ESIGNA SP. Z O. O.
ul. Królewska 65A, lok. 1, 30-081 Kraków
KRS: 0000917756, NIP: 6772467505

POLITYKA OCHRONY DANYCH OSOBOWYCH

Wersja dokumentu
1.0
Uwagi:
Przyjęta: 06.06.2022 r.

Spis treści:

Rozdział I – WSTĘP

Niniejsza dokumentacja zatytułowana „**Polityka Ochrony Danych Osobowych**" (dalej także: **Polityka**), ma za zadanie stanowić mapę zasad i regulacji w zakresie ochrony danych osobowych osób fizycznych, przetwarzanych w związku z prowadzoną działalnością gospodarczą Administratora Danych Osobowych.

Administratorem przetwarzanych danych osobowych jest ESIGNA Sp. z o. o. z siedzibą w Krakowie, ul. Królewska 65A, lok.1, 30-081 Kraków, NIP: 6772467505, REGON: 389743596, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie, Wydział XI Gospodarczy KRS, pod numerem rejestrowym KRS: 0000917756, (dalej zwana także **Administrator** lub **ADO** lub **Spółka**). Dokumentacja ta 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/W (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).

Administrator zaznacza, że niniejszy dokument to jeden ze środków o charakterze organizacyjnym, za pomocą którego wykazuje się zgodność przetwarzania danych osobowych z RODO. Odpowiedzialny za wdrożenie oraz bieżące aktualizowanie niniejszej Polityki Ochrony Danych Osobowych jest Administrator, który odpowiada również za nadzór i monitorowanie jej przestrzegania przez wszystkie osoby przetwarzające dane osobowe w przedsiębiorstwie lub przez inny podmiot przetwarzający (procesor), któremu Administrator w drodze umowy polecił przetwarzanie danych osobowych.

Administrator danych osobowych w duchu aktualnie obowiązujących przepisów określa podstawowe zasady będące filarami ochrony danych osobowych w jego przedsiębiorstwie, tj.:

1) **Legalność** – dane osobowe przetwarzane są zgodnie z prawem. Przez legalność należy rozumieć normy prawa materialnego jak i proceduralnego oraz zasady współżycia społecznego;

2) **Rzetelność i uczciwość** – uwzględnianie przez Administratora interesów i rozsądnych oczekiwań osób, których dane dotyczą. Administrator przetwarza dane z zgodnie z regułami uczciwości, rozumianymi jako poszanowanie interesów osób, których dane dotyczą, i nie wykorzystuje ich przymusowej sytuacji;

3) **Przejrzystość** – Administrator realizuje swoje obowiązki informacyjne w zwięzłej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem;

4) **Minimalizacja** – dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

5) **Prawidłowość** – Administrator zapewni prawidłowość danych w szczególności na etapie gromadzenia danych;

6) **Czasowość** – Administrator przechowuje dane osobowe w formie umożliwiającej identyfikację osoby, które dane dotyczą, przez okres nie dłuższym niż jest to niezbędne do celów, w których dane te są przetwarzane;

7) **Bezpieczeństwo** – dane osobowe są chronione przez zapewnienie odpowiedniego poziomu zabezpieczeń w sposób ciągły;

8) **Prawa Jednostki** – Podmioty, których dane są przetwarzane przez Administratora mają umożliwione wykonywanie praw im przysługujących;

9) **Rozliczalność** – Administrator dokumentuje to, w jaki sposób spełnia obowiązki w celu możliwości wykazania zgodności swojego postępowania przepisami prawa.

W związku z realizacją powyższych zasad Administrator danych osobowych w ramach przyjętej polityki ochrony danych osobowych, posługuje się dokumentacją taką jak m. in.:

1) **Rejestr czynności przetwarzania danych –** Administrator prowadzi rejestr w celu realizacji obowiązku wynikającego z art. 30 ust. 1 RODO;

2) **Rejestr kategorii czynności przetwarzania danych** – Administrator prowadzi rejestr kategorii czynności przetwarzania w razie przetwarzania danych na polecenie innego Administratora;

3) **Rejestr udostępniania danych osobowych** – stanowi formę dokumentowania czynności związanych z wnioskami i żądaniami podmiotów trzecich o udostępnienie danych osobowych;

