POLITYKA BEZPIECZEŃSTWA Dawno Temu App

w odniesieniu do przetwarzania danych osobowych w zakresie usług komunikacji elektronicznej

1. Definicje pojęć

1.1. **Administrator** — podmiot, który decyduje o celach i środkach przetwarzania danych osobowych, w tym zarządza ich ochroną zgodnie z przepisami prawa, w szczególności RODO, PKE oraz innymi obowiązującymi przepisami dotyczącymi ochrony danych i prywatności w komunikacji elektronicznej. Administrator jest również odpowiedzialny za zarządzanie ryzykiem oraz wdrażanie odpowiednich środków technicznych i organizacyjnych.

1.2. **Dane osobowe** — informacje dotyczące osoby fizycznej zidentyfikowanej lub możliwej do zidentyfikowania na podstawie specyficznych cech, takich jak: cechy fizyczne, fizjologiczne, genetyczne, psychiczne, ekonomiczne, kulturowe lub społeczne. Obejmuje m.in. wizerunek, nagrania głosu, dane kontaktowe, dane lokalizacyjne, informacje zawarte w korespondencji oraz dane zebrane za pomocą urządzeń rejestrujących lub podobnych technologii. W kontekście usług komunikacji elektronicznej obejmują także metadane komunikacyjne oraz dane o ruchu.

1.3. **Inspektor Ochrony Danych (IOD)** — osoba powołana przez Administratora do nadzorowania przestrzegania przepisów dotyczących ochrony danych osobowych w jego strukturach, odpowiedzialna za wykonywanie obowiązków określonych w art. 39 RODO, w tym za wdrażanie środków ochrony danych w komunikacji elektronicznej oraz współpracę z innymi organami nadzorczymi.

1.4. **Organ nadzorczy** — Prezes Urzędu Ochrony Danych Osobowych lub inny właściwy organ odpowiedzialny za nadzór nad ochroną danych osobowych, w tym także organy zajmujące się nadzorem nad przetwarzaniem danych w sektorze komunikacji elektronicznej, takie jak Prezes Urzędu Komunikacji Elektronicznej.

1.5. **Podmiot danych** — osoba fizyczna, której dane osobowe są przetwarzane przez Administratora. Podmiot danych posiada szereg praw, w tym prawo do sprzeciwu wobec przetwarzania jego danych w celach marketingowych oraz prawo do bycia zapomnianym.

1.6. **Polityka** — niniejszy dokument określający zasady ochrony danych osobowych w ramach działalności Administratora, zgodny z obowiązującymi przepisami prawa, w tym z RODO, PKE oraz dyrektywą o e-Prywatności.

1.7. **RODO** — rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. dotyczące ochrony osób fizycznych w kontekście przetwarzania danych osobowych oraz swobodnego przepływu tych danych, uchylające dyrektywę 95/46/WE. W sektorze komunikacji elektronicznej RODO współistnieje z przepisami dyrektywy o e-Prywatności, która określa zasady dotyczące przetwarzania danych o ruchu oraz metadanych komunikacyjnych.

1.8. **PKE**- ustawa z dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej (Dz. U. poz. 1221).

1.9. **Pracownik** — osoba fizyczna zatrudniona przez Administratora na podstawie umowy o pracę, wykonująca zadania związane z działalnością Administratora, mająca obowiązek przestrzegania Polityki bezpieczeństwa i zasad ochrony danych osobowych.

1.10. **Współpracownik** — osoba fizyczna świadcząca usługi na rzecz Administratora na podstawie umów cywilnoprawnych, takich jak umowa zlecenia czy umowa o dzieło, mająca dostęp do danych osobowych i zobowiązana do przestrzegania przepisów ochrony danych zgodnie z zawartymi umowami powierzenia.

1.11. **Usługi komunikacji interpersonalnej (usługi OTT-1)** — usługi umożliwiające bezpośrednią, interaktywną wymianę informacji pomiędzy użytkownikami za pośrednictwem sieci telekomunikacyjnej, takie jak komunikatory internetowe, usługi poczty elektronicznej i inne narzędzia umożliwiające komunikację na odległość. Przetwarzanie danych w ramach tych usług podlega rygorystycznym regulacjom dotyczącym ochrony prywatności i danych osobowych.

