POLITYKA OCHRONY DANYCH OSOBOWYCH

WPROWADZENIE

1. Polityka ochrony danych osobowych jest elementem systemu zarządzania bezpieczeństwem informacji oraz integralną częścią polityki bezpieczeństwa informacji.

ROZDZIAŁ I

CZĘŚĆ OGÓLNA (1-11 RODO)

PRZEDMIOT I CELE

1. W niniejszej polityce ustanowione zostają uregulowania wewnętrzne dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.
2. Niniejsza polityka zapewnić ma ochronę prawa i wolności osób fizycznych związku z przetwarzaniem ich danych osobowych.
3. Niniejsza polityka ma zapewnić przestrzeganie przepisów związanych z przetwarzaniem danych osobowych a w szczególności przepisów 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).

MATERIALNY ZAKRES ZASTOSOWANIA

4. Niniejsza polityka ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

TERYTORIALNY ZAKRES ZASTOSOWANIA

5. Niniejsza polityka ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.

DEFINICJE

6. Na użytek niniejszej polityki:
    a. **System Zarządzania Bezpieczeństwem Informacji lub SZBI** oznaczać będzie strategie działania, której celem jest zapewnienie właściwej ochrony informacji. Strategia ta ma zapewnić ciągłe doskonalenie podjętych działań i procedur w celu optymalizacji ryzyk związanych z naruszeniem poufności.
    b. **Polityka Bezpieczeństwa Informacji lub PBI** oznaczać będzie zbiór spójnych, precyzyjnych i zgodnych z obowiązującym prawem przepisów, reguł, procedur i zasad, według których organizacja zarządza i udostępnia swoje zasoby informacji.
    c. **Polityka Ochrony Danych Osobowych lub PODO** oznaczać będzie niniejszy dokument oraz część PBI dotycząca danych osobowych jako jednej z kategorii informacji.
    d. **Rozporządzenie 2016/679 lub RODO** oznaczać będzie Rozporządzenie 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);

e. **pełnomocnik administratora** – osoba, która zgodnie z przepisami krajowymi lub unijnymi może reprezentować administratora;
f. **jednostka przetwarzająca** – organizacja kierowana przez administratora;
g. **obowiązek informacyjny** – należy przez to rozumieć obowiązek prawny administratora wynikający z art. 12-14 rozporządzenia RODO, w związku z którym administrator musi przekazać określony zakres informacji o przetwarzaniu osobie fizycznej, której dane przetwarza;
h. **praca zdalna** – praca wykonywana poza stałym miejscem wykonywania pracy, lub praca wykonywana bez stałego miejsca pracy;

7. Definicje nie uregulowane w niniejszej polityce należy interpretować zgodnie z rozporządzeniem 2016/679.

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

8. Przetwarzając dane osobowe każdy zobowiązany jest przestrzegać następujących zasad (zwane dalej „zasady przetwarzania"):
   a. dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby fizycznej, której dane dotyczą – **zasad zgodności z prawem, rzetelności i przejrzystości;**
   b. dane osobowe mogą być zbierane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie mogą być przetwarzane dalej w sposób niezgodny z tymi celami – **zasada ograniczenia celu**;
   c. dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane – **zasada minimalizacji danych**;
   d. dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane - należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania zostały niezwłocznie usunięte lub sprostowane – **zasada prawidłowości**;
   e. dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane – **zasada ograniczenia przechowywania**;
   f. dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych – **zasada integralności i poufności**.

