ŚLĄSKI ZWIĄZEK GMIN I POWIATÓW

40-048 Katowice, ul. Kościuszki 43/5
tel.: +48 32 25-11-021, 25-11-241 fax: +48 32 25-10-985
www.silesia.org.pl, email: zwiazek@silesia.org.pl
NIP:634-10-87-850, Konto ING Bank Śląski 03 1050 1214 1000 0007 0001 3261

Katowice, dnia 11.08.2020 r.

PRACA ZDALNA - ANALIZA i REKOMENDACJA

Zespół ds. Ochrony Danych Osobowych

działający przy Śląskim Zawiązku Gmin i Powiatów

dotyczy: świadczenia pracy poza miejscem jej stałego wykonywania (**praca zdalna**).

W celu wypracowania wspólnego stanowiska i jednolitego postępowania gmin i powiatów zrzeszonych w Śląskim Związku Gmin i Powiatów w zakresie stosowania przepisów o ochronie danych osobowych, w związku z możliwością polecania przez pracodawcę (urząd) wykonywania pracy przez czas oznaczony, poza miejscem jej stałego wykonywania (praca zdalna), wskazuje się jak poniżej.

A. KONTEKST NORMATYWNY

Dla celów rozstrzygnięcia przedmiotowej sprawy należy uwzględnić przepisy prawa merytorycznego regulujące problematykę pracy zdalnej oraz przepisy prawa regulujące problematykę ochrony danych osobowych.

I. Przepisy prawa merytorycznego

1. Uprawnienie czy obowiązek pracodawcy?

Przepis art. 3 *ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2020r. poz. 374 ze zm.)*, zwanej dalej odpowiednio **„KoronawirusU”**, uregulował możliwość pracy zdalnej. W myśl przywołanego przepisu, w celu przeciwdziałania COVID-19 **pracodawca może polecić pracownikowi wykonywanie, przez czas oznaczony, pracy określonej w umowie o pracę, poza miejscem jej stałego wykonywania (praca zdalna)**.

Ten sposób wykonywania pracy charakteryzuje się kilkoma cechami, które z punktu widzenia przepisów o ochronie danych osobowych mają istotne znaczenie:

1) wykonywanie pracy w trybie zdalnym ma miejsce poza miejscem stałego wykonywania pracy – najczęściej chodzi tutaj o miejsce zamieszkania pracownika;

2) tak świadczona praca obejmuje obowiązki wynikające z umowy o pracę;

3) praca w trybie zdalnym może być zlecona na czas oznaczony;

4) praca zdalna ma na celu przeciwdziałanie rozprzestrzenianiu się epidemii COVID-19, co wynika wyraźnie z przepisu art. 3 ust. 1 zd. 1 KoronawirusU, bowiem ustawodawca wyraźnie zaakcentował ten cel, używając sformułowania „w celu przeciwdziałania COVID-19”.

Z powyższego wynika zatem nie tylko uprawnienie pracodawcy do przeorganizowania świadczenia pracy w urzędzie poprzez polecenie swoim pracownikom pracy zdalnej, ale również obowiązek pracodawcy wynikający z celu regulacji. W konsekwencji należy wskazać, że będzie dochodziło do przetwarzania danych osobowych poza siedzibą urzędu, co uzasadnia konieczność dokonania nie tylko odpowiedniej analizy ryzyka w tym zakresie, ale również opracowania najważniejszych wytycznych dla świadczenia pracy w tym trybie, biorąc pod uwagę regulacje prawne zawarte w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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. z 2016 r. Nr 119, str. 1 z późn. zm.), zwanego dalej odpowiednio „RODO".

II. Przepisy o ochronie danych osobowych

1. Dane osobowe

Zgodnie z art. 4 pkt 1 RODO dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą") przy czym możliwa do zidentyfikowania osoba fizyczna to osoba, 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.

Mieszkańcy gmin i powiatów tworzą z mocy prawa wspólnoty samorządowe, a głównym zadaniem tych jednostek samorządu terytorialnego jest zaspokajanie zbiorowych potrzeb wspólnoty. Nieodzownie wiąże się to z przetwarzaniem bardzo dużej ilości danych osobowych na podstawie wielu przepisów prawnych.