1.12. **Dane o ruchu** — dane przetwarzane w celu przekazywania komunikatów za pośrednictwem sieci telekomunikacyjnej, w tym dane lokalizacyjne, czas trwania połączenia, dane identyfikujące odbiorcę komunikacji i inne informacje techniczne dotyczące przesyłania sygnałów. Przetwarzanie tych danych podlega szczególnym zasadom ochrony zgodnie z dyrektywą o e-Prywatności.

1.13. **Metadane komunikacyjne** — dane generowane w trakcie korzystania z usług komunikacji elektronicznej, obejmujące m.in. adres IP, informacje o urządzeniach i protokołach używanych przez użytkowników. Metadane te, mimo że nie zawierają treści komunikatów, mogą ujawniać wiele

informacji o aktywności i zachowaniach użytkowników, dlatego ich przetwarzanie jest ściśle regulowane.

1.14. **Cookies i inne technologie śledzące** — pliki i technologie wykorzystywane do zbierania i przechowywania informacji o użytkownikach, ich preferencjach i aktywności online. W zależności od ich rodzaju, stosowanie cookies wymaga uzyskania zgody użytkownika zgodnie z przepisami dyrektywy o e-Prywatności.

1.15. **Dane o lokalizacji** — informacje wskazujące na położenie geograficzne urządzenia użytkownika, przetwarzane przez sieci komunikacji elektronicznej lub urządzenia przetwarzające dane. Przetwarzanie tych danych wymaga zgody użytkownika i jest ściśle regulowane.

1.16. **Tajemnica komunikacji elektronicznej** — zakaz przechwytywania, nagrywania, przechowywania i nadzorowania komunikatów przesyłanych przez użytkowników bez ich zgody, z wyjątkiem przypadków przewidzianych w przepisach prawa. Zasada ta obejmuje wszystkie formy danych związanych z komunikacją, w tym metadane.

1.17. **Zgoda użytkownika** — dobrowolne, świadome i jednoznaczne wyrażenie woli, poprzez które użytkownik wyraża zgodę na przetwarzanie jego danych osobowych, w tym na cele marketingowe oraz stosowanie technologii śledzących.

1.18. **Incydent bezpieczeństwa** — naruszenie ochrony danych osobowych, które może prowadzić do przypadkowego lub niezgodnego z prawem ujawnienia, zniszczenia, utraty, zmiany lub nieuprawnionego dostępu do danych. Administrator jest zobowiązany do zarządzania incydentami zgodnie z obowiązującymi procedurami i regulacjami prawnymi.

2. Postanowienia ogólne

2.1. Podstawy stworzenia polityki

Polityka została opracowana w oparciu o przepisy RODO, PKE oraz przepisy krajowe, mające na celu maksymalizację ochrony danych osobowych oraz bezpieczeństwa informacji przetwarzanych przez Administratora. Polityka jest zgodna z najlepszymi praktykami w zakresie zarządzania bezpieczeństwem danych, a także uwzględnia normy krajowe w zakresie ochrony danych i bezpieczeństwa IT.

2.2. Zakres i zastosowanie polityki

Polityka obejmuje wszystkie systemy informacyjne, procesy przetwarzania danych, aplikacje oraz infrastrukturę IT wykorzystywaną przez Administratora, a także podmioty zewnętrzne zaangażowane w przetwarzanie danych. Dotyczy pracowników, współpracowników, partnerów biznesowych, podwykonawców oraz dostawców usług.

2.3. Znaczenie polityki w kontekście zmian legislacyjnych i technologicznych

Polityka ma służyć nie tylko spełnianiu wymogów prawnych, ale także proaktywnemu podejściu do ochrony danych osobowych i bezpieczeństwa systemów informacyjnych, poprzez ciągłe dostosowywanie się do dynamicznie zmieniającego się środowiska prawno-technologicznego. Polityka uwzględnia zmiany w przepisach prawa, rozwój technologii oraz nowe rodzaje zagrożeń, takie jak ataki na infrastrukturę krytyczną, co wymaga zastosowania zaawansowanych metod ochrony i zarządzania danymi.