WARUNKI PRZETWARZANIA DANYCH OSOBOWYCH

9. Przed rozpoczęciem przetwarzania danych osobowych a także w trakcie ich przetwarzania każdy zobowiązany jest upewnić się, że przetwarzanie odbywa się na podstawie i w granicach prawa powszechnie obowiązującego.
10. Przetwarzanie danych osobowych odbywa się na podstawie i w granicach prawa, jeżeli spełniony jest jeden z następujących warunków:
    a. osoba, której dane osobowe dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w określonym celu (zwany dalej „**warunkiem zgody**");
    b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane osobowe dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (zwany dalej „**warunkiem umowy**");

c. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (zwany dalej „**warunek obowiązku prawnego**");
d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej (zwany dalej „**warunek ochrony żywotnego interesu**");
e. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (zwany dalej „**warunkiem interesu publicznego**");
f. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią (zwany dalej „**warunkiem prawnie uzasadnionego interesu**").

11. Przetwarzając dane osobowe na podstawie warunku zgody należy przestrzegać następujących zasad (zwane dalej „**zasady wyrażenia zgody**"):
    a. wyrażenie zgody musi być całkowicie dobrowolne i nieuzależnione od innych czynności prawnych;
    b. zgodę wyrazić może jedynie osoba posiadająca zdolność do czynności prawnych;
    c. w przypadku osób nieposiadających zdolności do czynności prawnych, zgodę w ich imieniu wyrazić może jedynie ich prawny opiekun;
    d. fakt wyrażenia zgody zawsze musi być udokumentowany;
    e. jeżeli zgodę wyrażono w pisemnym oświadczeniu, to zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem;
    f. zgodę wycofać można w każdym czasie bez żadnych konsekwencji prawnych o czym należy poinformować osobę, której zgoda dotyczy przed jej wyrażeniem;
    g. wycofanie zgody musi być co najmniej tak łatwe jak jej wyrażenie.
12. W przypadku nieprzestrzegania zasad wyrażenia zgody, wyrażona zgoda nie będzie wiążąca i zabronione jest przetwarzanie danych osobowych na jej podstawie.
13. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.
14. Warunek uzasadnionego interesu prawnego nie ma zastosowania do przetwarzania danych osobowych w ramach realizowanych zadań publicznych lub sprawowanej władzy publicznej.
15. W przypadku przetwarzania danych osobowych w ramach warunku interesu publicznego i obowiązku prawnego podstawa prawna musi być określona w prawie krajowym lub prawie Unii.
16. W przypadku przetwarzania danych osobowych w ramach warunku interesu publicznego cel przetwarzania musi być określony w podstawie prawnej lub przetwarzanie musi być niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.
17. Jeżeli przepisy krajowe lub unijne wskazują inne szczególne warunki przetwarzania danych osobowych (takie jak np.: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem), to należy spełnić te warunki.

WARUNKI PRZETWARZANIA SZCZEGÓLNYCH KATEGORII DANYCH OSOBOWYCH

18. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby (zwane dalej „**szczególne kategorie danych osobowych**").
19. Zakaz przetwarzania szczególnych kategorii danych osobowych nie obowiązuje w zakresie w jakim spełniony zostanie jeden z następujących warunków:
    a. osoba, której dane dotyczą, wyrazi zgodę na przetwarzanie tych danych osobowych, chyba że prawo przewiduje, iż osoba, której dane dotyczą, nie może uchylić zakazu;
    b. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone lub wymagane prawem;
    c. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, a osoba, której dane dotyczą jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
    d. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
    e. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
    f. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym na podstawie obowiązujących przepisów prawa;
    g. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie przepisów prawa lub zgodnie z umową z pracownikiem służby zdrowia;
    h. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego na podstawie obowiązujących przepisów prawa;
    i. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych oraz do celów statystycznych na podstawie obowiązującego prawa.
20. Przetwarzanie danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa, wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem.

