – takie naruszenie bezpieczeństwa, które prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,
3. Pracownik wykonujący pracę zdalną – osoba zatrudniona na podstawie przepisów kodeksu pracy, w jeden ze sposobów określonych w art. 67¹⁹ § 1 Kodeksu pracy (w rozumieniu procedury nie jest pracownikiem wykonującym pracę zdalną osoba zatrudniona na podstawie umów cywilnoprawnych).
4. Procedura – procedura ochrony danych osobowych w ramach pracy zdalnej.

§ 3. Obowiązki ogólne.

1. Każdy pracownik wykonujący pracę zdalną jest zobowiązany do stosowania obowiązujących w zakładzie pracy wewnętrznych aktów dotyczących ochrony informacji i danych osobowych, a także procedur lub instrukcji dotyczących działania systemów informatycznych obowiązujących u pracodawcy.
2. Pracodawca przeprowadza w miarę potrzeb, instruktaż i szkolenie w zakresie bezpieczeństwa ochrony danych w trakcie wykonywania pracy zdalnej dla pracowników wykonujących pracę zdalną.

3. Każdy pracownik ma obowiązek zgłaszania wszelkich podejrzeń naruszeń ochrony danych osobowych.

§ 4. Korzystanie ze sprzętu służbowego.

1. Do wykonywania obowiązków pracowniczych podczas Pracy zdalnej będą wykorzystane przez Pracownika następujące urządzenia elektroniczne, stanowiące mienie Pracodawcy:
 - 1) zestaw komputerowy stacjonarny;
 - 2) laptop/notebook - terminal służący do połączeń szyfrowych z komputerem znajdującym się w siedzibie pracodawcy, zwanym dalej terminalem;
 - 3) urządzenie fortitoken.
2. Pracodawca zapewni bezpieczeństwo (IT) komunikacji do niezbędnych zasobów IT przez szyfrowane połączenie VPN (Dostęp zdalny). Pracodawca odpowiada za zgodność ze standardami IT oraz bezpieczeństwa IT, natomiast Pracownik za ich przestrzeganie. Pracodawca na udostępnionym do pracy sprzęcie IT może zainstalować dodatkowe systemy lub aplikacje monitorujące poziom bezpieczeństwa i komunikacji.

§ 5. Prawa i obowiązki Pracownika wykonującego pracę zdalną

1. Pracownik zobowiązuje się przestrzegać przepisy prawa powszechnie obowiązujące, w tym przepisy prawa pracy oraz uregulowania wewnętrznie obowiązujące w Starostwie Powiatowym w Nowym Tomyszu, w szczególności przepisy:
 - 1) Regulaminu Pracy,
 - 2) Ustawy RODO oraz Politykę Ochrony Danych Osobowych obowiązującą w Starostwie Powiatowym w Nowym Tomyszu,
 - 3) procedury ochrony danych osobowych w ramach pracy zdalnej, oświadczenie o zapoznaniu się stanowi **załącznik nr 1** do procedury.
2. Praca zdalna świadczona jest wyłącznie za pośrednictwem dedykowanego szyfrowanego połączenia VPN udostępnionego przez Pracodawcę na sprzęcie służbowym.
3. Pracownik zobowiązuje się stosować adekwatne środki zabezpieczeń technicznych i organizacyjnych, w szczególności w sposób niżej określony:
 - 1) Urządzenia i oprogramowanie przekazane przez Pracodawcę do pracy zdalnej służą wyłącznie do wykonywania obowiązków służbowych.
 - 2) Urządzenia wykorzystywane do pracy zdalnej pracownik zobowiązuje się właściwie zabezpieczyć, aby uniknąć kradzieży lub zgubienia.
 - 3) W przypadku zgubienia lub kradzieży, dokumentów, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do Pracodawcy, pracowników IT, a także inspektora ochrony danych – tel. 61 44 26 705, e-mail: iod@powiatnowotomyski.pl. Pracownik stwierdzający naruszenie wraz z Inspektorem ochrony danych podejmują czynności