2.4. Polityka jako element zintegrowanego systemu zarządzania bezpieczeństwem

Niniejsza Polityka jest integralnym elementem systemu zarządzania bezpieczeństwem informacji, który obejmuje nie tylko ochronę danych osobowych, ale także inne aspekty bezpieczeństwa informacji, w tym ochronę przed cyberzagrożeniami, zarządzanie dostępem, oraz ochronę infrastruktury technicznej.

3. Cele polityki bezpieczeństwa

3.1. Główne cele bezpieczeństwa IT

Głównym celem Polityki jest zminimalizowanie ryzyka związanego z przetwarzaniem danych osobowych oraz zapewnienie poufności, integralności i dostępności informacji. Polityka obejmuje identyfikację i ocenę ryzyk, wdrożenie odpowiednich środków ochrony oraz ciągłe monitorowanie zgodności z przepisami prawa.

3.2. Regulacje prawne dotyczące ochrony danych osobowych

Polityka uwzględnia wymagania RODO, PKE oraz przepisy krajowe, w tym ustawę o ochronie danych osobowych i inne akty normatywne regulujące ochronę prywatności i bezpieczeństwo w sektorze komunikacji elektronicznej. Administrator zobowiązuje się do przestrzegania aktualnych regulacji prawnych oraz do ciągłej weryfikacji polityki w kontekście zmian legislacyjnych.

3.3. Ochrona systemów informacyjnych jako fundament bezpieczeństwa

Systemy informacyjne stanowią podstawę działalności biznesowej Administratora, wspierając kluczowe procesy. Administrator stosuje środki techniczne i organizacyjne, które chronią systemy IT przed zagrożeniami zewnętrznymi i wewnętrznymi, zapewniając niezakłócone funkcjonowanie i zgodność z regulacjami prawnymi.

3.4. Strategiczne cele bezpieczeństwa w kontekście komunikacji elektronicznej

Polityka uwzględnia specyfikę sektora komunikacji elektronicznej, gdzie kluczowe znaczenie mają ochrona danych ruchu, metadanych oraz komunikacji interpersonalnej, zgodnie z PKE. Cele strategiczne obejmują minimalizację ryzyka naruszeń prywatności w związku z przetwarzaniem danych w usługach OTT (Over-the-Top), zarządzanie ryzykiem przetwarzania danych w chmurze oraz wdrażanie środków mających na celu ochronę przed zagrożeniami związanymi z nowoczesnymi technologiami.

3.5. Zarządzanie ryzykiem i ciągłość działania

Administrator wdraża kompleksowe podejście do zarządzania ryzykiem, które obejmuje identyfikację, ocenę, monitorowanie i minimalizację ryzyka związanego z przetwarzaniem danych osobowych. Kluczowym elementem tej strategii jest zapewnienie ciągłości działania systemów IT, w tym planowanie awaryjne, zarządzanie incydentami oraz procedury przywracania działania po awarii.

4. Zasady ochrony danych osobowych

4.1. Legalność i przejrzystość przetwarzania

Administrator przetwarza dane osobowe zgodnie z prawem, w sposób przejrzysty i zrozumiały dla osób, których dane dotyczą. Każdy proces przetwarzania opiera się na odpowiedniej podstawie prawnej, takiej jak zgoda, umowa, obowiązek prawny lub uzasadniony interes Administratora.

4.2. Minimalizacja i adekwatność danych

Dane osobowe przetwarzane są wyłącznie w zakresie niezbędnym do realizacji określonych celów. Stosowana jest zasada minimalizacji, ograniczająca zbieranie danych do absolutnego minimum, co jest niezbędne do wykonywania działań operacyjnych i spełniania obowiązków prawnych.

4.3. Rozliczalność i dokumentacja

Administrator prowadzi pełną dokumentację procesów przetwarzania danych, w tym rejestry czynności przetwarzania, dokumenty dotyczące oceny ryzyka oraz mechanizmy rozliczalności, które umożliwiają wykazanie zgodności z przepisami prawa w razie kontroli.

