Zarządzenie 5/2020
Przewodniczącego Zarządu Związku Gmin Krajny w Złotowie
z dnia 03.11.2020 r.

w związku z wprowadzeniem Regulaminu Pracy Zdalnej w Związku Gmin Krajny
oraz
Procedury Ochrony Danych Osobowych pracy zdalnej

§ 1. Wprowadzam Regulamin Pracy Zdalnej w Związku Gmin Krajny w Złotowie, stanowiący załącznik nr 1 do zarządzenia.

§ 2. Wprowadzam Procedurę Ochrony Danych Osobowych pracy zdalnej stanowiącą załącznik nr 2 do zarządzenia. Zobowiązuję pracowników do zapoznania się i przestrzegania w/w procedury, co proszę udokumentować datą i czytelnym podpisem.

§ 3. Wykonanie zarządzenia powierza się Dyrektorowi Biura Związku Gmin Krajny w Złotowie.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.

PRZEWODNICZĄCY
ZARZĄDU ZWIĄZKU GMIN KRAJNY
W ZŁOTOWIE
Adam Pulit

Załącznik Nr 1 do Zarządzenia Nr 5/2020
Przewodniczącego Zarządu Związku
Gmin Krajny w Złotowie z dnia 03.11.2020 r.

REGULAMIN PRACY ZDALNEJ
W ZWIĄZKU GMIN KRAJNY W ZŁOTOWIE

§ 1
Postanowienia ogólne

1. Niniejszy Regulamin określa zasady wykonywania pracy zdalnej oraz związane z tym prawa i obowiązki **[Związek Gmin Krajny w Złotowie]** (dalej jako „Pracodawca") i Pracowników w związku z przeciwdziałaniem i zapobieganiem rozprzestrzeniania się COVID-19.
2. Ilekroć w Regulaminie jest mowa o:
   - **Pracy zdalnej** – należy przez to rozumieć pracę określoną w umowie o pracę, umowie zlecenia, umowie o współpracy oraz innej umowie cywilnoprawnej łączącej Pracownika z Pracodawcą, wykonywaną przez czas oznaczony poza miejscem jej stałego wykonywania w związku z przeciwdziałaniem COVID-19, jeżeli wykonywanie pracy poza takim miejscem jest możliwe,
   - **Pracowniku** – należy przez to rozumieć osobę zatrudnioną w oparciu o umowę o pracę oraz inną umowę cywilnoprawną, w tym umowę zlecenia, umowę o współpracy, umowę o dzieło, jeśli realizacja tej umowy wiąże się z wykonywaniem obowiązków na rzecz Pracodawcy w miejscu ich stałego wykonywania wyznaczonym przez Pracodawcę,
   - **Ustawie** – należy przez to rozumieć ustawę 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. 2020 poz. 374 z późn. zm.).
3. Praca zdalna nie stanowi telepracy, o której mowa w art. 675-6717 Kodeksu pracy (tj. z dnia 16 maja 2019 r., Dz.U. z 2019 r. poz. 1040 z późn. zm.).

§ 2

Warunki dopuszczalności pracy zdalnej

1. Pracownik jest zobowiązany do świadczenia pracy zdalnej w związku z przeciwdziałaniem COVID-19:
   - po złożeniu przez pracodawcę lub bezpośredniego przełożonego pracownika oświadczenia w formie pisemnej lub elektronicznej dot. polecenia wykonywania pracy zdalnej, którego wzór stanowi **Załącznik** nr 1 do Regulaminu.
   - po udzieleniu zgody na pracę zdalną od pracodawcy lub bezpośredniego przełożonego w związku z wnioskiem pracownika o umożliwienie pracy zdalnej, którego wzór stanowi **Załącznik nr 2** do Regulaminu, jeśli wykonywanie pracy na danym stanowisku umożliwia pracę w innym miejscu niż miejsce stałego jej wykonywania oraz jeśli jest to niezbędne do przeciwdziałania i zapobiegania rozprzestrzeniania się COVID-19.

§ 3

Prawa i obowiązki pracodawcy

Rozpoczęcie pracy zdalnej winno być poprzedzone co najmniej:

- zdefiniowaniem procesów realizowanych zdalnie,

- analizą ryzyka uwzględniającą zdalne środowisko pracy,

- adekwatnym zabezpieczeniem sprzętu i pozostałej infrastruktury biorącej udział w operacjach przetwarzania,

- zdefiniowaniem warunków bezpieczeństwa, które powinien zapewnić pracownik,

- przeszkoleniem pracownika.