ROZDZIAŁ II

PRAWA OSÓB FIZYCZNYCH (art. 12 – 22 RODO)

OBOWIĄZEK INFORMACYJNY

21. Pobierając dane osobowe należy udzielić niezbędnych informacji dotyczących przetwarzania danych osobowych osobie, której dane osobowe dotyczą (zwane dalej „**obowiązek informacyjny**").
22. Zakres informacji, który należy udzielić w ramach obowiązku informacyjnego jest następujący:
    a. tożsamość i dane kontaktowe administratora;
    b. dane kontaktowe inspektora ochrony danych;
    c. cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
    d. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców;

e. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe kryteria ustalania tego okresu;
f. jeżeli przysługują to informacje o prawie do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, prawie do cofnięcia zgody (jeżeli na niej opiera się przetwarzanie) oraz o prawie wniesienia skargi do organu nadzorczego;
g. jeżeli będzie występować to 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.

23. Jeżeli dane osobowe są pobierane bezpośrednio od osoby, której dane osobowe dotyczą to należy jej dodatkowo udostępnić 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.
24. Jeżeli dane osobowe są pobierane z innego źródła niż osoba, której dane dotyczą to należy dodatkowo udostępnić informacje dotyczące kategorii przetwarzanych danych osobowych oraz źródle ich pochodzenia.
25. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji wynikających z obowiązku informacyjnego.
26. Nie jest koniecznym realizowanie obowiązku informacyjnego w zakresie w jakim osoba, której dane dotyczą dysponuje informacjami dotyczącymi przetwarzania jej danych osobowych.
27. Jeżeli dane osobowe zostały pobrane z innego źródła niż osoba fizyczna, której dane osobowe dotyczą to nie ma wymogu realizacji obowiązku informacyjnego, jeżeli zostanie spełniony jeden z poniższych warunków:
    a. udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
    b. pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem, któremu podlega administrator,
    c. dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie, w tym ustawowym obowiązkiem zachowania tajemnicy.
28. Obowiązek informacyjny realizowany jest najpóźniej podczas pobierania danych osobowych chyba, że dane zostały pozyskane z innego źródła niż osoba fizyczna, której dane dotyczą, w takim wypadku obowiązek informacyjny realizujemy:
    a. bez zbędnej zwłoki, ale nie później niż w ciągu miesiąca od pozyskania danych osobowych;
    b. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
    c. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
29. Udzielanie wszelkich informacji w ramach obowiązku informacyjnego musi się odbywać w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
30. Realizacja obowiązku informacyjnego musi być udokumentowana w taki sposób, aby była możliwość wykazania, że faktycznie nastąpiła jego realizacja w stosunku do każdej konkretnej osoby fizycznej, której dane osobowe są przetwarzane.

ZASADY OGÓLNE PRAW (ŻĄDAŃ) OSÓB FIZYCZNYCH

31. Każda osoba fizyczna, której dane osobowe są przetwarzane, gdy jest to zasadne, może żądać realizacji jej praw przysługujących jej na podstawie art. 15-22 RODO (zwane dalej „**żądania RODO**").
32. Jeżeli zachodzą uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości tej osoby.
33. Należy ułatwiać realizację żądań RODO osobom fizycznym, których dane osobowe dotyczą, tym samym zabronione jest odmawianie przyjęcia wniosków czy realizacji procedur z powodu np. niezachowania wymogów formalnych czy nie zastosowania odpowiedniego druku.
34. Odpowiedzi dotyczące żądań RODO przekazujemy w sposób wskazany przez osobę, której dane dotyczą chyba, że nie został wskazany sposób udzielenia odpowiedzi to:
    a. odpowiedzi udzielamy na adres e-mail osoby, której dane dotyczą chyba, że nie został przekazany adres e-mail to;
    b. odpowiedzi udzielamy na adres do doręczeń elektronicznych, o którym mowa w KPA chyba, że nie został taki udostępniony to;
    c. odpowiedzi udzielamy na adres wskazany do korespondencji tradycyjne chyba, że nie został taki udostępniony to;
    d. odpowiedzi udzielamy ustnie poprzez wskazany telefon kontaktowy chyba, że nie został taki udostępniony to;
    e. odpowiedź pozostawiamy do osobistego odbioru z adnotacją „brak jakichkolwiek danych komunikacyjnych".
35. Bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela się osobie, której dane dotyczą, informacji o działaniach podjętych w związku z jej żądaniem RODO.
36. W razie potrzeby termin realizacji żądania RODO można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań, ale w terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu z podaniem przyczyn opóźnienia.
37. Jeżeli nie podejmuje się działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie, najpóźniej w terminie miesiąca od otrzymania żądania informuje się osobę, której dane dotyczą o powodach nie podjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.
38. Wszelkie działania wynikające z przyjęcia, rozpatrzenia i realizacji żądań RODO oraz z tym związana komunikacja są wolne od opłat.
39. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter to można odmówić podjęcia działań związku z tym żądaniem.