4) **Procedura zarządzania ryzykiem** – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych w oparciu o działania oparte na szacowaniu i analizie ryzyka, przeprowadza bieżące analizy ryzyka dla czynności przetwarzania danych lub ich kategorii. Administrator dokonuje również – w razie aktualizacji obowiązku oceny skutków przetwarzania danych dla praw osób, których dane dotyczą;

5) **Dokument realizacji obowiązku informacyjnego administratora** – Administrator posługuje się formularzem informacyjnym, który zawiera aktualne informacje na jego temat oraz na temat przetwarzania danych osobowych uzyskanych od podmiotów, które te dane dotyczą;

6) **Formularz żądań osoby, której dane dotyczą** – w związku z szeregiem obowiązków wynikających z art. 15-22 RODO Administrator realizuje możliwość skorzystania z praw osób, których dane dotyczą, w szczególności posługuje się formularzem ułatwiającym realizację praw;

7) **Rejestr naruszeń – instrukcja postępowania w sytuacji naruszeń praw osób, których dane są przetwarzane** – Administrator prowadzi rejestr naruszeń w celu realizacji obowiązku wynikającego z art. 33 RODO. Administrator prowadzi także raport z naruszeń oraz realizuje w razie aktualizacji obowiązek zgłaszania informacji o naruszeniu do organu nadzorczego;

8) **Ewidencja osób upoważnionych do przetwarzania danych** – Administrator prowadzi na bieżąco ewidencję osób, które posiadają lub posiadały upoważnienie do przetwarzania danych w celu zapewnienia przejrzystości przetwarzania danych w przedsiębiorstwie Administratora;

9) **Ewidencja podmiotów, którym powierzono przetwarzanie danych osobowych** – Administrator prowadzi ewidencję podmiotów zewnętrznych, którym polecił przetwarzanie danych osobowych;

10) **Procedura współpracy z podmiotami zewnętrznymi –** Administrator posiada określoną procedurę w celu weryfikacji podmiotu, którym powierza przetwarzanie danych osobowych w związku z prowadzoną działalnością gospodarczą;

11) **Procedura powołania inspektora ochrony danych** – na wypadek obowiązku lub podjęcia decyzji fakultatywnej o powołaniu Inspektora Ochrony Danych Administrator posiada procedurę określającą zasady jego powołania.

12) **Regulamin korzystania z poczty elektronicznej** – określa zasady korzystania z poczty elektronicznej, stanowi załącznik do Polityki.

Rozdział II – SŁOWNIK POJĘĆ

W dokumentacji stanowiącej politykę ochrony danych Administratora użyto następujących pojęć, które należy rozumieć następująco:

1. **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osoba, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to

osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

2. **Przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

3. **Ograniczenie przetwarzania** – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

4. **Profilowanie** – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

5. **Pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

6. **Zbiór danych** - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

7. **Administrator danych osobowych** lub **Administrator** lub **ADO –** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

8. **Inspektor ochrony danych** lub **IOD** – osoba powołana przez ADO, która ma zadanie informowania 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 doradztwo im w tej

sprawie, monitorowanie przestrzegania RODO, działanie zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty, udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO, współpraca z organem nadzorczym, pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych;

9. **Personel, Pracownicy** - osoby zatrudnione na podstawie stosunku pracy, umów cywilnoprawnych (umowa o dzieło, umowa zlecenia), przedsiębiorcy wykonujący działalność osobiście i jednoosobowo, osoby odbywające praktyki, stażyści, osoby skierowane do pracy w ramach umów z agencjami pracy tymczasowej wykonujące prace związane z przetwarzaniem danych osobowych u ADO;

10. **Podmiot przetwarzający** lub **Procesor** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

11. **Odbiorca** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

12. **Zgoda** – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

13. **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

14. **Organ nadzorczy** – oznacza niezależny organ publiczny, którym jest Urząd Ochrony Danych Osobowych (UODO);

15. **Dane szczególnych kategorii** – 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;

16. **Dane karne** – oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa;

17. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

18. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym;

19. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

20. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

21. **Integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

22. **Rozliczalność** – właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

23. **Poufność danych** – właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

24. **Dostępność danych** – właściwość zapewniająca, że dane są możliwe do wykorzystania w żądanym czasie przez podmiot uprawniony;

25. **Państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego;

26. **UODO** – Urząd Ochrony Danych Osobowych;

27. **RODO** - 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/W (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1);

28. **Upoważnienie do przetwarzania danych osobowych –** dokument wydany przez ADO lub Procesora, upoważniający wskazaną w nim osobę do przetwarzania danych osobowych administrowanych przez ADO.