Praca zdalna będzie wykonywana na sprzęcie prywatnym pracowników. Pracodawca udostępnia pulpit zdalny pracownikowi.

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 ma prawo kontrolować wykonywanie pracy zdalnej oraz żądać od pracownika informacji o jej wynikach.

§ 4

Prawa i obowiązki Pracownika

1. Pracownik wykonuje pracę zdalną w miejscu zamieszkania lub innym miejscu uzgodnionym z Pracodawcą. Pracownik jest zobowiązany do wykonywania pracy zgodnie z treścią umowy łączącej go z Pracodawcą oraz zakresem obowiązków.
2. Ponadto Pracownik zobowiązuje się do:

- pozostawania dyspozycyjnym dla Pracodawcy w ustalonych godzinach pracy i przyjmowania do realizacji bieżących zadań przekazywanych Pracownikowi w ramach zakresu jego obowiązków, w szczególności z wykorzystaniem środków komunikacji elektronicznej,
- bieżącego informowania o wynikach swojej pracy oraz przedstawiania wyników swojej pracy Pracodawcy,
- potwierdzania obecności w pracy w sposób określony przez Pracodawcę - przykładowo: poprzez zalogowanie do systemu, wysyłania komunikatu drogą mailową.

3. Pracownik ma prawo do wsparcia technicznego ze strony Pracodawcy. Pracownik niezwłocznie zgłasza Pracodawcy wszelkie uzasadnione potrzeby w tym zakresie.
4. Pracownik zobowiązuje się zorganizować stanowisko do pracy zdalnej w sposób zapewniający bezpieczne i higieniczne warunki pracy.

§ 5

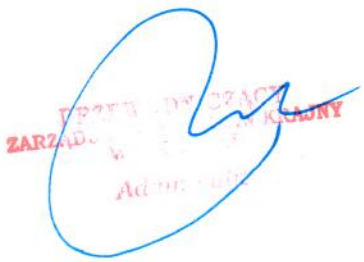
Ochrona informacji i danych osobowych

1. Pracownik zobowiązuje się do zabezpieczania dostępu do sprzętu służbowego oraz posiadanych danych i informacji (w tym także znajdujących się na nośnikach papierowych) przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi, oraz zniszczeniem.
2. Wykonywanie pracy w formie zdalnej nie zwalnia pracownika z obowiązku przestrzegania postanowień Polityki ochrony danych osobowych przyjętej u Pracodawcy wraz z dokumentami powiązanymi.
3. Dane osobowe pozyskane od Pracownika, w związku z wykonywaniem pracy zdalnej, będą przetwarzane w celu zapewnienia prawidłowej realizacji umowy zawartej pomiędzy Pracownikiem a Pracodawcą (art. 6 ust. 1 lit b RODO). W pozostałym zakresie tj. m.in. okresu przetwarzania danych osobowych, praw przysługujących osobom, których dane dotyczą, odbiorców danych oraz innych wymienionych w art. 13 RODO, aktualne pozostają dotychczasowe informacje przekazane przez Pracodawcę jako administratora danych osobowych Pracowników.

§ 6

Postanowienia końcowe

1. Praca zdalna jest wykonywana przez czas określony w poleceniu Pracodawcy. Pracodawca może dowolnie kształtować okres wykonywania pracy zdalnej, uwzględniając stopień zagrożenia rozprzestrzenianiem się COVID-19 na danym obszarze.
2. Przed przystąpieniem do wykonywania pracy zdalnej Pracownik zapoznaje z treścią niniejszego Regulaminu, co potwierdza pisemnym lub elektronicznym oświadczeniem i zobowiązaniem do jego przestrzegania. Wzór oświadczenia stanowi Załącznik nr 3 do Regulaminu.
3. W sprawach nieuregulowanych niniejszym Regulaminem zastosowanie znajdą wewnętrzne procedury obowiązujące u Pracodawcy oraz przepisy prawa powszechnie obowiązującego.