PRAWO DOSTĘPU

40. Osoba, której dane osobowe dotyczą jest uprawniona do uzyskania:
    a. potwierdzenia, czy są przetwarzane jej dane osobowe;
    b. dostępu do jej danych osobowych;
    c. informacji dotyczących przetwarzania jej danych osobowych.
41. Zakres informacji do jakich może mieć dostęp osoba, której dane osobowe są przetwarzane jest następujący:
    a. cel przetwarzania;
    b. kategorie danych osobowych;
    c. informacje o odbiorcach danych lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną przekazane;

d. planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
e. informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania oraz informacje o prawie wniesienia skargi do organu nadzorczego;
f. jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
g. 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;
h. jeżeli dane osobowe są lub będą przekazywane do państwa trzeciego lub organizacji międzynarodowej informacje o odpowiednich zabezpieczeniach związanych z przekazaniem.

42. W ramach dostępu do danych osobowych osobie, której dane osobowe dotyczą udostępniana jest kopia danych osobowych.
43. Kopia danych osobowych udostępniana jest w sposób i formie wskazanej przez osobę, której dane dotyczą chyba, że nie jest to technicznie możliwe lub wymagało niewspółmiernie dużego wysiłku lub nakładu finansowego.
44. Prawo do kopii danych osobowych nie może niekorzystnie wpływać na prawa i wolności innych a w szczególności na prawo do prywatności.

PRAWO DO SPROSTOWANIA

45. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
46. Z uwzględnieniem celów przetwarzania osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
47. Należy poinformować o sprostowaniu danych osobowych każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
48. Informuje się osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą tego zażąda.

PRAWO DO USUNIĘCIA („BYCIA ZAPOMNIANYM")

49. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego usunięcia dotyczących jej danych osobowych i bez zbędnej zwłoki należy je usunąć, jeżeli zachodzi jedna z następujących okoliczności:
    a. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
    b. osoba, której dane dotyczą, cofnęła zgodę, na której wyłącznie opiera się przetwarzanie;
    c. osoba, której dane dotyczą, wnosi zasadny sprzeciw wobec przetwarzania jej danych osobowych;
    d. dane osobowe były przetwarzane niezgodnie z prawem;
    e. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie, któremu podlega administrator;
    f. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

50. Nie ma zastosowania powyższy paragraf w zakresie w jakim przetwarzanie danych osobowych jest niezbędne:
    a. do korzystania z prawa do wolności wypowiedzi i informacji;
    b. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa, któremu podlega administrator lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
    c. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z prawem, któremu podlega administrator;
    d. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z obowiązującym prawem o ile prawdopodobne jest, że realizacja żądania uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
    e. do ustalenia, dochodzenia lub obrony roszczeń.
51. Należy poinformować o usunięciu danych osobowych każdego odbiorcę, któremu ujawniono dane osobowe chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
52. Informuje się osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą tego zażąda.