- do możliwie pełnego udokumentowania zdarzenia celem precyzyjnego określenia przyczyny i ewentualnych skutków naruszenia obowiązujących przepisów.
- 4) Wszystkie nieprawidłowości w działaniu poczty elektronicznej, a także wątpliwości związane ze sposobem korzystania z poczty elektronicznej, w tym związane z jej bezpieczeństwem, należy niezwłocznie konsultować z pracownikami IT.
 - 5) Jeżeli Pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych warunków pracy, zabezpieczeń, ze względu na siłę wyższą (np. brak prądu lub Internetu), Pracownik zobowiązuje się niezwłocznie zgłosić ten fakt to Pracodawcy i postępować zgodnie z jego instrukcjami.
 - 6) W przypadku wszelkich incydentów i naruszenia ochrony danych należy stosować procedury w zakresie zgłaszania i obsługi naruszeń ochrony danych zawarte w zarządzeniu w sprawie ochrony danych osobowych oraz w Polityce Bezpieczeństwa Informacji obowiązującej w Starostwie.
 - 7) Nie jest dopuszczalne korzystanie i zapisywanie na własnych nośnikach plików zawierających dane osobowe, których administratorem jest pracodawca, bez jego zgody i bez wcześniejszego zabezpieczenia przez pracowników IT.
 - 8) Nie jest dopuszczalne umożliwianie dostępu do danych, poczty elektronicznej lub systemów informatycznych osobom nieuprawnionym, próbującym uzyskać dostęp drogą telefoniczną lub mailową, podającym się za przedstawicieli serwisu lub konkretnych instytucji, bez ich weryfikacji i potwierdzenia w zakładzie pracy takiego kontaktu.
 - 9) W miejscach publicznych nie należy pozostawić bez nadzoru dokumentów i sprzętu.
 - 10) Zapewnić warunki uniemożliwiających domownikom oraz innym osobom nieuprawnionym wgląd w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera lub innych urządzeń udostępnionych Pracownikowi, a także zapewnienie pracy z dokumentami, w sposób uniemożliwiający wgląd w treść dokumentów.
 - 11) Pracownik w trakcie pracy zdalnej zobowiązany jest dbać o bezpieczeństwo danych, ich poufność oraz integralność. Na pracowniku ciąży obowiązek dbałości o dobro Starostwa w przypadku postępowania z danymi osobowymi w trakcie pracy zdalnej.
 - 12) Każdy pracownik korzystający z poczty elektronicznej jest zobowiązany do:
 - a) przechowywania loginu i hasła do poczty elektronicznej w bezpiecznym miejscu, niedostępnym dla osób nieuprawnionych, w tym domowników,
 - b) korzystania z poczty elektronicznej wyłącznie w celach służbowych,
 - c) archiwizowania korespondencji służbowej przy użyciu dedykowanych temu celowi narzędzi poczty elektronicznej.

§ 6 Prawa i obowiązki Pracodawcy

1. Pracodawca zobowiązuje się do przekazywania Pracownikowi zadań do wykonania, udzielania informacji merytorycznych oraz organizowania procesu pracy w sposób umożliwiający Pracownikowi pracę zdalną.
2. Pracodawca zobowiązuje się zapewnić wsparcie techniczne.
3. Pracodawca zapewnia warunki do wykonywania Pracy zdalnej poprzez:
 - 1) udostępnianie stosownego sprzętu oraz oprogramowania;
 - 2) inwentaryzację, instalację, serwis, konserwację narzędzi pracy, w tym urządzeń technicznych niezbędnych do wykonywania Pracy zdalnej.
4. Pracodawca zapewnia Pracownikowi świadczącemu Pracę zdalną dostęp do zasobów Pracodawcy z uwzględnieniem przedmiotu i charakteru pracy wykonywanej przez Pracownika.
5. Pracodawca zapewnia bezpieczeństwo informatyczne w zakresie dostępu Pracownika do niezbędnych zasobów przez szyfrowane połączenie związane z dostępem zdalnym. Pracodawca odpowiada za zgodność ze standardami bezpieczeństwa informatycznego, natomiast Pracownik za ich przestrzeganie.
6. Pracodawca zastrzega możliwość stosowania oprogramowania służącego do monitorowania wykonywania pracy przez pracownika.
7. Pracodawca uprawniony jest w każdym czasie do przeprowadzenia kontroli pracy zdalnej u Pracownika w ustalonym miejscu jej świadczenia.