Załącznik nr 1 do Regulaminu Pracy Zdalnej Związku Gmin Krajny

Polecenie wykonania pracy zdalnej

Z uwagi na panującą w kraju sytuację wywołaną zagrożeniem chorobą COVID-19 w dniach od .....do ...../ bezterminowo* ma Pani/ Pan .....wykonywać pracę zdalną w miejscu zamieszkania/inne* .....

.....

/imię i nazwisko bezpośredniego przełożonego
lub osoba działającej z upoważnienia pracodawcy/
/dział, stanowisko/

**niepotrzebne skreślić*

PRZEWODNICZĄCY
ZARZĄDU ZWIĄZKU GMIN KRAJNY
W ZŁOTOWIE
Adam Pulit

Załącznik nr 2 do Regulaminu Pracy Zdalnej Związku Gmin Krajny

(uzupełnia Pracownik, który nie otrzymał od Pracodawcy polecenia pracy zdalnej)

Wniosek o umożliwienie pracy zdalnej

Z uwagi na panującą w kraju sytuację wywołaną zagrożeniem chorobą COVID-19, zwracam się z prośbą o umożliwienie mi pracy zdalnej w dniach od ..... do ..... / bezterminowo*.

Pracę zdalną będę wykonywał/a w miejscu zamieszkania/inne*

..... .

Opcjonalnie: Prośbę swą uzasadniam

.....

.....

.....

.....

/imię i nazwisko Pracownika/

/dział, stanowisko/

**niepotrzebne skreślić*

PRZEWODNICZĄCY ZARZĄDU ZWIĄZKU GMIN KRAJNY

Adam Pulit

(uzupełnia każdy Pracownik, mający wykonywać pracę w formie zdalnej)

Oświadczenie Pracownika

Niniejszym oświadczam, że zapoznałem(-łam) się z Regulaminem pracy zdalnej w [***Związku Gmin Krajny w Złotowie***] i zobowiązuję się do jego przestrzegania.

Jednocześnie oznajmiam, że:

- znane są mi zasady ochrony danych osobowych wynikające z funkcjonujących w organizacji procedur ochrony danych osobowych i zobowiązuję się do ich przestrzegania w trakcie wykonywania pracy zdalnej,
- zobowiązuję się do zorganizowania stanowiska do pracy zdalnej w sposób zapewniający bezpieczne i higieniczne warunki pracy,
- zobowiązuje się do wykonywania obowiązków służbowych w ramach pracy zdalnej z poszanowaniem i ochronę informacji poufnych i innych tajemnic prawnie chronionych, w tym tajemnicy przedsiębiorstwa lub danych osobowych, a także informacji, których ujawnienie mogłoby narazić Pracodawcę na szkodę.

.....
/imię i nazwisko Pracownika/

PRZEWODNICZĄCY
ZARZĄDU ZWIĄZKU GMIN KRAJNY
W ZŁOTOWIE
Adam Pulit

Załącznik Nr 2 do Zarządzenia Nr 5/2020
Przewodniczącego Zarządu Związku
Gmin Krajny w Złotowie z dnia 03.11.2020

Pieczęć nagłówkowa

PROCEDURA OCHRONY DANYCH OSOBOWYCH

PRACA ZDALNA

Data opracowania:
22 października 2020r.

Wykonał:

inspektor ochrony danych

Marcin Misztal

BHP PARTNER
Marcin Misztal
mgr inż. Marcin Misztal
specjalista bhp, inspektor p.poż.

Zatwierdził:

PRZEWODNICZĄCY ZARZĄDU ZWIĄZKU GMIN KRAJNY W ZŁOTOWIE
Adam Fuhr

.....
data, podpis

BHP PARTNER Marcin Misztal
ul. Spichrzowa 10 77-400 Złotów tel. 691 707 120 NIP 767-130-71-89 REGON 300777021
szkolenia i kursy bhp, doradztwo p.poż., ocena ryzyka zawodowego, instruktaż stanowiskowy, pomiary, pozostałe

PODSTAWY PRAWNE:

art. 32 RODO:

administrator i podmiot przetwarzający zobowiązani są do wdrożenia odpowiednich środków technicznych i organizacyjnych, które zapewnią stopień bezpieczeństwa odpowiadający określonemu ryzyku naruszenia praw i wolności osób fizycznych.

art. 5 RODO:

regulacja zasad dotyczące przetwarzania danych, w tym zasady o zachowaniu integralności i poufności (art. 5 ust. 1 lit. f RODO), zgodnie z którymi dane powinny być przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem - należy w tym celu zastosować odpowiednie środki techniczne lub organizacyjne; co do zasady administrator jest odpowiedzialny za przestrzeganie zasad dotyczących przetwarzania danych osobowych, w tym integralności i poufności danych i musi być w stanie wykazać ich przestrzeganie, tzw. „rozliczalność" (art. 5 ust. 2 RODO) - administrator powinien dysponować dowodem potwierdzającym, że przyjęte w organizacji środki są adekwatne i zostały odpowiednio wdrożone.