2. Przetwarzanie

Zgodnie z art. 4 pkt 2 RODO **przetwarzanie danych oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych** w sposób zautomatyzowany lub niezautomatyzowany, taką 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.

Każdy rodzaj operacji na danych musi posiadać swe wyraźne uzasadnienie, a ich wykonywanie powinno być ograniczone co do zakresu przetwarzania danych osobowych, formy przetwarzania, jak i czasu ich trwania. Dotyczy to w szczególności wykonywania pracy poza siedzibą urzędu z czym wiążą się większe ryzyka we wszystkich najważniejszych obszarach bezpieczeństwa, to jest: prawnym, fizycznym, osobowym i teleinformatycznym.

3. Zasada zgodności z prawem, rzetelności i przejrzystości a zasada ochrony danych osobowych w fazie projektowania

Zgodnie z art. 5 ust. 1 lit a RODO dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość").

Odnosząc się do powyższego przepisu należy wskazać w szczególności, że wymóg zapewnienia zgodności z prawem operacji przetwarzania danych oznacza nie tylko konieczność spełnienia przesłanek legalności przetwarzania danych, które zostały określone w art. 6 RODO, ale również konieczność zapewnienia zgodności z pozostałymi przepisami prawa i wewnętrznymi politykami bezpieczeństwa informacji.

Szczególnego znaczenia nabiera zasada ochrony danych osobowych w fazie projektowania wyrażona w art. 25 ust. 1 RODO. Zgodnie z powyższą **administrator (pracodawca)**, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – **wdraża odpowiednie środki**

techniczne i organizacyjne (np. pseudonimizacja). Są one zaprojektowane w celu skutecznej realizacji zasad ochrony danych (takich jak minimalizacja danych) oraz nadania przetwarzaniu niezbędnych zabezpieczeń, by spełnić wymogi RODO i chronić prawa osób, których dane dotyczą.

Biorąc pod uwagę powołany wyżej przepis oraz charakter pracy zdalnej **pracodawca powinien podchodzić indywidualnie do każdej operacji przetwarzania danych osobowych i wdrożyć takie środki techniczne i organizacyjne, aby przeciwdziałać zmaterializowaniu się ryzyka naruszenia praw lub wolności osób fizycznych.**

B. REKOMENDACJA

Kodeks pracy wprost reguluje niektóre kwestie dotyczące ochrony danych osobowych w ramach wykonywania telepracy, natomiast żadne przepisy szczególne nie określają odrębnych wymogów ochrony danych osobowych podczas pracy zdalnej. Pracodawca, kierując do niej pracownika, musi zapewnić zgodność z przepisami RODO i KRI, w szczególności w zakresie przepisów dotyczących ochrony i bezpieczeństwa danych osobowych. W tym celu należy wdrożyć odpowiednie procedury oraz środki organizacyjne i techniczne tak, aby pracownicy mieli wystarczającą świadomość oraz odpowiednie narzędzia umożliwiające im przestrzeganie przepisów o ochronie danych osobowych podczas wykonywania pracy zdalnej.

1. Analiza ryzyka

Analiza ryzyka utraty poufności, integralności oraz dostępności danych osobowych w związku z wykonywaniem pracy zdalnej, powinna obejmować:

