Zał. nr 20 do Polityki	**Procedury ochrony danych osobowych przy okazjonalnej pracy zdalnej**

Art. 1 Postanowienia ogólne dotyczące pracy zdalnej

1. Praca zdalna to taka praca, która może być wykonywana całkowicie lub częściowo w miejscu wskazanym przez Pracownika i każdorazowo uzgodnionym z pracodawcą, w tym pod adresem zamieszkania Pracownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość.
2. Pracownika podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych oraz są zobowiązani zapewnić bezpieczeństwo tych danych, przestrzegając zasad wynikających z niniejszej Polityki oraz innych procedur przyjętych w tym zakresie w Jednostce.
3. Pracownicy w trakcie pracy zdalnej zobowiązani są dbać o należyte bezpieczeństwo danych osobowych w szczególności o ich dostępność, poufność oraz integralność.
4. Pracownicy zobowiązani są do zgłaszania bezpośredniemu przełożonemu każdego potencjalnego incydentu lub zdarzenia, skutkującego wystąpieniem naruszenia ochrony danych osobowych zgodnie z procedurą stanowiącą załącznik nr 17 do niniejszej Polityki, tak aby Administrator mógł się wywiązać z obowiązków nałożonych na niego na mocy art. 33 RODO.

Art.2 Praca na dokumentacji papierowej i elektronicznej w ramach wykonywania pracy zdalnej

1. Pracownicy nie powinni wynosić oryginalnej dokumentacji stanowiącej własność Jednostki w postaci papierowej poza określony przez Administratora obszar przetwarzania danych bez pisemnej zgody bezpośredniego przełożonego lub innego upoważnionego przedstawiciela Administratora.
2. Jeżeli Administrator dopuszcza przy pracy zdalnej możliwość korzystania przez Pracowników z dokumentacji papierowej, w tym również kopii dokumentów, wówczas Administrator zobowiązany jest:
   a) ewidencjonować wydane Pracownikom dokumenty na potrzeby pracy zdalnej,
   b) poinformować Pracowników o obowiązku ograniczonego przechowywania wydanych im dokumentów jedynie przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej (ograniczenie przechowywania),

c) zobowiązać Pracowników do wykorzystywania podczas pracy zdalnej pozyskanych dokumentów zawierających dane osobowe wyłącznie w takim celu, w jakim byłyby one wykorzystywane w siedzibie Administratora,
d) ograniczyć liczbę dokumentów wynoszonych poza obszar przetwarzania danych do tego, co niezbędne w stosunku do celu, w jakim te dane osobowe są przetwarzane przez Pracownika w ramach wykonywania pracy zdalnej,
e) zobowiązać Pracownika do odpowiedniego zabezpieczenia danych osobowych podczas wykonywania pracy zdalnej, w szczególności przed dostępem osób nieuprawnionych.

3. Pracownik/Użytkownik zobowiązany jest do zwrotu kopii dokumentów w następujących przypadkach:
4. Zwrot dokumentów podlega odnotowaniu w ewidencji, o której mowa w pkt 2 lit. a.
5. Praca zdalna na dokumentach papierowych przez Pracownika będzie nieuzasadniona jeżeli Administrator:
   a) wdrożył elektroniczny obieg dokumentów lub posiada możliwość szybkiego, sprawnego i bezpiecznego wdrożenia elektronicznego obiegu dokumentacji w zakresie związanym z obowiązkami Pracownika,
   b) Pracownik posiada bezpieczny szyfrowany dostęp do niezbędnych do pracy dokumentów, w tym danych osobowych, przy pomocy środków komunikacji elektronicznej,
   c) udostępnił Pracownikowi odpowiednio zabezpieczone (m.in. zaszyfrowane) elektroniczne kopie niezbędnych dokumentów.

Art.3 Zasady bezpieczeństwa stosowane w ramach wykonywania pracy zdalnej

W ramach pracy zdalnej Pracownicy mają obowiązek przestrzegać następujących zasad bezpiecznej pracy zdalnej:

1) prowadzenie rozmów i wideokonferencji służbowych powinno odbywać się w pomieszczeniach wewnętrznych bez dostępu osób nieupoważnionych przez Administratora do przekazywanych informacji (np. poprzez prowadzenie rozmów w odrębnym pokoju, a w przypadku wideokonferencji również w słuchawkach),

