POLITYKA OCHRONY DANYCH OSOBOWYCH (RODO)

1.Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych” (dalej jako Polityka) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w PEWNO Izabela Bartoszewicz (dalej jako Administrator).
Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1).
1.Polityka zawiera:
a.opis zasad ochrony danych obowiązujących u Administratora;
b.odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);
1.Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Administrator wszyscy członkowie personelu.
Administrator zapewnia także zgodność postępowania swoich kontrahentów z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych.
1.Skróty i definicje:
Polityka oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1).
Dane oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.
Dane wrażliwe oznaczają dane specjalne i dane karne.
Dane specjalne oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.
Dane dzieci oznaczają dane osób poniżej 16. roku życia.
Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
Podmiot przetwarzający oznacza organizację lub osobę, której Administrator powierzył przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość).
Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.
IOD lub Inspektor oznacza Inspektora Ochrony Danych Osobowych
RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.
Administrator oznacza PEWNO Izabela Bartoszewicz, ul. Żurawinowa 8, 83-010 Rotmanka, NIP 843-144-51
1.Ochrona danych osobowych u Administratora – zasady ogólne 1.Filary ochrony danych osobowych u Administratora:
b. – Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
c. – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
d. – Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
e. – Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.
1.Zasady ochrony danych

Administrator przetwarza dane osobowe z poszanowaniem następujących zasad:
a. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
b. rzetelnieiuczciwie(rzetelność);
c. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
d. wkonkretnychcelachinie„nazapas”(minimalizacja);
e. nie więcej niż potrzeba (adekwatność);
f. z dbałością o prawidłowość danych (prawidłowość);
g. niedłużejniżpotrzeba(czasowość);
h. zapewniającodpowiedniebezpieczeństwodanych(bezpieczeństwo).
1.System ochrony danych
System ochrony danych osobowych u Administratora składa się z następujących elementów:
a. Administrator dokonuje identyfikacji zasobów danych osobowych u Administratora, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:
a.przypadków przetwarzania danych specjalnych i danych „kryminalnych” (dane wrażliwe);
b.przypadków przetwarzania danych osób, których Administrator nie identyfikuje (dane niezidentyfikowane);
c.przypadków przetwarzania danych dzieci; d.profilowania;
e.współadministrowania danymi.
a. opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych.
b. Administrator zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
a.utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
b.inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy przetwarza dane na podstawie prawnie uzasadnionego interesu Administratora.
a.Obsługa praw jednostki. Administrator spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
c.Obowiązki informacyjne. Administrator przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
d.Możliwość wykonania żądań. Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
e.Obsługa żądań. Administrator zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane.
f.Zawiadamianie o naruszeniach. Administrator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.
a.Minimalizacja. Administrator posiada zasady i metody zarządzania minimalizacją (privacy by default), a w tym:
g.zasady zarządzania adekwatnością danych;

h.zasady reglamentacji i zarządzania dostępem do danych;
i.zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności;
a.Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
j.przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
k.przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
l.dostosowuje środki ochrony danych do ustalonego ryzyka;
m.posiada system zarządzania bezpieczeństwem informacji;
n.stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.
a.Przetwarzający. Administrator posiada zasady doboru przetwarzających dane na rzecz Administratora, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.
b.Eksport danych. Administrator posiada zasady weryfikacji, czy nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

c.Privacy by design. Administrator zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.
d.Przetwarzanie transgraniczne. Administrator posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.
a. Inwentaryzacja
2.Dane wrażliwe
Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe (dane specjalne i dane karne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, Administrator postępuje zgodnie z przyjętymi zasadami w tym zakresie.
1.Dane niezidentyfikowane
Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
1.Profilowanie
Administrator identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji, Administrator postępuje zgodnie z przyjętymi zasadami w tym zakresie.
1.Współadministrowanie
Administrator identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.
a.
2.RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
3.Administrator prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
4.Rejestr jest jednym z podstawowych narzędzi umożliwiających Administratorowi rozliczanie większości obowiązków ochrony danych.

5.W Rejestrze, dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru, odnotowuje co najmniej: (i) nazwę czynności, (ii) cel przetwarzania, (iii) opis kategorii osób, (iv) opis kategorii danych, (v) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Administratora, jeśli podstawą jest uzasadniony interes, (vi) sposób zbierania danych, (vii) opis kategorii odbiorców danych (w tym przetwarzających), (viii) informację o przekazaniu poza EU/EOG; (ix) ogólny opis technicznych i organizacyjnych środków ochrony danych.
6.Wzór Rejestru stanowi Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”. Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Administrator rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej
a. Podstawy przetwarzania
2.Administrator dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych
czynności przetwarzania.
3.Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Administratora) Administrator dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.

