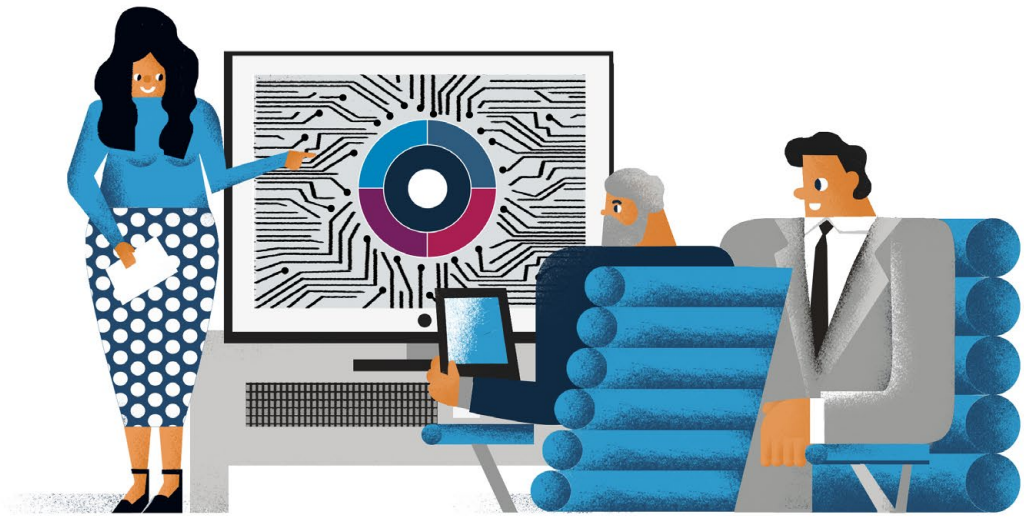
ODO 24

Zasady bezpiecznej pracy zdalnej



RODO i nie tylko

PORADNIK

Dla pracowników

Patron poradnika

ODO 24 sp. z o.o. oferuje kompleksowe rozwiązania w zakresie ochrony danych osobowych i bezpieczeństwa informacji. Dzięki doświadczonemu zespołowi ekspertów z dziedziny m.in. prawa, informatyki, zarządzania kryzysowego oraz ciągłości działania dostarcza organizacjom praktyczne rozwiązania, pozwalające skutecznie zabezpieczyć posiadane zasoby informacyjne.

Autor poradnika

Damian Gąska – audytor i konsultant w obszarze bezpieczeństwa informacji. Zajmuje się weryfikacją infrastruktury informatycznej, wykonuje testy i audyty bezpieczeństwa, tworzy procedury oraz dokumentacje. Przeprowadza analizy incydentów naruszenia bezpieczeństwa usług i procesów biznesowych. Specjalizuje się w bezpieczeństwie usług w chmurze obliczeniowej (ISO/IEC 27017) oraz zarządzaniu ryzykiem (ISO 31000). Posiada certyfikat „Bezpieczeństwo sieci komputerowych".

Wstęp

Oddajemy w ręce czytelnika poradnik, który w hasłowy sposób omawia najważniejsze obszary dotyczące bezpieczeństwa danych podczas pracy zdalnej. Szczególną uwagę poświęcamy: obszarom związanym z zapewnieniem bezpieczeństwa sieci domowej, podstawowym zasadom postępowania ze sprzętem komputerowym, efektywnym zabezpieczeniom urządzeń prywatnych wykorzystywanych do celów służbowych oraz organizacji przestrzeni w celu zapewnienia bezpieczeństwa przetwarzanym danym. Właściwe skonfigurowanie urządzeń i rozsądne postępowanie pozwolą na znaczne zminimalizowanie ryzyk związanych z ewentualnym wyciekiem lub utratą danych, w tym danych osobowych.

UWAGA

Przedstawione zasady są swego rodzaju drogowskazem, który powinien ułatwiać identyfikację zagrożeń oraz podpowiadać, jak im zapobiegać. Jednocześnie zachęcamy do samodzielnego poszerzania wiedzy w tym zakresie, a w razie wątpliwości – do kontaktu ze swoim przełożonym lub wsparciem IT.

Ilustracja na okładce Karol Banach (karolbanach.com)

Projekt i skład Radosław Zbytniewski (zbytniewski.pl)

Redakcja i korekta Ewa Walewska

ISBN: 978-83-943435-7-6

Wydanie I – Warszawa, maj 2020 r.

Spis treści

OTOCZENIE PRACY

Bezpieczeństwo domowej sieci

1. **Upewnij się**, że dostęp do panelu konfiguracyjnego urządzenia sieciowego oraz dostęp do rozgłaszanej sieci bezprzewodowej zabezpieczone są silnym hasłem, którym nie jest hasło domyślne, zdefiniowane przez producenta.