§ 7. Zasady postępowania z dokumentacją papierową niezbędna do wykonywania pracy zdalnej przez Pracownika:

1. Należy ograniczyć do niezbędnego minimum drukowanie dokumentacji zawierającej dane osobowe, a jeżeli taka konieczność zaistnieje, należy niszczyć wydruki po zakończeniu pracy z nimi.
2. Wnoszenie dokumentacji papierowej z siedziby Pracodawcy 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.
3. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, Pracownik zgłasza do Pracodawcy prośbę o możliwość ich:
 - 1) zeskanowania i przechowywania na dysku twardym stacji roboczej, do której dostęp jest możliwy za pomocą oprogramowania do zdalnego dostępu,
 - 2) skopiowania oraz zabrania kopii do miejsca pracy zdalnej 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. Po skopiowaniu dokumentów Pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane. Wzór zestawienia stanowi **Załącznik Nr 2** do procedury.
6. Jeżeli nie ma możliwości skopiowania dokumentów papierowych, a ich brak w czasie wykonywania pracy zdalnej uniemożliwia faktyczną pracę, Pracownik zgłasza do Pracodawcy prośbę o możliwość zabrania dokumentów oryginalnych z miejsca pracy na czas wykonywania pracy zdalnej.
7. W przypadku oryginałów dokumentów Pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostaną zabrane do miejsca pracy zdalnej, zgodnie ze wzorem stanowiącym **Załącznik nr 2** do procedury.
8. Po podpisaniu przez Pracodawcę (Kierownika Wydziału lub Sekretarza Powiatu) zgody na skopiowanie i zabranie dokumentów poza siedzibę Pracodawcy, Pracownik może zabrać dokumenty do miejsca pracy zdalnej.
9. Podczas przewożenia dokumentów do miejsca pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić lub aby nie doszło do ich kradzieży.
10. Zgodnie z obowiązującymi u Pracodawcy zasadami, wszystkie dokumenty zawierające informacje poufne, w tym dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w siedzibie Pracodawcy. Dokumenty przechowywane w miejscu pracy zdalnej podlegają takiej samej ochronie jak w siedzibie Pracodawcy.
11. Dokumenty wyniesione do miejsca pracy zdalnej mogą być wykorzystane wyłącznie w tym celu, w jakim byłyby wykorzystywane w siedzibie Pracodawcy. Żadna osoba nieupoważniona nie może mieć do nich dostępu.
12. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić do siedziby Pracodawcy. Weryfikacji dokumentów dokonują w imieniu Pracodawcy Kierownik Wydziału. Potwierdzenie zwrotu dokumentów stanowi **Załącznik Nr 4** do procedury.
13. Kopie dokumentów, które nie są elementem akt podlegają niezwłocznie zniszczeniu w siedzibie Pracodawcy.

§ 8. Obowiązki podczas spotkań zdalnych, wideokonferencji

1. Organizacja spotkań może nastąpić tylko przy użyciu dostarczonych przez pracodawcę rozwiązań informatycznych.
2. Podczas spotkań przebiegających z ujawnianiem wizerunków należy ograniczyć do minimum rejestrowanie spotkań.
3. W przypadku konieczności udostępniania konkretnych dokumentów podczas spotkań należy zamknąć używane wcześniej inne dokumenty, aplikacje, okna przeglądark, aby udostępnić uczestnikom spotkania tylko i wyłącznie dedykowany dla nich plik.

4. Wszystkie pliki zapisywane w zespołach lub dedykowanej do tego przestrzeni w aplikacji do wideokonferencji należy cyklicznie przeglądać i usuwać po ustaniu ich przydatności.
5. Linki do wideokonferencji powinny być udostępniane tylko i wyłącznie uczestnikom spotkania, bezpiecznym kanałem komunikacji, zaproszenia powinny być kierowane wyłącznie na służbowe adresy e-mail.

§ 9. 1. Niedozwolone jest:

