Polityka bezpieczeństwa danych osobowych



# Cel dokumentu

Celem Polityki jest ustanowienie zasad i reguł postępowania zabezpieczających przetwarzanie danych osobowych w MDH. Polityka reguluje sposób upoważniania, postępowania z danymi w formie tradycyjnej oraz nadzoru i prowadzonej w związku z tymi działaniami dokumentacją.

# Zasady przetwarzania danych osobowych

* 1. Administratorem przetwarzanych danych osobowych jest MDH Sp. z o.o.
  2. Obowiązki w zakresie bezpieczeństwa informacji zostały opisane w Polityce Bezpieczeństwa Informacji.
  3. Dostęp do danych osobowych oraz możliwość ich przetwarzania mają tylko osoby posiadające upoważnienie do przetwarzania danych osobowych.
  4. Wniosek o nadanie upoważnienia sporządza KKO. W razie wątpliwości, w celu poprawnego ustalenia zakresu upoważnienia, dokonuje konsultacji z IOD. Podczas zatrudnienia nowego pracownika przygotowywane jest upoważnienie, które zatwierdza Zarząd. Nadawanie uprawnień do systemów informatycznych opisuje Instrukcja zarządzania systemem informatycznym.
  5. Informacje o nowej osobie należy przekazać do IOD.
  6. Po nadaniu upoważnienia nowa osoba zostaje wpisana do ewidencji osób upoważnionych, zgodnie ze wzorem w załączniku nr 5 oraz zgodnie z informacjami przekazanymi od osoby przygotowującej upoważnienie oraz ASI.
  7. W przypadku zmian w zakresie zatrudnienia i związanymi z tym zmianami w zakresie upoważnienia, wymagane jest wydanie nowego upoważnienia, anulując obecne.
  8. W przypadku zakończenia zatrudnienia nadane upoważnienie wygasa automatycznie.
  9. Dane osobowe mogą zostać udostępnione podmiotom zewnętrznym jedynie na podstawie przepisów prawa.
  10. Każda sytuacja przekazania danych osobowych do przetwarzania w zakresie realizowanym przez MDH odbywa się na podstawie zawartej umowy powierzenia danych osobowych.
  11. Naruszenia bezpieczeństwa danych osobowych muszą być zgłaszane niezwłocznie po ich stwierdzeniu lub podejrzeniu ich wystąpienia do KKO lub bezpośrednio przedstawione Zarządowi, zgodnie z Procedurą zarządzania incydentami.
  12. Przetwarzanie danych osobowych podlega bieżącemu nadzorowi realizowanemu przez KKO oraz monitorowaniu realizowanemu przez IOD.
  13. Zbędne wydruki, tj. zawierające błędne dane lub dokumenty, których ważność ustała, nie powinny być gromadzone, ale niszczone w przeznaczonych do tego niszczarkach.
  14. Dokumentacja zawierająca dane osobowe powinna być chroniona przed wglądem osób trzecich. Dokumentacja powinna pozostać w obrębie obszarów przetwarzania.
  15. Na koniec pracy dokumentacja powinna zostać zabezpieczona w zamykanych szafach, szufladach lub archiwach.
  16. Nadzór nad zgodnością przetwarzania danych osobowych względem przyjętych zasad bezpieczeństwa względem podległych pracowników realizuje KKO.

# Obowiązek informacyjny

* 1. KKO są odpowiedzialni za spełnienie obowiązku informacyjnego względem osób, których dane przetwarzają.
  2. Obowiązek informacyjny z artykułu 13 RODO, należy spełnić w momencie pozyskiwania danych od osoby, której one dotyczą.
  3. Zakres przekazywanych informacji obejmuje:
     1. pełną nazwę i dane kontaktowe administratora danych;
     2. dane kontaktowe inspektora ochrony danych;
     3. cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
     4. wskazanie prawnie uzasadnionych interesów, jeśli są podstawą przetwarzania;
     5. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców;
     6. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
     7. okres, przez który dane osobowe będą przechowywane lub kryteria ustalania tego okresu;
     8. informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
     9. jeżeli przetwarzanie odbywa się na podstawie wyrażonej zgody – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
     10. informacje o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;
     11. informację czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
     12. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
  4. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, zgodnie z artykułem 14 RODO należy jej przekazać:
     1. pełną nazwę i dane kontaktowe administratora danych;
     2. dane kontaktowe inspektora ochrony danych;
     3. cele przetwarzania oraz podstawę prawną przetwarzania;
     4. kategorie odnośnych danych osobowych;
     5. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców;
     6. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej;
     7. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
     8. prawnie uzasadnione interesy, jeśli są podstawą przetwarzania;
     9. informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
     10. jeżeli przetwarzanie odbywa się na podstawie wyrażonej zgody, to informacje o prawie do jej cofnięcia w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
     11. informacje o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;
     12. źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
     13. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
  5. Informacje, o których mowa w punkcie 3.4 (przy pozyskiwaniu danych z innego źródła) podaje się:
     1. w rozsądnym terminie po pozyskaniu danych osobowych – do 30 dni, lub
     2. najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą, lub
     3. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
  6. Spełnianie obowiązku informacyjnego odbywa się poprzez:
     1. umieszczanie na wzorach dokumentów (wniosków, kwestionariuszy, umów, itp.) klauzul informacyjnych;
     2. umieszczenie klauzul w ogólnodostępnym miejscu, gdzie przyjmowani są interesariusze;
     3. umieszczenie klauzul na stronie internetowej;
     4. przesyłanie klauzul w formie wiadomości elektronicznych lub tradycyjnych, w odpowiedzi na kontakt osoby;
     5. przekazywanie słowne treści klauzul, jeśli nie jest możliwe zapoznanie osoby przez powyższe sposoby.