PRAWO DO OGRANICZENIA PRZETWARZANIA

53. Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania w następujących przypadkach:
    a. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający sprawdzić prawidłowość tych danych;
    b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
    c. administrator nie potrzebuje już danych osobowych do celów przetwarzania ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
    d. osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
54. Jeżeli na podstawie złożonego żądania przetwarzanie danych osobowych zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania:
    a. wyłącznie za zgodą osoby, której dane dotyczą
    b. w celu ustalenia, dochodzenia lub obrony roszczeń
    c. w celu ochrony praw innej osoby fizycznej lub prawnej
    d. z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.
55. Przed uchyleniem ograniczenia przetwarzania należy poinformować o tym osobę fizyczną, której dane osobowe dotyczą (która żądała ograniczenia przetwarzania jej danych osobowych).
56. Należy poinformować o ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
57. Informuje się osobę, której dane dotyczą, o tych odbiorcach jeżeli osoba, której dane dotyczą tego zażąda.

PRAWO DO PRZENOSZENIA DANYCH OSOBOWYCH

58. Jeżeli przetwarzanie danych osobowych odbywa się w sposób zautomatyzowany, a podstawą prawną przetwarzania tych danych jest zgoda osoby, której dane dotyczą lub umowa, której stroną jest ta osoba fizyczna to ma ona prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła

administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.

59. Wykonując prawo do przenoszenia danych wynikające z powyższego paragrafu, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.
60. Prawo do przenoszenia danych osobowych nie może niekorzystnie wpływać na prawa i wolności innych a w szczególności na prawo do prywatności.

PRAWO DO SPRZECIWU

61. Osoba, której dane dotyczą ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania dotyczących jej danych osobowych, opartego na warunku interesu publicznego lub uzasadnionego prawnie interesu (art. 6 ust. 1 lit. e) lub f) RODO).
62. Nie wolno przetwarzać danych osobowych w stosunku do których został wniesiony sprzeciw, chyba że zostanie wykazane istnienie:
    a. ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą lub;
    b. podstaw do ustalenia, dochodzenia lub obrony roszczeń.
63. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.
64. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.
65. Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na podstawie prawa, osoba, której dane dotyczą, ma prawo wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI

66. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.
67. Powyższy paragraf nie ma zastosowanie jeżeli ta decyzja:
    a. jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
    b. jest dozwolona prawem, któremu podlega administrator;
    c. opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

ROZDZIAŁ III

ŚRODKI (PROCEDURY) BEZPIECZEŃSTWA

68. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych odbywało się zgodnie z RODO (zwane dalej „**środki bezpieczeństwa**”).
69. Ustalając odpowiednie środki bezpieczeństwa uwzględnia się:
    a. charakter, zakres, kontekst i cele przetwarzania

b. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia
c. stan wiedzy technicznej
d. koszty wdrożenia
e. obowiązki wynikające z zasad przetwarzania danych osobowych
f. warunki uprawniające do przetwarzania danych osobowych.

70. Ustalanie odpowiednich środków bezpieczeństwa odbywa się przed rozpoczęciem przetwarzania danych osobowych oraz w razie potrzeby w trakcie przetwarzania danych.
71. Środki bezpieczeństwa ustalane są w odrębnych procedurach (zwane dalej „**procedury bezpieczeństwa**"), które w razie potrzeby są poddawane przeglądom i uaktualnienia.
72. Procedury bezpieczeństwa obejmują wszystkie procesy w ramach, których odbywa się przetwarzanie danych osobowych oraz regulują szczegółowo obowiązki wynikające bezpośrednio z RODO.
73. Procedury bezpieczeństwa są dokumentacją poufną, dostępną tylko dla osób uprawnionych, chyba, że inaczej stanowią poszczególne procedury.
74. Procedury bezpieczeństwa mogą być dokumentacją regulującą wyłącznie elementy bezpieczeństwa danych osobowych, ale również mogą stanowić część dokumentacji regulującej inne obszary prowadzonej działalności.