OGÓLNE ZASADY BEZPIECZEŃSTWA OCHRONY DANYCH PODCZAS PRACY ZDALNEJ:

1. Na bieżąco aktualizuj systemy operacyjne.
2. Systematycznie aktualizuj programy antywirusowe, antymalware i antyspyware.
3. Regularnie skanuj stacje robocze programami antywirusowymi, antymalware i antyspyware.
4. Pobieraj oprogramowanie wyłącznie ze stron producentów.

Nie otwieraj załączników z nieznanych źródeł dostarczanych poprzez korespondencję elektroniczną.

5. Nie zapamiętuj haseł w aplikacjach webowych.

6. Nie zapisuj haseł na kartkach.
7. Nie używaj tych samych haseł w różnych systemach informatycznych.
8. Zabezpieczaj serwery plików czy inne zasoby sieciowe.
9. Zabezpieczaj sieci bezprzewodowe – Access Point.
10. Dostosuj złożoność haseł odpowiednio do zagrożeń.
11. Unikaj wchodzenia na nieznane czy przypadkowe strony internetowe.

Nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi.

12. Wykonuj regularne kopie zapasowe.
13. Korzystaj ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.
14. Szyfruj dane przesyłane pocztą elektroniczną.
15. Szyfruj dyski twarde w komputerach przenośnych.
16. Przy pracy zdalnej korzystaj z szyfrowanego połączenia VPN.
17. Odchodząc od komputera, blokuj stację komputerową.

Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB. Może znajdować się na nich złośliwe oprogramowanie.

URZĄDZENIA I PROGRAMY- ZASADY OCHRONYCH DANYCH W PRACY ZDALNEJ:

1. Urządzenia i oprogramowanie przekazane przez pracodawcę do pracy zdalnej służą do wykonywania obowiązków służbowych. Dlatego też należy postępować zgodnie z przyjętą w pracy/instytucji procedurą bezpieczeństwa.
2. Nie instaluj dodatkowych aplikacji i oprogramowania niezgodnych z procedurą bezpieczeństwa w pracy/instytucji .
3. Upewnij się, że wszystkie urządzenia z jakich korzystasz mają niezbędne aktualizacje systemu operacyjnego (IOS lub Android), oprogramowania oraz systemu antywirusowego.
4. Zanim przystąpisz do pracy, wydziel sobie odpowiednią przestrzeń, tak aby ewentualne osoby postronne, nie miały dostępu do dokumentów, nad którymi pracujesz.
5. Odchodząc od stanowiska pracy każdorazowo blokuj urządzenie, na którym pracujesz.

6. Zabezpieczaj swój komputer poprzez używanie silnych haseł dostępu, wielopoziomowe uwierzytelnianie. Pozwoli to na ograniczenia dostępu do urządzenia, a jednocześnie na ograniczenia ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia.
7. Podejmij szczególne środki, aby urządzenia z których korzystasz podczas pracy, szczególnie te wykorzystywane do przenoszenia danych, jak dyski zewnętrzne nie zostały zgubione.
8. Jeśli zgubiłeś urządzenie, na którym pracujesz lub zostało skradzione natychmiast podejmij odpowiednie kroki, aby o ile to możliwie, zdalnie wyczyścić jego pamięć.