1) ocenę, czy do wykonania konkretnej pracy w trybie zdalnym niezbędny jest dostęp do danych osobowych, czy też jest możliwe skorzystanie z dokumentów zanonimizowanych;
2) ocenę niezbędności wykorzystywania dokumentacji papierowej podczas pracy zdalnej, biorąc pod uwagę charakter danych, cele, dla których są przetwarzane oraz dostępne zasoby;
3) zdefiniowanie operacji przetwarzania realizowanych zdalnie. Punktem wyjścia do dokonania takiej identyfikacji powinny być prowadzone rejestry czynności przetwarzania danych osobowych oraz rejestry kategorii czynności przetwarzania danych osobowych;
4) identyfikację zasobów biorących udział w operacjach przetwarzania realizowanych zdalnie, przy czym określając zasoby należy uwzględnić zasoby urzędu oraz - w przypadku akceptacji pracy zdalnej na komputerach prywatnych – zasoby będące własnością pracowników;
5) określenie zabezpieczeń technicznych i organizacyjnych stosowanych dla danych zasobów. Podczas identyfikacji istniejących lub planowanych zabezpieczeń zaleca się przegląd przyjętych dokumentów i procedur zawierających informacje o zabezpieczeniach oraz zebranie informacji wpływających na sposób świadczenia pracy:
    a) od osób odpowiedzialnych w urzędzie za organizację pracy, bezpieczeństwo danych osobowych oraz bezpieczeństwo teleinformatyczne;
    b) od pracowników przetwarzających dane osobowe w trybie pracy zdalnej poza siedzibą urzędu;
6) określenie możliwych zagrożeń dla danych osobowych w ramach zidentyfikowanych operacji przetwarzania realizowanych zdalnie, biorąc pod uwagę w szczególności zagrożenia wynikające z art. 4 pkt 12 RODO, to jest:
    a) przypadkowe lub niezgodne z prawem zniszczenie danych osobowych;
    b) utratę danych osobowych;

c) modyfikację danych osobowych;

d) nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

7) oszacowanie poziomu ryzyka zgodnie z przyjętą w urzędzie metodyką,

8) przygotowanie planu postępowania z ryzykiem, w tym wskazanie osób odpowiedzialnych za postępowanie z ryzykiem oraz ustalenie harmonogramu działań;

9) monitorowanie ryzyka, a w razie konieczności podjęcie działań ograniczających zmaterializowanie się ryzyka;

10) monitorowanie środowiska zewnętrznego w celu odpowiednio wczesnego wykrycia zmian prawnych i organizacyjnych, mających wpływ na operacje przetwarzania realizowane zdalnie.

2. Dokumentacja papierowa

Zgodnie z wytycznymi Prezesa Urzędu Ochrony Danych Osobowych (dostępnymi na stronie https://uodo.gov.pl/pl/138/1513) praca na dokumentach papierowych nie będzie uzasadniona, jeżeli pracodawca:

1) wdrożył elektroniczny obieg dokumentów, a pracownik ma bezpieczny dostęp do niezbędnych do pracy danych osobowych przy pomocy środków komunikacji elektronicznej;

2) ma możliwość szybkiego, sprawnego i bezpiecznego wdrożenia elektronicznego obiegu dokumentacji;

3) może udostępnić pracownikowi odpowiednio zabezpieczone (m.in. zaszyfrowane) elektroniczne kopie niezbędnych dokumentów.

Jeżeli nie jest to możliwe, zaleca się pracę na kopiach niezbędnych dokumentów. Zmniejsza to ryzyko naruszenia integralności danych oraz utraty ich dostępności. Równocześnie wzrasta ryzyko utraty poufności. W związku z tym należy uświadomić pracownika, że musi on chronić dane zawarte w takich dokumentach, tak samo jak w dokumentacji oryginalnej.

Jeżeli pracodawca zdecyduje o możliwości wykorzystywania przez pracowników podczas pracy zdalnej dokumentacji papierowej, w tym kopii dokumentów oryginalnych, musi:

1) ewidencjonować wydane pracownikom dokumenty;

2) zapewnić, że wydane pracownikom dokumenty będą przechowywane przez pracownika przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej (ograniczenie przechowywania);

3) zapewnić, że pracownik będzie wykorzystywał pozyskane dane osobowe wyłącznie w celu, w jakim byłyby wykorzystywane w siedzibie urzędu (zasada ograniczenia celu);

4) ograniczyć liczbę dokumentów wynoszonych z urzędu do tego, co niezbędne w stosunku do celu przetwarzania danych osobowych przez pracownika w ramach pracy zdalnej (zasada niezbędności);

5) zobowiązać pracownika do odpowiedniego zabezpieczenia danych osobowych podczas wynoszenia dokumentacji oraz wykonywania pracy zdalnej, w szczególności przed wglądem nieuprawnionych osób trzecich (zasada integralności i poufności);

6) określić procedurę związaną z niszczeniem kopii dokumentów oraz zbędnych dokumentów roboczych po zakończeniu pracy zdalnej, jeżeli obowiązujące w urzędzie procedury lub polityka bezpieczeństwa informacji tego nie regulowały;

7) zobowiązać pracownika do zgłaszania pracodawcy każdego incydentu bezpieczeństwa zgodnie z obowiązującymi procedurami w tym zakresie przyjętymi w urzędzie, tak aby pracodawca (administrator) mógł się wywiązać z obowiązku nałożonego na mocy art. 33 ust. 1 RODO.

