

Zabezpieczenia fizyczne

Poniższy dokument opisuje środki organizacyjne i zabezpieczenia fizyczne, stosowane przez ADO dla zapewnienia ochrony danych osobowych i bezpieczeństwa informacji na obszarze przetwarzania danych osobowych.

Spis treści

1. Fizyczne zabezpieczenie pomieszczeń.....	2
1.1 System alarmowy	2
1.2 Okna	2
1.3 Monitoring.....	2
2. Dostęp do pomieszczeń.....	2
2. Zarządzanie kluczami.....	2
2.1 Klucze do pomieszczeń.....	2
2.2 Klucze do szafek, szaf lub szuflad	3
3. Sprzątanie pomieszczeń	3
4. Przechowywanie papierowej dokumentacji	3
5. Przechowywanie papierowej dokumentacji archiwalnej.....	4
5.1 Pomieszczenie pełniące rolę archiwum	4
5.2 Dokumentacja archiwalna	4
6. Niszczenie papierowej dokumentacji	5
7. Fizyczne zabezpieczenie serwera	5

1. Fizyczne zabezpieczenie pomieszczeń

1.1 System alarmowy

1. W przypadku wykorzystywania przez ADO systemu alarmowego, możliwość uruchomienia/wyłączenia systemu alarmowego powinna mieć jak najmniejsza liczba osób.
2. W przypadku zakończenia współpracy ADO z osobą znającą kod do alarmu, należy dokonać:
 - 1) zmiany kodu (jeżeli wszystkie osoby używały tego samego kodu) lub
 - 2) zmiany kodu używanego przez osobę, z którą ADO zakończył współpracę (jeżeli osoba ta miała własny kod).
3. Czujki alarmu obejmują swym zasięgiem miejsca, przez które do pomieszczeń ADO mogą dostać się osoby nieupoważnione.
4. Wykorzystywane przez ADO czujki alarmu nie mogą być zasłaniane przez parawany, pudła stojące na szafach itp. przeszkody.

1.2 Okna

Okna znajdujące się na parterze lub w miejscach, do których mogą mieć łatwy dostęp osoby nieupoważnione, powinny zostać zabezpieczone np. poprzez:

- 1) montaż krat w oknach,
- 2) montaż rolet antywłamaniowych,
- 3) montaż folii włamaniowych.

1.3 Monitoring

1. W celu zapewnienia:
 - 1) bezpieczeństwa osób zatrudnionych u ADO,
 - 2) bezpieczeństwa osób korzystających z usług ADO,
 - 3) ochrony mienia ADO,
 - 4) realizacji innych celów przewidzianych przepisami prawa– ADO może stosować monitoring wizyjny.
2. ADO stosuje monitoring wizyjny zgodnie z przepisami prawa, w szczególności Kodeksu pracy lub przepisów branżowych ADO.

2. Dostęp do pomieszczeń

1. W pomieszczeniach ADO, w których na stałe przetwarza się dane osobowe w formie papierowej lub elektronicznej, osoby nieupoważnione mogą przebywać jedynie pod nadzorem osoby upoważnionej.
2. W razie braku możliwości zapewnienia nadzoru nad osobą upoważnioną w pomieszczeniu, o którym mowa w ust. 1, należy zapewnić takiej osobie możliwość oczekiwania na osobę upoważnioną w innym miejscu (np. na sali konferencyjnej, w recepcji lub na korytarzu).

2. Zarządzanie kluczami

2.1 Klucze do pomieszczeń

1. Pomieszczenia ADO, w których na stałe przetwarza się dane osobowe w formie papierowej lub elektronicznej, są zamykane na klucz.
2. Poza godzinami pracy ADO klucze do pomieszczeń, o których mowa w ust. 1, są przechowywane w bezpiecznym miejscu, do którego nie mają dostępu osoby nieupoważnione (np. w wydzielonym kluczniku lub na recepcji).

3. Pozostawianie kluczy w zamkach pomieszczeń, o których mowa w ust. 1 powyżej jest niedopuszczalne w warunkach, w których osoby upoważnione nie mają kontroli nad osobami wchodzącymi do tych pomieszczeń (np. poza godzinami pracy).
4. ADO może wprowadzić politykę kluczy, doprecyzowującą powyższe zasady.
5. W przypadku zapewnienia bezpieczeństwa pomieszczeń, o których mowa w ust. 1, w inny sposób (np. przez wykorzystanie kart dostępu), zasady opisane w niniejszym rozdziale stosuje się odpowiednio.