4.Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
5.Sposób obsługi praw jednostki i obowiązków informacyjnych
6.Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane
przetwarza.
7.Administrator ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu ze Administratorem w tym celu, ewentualnym cenniku żądań „dodatkowych" itp.
8.Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
9.Administrator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw
jednostki i obowiązków informacyjnych.
10.W celu realizacji praw jednostki Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
11.Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.
12.Obowiązki informacyjne
13.Administrator określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
14.Administrator informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
15.Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby. 16.Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie
niebezpośrednio od niej.
17.Administrator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
18.Administrator informuje osobę o planowanej zmianie celu przetwarzania danych.
19.Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.
20.Administrator informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

21.Administrator informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
22.Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.
23.Żądania osób
24.Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, Administrator wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), Administrator może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
25.Nieprzetwarzanie. Administrator informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
26.Odmowa. Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
27.Dostęp do danych. Na żądanie osoby dotyczące dostępu do jej danych, Administrator informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu

prawa dostępu do danych Administrator nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
28.Kopie danych. Na żądanie Administrator wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.
29.Sprostowanie danych. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Administrator ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.
30.Uzupełnienie danych. Administrator uzupełnia i aktualizuje dane na żądanie osoby. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Administrator nie musi przetwarzać danych, które są mu zbędne). Administrator może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administrator procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
31.Usunięcie danych. Na żądanie osoby, Administrator usuwa dane, gdy:
a.dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
b.zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
c.osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
d.dane były przetwarzane niezgodnie z prawem,
e.konieczność usunięcia wynika z obowiązku prawnego,
f.żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).
Administrator określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.
Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, Administrator podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.

W przypadku usunięcia danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.
1. Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
o.osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
p.przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
q.Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
r.osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.
Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.
W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.
1.Przenoszenie danych. Na żądanie osoby Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Administratora.
2.Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o jego uzasadniony interes lub o powierzone Administratorowi zadanie w interesie publicznym, Administrator uwzględni sprzeciw, o ile nie zachodzą po jego stronie ważne prawnie

uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
3.Sprzeciw względem marketingu bezpośredniego. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administratora na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
4.Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu. Jeżeli Administrator przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Administrator zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie, chyba że taka automatyczna decyzja (i) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Administratorem; lub (ii) jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej osoby.
5.MINIMALIZACJA
Administrator dba o minimalizację przetwarzania danych pod kątem: (i) adekwatności danych do celów (ilości danych i zakresu przetwarzania), (ii) dostępu do danych, (iii) czasu przechowywania danych.
1.Minimalizacja zakresu
Administrator zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.
Administrator dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
Administrator przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (privacy by design).
1.
Administrator stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).

Administrator stosuje kontrolę dostępu fizycznego.
Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.
Administrator dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
1.Minimalizacja czasu
Administrator wdraża mechanizmy kontroli cyklu życia danych osobowych, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów Administratora, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Administratora.
1.BEZPIECZEŃSTWO
Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych.
1.Analizy ryzyka i adekwatności środków bezpieczeństwa
Administrator przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
a.Administrator zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
b.Administrator kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
c.Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Administrator analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

d.Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Administrator ustala przydatność i stosuje takie środki i podejście jak:
a.pseudonimizacja,
b.szyfrowanie danych osobowych,
c.inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
d.środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
1.Oceny skutków dla ochrony danych
Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
1.Środki bezpieczeństwa
Administrator stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.
Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa.
1.
Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.
1.PRZETWARZAJĄCY
Administrator posiada zasady doboru i weryfikacji przetwarzających dane na jego rzecz opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków

organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Administratorze.
Administrator przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiących „Wzór umowy powierzenia przetwarzania danych".
Administrator rozlicza przetwarzających z wykorzystania podprzetwarzających.
1.EKSPORT DANYCH
Administrator rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2017 r. = Unia Europejska, Islandia, Lichtenstein i Norwegia).
Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych, Administrator okresowo weryfikuje zachowania użytkowników.
1.PROJEKTOWANIE PRYWATNOŚCI
Administrator zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.
W tym celu zasady prowadzenia projektów i inwestycji przez Administratora odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.