2) zakazane jest prowadzenie służbowych rozmów telefonicznych, w tym wideokonferencji, w miejscach narażonych na brak poufności informacji w szczególności np. na balkonach, tarasach czy innych otwartych przestrzeniach,
3) zakazane jest udostępnianie służbowych urządzeń osobom nieupoważnionym przez Administratora, w tym członkom rodziny Pracownika,
4) zakazane jest niszczenie dokumentacji papierowej w miejscu pracy zdalnej – tego rodzaju czynności powinny odbywać się wyłącznie w siedzibie Administratora,
5) dokumentacja w formie papierowej oraz nośniki elektroniczne powinny być bezpiecznie przechowywane (np. szafa lub szuflada zamykana na klucz lub inne miejsca niedostępne dla pozostałych domowników Pracownika),
6) zakazane jest udostępnianie osobom nieupoważnionym przez Administratora treści wyświetlanych na ekranie komputera, który jest wykorzystywany do pracy zdalnej – należy przestrzegać zasady „czystego ekranu", a także zadbać o odpowiednie ustawienie ekranu i/lub zastosowanie filtra prywatyzującego przekazanego przez Administratora,
7) przestrzeganie polityki „czystego biurka",
8) konta systemowe powinny być blokowane przed każdorazowym odejściem Pracownika od stanowiska pracy,
9) wygaszacz ekranu powinien być uruchamiany automatycznie po upływie oznaczonego czasu w razie braku aktywności Pracownika,
10) komputer służący do pracy zdalnej powinien być zabezpieczony przed dostępem osób nieupoważnionych przez Administratora z wykorzystaniem indywidualnego identyfikatora oraz hasła Pracownika (podobne zasady obowiązują w zakresie telefonu wykorzystywanego do celów pracy zdalnej poprzez stosowanie PIN-u lub innej formy uwierzytelniania,
11) zakazane jest udostępnianie przez Pracownika haseł osobom postronnym,
12) nośniki elektroniczne i urządzenia mobilne (w tym pen drivy, karty pamięci, laptopy, telefony i tablety) powinny być szyfrowane,
13) dokumentacja i inne źródła danych osobowych nie mogą być wykorzystywane przez Pracownika w publicznych chmurach obliczeniowych, komunikatorach lub innych usługach dostępnych w sieci publicznej, które nie zostały uprzednio autoryzowane przez Administratora,

14) zakazane jest utrwalanie danych na lokalnym dysku komputera – możliwość wykorzystania wyłącznie wskazanych przez Administratora zasobów sieciowych, z których wykonywane są regularnie kopie zapasowe,
15) stosowanie rozwiązań umożliwiających zdalne zarządzanie urządzeniami mobilnymi, w tym ich zdalne zlokalizowanie lub przywrócenie do stanu fabrycznego,
16) sprzęt informatyczny powinien zostać wyposażony w uruchomione oprogramowanie antywirusowe i zaporę sieciową,
17) użytkowana wersja systemu operacyjnego winna być wspierana przez producenta,
18) obowiązek aktualizowania systemu operacyjnego, z których korzysta Pracownik, w tym systemu antywirusowego,
19) zakazane jest samodzielne pobieranie i instalacja oprogramowania bez wyraźnej zgody Administratora,
20) co do zasady zakazane jest korzystanie z uprawnień administratora na komputerach służbowych wykorzystywanych do pracy zdalnej (chyba, że nie istnieje odmienna możliwość korzystania z urządzenia lub systemu teleinformatycznego),
21) zakazane jest naprawianie sprzętu informatycznego, na którym znajdują się dane osobowe Administratora z wykorzystaniem wsparcia podmiotów zewnętrznych bez uzyskania uprzedniej pisemnej zgody Administratora,
22) zakazane jest drukowanie dokumentów służbowych w punktach ksero lub z pomocą innych podmiotów/osób trzecich,
23) uużytkowanie sprzętu informatycznego powinno być zgodne z zasadami ostrożności z uwagi na konieczność uwzględnienia zagrożeń sieciowych typu phishing, na które sieć domowa może być bardziej podatna niż sieć Administratora.

Art. 4 Postanowienia końcowe

1. Obsługa informatyczna lub inna osoba upoważniona przez Administratora prowadzi wykaz sprzętu [np. laptopy, smartfony] wydanego Pracownikowi na potrzeby pracy zdalnej.
2. Obsługa informatyczna zapewnia, żeby sprzęt wydawany Pracownikowi został wcześniej odpowiednio skonfigurowany, zabezpieczony przed ujawnieniem lub utratą

danych, zgodnie z Instrukcją zarządzania systemami informatycznymi oraz innymi dokumentami dotyczącymi bezpieczeństwa sprzętu przyjętymi w Jednostce.

3. Obsługa informatyczna przygotowuje dla Pracowników pracujących zdalnie, instrukcję dotyczącą instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonych Pracownikowi narzędzi pracy, w tym urządzeń technicznych.
4. Pracownik jest zobowiązany stosować się do ustalonych przez Administratora zasad dotyczących instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonych mu narzędzi pracy, w tym urządzeń technicznych.