POCZTA ELEKTRONICZNA - ZASADY OCHRONYCH DANYCH W PRACY ZDALNEJ:

1. Postępuj zgodnie z obowiązującymi zasadami w pracy/instytucji dotyczącymi korzystania ze służbowej poczty elektronicznej (e-mail).
2. Używaj przede wszystkim służbowych kont email. Jeśli pracujesz przetwarzając dane osobowe i musisz używać prywatnego e-maila, upewnij się, że treść i załączniki są właściwie szyfrowane.
3. Unikaj używania danych osobowych lub poufnych informacji w temacie wiadomości.
4. Przed wysłaniem maila upewnij się, że wysyłasz go do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe.
5. Dokładnie sprawdź nadawcę maila.
6. Nie otwieraj wiadomości od nieznanych adresatów, a zwłaszcza nie otwieraj załączników oraz nie klikaj w link zawarty w takiej wiadomości. To może być atak phishingowy – podszywanie się pod inną osobę/instytucję.
7. Nie przesyłaj mailem informacji zaszyfrowanej razem z hasłem. Nawet w osobnej wiadomości. Ten kto ma dostęp do Twojej poczty bez problemu odszyfruje wiadomość.

DOSTĘP DO SIECI I CHMURY - ZASADY OCHRONYCH DANYCH W PRACY ZDALNEJ:

1. Używaj tylko z zaufanego dostępu do sieci lub chmury oraz przestrzegaj wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych.

2. Jeśli natomiast nie pracujesz w chmurze lub nie masz dostępu do sieci, zadbaj aby przechowywane dane były w bezpieczny sposób zarchiwizowane.

OBOWIĄZKI PRACODAWCY/ADMINISTRATORA - ZASADY OCHRONYCH DANYCH W PRACY ZDALNEJ:

1. Pracodawca w pracy zdalnej powinien dokonać wyboru właściwego narzędzia przy uwzględnieniu wszystkich aspektów związanych z możliwościami instytucji i pracowników a przede wszystkim, biorąc pod uwagę możliwości techniczne i organizacyjne.
2. Pracodawca ma obowiązek poinformować pracowników o sposobie realizacji pracy zdalnej. Informacja ta powinna zostać przekazana w prosty sposób, tak aby była zrozumiała dla wszystkich, do których skierowany jest komunikat. W celu realizacji pracy zdalnej będzie korzystać z nowych narzędzi lub usług świadczonych przez podmioty zewnętrzne, to musi także poinformować o tym, jak w tym zakresie będą przetwarzane dane osobowe.
3. Pracodawca powinien zapewnić narzędzia umożliwiające pracownikom prowadzenie pracy zdalnej oraz bezpieczną komunikację z klientami, wdrażając je kompleksowo w całej instytucji.
4. Instytucja może wymagać od klienta lub reprezentującej go osoby podania danych w systemie zdalnym, ale tylko w zakresie niezbędnym do tego, aby zrealizować usługę/obsługę. Nie należy przy takiej okazji gromadzić danych nadmiarowych bądź służących do realizacji innych celów.
5. Instytucja, która chce skorzystać z usług przetwarzania danych z wykorzystaniem innych niż wcześniej używane narzędzia, powinna – wraz z pomocą wyznaczonego inspektora ochrony danych, w pierwszej kolejności przeprowadzić analizę zagrożeń. Szczególna uwaga powinna zostać zwrócona na bezpieczeństwo danych oraz zapewnienie odpowiednich gwarancji praw osób, których dane dotyczą.
6. Jednym z głównych obowiązków ADMINISTRATORA – związanych z ochroną danych osobowych – jest zabezpieczenie danych przez zastosowanie odpowiednich środków technicznych i organizacyjnych. Chodzi o to, aby dane te nie były udostępniane osobom nieupoważnionym oraz nie uległy zniszczeniu, zmodyfikowaniu lub utracie. Przykładowe środki służące zabezpieczeniu danych to: pseudonimizacja, anonimizacja, szyfrowanie danych.

7. W razie wykonywania obowiązków służbowych przez pracowników poza jednostką/siedzibą instytucji – pracodawca/administrator w każdym wypadku musi rozważyć możliwości odpowiedniego zabezpieczenia danych osobowych, uwzględniając stopień ryzyka naruszenia ochrony danych osobowych i ewentualnie wdrożyć odpowiednie środki minimalizujące to ryzyko lub zrezygnować z tego rodzaju praktyki, np. umożliwiając pracownikowi, który nie ma właściwych warunków do pracy zdalnej, korzystanie ze sprzętu znajdującego się w instytucji.
8. Gdy instytucja powierzyła podmiotowi zewnętrznemu np. obsługę danych, ADMINISTRATOR musi mieć pewność, że usługodawca zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi wskazane w RODO i chroniło prawa osób, których dane dotyczą. Dlatego też, przed podjęciem takiej decyzji instytucja/administrator powinni przeanalizować wszystkie możliwe rozwiązania oraz oszacować ryzyko.
9. Pracodawca nie powinien zalecać pracownikom używania przez nich prywatnych adresów poczty elektronicznej do kontaktu z klientami. Rekomendowane jest, by pracownicy do korespondencji e-mailowej z klientami korzystali ze służbowych adresów e-mail. Niemniej w obu przypadkach powinni odpowiednio zabezpieczać dane osobowe udostępniane w przesyłanych wiadomościach.