3. W celu minimalizacji wspomnianych wyżej ryzyk w pracy zdalnej należy stosować się do porad Prezesa Urzędu Ochrony Danych Osobowych odnoszących się do bezpieczeństwa danych osobowych podczas pracy poza siedzibą pracodawcy dostępnych pod adresem https://uodo.gov.pl/pl/138/1459.

4. Zasady bezpiecznej pracy zdalnej – pracodawca, pracownik

1) Otoczenie pracy

W przypadku świadczenia pracy w trybie zdalnym należy ustalić następujące zasady i wytyczne, którymi pracownicy w trakcie wykonywania pracy powinni się kierować:

- nie prowadź służbowych rozmów telefonicznych, w tym wideokonferencji, w miejscach narażonych na brak poufności wymienianych informacji;
- nie udostępniaj służbowych urządzeń osobom postronnym, w tym członkom rodziny;
- bezpiecznie niszcz dokumenty papierowe, a w przypadku, gdy nie dysponujesz odpowiednią niszczarką dokumentów wykonaj taką czynność w urzędzie;
- bezpiecznie przechowuj dokumentację w formie papierowej oraz nośniki elektroniczne, na których taka dokumentacja jest odwzorowana (np. szafa czy szuflada w biurku zamykana na klucz);
- upewnij się, że osoby postronne nie mają wglądu w treści wyświetlane na ekranie komputera, który wykorzystujesz do pracy zdalnej. Zadbaj o odpowiednie ustawienie ekranu lub zastosuj filtr prywatyzujący;
- stosuj się do polityki czystego ekranu;
- blokuj konto systemowe przed każdorazowym odejściem od stanowiska pracy;
- uruchom wygaszacz ekranu, który taką czynność wykona automatycznie po upływie oznaczonego czasu w razie braku aktywności;
- upewnij się, że dostęp do komputera jest możliwy tylko i wyłącznie z wykorzystaniem indywidualnego identyfikatora oraz hasła, a dla telefonu wykorzystywanego do celów służbowych PIN-u lub innej formy uwierzytelniania;
- nie udostępniaj osobom trzecim haseł;
- buduj hasła zgodnie z polityką haseł przyjętą w urzędzie i nie zapominaj o ich cyklicznej zmianie;
- upewnij się, że nośniki urządzeń mobilnych, w tym w szczególności laptopa, telefonu lub tabletu, zostały zaszyfrowane;
- nie zapominaj o szyfrowaniu zewnętrznych kart pamięci, a także innych nośników danych, takich jak pendrive lub dysk zewnętrzny. Nie jest zalecane używanie zewnętrznych nośników pamięci!
- nie umieszczaj danych w publicznych chmurach obliczeniowych, komunikatorach lub innych usługach dostępnych w sieci publicznej, które nie są autoryzowane przez pracodawcę;
- nie utrwalaj danych na lokalnym dysku komputera. Do tego celu wykorzystuj tylko i wyłącznie wskazane przez pracodawcę zasoby sieciowe, które podlegają wykonywaniu kopii zapasowych;