4.4. Zasady przetwarzania danych w kontekście usług komunikacji elektronicznej

Zasady przetwarzania danych uwzględniają specyfikę sektora komunikacji elektronicznej, w tym przetwarzanie danych ruchu, metadanych oraz danych osobowych w kontekście usług OTT, takich jak komunikatory, poczta internetowa czy aplikacje VoIP. Administrator stosuje specjalne środki ochrony danych komunikacyjnych, takie jak szyfrowanie end-to-end oraz anonimizacja danych ruchu, aby zapewnić zgodność z wymogami PKE.

4.5. Ochrona danych szczególnych kategorii

Dane szczególnych kategorii, takie jak dane zdrowotne, biometryczne czy dotyczące przekonań, przetwarzane są wyłącznie zgodnie z prawem i przy zastosowaniu najwyższych standardów ochrony, w tym pseudonimizacji i anonimizacji. Administrator wdraża dodatkowe środki ochrony, takie jak ograniczenia dostępu do danych oraz monitorowanie zgodności z obowiązującymi przepisami.

5. Systemy ochrony danych

5.1 Inwentaryzacja danych i Rejestr Czynności Przetwarzania Danych

Administrator prowadzi szczegółowy Rejestr Czynności Przetwarzania Danych, który inwentaryzuje procesy przetwarzania, kategorie danych oraz stosowane środki ochrony. Rejestr jest kluczowym elementem zarządzania ryzykiem oraz spełnienia wymogów rozliczalności.

5.2 Zarządzanie dostępem i tożsamością

Polityka przewiduje ścisłą kontrolę dostępu do danych, obejmującą autoryzację użytkowników, kontrolę uprawnień oraz ich regularne przeglądy. Wdrożone są także wielopoziomowe mechanizmy uwierzytelniania, aby zapewnić dostęp do danych tylko osobom uprawnionym.

5.3 Zasady profilowania i przetwarzania danych szczególnych kategorii

Profilowanie oraz przetwarzanie danych szczególnych kategorii, takich jak dane zdrowotne czy biometryczne, odbywa się tylko w przypadkach określonych przez prawo i zgodnie z najwyższymi standardami ochrony. Stosowane są zaawansowane techniki pseudonimizacji i anonimizacji w celu zminimalizowania ryzyka naruszenia danych.

5.4 Zarządzanie dostępem oparte na kontekście i dynamiczne zarządzanie tożsamością

Administrator stosuje zaawansowane techniki zarządzania dostępem, gdzie wdrożone systemy umożliwiają bieżącą analizę ryzyka i dynamiczne dostosowywanie uprawnień, co zwiększa poziom ochrony danych.

5.5 Technologie ochrony danych w usługach komunikacji elektronicznej

W celu ochrony danych osobowych w usługach komunikacji elektronicznej, Administrator stosuje technologie takie jak szyfrowanie oraz narzędzia do monitorowania ruchu sieciowego pod kątem

złośliwych działań. Polityka określa wymogi dotyczące stosowania bezpiecznych protokołów komunikacyjnych oraz zabezpieczeń na poziomie warstwy aplikacyjnej.

6. Naruszenia ochrony danych osobowych

6.1 Dokumentacja naruszeń ochrony danych osobowych

Administrator prowadzi szczegółową dokumentację wszystkich naruszeń ochrony danych osobowych, w której zawiera informacje dotyczące okoliczności naruszenia, jego skutków oraz podjętych działań naprawczych i prewencyjnych.

6.2 Zgłaszanie naruszeń do organu nadzorczego

Administrator zobowiązuje się do zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego, chyba że istnieje małe prawdopodobieństwo, iż naruszenie spowoduje ryzyko dla praw i wolności osób fizycznych. W ramach tych działań Administrator wymaga od wszystkich osób zaangażowanych w przetwarzanie danych osobowych, aby niezwłocznie raportowały każde zauważone naruszenie bezpieczeństwa danych.