Rozdział III – SYSTEM OCHRONY DANYCH

1.Informacje ogólne

a) Inwentaryzacja danych osobowych

Administrator w związku z prowadzoną działalnością przetwarza:

I. Dane osobowe klientów

- w zakresie: imion i nazwisk osób reprezentujących firmę/instytucję, nazwę firmy/instytucji, adresu do korespondencji, adresu mailowego, numeru telefonu, NIP. Zakres przetwarzanych danych jest niezmienny od dłuższego czasu z uwagi na określony przedmiot działalności firmy.
- cel przetwarzania: wykonanie umowy lub podjęcie działań zmierzających do jej zawarcia.
- podstawa prawna przetwarzania: art. 6 ust. 1 lit. b RODO - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

II. Dane osobowe potencjalnych klientów

- w zakresie: imienia i nazwiska, numeru telefonu, adresu e-mail
- cel przetwarzania: udzielenie odpowiedzi na zapytanie potencjalnego klienta; podjęcie działań zmierzających do zawarcia umowy;
- podstawa prawna przetwarzania: art. 6 ust. 1 lit. b RODO - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy

III. Dane osobowe klientów – szkolenia (webinary)

- w zakresie: imienia i nazwiska, numeru telefonu, adresu e-mail, w przypadku wystawiania fv - adresu do korespondencji, NIP.
- cel przetwarzania: wykonanie umowy lub podjęcie działań zmierzających do jej zawarcia.
- podstawa prawna przetwarzania: art. 6 ust. 1 lit. b RODO - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane

dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

IV. Dane osób trzecich udostępniane przez klientów w przekazanej dokumentacji w ramach wykonywania usług cyfrowej digitalizacji dokumentów (w ramach powierzenia przetwarzania danych osobowych)

- kategorie przetwarzanych danych osobowych:
  - ustalane każdorazowo w umowie powierzenia przetwarzania danych osobowych;
- zakres:
  - ustalane każdorazowo w umowie powierzenia przetwarzania danych osobowych;
- cel przetwarzania: wykonanie umowy lub podjęcie działań zmierzających do jej zawarcia,
- podstawa prawna przetwarzania: art. 6 ust. 1 lit. b RODO - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

V. Użytkownicy z portali społecznościowych

- W zakresie: imię, nazwisko, nick, dane kontaktowe
- cel przetwarzania: komunikacja z osobami zainteresowanymi działalnością ADO
- podstawa prawna przetwarzania: art. 6 ust. 1 lit. f RODO – prawnie uzasadniony interes

VI. Dane osobowe podwykonawców (zleceniobiorców w ramach zawieranych umów cywilnoprawnych)

- w zakresie: imię i nazwisko, data urodzenia, obywatelstwo, nr PESEL, adres korespondencyjny, nr telefonu, NIP
- cel przetwarzania: wykonanie umowy lub podjęcie działań zmierzających do jej zawarcia;
- podstawa prawna przetwarzania: art. 6 ust. 1 lit. b RODO - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy

VII. Dane osobowe potencjalnych współpracowników (zleceniobiorców)

- w zakresie: imię, nazwisko, nr telefonu, adres zamieszkania lub pobytu, adres e-mail, inne dane podane przez kandydata w dokumentach aplikacyjnych (cv, list motywacyjny), dane o wykształceniu, przebiegu pracy oraz inne dane wymagane zgodnie z Kodeksem Pracy, dane pozyskane podczas rozmowy kwalifikacyjnej
- cel przetwarzania: rekrutacja zleceniobiorców, zawarcie umowy cywilnoprawnej;
- podstawa prawna przetwarzania: art. 6 ust. 1 lit. a i b RODO

VIII. Baza marketing (zgody)

- W zakresie: imię, nazwisko, adres mailowy
- cel przetwarzania: ewidencja wyrażonych zgód marketingowych, marketing produktów ADO
- podstawa prawna przetwarzania: art. 6 ust. 1 lit. a RODO – zgoda osoby, której dane dotyczą

Administrator identyfikuje przypadki przetwarzania danych szczególnych kategorii lub danych dotyczących wyroków skazujących i naruszeń prawa, Administrator analizuje to przetwarzanie przede wszystkim w kontekście art. 9 i 10 RODO, a także ich odpowiedniego zabezpieczania.