WIĘCEJ

2. **Zweryfikuj**, czy wersja oprogramowania Twojego urządzenia sieciowego jest aktualna, i ewentualnie dokonaj aktualizacji.

WIĘCEJ

3. **Wyłącz** możliwość konfiguracji swojego sprzętu sieciowego z urządzeń znajdujących się poza siecią LAN lub ogranicz taką możliwość tylko do zdefiniowanych adresów IP. W większości przypadków, w zależności od wykorzystywanego sprzętu, takiej konfiguracji dokonasz z wykorzystaniem funkcjonalności ACL (Access Control List). Jeżeli nie wiesz jak to zrobić, a wątki w tym temacie znalezione w Internecie nie są wystarczające, poproś o pomoc dział IT.

4. **Zdefiniuj** urządzenia, które mogą uzyskać dostęp do Twojej sieci, np. z wykorzystaniem filtracji adresów MAC.

WIĘCEJ

OTOCZENIE PRACY

Bezpieczeństwo obszaru przetwarzania

1. **Nie prowadź** służbowych rozmów telefonicznych, w tym wideokonferencji, w miejscach narażonych na brak poufności wymienianych informacji.
2. **Pamiętaj**, aby nie udostępniać służbowych urządzeń osobom postronnym, w tym znajomym, dzieciom lub innym członkom rodziny.
3. **Nie zapominaj** o bezpiecznym przechowywaniu dokumentacji w formie papierowej. W tym celu staraj się korzystać z mebli zamykanych na klucz.
4. **Zapewnij bezpieczne** niszczenie dokumentów papierowych. Jeżeli nie dysponujesz niszczarką dokumentów, lepszym rozwiązaniem będzie ich utylizacja po powrocie do biura, ale nie zapominaj, żeby na czas pracy zdalnej przechowywać je bezpiecznie.

OTOCZENIE PRACY

Bezpieczeństwo stanowiska pracy

1. **Unikaj** spożywania posiłków i napojów w czasie wykonywania swojej pracy. Miej na uwadze, że serwis lub wymiana sprzętu, np. na skutek zalania, w obecnej sytuacji mogą być bardzo utrudnione.

2. **Upewnij się**, że osoby postronne nie mają wglądu w treści wyświetlane na ekranie. Zadbaj o odpowiednie ustawienie ekranu lub zastosuj filtr prywatyzujący.

3. **Nie zapominaj** o polityce czystego ekranu, w tym o konieczności blokowania konta systemowego przed każdorazowym odejściem od stanowiska pracy. Dodatkowo uruchom wygaszacz ekranu, który taką czynność wykona automatycznie w razie braku Twojej aktywności.

SPRZĘT I SYSTEMY INFORMATYCZNE

Procedury bezpiecznego logowania

1. **Upewnij się**, że dostęp do Twojego komputera jest możliwy tylko i wyłącznie z wykorzystaniem indywidualnego identyfikatora oraz hasła. Nie zapominaj o ustawieniu PIN-u lub innej formy uwierzytelniania dla telefonu wykorzystywanego do celów służbowych.

2. **Pamiętaj** o zakazie udostępniania osobom trzecim haseł oraz o konieczności przechowywania ich w miejscach gwarantujących poufność.

3. **Staraj się** budować silne hasła, tj. długie i złożone, które nie będą ciągiem znajdujących się obok siebie znaków na klawiaturze ani nie będą oparte na prostych skojarzeniach, np. numer telefonu, data urodzin, imiona lub nazwiska. Nie zapominaj o cyklicznej zmianie swoich haseł.

SPRZĘT I SYSTEMY INFORMATYCZNE

Bezpieczne przechowywanie danych

1. **Upewnij się**, że nośniki Twoich urządzeń mobilnych, w tym komputera, telefonu lub tabletu, zostały zaszyfrowane.
2. **Nie zapominaj o szyfrowaniu** zewnętrznych kart pamięci, a także innych nośników danych, takich jak pendrive lub dysk zewnętrzny.
3. **Wybierz bezpieczną formę uwierzytelniania** do odszyfrowania nośników. Najpopularniejszą formą uwierzytelniania, a zarazem jedną z bezpieczniejszych, jest hasło.
4. **Nie umieszczaj danych** w publicznych chmurach obliczeniowych, komunikatorach lub innych usługach dostępnych w sieci, które nie są autoryzowane przez Twoją organizację.
5. **Staraj się nie utrwalać danych** na lokalnym dysku komputera. Do tego celu wykorzystuj tylko i wyłącznie wskazane przez Twoją organizację zasoby sieciowe, które podlegają wykonywaniu kopii zapasowych.
6. **Stosuj rozwiązania** umożliwiające zdalne zarządzanie urządzeniami mobilnymi, w tym ich zdalne zlokalizowanie lub przywrócenie do stanu fabrycznego, np. MDM(Mobile Device Management).
7. Jeżeli pracujesz na urządzeniu prywatnym, poproś swoją organizację o regulamin wszystkich **zasad konfiguracji sprzętu**.