6.3 Analiza incydentów i wdrażanie środków zaradczych

W przypadku każdego naruszenia ochrony danych, Administrator przeprowadza dogłębną analizę incydentu oraz wdraża odpowiednie środki zaradcze, zarówno techniczne, jak i organizacyjne, mające na celu zapobieganie podobnym zdarzeniom w przyszłości.

6.4 Informowanie Podmiotów danych o naruszeniach

W sytuacji, gdy naruszenie ochrony danych osobowych może wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki informuje o tym Podmioty danych, dostarczając im wszelkie istotne informacje dotyczące incydentu.

7. Realizacja uprawnień Podmiotów danych

Administrator zapewnia Podmiotom danych możliwość realizacji przysługujących im uprawnień zgodnie z zasadami określonymi w RODO, w tym w szczególności.

7.1 Prawo do informacji o przetwarzaniu danych

Osoba zgłaszająca żądanie otrzymuje od Administratora kompleksowe informacje dotyczące przetwarzania jej danych osobowych, w tym informacje o celach przetwarzania, podstawach prawnych, zakresie zbieranych danych, podmiotach, którym dane są udostępniane, oraz planowanym okresie przechowywania danych.

7.2 Prawo do uzyskania kopii danych

Administrator na żądanie Podmiotu danych przekazuje kopię posiadanych danych osobowych, które są przetwarzane w związku z żądaniem zgłoszonym przez Podmiot danych.

7.3 Prawo do sprostowania danych

Administrator, na żądanie Podmiotu danych, niezwłocznie koryguje wszelkie nieścisłości lub błędy w przetwarzanych danych osobowych i uzupełnia je, jeśli są niekompletne.

7.4 Prawo do usunięcia danych (prawo do bycia zapomnianym)

Administrator na żądanie usuwa lub anonimizuje dane osobowe, których dalsze przetwarzanie nie jest już niezbędne do realizacji celów, dla których dane te zostały pierwotnie zebrane.

7.5 Prawo do ograniczenia przetwarzania

Na wniosek Podmiotu danych, Administrator wstrzymuje operacje przetwarzania danych, z wyjątkiem sytuacji, gdy Podmiot danych wyrazi na to zgodę lub gdy operacje te są niezbędne do przechowywania danych zgodnie z polityką retencji lub do czasu ustania powodów ograniczenia (np. decyzji organu nadzorczego).

7.6 Prawo do przenoszenia danych

W przypadku przetwarzania danych osobowych w sposób zautomatyzowany na podstawie zgody lub umowy, Administrator dostarcza na żądanie Podmiotowi danych jego dane osobowe w powszechnie używanym formacie umożliwiającym ich odczyt przez komputer.

7.7 Prawo do sprzeciwu wobec przetwarzania danych w celach marketingowych

Podmiot danych może w każdej chwili wyrazić sprzeciw wobec przetwarzania jego danych osobowych do celów marketingowych, bez potrzeby uzasadnienia swojej decyzji.

7.8 Prawo do sprzeciwu wobec przetwarzania danych z innych przyczyn

Podmiot danych ma prawo w dowolnym momencie sprzeciwić się przetwarzaniu jego danych osobowych, gdy jest ono realizowane na podstawie prawnie uzasadnionego interesu Administratora, z uwagi na swoją szczególną sytuację.

7.9 Prawo do wycofania zgody

Podmiot danych, którego dane są przetwarzane na podstawie zgody, ma prawo w każdym momencie ją wycofać, przy czym wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, które miało miejsce przed jej wycofaniem.

8. Komunikacja z podmiotami danych

8.1 Komunikacja z podmiotami danych

Administrator podejmuje kroki mające na celu zapewnienie, że komunikacja z Podmiotami danych jest przejrzysta, zrozumiała i dostępna. Administrator stosuje zwięzły, jasnyi prosty język, dostosowany do potrzeb odbiorców.

8.2 Formy dostarczania informacji

Administrator dostarcza informacje Podmiotom danych na piśmie, w formie elektronicznej lub w inny odpowiedni sposób. Na prośbę Podmiotu danych, Administrator może również udzielić informacji ustnie, o ile istnieje możliwość potwierdzenia tożsamości Podmiotu danymi innymi metodami.