- 1) udostępnianie innym osobom danych służących do uwierzytelnienia do systemów lub usług;
- 2) nie dopuszcza się przechowywania danych na terminalach;
- 3) przekazywanie poza systemem teleinformatycznym Starostwa informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, przede wszystkim w treści wiadomości e-mail;
- 4) przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
- 5) niszczenie dokumentów w miejscu pracy zdalnej;
- 6) dzielenie się informacjami poufnymi z osobami nieupoważnionymi do dostępu do niniejszych informacji, w szczególności domownikami;
- 7) logowanie się na konto lub urządzenie innego użytkownika;
- 8) zabranie dokumentów bez pisemnej lub elektronicznej zgody Pracodawcy;
- 9) niezwrócenie dokumentów;
- 10) niepotwierdzenie z Pracodawcą zakresu zwróconych danych;
- 11) udostępnianie służbowego Urzędu wykorzystywanego do realizowania zadań w formie pracy zdalnej innym osobom;
2. Niedozwolone jest używanie służbowej poczty elektronicznej:
 - 1) do oficjalnego reprezentowania Pracodawcy bez odpowiedniego upoważnienia;
 - 2) do korespondencji prywatnej, komercyjnej lub pracy charytatywnej niepowiązanej z działalnością Pracodawcy;
 - 3) do wysyłania wiadomości e-mail z cudzego konta lub w cudzym imieniu (włączając w to użycie zmienionego pola From:/Od:);
 - 4) do każdego innego niezgodnego z prawem, nieetycznego celu.
3. Niedozwolone jest korzystanie w celach służbowych z innego niż służbowego konta e-mail, w tym z prywatnej poczty e-mail.
4. Niedopuszczalna jest zmiana miejsca wykonywania pracy zdalnej bez wcześniejszego uzgodnienia z Pracodawcą. Pracownik powinien z wyprzedzeniem nie krótszym niż 2 dni robocze skutecznie powiadomić i uzyskać zgodę na zmianę miejsca wykonywania pracy zdalnej.
5. Każdy pracownik korzystający z poczty elektronicznej i systemów teleinformatycznych jest zobowiązany do:

- 1) nieudostępniania danych dostępowych do systemów informatycznych osobom nieuprawnionym, w tym domownikom,
- 2) niepobierania danych osobowych z systemów informatycznych w celu innym niż służbowy,
- 3) nieprzesyłania korespondencji służbowej na jakąkolwiek prywatną skrzynkę pocztową,
- 4) pobierania i zapisywania tylko niezbędnych dokumentów.

§ 10. Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy pracownik zobowiązany jest do powiadomienia bezpośredniego przełożonego, informatyka lub Inspektora Ochrony Danych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do incydentów wymagających powiadomienia należą:
 - 1) zdarzenia losowe zewnętrzne (utrata zasilania, utrata łączności),
 - 2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki użytkowników, utrata/zagubienie danych),
 - 3) umyślne incydenty (włamania do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, nieświadome zniszczenie dokumentów/danych, działania wirusów i innego szkodliwego oprogramowania).

§ 11 Procedura przeprowadzania kontroli przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych, w związku z pracą zdalną

1. Każda osoba wykonująca pracę zdalną jest zobowiązana do zapewniania ochrony informacji przetwarzanych w związku z wykonywanymi zadaniami, w tym do przestrzegania procedur ochrony danych osobowych obowiązujących u pracodawcy oraz zasad zapewniania bezpieczeństwa i ochrony informacji podczas pracy zdalnej,
2. Pracodawca jest uprawniony do przeprowadzenia kontroli przestrzegania obowiązków, o których mowa w ust. 1, na zasadach określonych w porozumieniu o pracę zdalną z pracownikiem podlegającym kontroli.
3. W powiadomieniu o przeprowadzeniu kontroli, pracodawca przekazuje informacje w zakresie:
 1. daty i godziny przeprowadzenia kontroli;
 2. sposobu przeprowadzenia kontroli;
 3. zakresu kontroli;
 4. osób uprawnionych do przeprowadzenia kontroli.

4. Kontrola odbywa się po uprzednim poinformowaniu pracownika, przy czym informacja musi zostać przekazana z wyprzedzeniem, zgodnie z terminem określonym w Porozumieniu.
5. Zakresem kontroli mogą być objęte:
 1. pomieszczenia, w których wykonywana jest praca zdalna;
 2. sposób zapewniania poufności w miejscu wykonywania pracy (środki techniczne oraz organizacyjne);
 3. sposób zabezpieczenia nośników danych;
 4. sposób postępowania ze zbędnymi danymi;
 5. stosowanie wewnętrznych procedur w zakresie blokowania ekranu, nieudostępniania urządzeń służbowych innym osobom, polityki czystego biurka, polityki czystego monitora;
 6. bezpieczeństwo sieciowe,
 7. wykorzystywane narzędzia pracy i środki komunikacji elektronicznej;
 8. znajomość procedur postępowania w przypadku naruszenia ochrony danych;
 9. zapisywanie danych elektronicznych w wyznaczonych przez pracodawcę lokalizacjach;
 10. szyfrowanie danych przekazywanych drogą elektroniczną w związku z wykonywaną pracą zdalną;
 11. inne obowiązki pracownika wynikające z obowiązujących zasad ochrony informacji.
6. Pracownik zapewnia, aby w momencie kontroli, w kontrolowanych pomieszczeniach, nie przebywały inne osoby.
7. Kontrola może zostać przeprowadzona w miejscu świadczenia pracy zdalnej, które wskazał pracownik w Porozumieniu lub poprzez elektroniczne środki porozumienia się na odległość.
8. Pracodawca dostosowuje sposób przeprowadzania kontroli do miejsca wykonywania pracy zdalnej i jej rodzaju.
9. Wykonywanie czynności kontrolnych nie może naruszać prywatności pracownika wykonującego pracę zdalną i innych osób ani utrudniać korzystania z pomieszczeń domowych w sposób zgodny z ich przeznaczeniem.
10. Kontrola w miejscu wykonywania pracy jest realizowana przez uprawnionych pracowników i obejmuje:
 1. wstęp do pomieszczeń, w których wykonywana jest praca zdalna;
 2. weryfikację, czy przestrzegane są procedury ochrony danych osobowych obowiązujące u pracodawcy oraz zasady zapewniania bezpieczeństwa i ochrony informacji podczas pracy zdalnej, które zostały określone w Regulaminie pracy zdalnej;
 3. dokumentowanie fotograficzne stanu faktycznego, przy czym zdjęcia nie mogą obejmować osób fizycznych.