SPRZĘT I SYSTEMY INFORMATYCZNE

Ochrona przed cyberatakami

1. **Upewnij się**, że Twoje urządzenia zostały wyposażone w uruchomione oprogramowanie antywirusowe.
2. **Sprawdź**, czy wersja Twojego systemu operacyjnego jest wspierana przez producenta, np. Windows XP lub Windows 7, czy może takie wsparcie już utraciła. np. Windows XP i Windows 7, takiego wsparcia już nie ma.
3. **Zweryfikuj**, czy systemy, z których korzystasz, w tym system operacyjny oraz system antywirusowy, są aktualizowane.
4. Upewnij się, że na Twoim komputerze została uruchomiona **zapora sieciowa**.
5. Nigdy **nie korzystaj z uprawnień administracyjnych** do realizowania swoich codziennych obowiązków. Takie konta powinny być uruchamiane tylko doraźnie, w razie potrzeby.
6. **Nie pobieraj** ani nie instaluj oprogramowania bez zgody działu IT.

PERSONEL

Procedury bezpieczeństwa

1. **Zweryfikuj**, czy masz dostęp do polityk i procedur obowiązujących w Twojej organizacji, oraz przypomnij je sobie.
2. **Upewnij się**, że wiesz, z kim możesz skontaktować się na wypadek nieprzewidzianej awarii lub incydentu.
3. **Nie naprawiaj sprzętu**, na którym znajdują się dane służbowe, z wykorzystaniem wsparcia podmiotów zewnętrznych bez uzyskania wcześniejszej zgody organizacji.
4. **Nie drukuj dokumentów** służbowych w punktach ksero lub z pomocą innych podmiotów/osób trzecich.
5. **Nie zapominaj** o zagrożeniach w sieci, w tym phishingu, na które Twoja sieć domowa może być bardziej podatna niż sieć firmowa.

PERSONEL

Procedury bezpieczeństwa

6. Dokładnie **weryfikuj nadawców** wiadomości mailowych, a w razie wątpliwości nie otwieraj załączników oraz hiperłączy znajdujących się w tekście. Pamiętaj, że zawsze możesz zadzwonić i potwierdzić intencje osoby.

7. **Szyfruj załączniki** wiadomości mailowych, a hasło wysyłaj zawsze inną formą kontaktu, np. SMS.

8. **Nie wysyłaj wiadomości** służbowych na swoje prywatne konta mailowe.

9. **Nie ufaj stronom internetowym**, na których nie zaimplementowano protokołu szyfrującego (poinformuje Cię o tym brak kłódki obok paska adresu), ani nie podawaj na nich danych. Niezależnie od tego dokładnie weryfikuj, czy wprowadzony adres strony jest poprawny i nie ma w nim żadnej literówki.

10. Nigdy i nikomu **nie udostępniaj swojego hasła**, nawet jeśli poprosi Cię o to dział IT.

PRYWATNE URZĄDZENIA

Zasady wykorzystania prywatnego sprzętu komputerowego

W przypadku gdy musisz wykorzystywać sprzęt prywatny do użytku służbowego, zapewnij co najmniej, że:

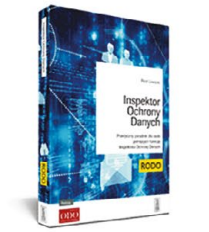
1. wykorzystywane przez Ciebie systemy, w szczególności systemy operacyjne, dysponują wsparciem producenta. **Warto wiedzieć**, że popularny Windows XP takiego wsparcia już nie zapewnia, podobnie jak Windows 7, którego asysta skończyła się w styczniu 2020 r.,
2. wykorzystywane przez Ciebie **systemy podlegają** automatycznej, cyklicznej **aktualizacji**, a jej przebieg nie jest zakłócony żadnymi błędami. W szczególności zwróć uwagę na system operacyjny oraz oprogramowanie antywirusowe,
3. Twój system operacyjny dysponuje uruchomioną **zaporą ogniową**, a na komputerze skonfigurowano oprogramowanie antywirusowe,
4. dostęp do Twojego komputera realizowany jest z wykorzystaniem **hasła dostępowego** znanego tylko i wyłącznie Tobie. Pamiętaj, że jego długość, złożoność i częstotliwość zmiany powinny zapewniać minimalizację ryzyka nieuprawnionego dostępu do danych, np. budowane hasła mogą składać się z co najmniej 8 znaków, w tym małych i dużych liter, cyfr lub znaków specjalnych, a ich zmiana powinna następować w cyklach 30-dniowych,
5. konto systemowe, na którym wykonujesz obowiązki służbowe, jest kontem o **ograniczonych uprawnieniach**, a jedyną osobą posiadającą uprawnienia administracyjne na Twoim komputerze jesteś Ty,