b) Profilowanie

Administrator może przetwarzać dane na potrzeby marketingu bezpośredniego (w tym profilowania) w oparciu o swój prawnie uzasadniony interes. W przypadku złożenia przez podmiot danych sprzeciwu wobec takiego rodzaju przetwarzania, Administrator nie przetwarza dłużej danych w tym celu. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego przetwarzania wywołującego wobec osoby, której dane dotyczą skutki prawne lub w podobny sposób istotnie na nią wpływają ADO realizuje zasady związane z tego typu działalnością, w szczególności te opisane w art. 22 RODO.

c) Współadministrowanie

Administrator nie zidentyfikował współadministrowania danymi w dotychczasowej działalności.

d) Podstawy przetwarzania

Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:

I. osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
II. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
III. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
IV. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
V. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
VI. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel), Administrator dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą wynika z przepisów prawa – 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.

ADO 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.). Zebrane zgody, jeżeli posiadają formę papierową, przechowywane są w głównym miejscu wykonywania działalności gospodarczej ADO. W przypadku zgód udzielonych drogą elektroniczną, przechowywane są w oprogramowaniu wykorzystywanym przez Administratora do przetwarzania danych.

e) Minimalizacja

Administrator dba o minimalizację przetwarzania danych pod kątem:

I. zakresu przetwarzanych danych:

Administrator przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (privacy by design).

II. dostępu do przetwarzania:

Administrator stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których zawarte są dane osobowe). 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.

III. czasu przechowywania danych:

Administrator wdraża mechanizmy kontroli cyklu życia danych osobowych w firmie, 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 i baz ADO, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez ADO.

f) Bezpieczeństwo

Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych.

g) Środki bezpieczeństwa

Administrator stosuje środki bezpieczeństwa uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym

prawdopodobieństwie i wadze zagrożenia. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

h) Prywatność (privacy by design, privacy by default)

Administrator w prowadzonych przez siebie działaniach biznesowych domyślnie przyjmuje prywatność osób, których dane przetwarza jako wartość podstawową, w oparciu o którą buduje długofalowe relacje z osobami, których dane dotyczą.

Prywatność jest również wartością istotną w przypadku tworzenia i prowadzenia nowych projektów i inwestycji. W tym zakresie bezpieczeństwo, minimalizacja, analiza ryzyka jest uwzględniana od początkowych etapów projektu lub inwestycji.

2. Ryzyko

a) Analizy ryzyka i adekwatności środków bezpieczeństwa

Administrator przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu Administrator zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych, w szczególności w zakresie bezpieczeństwa IT. Administrator kategoryzuje aktywa ustalając ich wartość pod kątem zagrożeń utraty poufności, integralności i dostępności.

Administrator analizuje możliwe 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. Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym celu Administrator ustala przydatność i stosuje między innymi w stosownym przypadku takie środki i podejście jak:

I. szyfrowanie danych osobowych, w sytuacji gdy dochodzi do ich przesyłania drogą elektroniczną,
II. inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
III. 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.
IV. Regularne testuje, mierzy i ocenia skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Administrator ocenia ryzyko związane z przetwarzaniem danych osobowych. Metoda szacowania ryzyka jest efektem adaptacji zaleceń stosowania podejścia opartego na ryzyku wydanych przez organ nadzorczy. Dokumentacja czynności związanych z analizą ryzyka i jego szacowanie zawiera się w dokumentacji, na którą składa się część opisowa i kalkulacyjna.

b) Oceny skutków dla ochrony danych

Administrator, w razie potrzeby dokonuje oceny skutków operacji przetwarzania dla ochrony danych osobowych osób fizycznych, które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia ich praw lub wolności w rozumieniu art. 35 RODO.

3. Rejestry

a) Rejestr Czynności Przetwarzania Danych

Rejestr Czynności Przetwarzania Danych 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.

Administrator prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

Rejestr jest jednym z podstawowych narzędzi umożliwiających Administratorowi rozliczanie większości obowiązków ochrony danych.

