Załącznik nr 4

Procedura ochrony danych osobowych w pracy zdalnej

1. Niniejsza Procedura określa zasady bezpieczeństwa informacji i danych osobowych w trakcie pracy zdalnej.
2. Pracodawca przeprowadza, w miarę potrzeb, instruktaż i szkolenie w tym zakresie dla Pracowników wykonujących pracę zdalną.
3. Pracownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
4. Pracownik w trakcie pracy zdalnej zobowiązany jest dbać o bezpieczeństwo danych, ich poufność oraz integralność. Na pracowniku ciąży obowiązek dbałości o dobro zakładu pracy w przypadku postępowania z danymi osobowymi w trakcie pracy zdalnej.
5. Pracownik zobowiązany jest natychmiastowo powiadomić służby informatyczne Pracodawcy oraz bezpośredniego przełożonego o jakimkolwiek incydencie związanym z wyciekiem danych, zarówno w formie elektronicznej, jak i papierowej, jak również o kradzieży lub zaginięciu powierzonego mu sprzętu.

Praca z danymi w obiegu elektronicznym

6. Instalowanie jakiegokolwiek oprogramowania na laptopie służbowym jest możliwe tylko przez informatyków lub za ich zgodą i zgodnie z ich wytycznymi.
7. Na laptopie służbowym nie może być instalowane żadne nielegalne oprogramowanie.
8. Pracownik odpowiada za zabezpieczenie sprzętu służbowego przed dostępem osób trzecich, a w szczególności domowników i dzieci.
9. Pracownik nie może przechowywać żadnych danych ani informacji na innych nośnikach niż udostępnione mu przez Pracodawcę.
10. Zabronione jest używanie prywatnego sprzętu lub prywatnych kont pocztowych do przetwarzania danych osobowych. Sprawy służbowe mogą być załatwiane tylko i wyłącznie przy użyciu laptopa służbowego oraz telefonu służbowego.
11. Pracownik nie może przechowywać na laptopie plików niezwiązanych z wykonywaną pracą lub jakichkolwiek innych plików lub programów, które nie posiadają stosownej licencji.
12. Pracownik odpowiada za ochronę powierzonego mu sprzętu służbowego, w związku z tym nie może korzystać z laptopa służbowego w miejscach publicznych.
13. Laptop służbowy chroniony jest hasłem.
14. Pracownik nie może łączyć się z firmowymi systemami i dyskami sieciowymi z innego sprzętu niż sprzęt służbowy. Łącząc się z zasobami sieciowymi Pracodawcy Pracownik jest zobowiązany korzystać z bezpiecznego połączenia za pomocą sieci VPN.
15. Hasła do poczty elektronicznej nie powinny być zapisywane przez przeglądarkę internetową.
16. Przy wysyłaniu wiadomości e-mail Pracownik zobowiązany jest każdorazowo upewnić się co do poprawności wpisanych adresów mailowych jej adresatów.
17. Pracownik nie może przesyłać treści podejrzanych, naruszających prawa własności intelektualnej, zabronionych prawnie.
18. W przypadku wiadomości zawierających informacje poufne lub o charakterze tajemnicy przedsiębiorstwa konieczne jest szyfrowanie wiadomości z podwójną weryfikacją hasłem.
19. W przypadku identyfikacji wirusa lub nieaktualności oprogramowania antywirusowego konieczne jest natychmiastowe skontaktowanie się ze służbami informatycznymi.

Praca z dokumentami papierowymi

21. Wynoszenie 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.
22. W przypadku konieczności korzystania z dokumentacji papierowej poza siedzibą zakładu pracy w pierwszej kolejności należy rozważyć wykonanie kopii dokumentacji, na której Pracownik będzie pracował. Kopie dokumentów z danymi osobowymi podlegają takiej samej ochronie jak oryginały.
23. Drukowanie dokumentów na potrzeby pracy zdalnej należy ograniczyć do niezbędnego minimum. W przypadku dokumentów zawierających dane osobowe należy w miarę możliwości dokonać anonimizacji danych.
24. Wydawane oryginały dokumentów na potrzeby pracy zdalnej podlegają ewidencji przez przełożonego.
25. Wynoszenie dokumentów lub ich kopii powinno mieć miejsce w zabezpieczonej aktówce i w taki sposób, aby były niewidocznie dla osób trzecich.
26. Pracownik zobowiązany jest do odpowiedniego zabezpieczenia danych w miejscu wykonywania pracy zdalnej - dokumenty i ich kopie powinny być przechowywane w zamykanych na klucz szufladach biurka lub szafach, należy zabezpieczyć dostęp do nich osób nieuprawnionych, w tym dzieci oraz pozostałych domowników.
27. Po wykorzystaniu oryginałów dokumentów powinny one zostać niezwłocznie zwrócone. Zwrot dokumentów podlega odnotowaniu w prowadzonej ewidencji.
28. Po wykorzystaniu kopii dokumentacji powinny one zostać w całości zniszczone przez Pracownika. W przypadku nieposiadania niszczarki w miejscu pracy Pracownika powinien on wykonane kopie zniszczyć niezwłocznie w siedzibie zakładu pracy.
29. Po zakończeniu pracy Pracownik powinien bezwzględnie przestrzegać zasady czystego biurka.

Burmistrz Brus
/-/ dr inż. Witold Ossowski