8.3 Ułatwienia w realizacji praw Podmiotów danych

Administrator ułatwia Podmiotom danych realizację przysługujących im praw, wynikających z RODO, w tym praw określonych w artykułach 15–22 RODO, zapewniając dostępne i proste w obsłudze kanały komunikacji.

8.4 Informowanie o podjętych działaniach

Administrator bez zbędnej zwłoki informuje Podmioty danych o podjętych działaniach w odpowiedzi na zgłoszone przez nich żądania wynikające z przepisów RODO, w szczególności w zakresie dostępu do danych, sprostowania, usunięcia, ograniczenia przetwarzania oraz przenoszenia danych.

9. Udostępnianie i powierzanie przetwarzania danych osobowych

9.1 Udostępnianie i powierzanie przetwarzania danych osobowych

Dane osobowe mogą być udostępniane innym administratorom tylko wtedy, gdy spełnione są przesłanki wskazane w art. 6 ust. 1 lub art. 9 ust. 2 RODO. Administrator dokładnie analizuje podstawy prawne przed podjęciem decyzji o udostępnieniu danych innym podmiotom.

9.2 Powierzanie przetwarzania danych osobowych

Powierzenie przetwarzania danych osobowych przez Administratora odbywa się na podstawie umowy powierzenia przetwarzania danych osobowych lub innego właściwego instrumentu prawnego, określonego w art. 28 RODO. Umowa ta precyzuje zakres i cel przetwarzania, obowiązki i odpowiedzialność stron oraz wymagane środki ochrony danych.

9.3 Weryfikacja podmiotów przetwarzających

Przed powierzeniem przetwarzania danych osobowych, Administrator przeprowadza weryfikację, czy podmiot przetwarzający spełnia odpowiednie wymagania bezpieczeństwa i posiada odpowiednie środki techniczne oraz organizacyjne, które gwarantują zgodność z RODO oraz ochronę praw Podmiotów danych. Administrator dokłada wszelkich starań, aby podwykonawcy i inne współpracujące podmioty stosowały równie rygorystyczne standardy ochrony danych.

10. Retencja i usuwanie danych

10.1 Polityka retencji danych

Dane są przechowywane przez okres niezbędny do realizacji celów przetwarzania, po czym są usuwane lub archiwizowane w sposób zapewniający ich ochronę. Polityka określa szczegółowe zasady retencji dla różnych kategorii danych, z uwzględnieniem specyficznych wymagań sektorowych i przepisów prawa.

10.2 Mechanizmy minimalizacji czasu przetwarzania

Administrator wdraża procedury regularnej weryfikacji przydatności danych, mające na celu ograniczenie ich przetwarzania do niezbędnego minimum. Dane są usuwane lub archiwizowane zgodnie z określonymi procedurami po upływie ustalonych okresów retencji.

10.3 Automatyzacja procesów retencji i usuwania danych

Polityka przewiduje zautomatyzowane systemy zarządzania retencją danych, które monitorują okresy przechowywania i automatycznie inicjują procesy usuwania danych po upływie ustalonych terminów. Automatyzacja minimalizuje ryzyko przetwarzania danych po okresie, na który udzielono zgody, oraz zwiększa zgodność z zasadami minimalizacji przetwarzania.

10.4 Retencja i usuwanie danych w kontekście komunikacji elektronicznej

Administrator stosuje szczególne zasady retencji i usuwania danych dotyczących komunikacji elektronicznej, w tym danych ruchu i metadanych, zgodnie z wymogami PKE. Retencja tych danych jest ściśle regulowana i ograniczona do sytuacji, w których jest to absolutnie konieczne do realizacji celów określonych przepisami prawa.

11. Zarządzanie bezpieczeństwem systemów informacji

11.1 Audyty i monitorowanie zgodności

Administrator regularnie przeprowadza audyty wewnętrzne i zewnętrzne, mające na celu weryfikację zgodności z przepisami prawa oraz ocenę skuteczności wdrożonych środków ochrony. Audyty te obejmują systemy IT, procedury przetwarzania danych oraz bezpieczeństwo fizyczne.