W Rejestrze, dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru, odnotowuje co najmniej:

I. nazwę czynności,
II. jednostkę organizacyjną,
III. cel przetwarzania,
IV. opis kategorii osób,
V. opis kategorii danych,
VI. podstawę prawną przetwarzania,
VII. sposób zbierania danych,
VIII. jeżeli jest to możliwe planowany termin usunięcia danych,
IX. jeżeli dotyczy dane współadministratora,
X. jeżeli dotyczy dane podmiotu przetwarzającego,
XI. opis kategorii odbiorców danych,
XII. nazwa systemu lub oprogramowania,

XIII. jeśli jest to możliwe ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,
XIV. DPIA – jeśli zostało przeprowadzone
XV. transfer do kraju trzeciego.

b) Rejestr kategorii czynności przetwarzania

Rejestr kategorii czynności przetwarzania stanowi formę dokumentowania czynności przetwarzania danych na polecenie innego administratora.

W rejestrze, dla każdej czynności przetwarzania danych Administrator odnotowuje co najmniej:

I. kategorię przetwarzań,
II. jeśli jest to możliwe ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,
III. dane kontaktowe administratora,
IV. jeżeli dotyczy dane kontaktowe współadministratora,
V. jeżeli dotyczy dane przedstawiciela administratora,
VI. jeżeli powołano dane IOD,
VII. czas trwania przetwarzania,
VIII. transfer do kraju trzeciego.

c) Rejestr udostępniania danych osobowych

Rejestr udostępniania danych osobowych stanowi formę dokumentowania czynności związanych z wnioskami i żądaniami podmiotów trzecich o udostępnienie danych osobowych.

Należy mieć na uwadze że udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne dla zrealizowania obowiązku wynikającego z przepisu prawa. Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione. Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowić naruszenia zasad ochrony danych osobowych. Przetwarzanie, w tym udostępnianie danych osobowych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celu badań naukowych, dydaktycznych, historycznych oraz statystycznych.

W prowadzonym rejestrze udostępnień danych osobowych, Administrator odnotowuje co najmniej:

I. Datę złożenia wniosku;

II. Nazwę instytucji składającej wniosek wraz z adresem siedziby;
III. Podstawę prawną upoważniającą wnioskodawcę do otrzymywania danych osobowych;
IV. Datę wydania wnioskowanej informacji lub kopii dokumentów a także ich rodzaj i kategorie danych osobowych;
V. Datę zwrotu dokumentów;
VI. Informację o odmowie udostępnienia wnioskowanej dokumentacji;
VII. Imię i nazwisko osoby realizującej sprawę.

4. Naruszenia

Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych (które to naruszenie skutkowałoby ryzykiem naruszenia praw lub wolności osób fizycznych), Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia. Szczegółowa ścieżka postępowania zawarta jest w instrukcji postępowania w sytuacji naruszenia ochrony danych – odrębnym dokumencie wdrożonym przez Administratora.

5. Personel i podmioty zewnętrzne

a) Personel

Administrator zabezpiecza prawidłowe przetwarzanie danych przez personel w szczególności przez stosowanie odpowiednich upoważnień dla pracowników i zleceniobiorców, które zawierają również obowiązek zachowania w tajemnicy informacji, do których mają oni dostęp w związku z wykonywaniem obowiązków służbowych (oświadczenie o poufności). Administrator prowadzi również ewidencję nadanych upoważnień. Administrator dokonuje również okresowego przeglądu udzielonych upoważnień pod kątem zasadności dalszego upoważnienia konkretnych osób w zakresie przetwarzania danych.

I. Każda z osób dopuszczona do przetwarzania danych osobowych lub współpracująca z Administratorem jest zobowiązana do:

    i. przetwarzania danych osobowych jedynie w zakresie i jedynie w celu w jakim zostało im wydane upoważnienie do przetwarzania danych osobowych,

    ii. zachowania w tajemnicy informacji i danych osobowych, do których posiada dostęp,

iii. niewykorzystywania dostępnych danych osobowych do celów sprzecznych z zakresem upoważnienia do przetwarzania danych osobowych.

iv. zachowania poufności procesów i metod zabezpieczeń danych osobowych w firmie ADO,

v. ochrony informacji i danych osobowych przed przypadkowym, niepożądanym ujawnieniem, modyfikacjom, utratą, zniszczeniem danych osobowych czy też nieuprawnionym dostępem osób nieuprawnionych,

II. Osoby, które zostają dopuszczone do przetwarzania danych osobowych, a które zapoznały się treścią niniejszej Polityki, są zobowiązane do podpisania tzw. oświadczenia o poufności.

b) Przetwarzający

Jeżeli przetwarzanie ma być dokonywane w imieniu Administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii Europejskiej lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

I. przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

II. zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

III. podejmuje wszelkie środki wymagane na mocy RODO, mając na względzie w szczególności art. 24 i 32;

IV. biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;

V. uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO;

VI. po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

VII. udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich;

VIII. udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. W związku z obowiązkiem wskazanym w art. Ust. 3 lit. h) podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

Jeżeli do wykonania w imieniu Administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii Europejskiej lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie

wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.