- stosuj rozwiązania umożliwiające zdalne zarządzanie urządzeniami mobilnymi, w tym ich zdalne zlokalizowanie lub przywrócenie do stanu fabrycznego.
- upewnij się, że sprzęt informatyczny został wyposażony w uruchomione oprogramowanie antywirusowe;
- sprawdź, czy wersja systemu operacyjnego jest wspierana przez producenta;
- zweryfikuj, czy systemy, z których korzystasz, w tym system operacyjny oraz system antywirusowy, są zaktualizowane;
- upewnij się, że na sprzęcie informatycznym została uruchomiona zapora sieciowa;
- nie pobieraj ani nie instaluj oprogramowania bez zgody odpowiedniego administratora systemu informatycznego pracodawcy;
- nigdy nie korzystaj z uprawnień administratora do realizowania swoich codziennych obowiązków. Takie konta powinny być wykorzystywane tylko doraźnie, w razie potrzeby;
- zweryfikuj, czy masz dostęp do polityk i procedur obowiązujących u pracodawcy, oraz przypomnij je sobie;
- upewnij się, że wiesz z kim możesz skontaktować się na wypadek nieprzewidzianej awarii sprzętu informatycznego lub incydentu;
- nie naprawiaj sprzętu informatycznego, na którym znajdują się dane służbowe, z wykorzystaniem wsparcia podmiotów zewnętrznych bez uzyskania wcześniejszej zgody pracodawcy;
- nie drukuj dokumentów służbowych w punktach ksero lub z pomocą innych podmiotów/osób trzecich;
- nie zapominaj o zagrożeniach w sieci, w tym phishingu, na które sieć domowa może być bardziej podatna niż sieć pracodawcy;
- szyfruj załączniki wiadomości mailowych, a hasło wysyłaj zawsze inną formą kontaktu, np. SMS;
- dokładnie weryfikuj nadawców wiadomości mailowych, a w razie wątpliwości nie otwieraj załączników oraz hiperłączy znajdujących się w tekście;
- nie wysyłaj wiadomości służbowych na swoje prywatne konta mailowe;
- nie ufaj stronom internetowym, na których nie zaimplementowano protokołu szyfrującego (brak kłódki obok paska adresu), a w szczególności nie podawaj na nich danych osobowych.

2) Informatyczny sprzęt prywatny

Co do zasady nie jest rekomendowane korzystanie ze sprzętu prywatnego jako rozwiązania, które znacząco podnosi ryzyko utraty bezpieczeństwa informacji podczas pracy zdalnej. Rozwiązanie to powinno mieć zastosowane tylko w sytuacjach, gdy użycie sprzętu służbowego jest niemożliwe i powinno być poprzedzone dogłębną analizą ryzyka oraz każdorazowo wymaga akceptacji pracodawcy. W takich przypadkach należy zapewnić, aby:

- wykorzystywane przez pracownika systemy informatyczne, w szczególności systemy operacyjne, dysponowały wsparciem producenta;
- wykorzystywane przez pracownika systemy informatyczne podlegały automatycznej, cyklicznej aktualizacji, a jej przebieg nie był zakłócony żadnymi błędami, w szczególności w zakresie systemu operacyjnego oraz oprogramowania antywirusowego;

- konto systemowe, na którym pracownik wykonuje obowiązki służbowe było kontem o ograniczonych uprawnieniach, a jedyną osobą posiadającą uprawnienia administracyjne był pracownik;
- uruchomiona była zapora ogniowa;
- dostęp do prywatnego sprzętu informatycznego realizowany był z wykorzystaniem hasła dostępowego znanego tylko i wyłącznie pracownikowi;
- dysk bądź jego wydzielona część była zaszyfrowana;
- smartfon miał ustawioną kontrolę dostępu (np. PIN, znak graficzny, czytnik linii papilarnych), aktualne oprogramowanie oraz skonfigurowane szyfrowanie pamięci wbudowanej i zewnętrznej (jeśli występuje);
- wykorzystywany sprzęt informatyczny miał ustawiony wygaszacz ekranu, który blokuje urządzenie na wypadek kilkuminutowej nieaktywności użytkownika.

Przy wypracowaniu stanowiska wzięto pod uwagę:

1) przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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. z 2016 r. Nr 119, str. 1 z późn. zm.),
2) przepisy ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2020r. poz. 374 ze zm.),
3) komunikat opublikowany przez Prezesa Urzędu Ochrony Danych Osobowych dnia 4 maja 2020 roku pod adresem: https://uodo.gov.pl/pl/138/1513.