2.2 Klucze do szafek, szaf lub szuflad

1. Osoby zatrudnione u ADO mają do swojej dyspozycji szafki, szafy lub szuflady zamykane na klucz, gdzie poza godzinami pracy mogą być przechowywane papierowe dokumenty zawierające dane osobowe, informatyczne nośniki danych, komputery przenośne itp.
2. Poza godzinami pracy klucze do szafek, szaf lub szuflad są przechowywane w bezpiecznym miejscu, do którego nie mają dostępu osoby nieupoważnione (np. w wydzielonym szufladzie).
3. Pozostawianie kluczy w zamkach szafek, szaf lub szuflad jest niedopuszczalne w warunkach, w których osoby upoważnione nie mają kontroli nad osobami mającymi dostęp do tych miejsc (np. poza godzinami pracy).
4. W przypadku stosowania innych zabezpieczeń związanych z przechowywaniem dokumentów, nośników itp., zasady opisane w niniejszym rozdziale stosuje się odpowiednio.

3. Sprzątanie pomieszczeń

1. Sprzątanie pomieszczeń, w których na stałe przetwarza się dane osobowe w formie papierowej lub elektronicznej, odbywa się w godzinach pracy ADO, pod nadzorem osoby upoważnionej.
2. Osoby należące do personelu sprząającego zobowiązane są nie dokonywać przetwarzania danych osobowych oraz zachowania informacji, w których posiadanie weszły w związku z wykonywaniem swoich obowiązków w tajemnicy. W tym celu ADO odbiera od tych osób oświadczenia o zachowaniu poufności (zgodnie ze wzorem stanowiącym załącznik do Polityki bezpieczeństwa) lub zapewnia, by stosowne zobowiązanie znalazło się w umowie będącej podstawą wykonywania przez osoby sprząające ich obowiązków.
3. Powyższe zasady stosuje się odpowiednio wobec osób z personelu technicznego, gospodarczego itp., które dla wykonywania swoich obowiązków nie muszą dokonywać przetwarzania danych osobowych.

4. Przechowywanie papierowej dokumentacji

1. Osoby zatrudnione u ADO stosują zasadę czystego biurka. Poza godzinami pracy dokumenty zawierające dane osobowe:
 - 1) które będą wykorzystywane są przechowywane w bezpiecznym miejscu,
 - 2) które nie będą wykorzystywane są niszczone w sposób opisany w rozdziale 6. tego dokumentu.
2. Papierowe dokumenty zawierające dane osobowe są przechowywane:
 - 1) w zapewnionych przez ADO szafkach, szafach lub szufladach zamykanych na klucz,
 - 2) na innych, uzgodnionych z ADO zasadach.
3. Papierowe dokumenty zawierające dane osobowe nie mogą być przechowywane na stałe lub tymczasowo w miejscach, gdzie mogą uzyskać do nich dostęp osoby nieupoważnione (np. przy przezroczystym oknie na parterze lub w niezamykanym regale na publicznie dostępnym korytarzu).

5. Przechowywanie papierowej dokumentacji archiwalnej

5.1 Pomieszczenie pełniące rolę archiwum

1. Pomieszczenie pełniące rolę archiwum powinno zapewnić ochronę dokumentacji archiwalnej przed takimi zjawiskami lub czynnikami jak kurz, infekcja grzybów pleśniowych, zniszczenia powodowane przez owady i gryzonie, zalania, pożary itp., których skutkiem jest zniszczenie lub zniekształcenie treści dokumentacji archiwalnej.
2. W celu zapewnienia ochrony przed zjawiskami lub czynnikami, o których mowa w ust. 1.:
 - 1) pomieszczenie pełniące rolę archiwum nie powinno znajdować się w niezabezpieczonej piwnicy lub na niezabezpieczonym strychu,
 - 2) pomieszczenie pełniące rolę archiwum nie powinno znajdować się w pomieszczeniu, w którym znajduje się instalacja wodociągowa lub kanalizacyjna,
 - 3) dokumentacja nie powinna być przechowywana bezpośrednio na podłodze (najniższa półka powinna znajdować się kilka centymetrów nad podłogą),
 - 4) dokumentacja nie powinna być przechowywana bezpośrednio na półkach (należy ją przechowywać w teczkach, segregatorach, kartonach, pojemnikach itp.).
3. Pomieszczenie pełniące rolę archiwum powinno być zabezpieczone przed dostępem osób nieupoważnionych. W tym celu należy:
 - 1) w miarę możliwości wyposażyć pomieszczenie pełniące rolę archiwum w dodatkowe zabezpieczenia, jak system alarmowy czy drzwi ogniotrwałe,
 - 2) organizować sprzątanie, remonty itp. działania jedynie w obecności i pod nadzorem osób upoważnionych.
4. W pomieszczeniu pełniącym rolę archiwum należy w miarę możliwości utrzymywać parametry, pozwalające na przechowywanie dokumentacji archiwalnej przez okres przewidziany przepisami prawa lub wewnętrznymi regulacjami ADO:
 - 1) temperatura: 14-20 stopni Celsjusza (plus minus 2 stopnie Celsjusza wahania w ciągu 24 godzin),
 - 2) wilgotność względna: 45%-60% (plus minus 5% wahania w ciągu 24 godzin),
 - 3) oświetlenie: świetlówki o obniżonej emisji promieniowania UV, maksymalne natężenie światła nieprzekraczające 200 luksów.
5. Powyższe zalecenia stosuje się odpowiednio w przypadku:
 - 1) przechowywania dokumentacji archiwalnej w pomieszczeniach należących do podmiotu innego niż ADO,
 - 2) przechowywania dokumentacji archiwalnej w wydzielonej szafie lub szafce.