OBOWIĄZKI PRACOWNIKA - ZASADY OCHRONYCH DANYCH W PRACY ZDALNEJ:

1. PRACOWNIK może przetwarzać dane osobowe klientów tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.

2. PRACOWNIK musi pamiętać o bezpiecznym korzystaniu z komputerów i innych urządzeń zarówno wtedy, gdy zapewnił mu je pracodawca, jak i wtedy, gdy korzysta z własnych.

3. RODO nie zabrania wykorzystywania przez PRACOWNIKA prywatnego komputera, tabletu, czy telefonu do przetwarzania danych osobowych w związku ze zdalnym świadczeniem pracy. Urządzenia te muszą być jednak odpowiednio zabezpieczone, a PRACOWNIK powinien postępować zgodnie z polityką lub inną procedurą wprowadzoną w tym zakresie w instytucji.

4. Jeżeli PRACOWNIK używa własnego urządzenia, powinien samodzielnie spełnić podstawowe wymogi bezpieczeństwa. Przede wszystkim należy sprawdzić, czy wykorzystywane urządzenie ma aktualny system operacyjny, czy używane są na nim programy, w szczególności programy antywirusowe, czy dokonane są niezbędne aktualizacje. Na bieżąco aktualizowane powinny być także zainstalowane programy antymalware i antyspyware. Należy rozważnie instalować na swoich urządzeniach oprogramowanie i pobierać je tylko z wiarygodnych źródeł (ze stron producentów).
5. Przechowując dane na sprzęcie, do którego mogą mieć dostęp inne osoby, należy używać mocnych haseł dostępowych, a przed odejściem od stanowiska pracy urządzenie powinno zostać zablokowane. Zalecane jest także skonfigurowanie automatycznego blokowania komputera po pewnym czasie bezczynności, oraz założenie odrębnych kont użytkowników w przypadku korzystania z komputera przez wiele osób.
6. Podczas korzystania z programów lub aplikacji mobilnych należy korzystać z możliwych do zastosowania w nich mechanizmów ochrony prywatności użytkowników. Jeśli użycie jakiegoś programu wymaga logowania, warto zadbać o silne hasło dostępu, a dodatkowo chronić je przed utratą czy dostępem osób nieuprawnionych.
7. Gdy dane są przechowywane na urządzeniach przenośnych (np. pamięć USB), muszą być bezwzględnie szyfrowane i chronione hasłem, by zapewnić odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.
8. W podstawowym zakresie komunikację z klientami prowadzi się poprzez wdrożone w instytucji rozwiązania teleinformatyczne. W takiej sytuacji PRACOWNIK musi nadal zachowywać podstawowe zasady bezpieczeństwa przy zdalnym łączeniu się ze swojego urządzenia w domu.
9. Prowadzenie pracy zdalnej może wymagać korzystania przez PRACOWNIKA z poczty elektronicznej do kontaktu z klientami. PRACOWNIK powinien prowadzić taką korespondencję ze służbowej skrzynki pocztowej, którą powinna zapewnić mu instytucja. Jeżeli instytucja nie zapewniła PRACOWNIKOWI służbowych skrzynek poczty elektronicznej, to jeżeli wykorzystują oni do celów służbowych prywatną skrzynkę pocztową muszą pamiętać, aby korzystać z niej w sposób rozważny i bezpieczny.