11.2 Ocena wpływu na ochronę danych

Dla operacji przetwarzania, które mogą mieć wysokie ryzyko dla praw i wolności osób, przeprowadzana jest ocena skutków dla ochrony danych, aby zidentyfikować zagrożenia i wprowadzić adekwatne środki ochrony.

11.3 Privacy by Design i Privacy by Default

Każdy nowy system, aplikacja lub proces są projektowane zgodnie zasadą, że ochrona danych jest uwzględniana już na etapie projektowania i wdrażania, a domyślne ustawienia zapewniają najwyższy poziom ochrony prywatności.

12. Zarządzanie incydentami bezpieczeństwa

12.1 Plan reagowania na incydenty

Administrator posiada plan zarządzania incydentami bezpieczeństwa, w tym procedury identyfikacji, oceny i reakcji na naruszenia ochrony danych. W przypadku incydentu, Administrator niezwłocznie podejmuje działania naprawcze oraz informuje osoby, których dane dotyczą, zgodnie z przepisami prawa.

12.2 Raportowanie naruszeń

Naruszenia ochrony danych są zgłaszane odpowiednim organom nadzorczym, takim jak Prezes UKE lub PUODO, w ciągu 72 godzin od wykrycia incydentu. Osoby, których dane dotyczą, są niezwłocznie informowane o naruszeniu i o możliwych środkach ochrony swoich praw.

12.3 Zarządzanie cyberzagrożeniami

Administrator wprowadza szczególne środki mające na celu ochronę przed specyficznymi zagrożeniami komunikacji elektronicznej, takimi jak ataki DDoS, ransomware, phishing oraz nieautoryzowany dostęp do danych. Regularnie przeprowadzane są testy penetracyjne oraz aktualizacje oprogramowania zabezpieczającego.

12.4 Współpraca z podmiotami zewnętrznymi w zarządzaniu incydentami

Administrator współpracuje z podmiotami zewnętrznymi, w tym dostawcami usług zarządzania incydentami, oraz specjalistami ds. cyberbezpieczeństwa, aby zapewnić kompleksowe podejście do zarządzania incydentami i ochrony przed naruszeniami. Polityka zawiera szczegółowe procedury współpracy i wymiany informacji w celu szybkiej reakcji na zagrożenia.

13. Utrzymywanie ciągłości zgodności z regulacjami

13.1 Zapewnienie zgodności operacyjnej z RODO

Administrator stale zapewnia zgodność operacji organizacyjnych z przepisami dotyczącymi ochrony danych osobowych określonymi w RODO, poprzez regularną weryfikację oraz dostosowywanie obowiązujących procedur i rejestrów w organizacji.

13.2 Monitorowanie zmian legislacyjnych i adaptacja praktyk

W ramach realizacji tego celu, Administrator monitoruje zmiany legislacyjne, analizuje wytyczne organów ochrony danych osobowych na poziomie krajowym i międzynarodowym, śledzi aktualne orzecznictwo sądów oraz trybunałów, a także adaptuje najlepsze praktyki rynkowe do wewnętrznych procesów.

14. Przetwarzanie danych transgranicznych

14.1 Przekazywanie danych do państw trzecich

Przekazywanie danych osobowych poza Europejski Obszar Gospodarczy (EOG) odbywa się tylko wtedy, gdy zapewniony jest odpowiedni poziom ochrony, zgodny z wymaganiami RODO i PKE. Stosowane są standardowe klauzule umowne oraz inne zatwierdzone mechanizmy zabezpieczeń.

14.2 Ocena ryzyka transgranicznego przetwarzania

Administrator regularnie ocenia ryzyko związane z przetwarzaniem danych poza EOG, w tym zgodność z lokalnymi przepisami i poziom ochrony danych w państwach trzecich. Wdrożone środki ochrony są systematycznie monitorowane i oceniane pod kątem skuteczności.

14.3 Specyficzne zasady dla współpracy z międzynarodowymi podmiotami

Polityka określa zasady współpracy z podmiotami spoza UE, w tym wymagania dotyczące umów, audytów i okresowych przeglądów zgodności, aby zapewnić zgodność z wymogami europejskimi.