5.2 Dokumentacja archiwalna

1. Dokumentacja archiwalna jest regularnie sprawdzana pod kątem:
 - 1) wystąpienia szkodliwych zjawisk lub czynników,
 - 2) uzyskania dostępu do niej przez osoby nieupoważnione,
 - 3) upływu okresu, po którym – zgodnie z przepisami prawa lub obowiązującą u ADO procedurą – powinna być usunięta.
2. W razie zaistnienia szkodliwych zjawisk lub czynników lub uzyskania dostępu do dokumentacji archiwalnej przez osoby nieupoważnione, których skutkiem jest zniekształcenie lub zniszczenie dokumentacji, ADO:
 - 1) ocenia przyczyny oraz stopień zniekształcenia lub zniszczenia dokumentacji,
 - 2) ocenia możliwość częściowego choćby odtworzenia treści dokumentacji,
 - 3) ustala środki i działania mające na celu uniknięcie podobnych sytuacji w przyszłości,

- 4) na podstawie przeprowadzonej analizy podejmuje stosowne działania zmierzające do częściowego choćby odtworzenia treści dokumentacji i uniknięcia podobnych sytuacji w przyszłości,
 - 5) dokumentuje podjęte w sprawie działania.
3. W przypadku ustalenia, że upłynął okres przechowywania dokumentacji archiwalnej, wynikający z przepisów prawa lub obowiązującej u Administratora procedury, ADO przystępuje do zniszczenia dokumentacji. W sytuacji, gdy dokumentacja niszczona jest:
 - 1) na własną rękę – ADO powołuje komisję likwidacyjną i sporządza protokół zniszczenia (zgodnie ze wzorem stanowiącym załącznik do Polityki bezpieczeństwa),
 - 2) przez zewnętrzny podmiot – ADO zobowiązuje podmiot do przekazania dokumentu potwierdzającego zniszczenie dokumentacji oraz podpisuje z tym podmiotem umowę powierzenia przetwarzania danych osobowych.

6. Niszczenie papierowej dokumentacji

1. Zbędna dokumentacja papierowa (np. błędne wydruki zawierające dane osobowe) musi być niszczona w sposób uniemożliwiający identyfikację osoby, której dotyczyła.
2. W przypadku niszczenia większej liczby dokumentów:
 - 1) na własną rękę – ADO powołuje komisję likwidacyjną oraz sporządza protokół zniszczenia wraz z opisem niszczonej dokumentacji (zgodnie ze wzorem stanowiącym załącznik nr 14 do Polityki bezpieczeństwa),
 - 2) z pomocą zewnętrznego podmiotu – konieczne jest zawarcie z tym podmiotem umowy powierzenia przetwarzania danych osobowych.
3. Niszczenie na własną rękę powinno odbywać się z pomocą niszczarek, spełniających minimum poziom P-3 normy DIN 66399 (szerokość ścinka ≤ 2 mm; powierzchnia ścinka ≤ 320 mm²).
4. ADO powinien zapewnić osobom zatrudnionym liczbę niszczarek gwarantującą, że zbędna dokumentacja będzie niszczona na bieżąco.

7. Fizyczne zabezpieczenie serwera

1. Serwer (komputer główny / jednostka centralna) nie jest wykorzystywany do codziennej pracy (np. sprawdzania poczty lub przeglądania stron internetowych).
2. Serwer jest w miarę możliwości przechowywany w wydzielonym pomieszczeniu, które:
 - 1) będzie zabezpieczone przed dostępem osób nieupoważnionych,
 - 2) zapewni optymalne warunki pracy serwera
 - 3) zabezpieczy serwer przed szkodliwymi czynnikami lub zjawiskami.
3. Realizacja wymogów, o których mowa w ust. 2 powyżej, następuje w szczególności poprzez:
 - 1) zabezpieczenie dostępu do pomieszczenia przez wykorzystanie zamka kodowego lub karty magnetycznej,
 - 2) zabezpieczenie okien pomieszczenia przez ich wyposażenie w kraty lub rolety antywłamaniowe (dla zabezpieczenia przed dostępem osób nieupoważnionych) oraz żaluzje lub rolety (dla zabezpieczenia przed słońcem),
 - 3) zapewnienie w pomieszczeniu temperatury, wilgotności i wentylacji zgodnie ze specyfikacją producenta serwera,
 - 4) stosowanie instalacji elektrycznej, podzielonej na kilka faz i będącej w stanie znieść duże obciążenie,
 - 5) wyposażenie pomieszczenia w urządzenia typu UPS i filtry antyprzepięciowe,
 - 6) zabezpieczenie przed pożarem w zakresie skonsultowanym z inspektorem BHP,
 - 7) umieszczenia serwera w odpowiedniej szafie (np. obudowie typu RACK).