# Postępowanie z danymi nadmiarowymi i anonimizacja danych

* 1. Względem celu w jakim przetwarzane są dane osobowe określony został maksymalny zakres danych niezbędny do jego realizacji.
  2. Niezależnie od podstaw prawnych dla realizowanych celów osoby mogą kierować do MDH pisma zawierające dane nadmiarowe względem tych celów.
  3. Dopuszcza się niezwłoczne zastosowanie anonimizacji lub usunięcia przekazanych dokumentów z zasobów MDH.
  4. Powyższe dokonuje się poprzez:
     1. zamazanie danych nadmiarowych na dokumencie zawierającym również dane niezbędne do realizacji celu, przy czym zamazanie musi zapewniać brak możliwości odtworzenia danych;
     2. usunięcie danych poprzez zniszczenie w niszczarce dokumentu lub usunięcie plików z komputera lub poczty elektronicznej, w tym również z „kosza”;
     3. odesłanie nadmiarowych danych – jeśli są one w formie oryginału.
  5. W przypadku stwierdzenia powtarzających się sytuacji przekazywania nadmiarowych danych w konkretnych celach, KKO wraz z IOD podejmuje wybrane działania:
     1. opracowuje formularze ograniczające podawanie nadmiarowych danych;
     2. wskazuje w formie komunikatu na jasne warunki podejmowania decyzji w ramach realizacji celu, tak aby bezpośrednio z nich wynikał brak zasadności podawania dodatkowych danych;
     3. zwraca się do osób z prośbą o nieprzekazywanie danych nadmiarowych

# Realizacja praw osób, których dane dotyczą

* 1. Osobom, których dane są przetwarzane przysługują prawa wynikające z rozdziału III RODO. Są to prawa do żądania od MDH dostępu do swoich danych osobowych oraz informacji o ich przetwarzaniu, prawa do ich sprostowania, usunięcia, przeniesienia, ograniczenia przetwarzania lub prawa do wniesienia sprzeciwu wobec przetwarzania.
  2. Każda osoba, która wystąpi z wnioskiem o skorzystanie z przysługującego jej prawa należy zrealizować w oparciu o „Procedurę realizacji praw osób, których dane dotyczą”.
  3. W przypadku wątpliwości co do zakresu udzielanych informacji lub ich zasadności, wniosek należy skonsultować z KKO lub IOD.

# Zasady udostępniania danych osobowych

* 1. MDH udostępnia przetwarzane dane osobowe tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
  2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej.
  3. Wniosek powinien zawierać informacje, umożliwiające wyszukanie żądanych danych osobowych, wskazywać ich zakres i przeznaczenie oraz podstawę prawną.
  4. Wniosek jest rozpatrywany przez KKO oraz w razie wątpliwości z IOD.
  5. W sytuacjach spornych, decyzję w sprawie udostępnienia podejmuje Zarząd.
  6. Zarząd może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą, innych osób lub byłoby niezgodne z przepisami prawa.