15. Szkolenia i budowanie świadomości bezpieczeństwa

15.1 Programy edukacyjne i szkoleniowe

Administrator prowadzi regularne szkolenia z zakresu ochrony danych osobowych oraz bezpieczeństwa informacji dla pracowników i współpracowników. Szkolenia obejmują m.in. tematy związane z przetwarzaniem danych w komunikacji elektronicznej, ochroną przed phishingiem i innymi zagrożeniami specyficznymi dla sektora.

15.2 Kultura bezpieczeństwa i odpowiedzialności

Administrator promuje kulturę bezpieczeństwa, podnosząc świadomość pracowników i współpracowników na temat ochrony danych. Regularne kampanie informacyjne i dostępność narzędzi wspierających utrzymanie wysokich standardów ochrony stanowią kluczowy element tej strategii.

15.3 Szkolenia z zakresu zarządzania kryzysowego i reagowania na incydenty

Administrator zapewnia szkolenia dotyczące zarządzania kryzysowego i reagowania na incydenty bezpieczeństwa, skierowane do kadry zarządzającej oraz kluczowego personelu technicznego. Szkolenia obejmują symulacje rzeczywistych incydentów, analizy przypadków oraz ćwiczenia z reagowania na zagrożenia.

16. Podmioty przetwarzające i zasady współpracy z podmiotami zewnętrznymi

16.1 Weryfikacja podmiotów przetwarzających

Administrator weryfikuje podmioty przetwarzające, oceniając ich zdolność do zapewnienia odpowiedniego poziomu ochrony danych zgodnie z normami RODO. Współpraca z podmiotami przetwarzającymi wymaga zawarcia umów powierzenia przetwarzania danych, które określają obowiązki stron oraz wymagania dotyczące zabezpieczeń.

16.2 Umowy powierzenia przetwarzania

Umowy powierzenia przetwarzania danych są regularnie weryfikowane i aktualizowane w celu zapewnienia ich zgodności z obowiązującymi przepisami prawa oraz najlepszymi praktykami w zakresie bezpieczeństwa danych.

17. Klasyfikacja i ochrona dokumentów

17.1 Klasyfikacja dokumentów pod kątem bezpieczeństwa

Dokumenty zawierające dane osobowe są klasyfikowane zgodnie z poziomem wrażliwości. Administrator stosuje odpowiednie procedury przechowywania, archiwizacji i niszczenia dokumentów, aby zapewnić ich ochronę przed nieuprawnionym dostępem.

17.2 Zasady przechowywania i niszczenia dokumentów

Dokumenty przechowywane są w zabezpieczonych miejscach, a ich niszczenie odbywa się zgodnie z procedurami zapewniającymi trwałe usunięcie danych. Procesy te są zgodne z wymogami prawa oraz standardami bezpieczeństwa informacji.

17.3 Mechanizmy zabezpieczeń fizycznych i technicznych

Administrator wprowadził środki ochrony fizycznej, takie jak szyfrowanie, monitoring dostępu oraz systemy kontroli dokumentów, aby zminimalizować ryzyko nieautoryzowanego dostępu i kradzieży danych oraz zasady zarządzania dostępem do dokumentów zarówno w formie elektronicznej, jak i fizycznej. Zasady te obejmują stosowanie zabezpieczeń dostępu, takich jak szyfrowanie, kontrola uprawnień oraz logowanie działań użytkowników. Regularne przeglądy i audyty dostępu są integralnym elementem zarządzania dokumentami.

18. Dodatkowe rejestry i procedury

Administrator prowadzi i stosuje następujące rejestry i procedury dotyczące ochrony Danych osobowych, które stanowią integralną część Polityki:

- Polityka Prywatności i Cookies;
- Procedura ochrony przechowywanych lub przekazywanych danych osobowych przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą lub zmianą oraz nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem.
- Polityka Bezpieczeństwa Systemów IT.

19. Wejście w życie

19.1 Polityka wchodzi w życie z dniem 1 kwietnia 2025 roku