PRYWATNE URZĄDZENIA

Zasady wykorzystania prywatnego sprzętu komputerowego

6. jeżeli nie masz dostępu do zasobów sieciowych organizacji – będziesz systematycznie wykonywać **kopię zapasową**, np. na zewnętrznych, zaszyfrowanych nośnikach danych,
7. dysk Twojego komputera **jest zaszyfrowany**, a odszyfrowanie odbywa się za pomocą np. dodatkowego hasła lub hasła połączonego z tokenem,
8. Twój smartfon ma ustawioną **kontrolę dostępu** (np. PIN, znak graficzny, czytnik linii papilarnych), aktualne oprogramowanie oraz skonfigurowane szyfrowanie pamięci wbudowanej i zewnętrznej (jeśli występuje),
9. Twój komputer i telefon mają ustawiony **wygaszacz ekranu**, który blokuje urządzenie na wypadek kilkuminutowej nieaktywności użytkownika, np. po 5 minutach nieaktywności w przypadku komputera i po 1 minucie nieaktywności w przypadku telefonu,
10. będziesz stosować wszystkie wymienione wyżej **dobre praktyki bezpiecznej pracy zdalnej**. Niezależnie od tego dowiedź się w swojej organizacji, jakie jeszcze wymagania powinieneś spełnić.

Publikacje naszych ekspertów



ODO24.pl/publikacje

Ochrona Danych Osobowych

BEZPIECZEŃSTWO INFORMACJI

Audyt zgodności

Wykonujemy pełny audyt zgodności z RODO. Badamy zarówno bezpieczeństwo urządzeń, systemów, sieci i aplikacji, jak i poprawność klauzul, regulaminów oraz rejestrów. Doradzamy, jak praktycznie wdrożyć nasze zalecenia.

Szkolenia otwarte

Dzielimy się wiedzą, pomagamy w zdobyciu umiejętności i wyposażamy w narzędzia, które umożliwią Państwu skuteczne wykonywanie obowiązków związanych z ochroną danych osobowych.

DPIA i analiza ryzyka

Analizę ryzyka i DPIA rozumiemy jako fundament RODO – sposób na racjonalizację kosztów ochrony danych oraz troskę o prywatność osób, których dane Państwo przetwarzają.

Szkolenia zamknięte

Dostosowujemy je do potrzeb organizacji oraz specyfiki branży, w której działa. Stawiamy na praktykę – Państwa pracownicy nauczą się wykorzystywać wiedzę o RODO w swojej codziennej pracy.

Wdrożenie RODO

Wypełniamy „neutralne" technologicznie RODO. Pomagamy dostosować: procesy biznesowe (np. marketing, rekrutacja), środowisko teleinformatyczne, dokumentację ochrony danych.

E-learning

Nasza platforma pozwala w krótkim czasie (nawet w największej organizacji) przeszkolić personel oraz zweryfikować nabytą wiedzę. Minimalizujemy w ten sposób najczęstszą przyczynę incydentów – nieświadomość pracowników.

Przejęcie funkcji IOD

Pełniąc funkcję IOD, wspomagamy i nadzorujemy organizację w utrzymaniu zgodności z RODO. Działamy szybko i efektywnie dzięki doświadczonym ekspertom z obszaru prawa, IT oraz zarządzania ryzykiem.

Narzędzia

Dostarczamy rozwiązania pozwalające kontrolować przepływ danych w organizacji, w tym prowadzić niezbędne rejestry oraz zarządzać szkoleniami, incydentami, upoważnieniami etc.

Bieżące wsparcie

Dzięki dostarczanym przez nas narzędziom oraz wiedzy jesteśmy w stanie przyczynić się do monitorowania i rozwoju funkcjonującego u Państwa systemu ochrony danych osobowych.

Usługi powiązane

Pomoc w razie kontroli UODO, cyberbezpieczeństwo, wsparcie we wdrożeniu systemu ISO 27001, ISO 20000, ISO 22301, a także dyrektywy NIS.

Jedna specjalizacja

SZEROKA PERSPEKTYWA

- Przepisy prawa
- Bezpieczeństwo sieci i systemów IT
- Zarządzanie ryzykiem
- Bezpieczeństwo fizyczne
- Wiedza i świadomość personelu

ODO24.pl
tel. 22 740 99 00