# Zasady powierzenia danych osobowych

* 1. MDH może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej lub na podstawie przepisów prawa, które to powierzenie regulują.
  2. Umowa powierzenia jest wymagana w każdym przypadku, kiedy występuje przekazanie danych osobowych lub ich gromadzenie przez podmiot zewnętrzny.
  3. W przypadkach, kiedy pracownik pomiotu zewnętrznego uzyskuje dostęp do danych osobowych, jednak przetwarzanie odbywa się w obszarze MDH, możliwe jest wydanie upoważnienia.
  4. Zawarta z podmiotem zewnętrznym umowa powierzenia, w związku z RODO czyni ten podmiot Podmiotem Przetwarzającym (PP). Umowa, musi zawierać poniższe elementy:
     1. cel przetwarzania, z zastrzeżeniem zakazu wykorzystania danych w innym celu;
     2. zakres, kategorie oraz charakter powierzanych danych;
     3. odpowiedzialność stron, w tym za przestrzeganie postanowień umownych oraz przestrzeganie obowiązujących przepisów prawa – zwłaszcza w zakresie wdrożenia odpowiednich środków technicznych i organizacyjnych zabezpieczających dane osobowe;
     4. konieczność upoważnienia przez PP, osób przetwarzających dane w jego imieniu oraz zobowiązanie ich do zachowania poufności;
     5. zakaz korzystania z podwykonawców bez pisemnej zgody lub aneksu do umowy;
     6. konieczność uczestniczenia PP w wypełnianiu obowiązków ciążących na MDH jako administratorze danych, w tym realizacji praw osób, których dane dotyczą oraz przekazywania informacji o sposobach przetwarzania oraz informacji potrzebnych do szacowania ryzyka i oceny skutków naruszeń;
     7. zgłaszanie wszelkich incydentów lub podejrzeń incydentów, z zapewnieniem wszystkich niezbędnych informacji do poprawnej realizacji zgłaszania incydentów zgodnie z przepisami prawa;
     8. sposób potwierdzania przestrzegania przepisów prawa i zasad bezpieczeństwa, w tym umożliwienie monitorowania, audytowania PP;
     9. konieczność usunięcia lub zwrócenia powierzonych danych osobowych w przypadku wygaśnięcia umowy lub jej rozwiązania.
  5. Wzór umowy powierzenia danych osobowych stanowi Załącznik nr 4.
  6. Każdy Podmiot Przetwarzający oraz ewentualni podwykonawcy zostają wpisani do rejestru podmiotów przetwarzających prowadzonego przez IOD zgodnie z Załącznikiem nr 3.

# Ewidencjonowanie procesów przetwarzania danych osobowych

* 1. Osoby odpowiedzialne za procesy przetwarzania danych osobowych są zobowiązani do zgłoszenia do Zarządu:
     1. planowanego utworzenia nowych procesów danych osobowych lub usunięcia istniejących;
     2. wnoszenia zmian w procesach już istniejących, np. rozszerzenia lub zmniejszenia zakresu procesów, co może wynikać z przepisów prawa;
     3. planowanych zmian w zakresie procesów przetwarzania danych, w tym utworzenia nowych lub zakończenia istniejących.
  2. Na podstawie powyższych informacji wyznaczona przez Zarząd osoba, dokonuje aktualizacji prowadzonego Rejestru Czynności Przetwarzania lub opiniuje planowane zmiany pod kątem wdrożenia dodatkowych zabezpieczeń.
  3. Rejestr jest prowadzony w formie elektronicznej zgodnie ze wzorem z załącznika nr 6 do Polityki bezpieczeństwa danych osobowych.

# Ochrona pomieszczeń

* 1. Wszystkie pomieszczenia, w których przetwarzane są dane osobowe zostały wyposażone w drzwi z zamkiem oraz posiadają środki ochrony przeciwpożarowej.
  2. Dostęp do budynku jest monitorowany za pomocą systemu alarmowego.
  3. Dokumentację zawierającą dane osobowe należy przechowywać w szafach lub szufladach zamykanych na klucz.
  4. Klucze do szaf, w których przechowywane są dane osobowe posiadają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z upoważnieniem.
  5. Poza godzinami pracy kontrolę nad obiektem sprawuje grupa interwencyjna.
  6. Przebywanie w pomieszczeniach, w których przetwarzane są dane osobowe, osób trzecich jest możliwe tylko w obecności osoby upoważnionej. W szczególności niedozwolone jest pozostawianie bez nadzoru osób trzecich w tym pomieszczeniach.
  7. Pomieszczenia te, powinny być zamykane na czas nieobecności w nich osób upoważnionych, w sposób uniemożliwiający uzyskanie dostępu do nich osób trzecich.
  8. Przy opuszczaniu pomieszczeń i budynku, osoba ostatnia powinna się upewnić, że zostały zamknięte drzwi.

# Wydruki dokumentów zawierających dane osobowe

* 1. Drukarki nie mogą być pozostawione bez kontroli, jeśli są lub wkrótce będą drukowane na nich dane osobowe z systemu informatycznego, o ile dostęp osób postronnych do pomieszczeń drukarek nie jest odpowiednio ograniczony.
  2. Wydruki z systemu informatycznego zawierające dane osobowe po zakończeniu pracy powinny być przechowywane w zamkniętych szafach, jeśli jest to możliwe.
  3. Wydruki, notatki, kserokopie dokumentów itp. niewykorzystane, a zawierające dane osobowe, muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści.

# Sankcje

* 1. Nieprzestrzeganie zasad bezpieczeństwa opisanych w dokumentacji SZBI oraz przepisów prawa określających ochronę danych osobowych stanowi naruszenie obowiązków pracowniczych i może być przyczyną postępowania dyscyplinarnego lub wiązać się z konsekwencjami określonymi przepisami Ustawy lub RODO.

**25 maja 2018, Łódź Zarząd**

Piotr Baczyński

Anetta Włodarczyk

Mariusz Gierałt