ROZDZIAŁ IV

REJESTROWANIE CZYNNOŚCI PRZETWARZANIA

REJESTR CZYNNOŚCI PRZETWARZANIA

75. Administrator prowadzi rejestr wszystkich czynności przetwarzania (zwany dalej „RCP").
76. W RCP zawiera się wszystkie następujące informacje:
    a. dane identyfikacyjne i kontaktowe administratora;
    b. dane kontaktowe inspektora ochrony danych;
    c. cele przetwarzania;
    d. kategorie osób fizycznych, których dane osobowe dotyczą;
    e. kategorie danych osobowych;
    f. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
    g. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
    h. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa;
    i. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń.
77. RCP musi być dostępny w formie papierowej i elektronicznej.
78. RCP jest dokumentem poufnym i dostępnym tylko dla osób upoważnionych.
79. RCP udostępniany jest każdorazowo na żądanie organu nadzorczego i w formie przez niego wskazanej.

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

80. Jeżeli administrator występuje w roli podmiotu przetwarzającego to prowadzi rejestr wszystkich kategorii czynności przetwarzania (zwany dalej „RKC") dokonywanych w imieniu administratora, który zlecił mu przetwarzanie danych osobowych.

81. W RKC zawiera się wszystkie następujące informacje:
    a. dane identyfikacyjne i kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający,
    b. dane identyfikacyjne i kontaktowe inspektora ochrony danych;
    c. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
    d. gdy ma to zastosowanie –przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
    e. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
82.
83. RKC musi być dostępny w formie papierowej i elektronicznej.
84. RKC jest dokumentem poufnym i dostępnym tylko dla osób upoważnionych.
85. RKC udostępniany jest każdorazowo na żądanie organu nadzorczego i w formie przez niego wskazanej.
86. RKC udostępniany jest każdorazowo na żądanie administratora i w formie przez niego wskazanej, w zakresie w jakim on go dotyczy.

ROZDZIAŁ V

INSPEKTOR OCHRONY DANYCH

WYZNACZENIE IOD

87. Administrator zgodnie art. 37 RODO wyznaczył i będzie wyznaczał inspektora ochrony danych..
88. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia ustawowych zadań.
89. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.
90. Administrator publikuje dane kontaktowe inspektora ochrony danych i powiadamiają o nich organ nadzorczy.

STATUT IOD

91. Administrator i podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
92. Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań ustawowych zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
93. Administrator oraz podmiot przetwarzający zapewniają aby inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania swoich zadań.
94. Inspektor ochrony danych nie jest odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań.
95. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

96. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.
97. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.

ZADANIA IOD

98. Inspektor ochrony danych ma następujące zadania ustawowe
    a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
    b) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    c) udzielanie na żądanie ,zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
    d) współpraca z organem nadzorczym;
    e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
99. Inspektor ochrony danych może wykonywać inne zadania i obowiązki, ale administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.
100. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

ROZDZIAŁ VI

PRZEGLĄDY I AKTUALIZACJE

101. Administrator regularnie testuje, mierzy i ocenia skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
102. Administrator dokonuje regularnych przeglądów polityki ochrony danych i procedur bezpieczeństwa.
103. Przeglądy, testy lub oceny wykonywane są w regularnych odstępach czasu, w sposób zaplanowany i pod nadzorem inspektora ochrony danych.
104. Administrator decyduje w jakich odstępach czasu wykonywane są przeglądy oraz kto jest za nie odpowiedzialny i w jakim zakresie.
105. W wyniku przeglądów administrator dokonuje aktualizacji polityk, procedur i środków bezpieczeństwa, chyba że nie jest to wymagane.
106. Z przeprowadzonych przeglądów sporządza się dokumentację dowodową obejmującą:
    a. zakres obszaru podlegającemu przeglądowi;
    b. sposób przeprowadzenia przeglądu;
    c. czas trwania przeglądu;
    d. osoby przeprowadzające przegląd i w nim uczestniczące;
    e. wyniki przeprowadzonego przeglądu;

f. wnioski i zalecenia z przeglądu.

107. Jeżeli jest to wymagane lub uzasadnione dokonuje się stosownych przeglądów, zgodnie z obowiązującymi procedurami.