11. Kontrola poprzez elektroniczne środki porozumienia się na odległość, jest realizowana poprzez komunikator internetowy i obejmuje:
 1. zdalne połączenie przez wskazany przez pracodawcę komunikator, z obowiązkiem włączenia kamery;
 2. weryfikację, czy przestrzegane są procedury ochrony danych osobowych obowiązujące u pracodawcy oraz zasady zapewniania bezpieczeństwa i ochrony informacji podczas pracy zdalnej, które zostały określone w Regulaminie pracy zdalnej;
 3. dokumentowanie stanu faktycznego poprzez włączenie nagrywania lub wykonanie zrzutów ekranu.
12. Dokumentowanie stanu faktycznego jest uprawnieniem pracodawcy, z którego może, ale nie musi skorzystać.
13. Pracodawca może także dokonać kontroli na podstawie przekazanego przez pracownika nagrania lub zdjęć, z miejsca wykonywania pracy zdalnej.
14. Kontrola obejmuje wyłącznie w pomieszczenia wskazane przez pracownika jako służące do realizowania pracy zdalnej.
15. Z kontroli jest sporządzany raport.
16. W przypadku stwierdzenia uchybień w zapewnianiu ochrony informacji podczas pracy zdalnej, pracownik jest zobowiązany do ich usunięcia w terminie wskazanym przez pracodawcę.
17. W przypadku rażącego naruszenia zasad ochrony danych osobowych, pracodawca może cofnąć zgodę na wykonywanie pracy zdalnej przez pracownika.

Nowy Tomyśl, dnia r.

.....
(imię i nazwisko pracownika)

.....
(stanowisko, Wydział)

.....
.....
(adres stanowiska pracy)

Oświadczenie w sprawie pracy (zdalnej)

Oświadczam, że przed rozpoczęciem wykonywania pracy zdalnej pracy zapoznałam (-em) się z Zarządzeniem nr AO. 120.28.2023 Starosty Nowotomyskiego z dnia 1 sierpnia 2023r. w sprawie wprowadzenia procedury ochrony danych osobowych w pracy zdalnej w Starostwie Powiatowym w Nowym Tomyślu oraz zobowiązuje się do ich przestrzegania.

.....
(czytelny podpis pracownika)

.....
(Nazwisko i Imię pracownika)

.....
(Stanowisko-Wydział)

ZESTAWIENIE WYPOŻYCZONYCH DOKUMENTÓW PAPIEROWYCH NA CZAS WYKONYWANIA PRACY ZDALNEJ

L.p.	Nr sprawy	Kopia/oryginał	Ilość teczek/ilość stron	Opis sprawy

Wyrażam zgodę na wypożyczenie
ww. dokumentów

.....
(podpis Kierownika/Sekretarza)

Potwierdzam otrzymanie
ww. dokumentów

.....
(podpis pracownika)

POTWIERDZENIE ZWROTU DOKUMENTÓW

Potwierdzam otrzymanie dokumentów, wypożyczonych przez Panią/Pana

.....

w dniu, zgodnie z zestawieniem wypożyczonych dokumentów, na czas wykonywania pracy zdalnej od dnia do dnia

Pracownik przekazujący dokumenty:

Pracownik potwierdzający zwrot:

.....

(data i podpis)

.....

(data i podpis)