Wystarczające gwarancje, podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO.

Bez uszczerbku dla indywidualnych umów między Administratorem a podmiotem przetwarzającym, umowa lub inny akt prawny, mogą się opierać w całości lub w części na standardowych klauzulach umownych, także gdy są one elementem certyfikacji udzielonej administratorowi lub podmiotowi przetwarzającemu zgodnie z art. 42 i 43 RODO.

Bez uszczerbku dla art. 82, 83 i 84 RODO, jeżeli podmiot przetwarzający naruszy RODO przy określaniu celów i sposobów przetwarzania, uznaje się go za Administratora w odniesieniu do tego przetwarzania.

W celu zapewnienia ochrony danych w przypadku powierzenia przetwarzania danych w postaci umów powierzenia z podmiotami przetwarzającymi, Administrator powinien przesłać do podmiotu przetwarzającego formularz wstępnej weryfikacji zabezpieczania danych osobowych.

6. Prawa osób, których dane dotyczą

a) Sposób obsługi praw jednostki i obowiązków informacyjnych

Osoba, której dane dotyczą, jest informowana o prowadzeniu operacji przetwarzania i o jej celach. Ponadto Administrator podaje wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i kontekst przetwarzania danych osobowych. Dodatkowo informuje o fakcie profilowania oraz o konsekwencjach. W przypadku zbierania danych od osoby, której dane dotyczą, wskazuje czy ma ona obowiązek je podać, oraz o konsekwencjach ich niepodania. Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie bezpośrednio. W przypadku pozyskania danych niebezpośrednio od osoby której dane dotyczą, Administrator informuje taką osobę w rozsądnym terminie, nie później niż w ciągu miesiąca od pozyskania danych, chyba że wcześniej zamierza się z nią komunikować lub ujawnić jej dane innemu odbiorcy – informuje najpóźniej w momencie ich dokonania. Administrator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym). Administrator informuje osobę o planowanej zmianie celu przetwarzania danych.

Administrator, w przypadku gdy zbiera dane osobowe, od osoby której dane dotyczą, zgodnie z art. 13 ust. 1 i 2 RODO informuje o:

I. swojej tożsamości i danych kontaktowych oraz tożsamość i danych kontaktowych swojego przedstawiciela, jeżeli został powołany;

II. danych kontaktowych inspektora ochrony danych (jeżeli został wyznaczony);

III. celach przetwarzania, do których mają posłużyć dane osobowe;

IV. podstawie prawnej przetwarzania;

V. prawnie uzasadnionym interesie realizowanym przez administratora lub przez stronę trzecią – jeżeli przetwarzanie odbywa się na podstawie prawnie usprawiedliwionego interesu administratora (art. 6 ust. 1 lit. f RODO);

VI. odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

VII. transferze danych do państwa trzeciego, w tym o:

i. zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

ii. stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony;

iii. lub wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych w przypadku przekazania danych do państwa trzeciego , o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO;

VIII. okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

IX. prawie do:

i. żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą ich sprostowania, usunięcia lub ograniczenia przetwarzania lub wniesienia sprzeciwu wobec przetwarzania, a także przenoszenia danych;

ii. cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych zwykłych (art. 6 ust. 1 lit. a) RODO) lub szczególnej kategorii (art. 9 ust. 2 lit. a RODO);

iii. wniesienia skargi do organu nadzorczego;

iv. informacji, 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;

v. informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotnych informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Administrator, w przypadku gdy zbiera dane osobowe w sposób inny niż od osoby której dane dotyczą zgodnie z art. 14 ust. 1 i 2 RODO informuje o:

X. swojej tożsamości i danych kontaktowych oraz tożsamość i danych kontaktowych swojego przedstawiciela, jeżeli istnieje;