10. Szczególną uwagę PRACOWNIK musi zwrócić na zabezpieczenie danych osobowych udostępnianych w przesyłanych wiadomościach. Zawsze przed wysłaniem wiadomości, należy upewnić się, czy niezbędne jest wysłanie danych osobowych, oraz że zamierza wysyłać ją do właściwego adresata. Ponadto trzeba sprawdzić, czy w nazwie adresu e-mail adresata nie ma np. przestawionych lub pominiętych znaków tak, aby nie wysłać takiej wiadomości do osób nieupoważnionych. Podczas wysyłania korespondencji zbiorczej powinno się korzystać z opcji „UDW", dzięki której odbiorcy wiadomości nie będą widzieć wzajemnie swoich adresów e-mail.
11. PRACOWNIK powinien wykorzystywać w pracy zdalnej te platformy lub narzędzia, które zostały wdrożone w instytucji. W takiej sytuacji może oczekiwać, że praca zdalna będzie bezpieczna. Powinien wtedy przestrzegać przyjętych przez instytucję instrukcji i procedur dotyczących ochrony danych osobowych oraz musi zachować podstawowe zasady bezpieczeństwa przy zdalnym łączeniu się z taką platformą ze swojego urządzenia w domu.
12. Instytucja powinna samodzielnie wdrożyć wybraną spośród dostępnych metodę i technikę pracy na odległość lub inny sposób realizacji zadań zdalnie. PRACOWNICY nie powinni jednak sami decydować o korzystaniu z konkretnych. Należy jednak pamiętać, że za przetwarzanie danych klientów przy wykorzystaniu narzędzi wdrożonych samodzielnie przez PRACOWNIKA zawsze odpowiedzialność ponosi instytucja/administrator. Dlatego przyjmowanie określonego rozwiązania powinno się odbywać w uzgodnieniu z pracodawcą/administratorem, który musi mieć świadomość, jakie narzędzia są wykorzystywane do prowadzenia pracy zdalnej, lub wyznaczonym przez niego koordynatorem pracy zdalnej. Takie rozwiązanie powinno być traktowane jako tymczasowe.
13. Zawsze przy wyborze aplikacji lub innych narzędzi wykorzystywanych do pracy zdalnej bądź komunikacji z klientami należy się zastanowić, czy jest niezbędne, aby przetwarzały one dane osobowe, a jeżeli tak, czy można zminimalizować ich zakres, bądź wykorzystywać tylko pseudonimy (np. pierwsza litera imienia itp.) Należy także sprawdzić zasady świadczenia usługi i zasady przetwarzania danych przez usługodawcę (politykę prywatności).
14. W obecnej sytuacji PRACOWNIK w porozumieniu z pracodawcą powinien uwzględnić, jakie realne możliwości komunikowania się z nim mają klienci, pod warunkiem, że

wskazany przez nich konkretny rodzaj komunikatora internetowego zapewnia bezpieczeństwo komunikacji.

15. W celu sprawdzania i monitorowania klientów w pracy zdalnej PRACOWNIK powinien zachować proporcjonalność i minimalizację danych. Dla przykładu nie może w tym celu korzystać z narzędzi zbierających dane biometryczne, w tym wykorzystujących systemy wykrywania twarzy.

OBOWIĄZKI/PRAWA KLIENTA - ZASADY OCHRONYCH DANYCH W PRACY ZDALNEJ:

1. Instytucja może wymagać od klienta jedynie danych niezbędnych do realizacji usługi/obsługi.
2. Klient ma prawo wiedzieć, jak instytucja jako administrator będzie przetwarzała dane osobowe w trakcie pracy zdalnej oraz jakie w związku z tym przysługują mu prawa.
3. Jeżeli platformy wykorzystywane do pracy zdalnej są odrębnymi od instytucji administratorami przetwarzanych przez siebie danych, to klienci powinni od nich otrzymać klauzulę informacyjną o podstawowych zasadach i zakresie zbierania danych oraz administratorze.

OPRACOWAŁ: na podstawie wytycznych RODO, URZĘDU OCHRONY DANYCH OSOBOWYCH

inspektor ochrony danych osobowych Marcin Misztal

LISTA PRACOWNIKÓW ZAPOZNANYCH Z PROCEDURĄ

Oświadczam, że zostałem zapoznany z PROCEDURĄ OCHRONY DANYCH OSOBOWYCH PODCZAS PRACY ZDALNEJ.
Znam zasady i środki ochrony danych osobowych podczas pracy/nauki zdalnej.

Imię i nazwisko pracownika	Data zapoznania z procedurą	Podpis