XI. danych kontaktowy inspektora ochrony danych (jeżeli został wyznaczony);

XII. celach przetwarzania, do których mają posłużyć dane osobowe;

XIII. kategoriach odnośnych danych osobowych;

XIV. odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

XV. transferze danych do państwa trzeciego, w tym o:

i. zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

ii. stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony;

iii. lub wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych w przypadku przekazania danych do państwa trzeciego , o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO;

XVI. okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

XVII. prawnie uzasadnionych interesach realizowanych przez administratora lub prezz stronę trzecią, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 RODO

XVIII. prawie do:

i. żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą ich sprostowania, usunięcia lub ograniczenia przetwarzania lub wniesienia sprzeciwu wobec przetwarzania, a także przenoszenia danych;

ii. cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych zwykłych (art. 6 ust. 1 lit. a) RODO) lub szczególnej kategorii (art. 9 ust. 2 lit. a RODO);

iii. wniesienia skargi do organu nadzorczego;

iv. źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;

v. informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotnych informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

b) Prawo dostępu do danych

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

I. cele przetwarzania;
II. kategorie odnośnych danych osobowych;
III. informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
IV. w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
V. prawo do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
VI. prawo wniesienia skargi do organu nadzorczego;
VII. jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
VIII. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także znaczeniu i przewidywane konsekwencje takiego przetwarzania dla osoby, której dane dotyczą.

Wniosek od osoby uprawnionej jest przekazywany Administratorowi, a następnie dokonuje się potwierdzenia tych danych.

c) Prawo do sprostowania

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia. Sprostowania danych, na zlecenie administratora dokonuje inspektor ochrony danych lub administrator systemów informatycznych.

d) Prawo do usunięcia danych (prawo do bycia zapomnianym)

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, o ile zachodzi jedna z przesłanek wskazana w art. 17 RODO. Usunięcia danych, na zlecenie administratora dokonuje wyznaczona do tego osoba.

Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, to podejmuje ona 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.

e) Prawo do ograniczenia przetwarzania

Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:

I. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
II. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
III. administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
IV. osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

f) Powiadomienie o sprostowaniu lub usunięciu danych

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18 RODO, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Podmiot danych w celu realizacji swoich praw wypełnia wniosek przekazany mu przez Spółkę. Celem stosowania formularza jest przejrzystość procesu realizacji praw osób, których dane dotyczą oraz umożliwienie konkretnej osobie przedstawienie swoich żądań bez nacisków i wywierania presji.

g) Przenoszenie danych

Przenoszenie danych polega na możliwości otrzymywania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych, które dostarczyły Administratorowi osoby, który dane dotyczą, oraz możliwość przesłania tych

danych osobowych innemu administratorowi bez przeszkód. Przenoszenie danych może mieć miejsce przy zaistnieniu przesłanek z art. 20 RODO.

Administrator posiada formularz umożliwiający podmiotowi danych skorzystanie z przysługującego mu uprawnienia. Zgodnie z treścią art. 20 ust. 1 lit. a) RODO, prawo do przenoszenia danych znajduje zastosowanie wobec operacji przetwarzania danych na podstawie zgody podmiotu danych oraz umowy, której podmiot danych jest stroną, w sytuacji gdy przetwarzanie odbywa się w sposób zautomatyzowany.

Administrator, po konsultacjach z osobą posiadającą wiedzę w tym zakresie przekazuje dane za pomocą takich narzędzi jak: „streaming", płyta CD, DVD lub inny fizyczny nośnik bądź przesyła dane bezpośrednio innemu administratorowi (zgodnie z artykułem 20 ust. 2 RODO, gdy jest to technicznie wykonalne).

Administrator dba o czytelność komunikacji z osobami, których dane przetwarza. Ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób, wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych. W celu realizacji praw jednostki Administrator posiada sprawdzoną metodę zidentyfikowania danych konkretnych osób, jest w stanie zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

h) Prawa osób trzecich

Realizując prawa osób, których dane dotyczą, Administrator wprowadza 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.

i) Odmowa

Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

j) Kopie danych

Na żądanie uprawnionej osoby ADO wydaje tej osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Administrator wprowadza i utrzymuje cennik

kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.

k) Uzupełnienie danych

Administrator uzupełnia i aktualizuje dane na żądanie osoby. ADO ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. ADO nie musi przetwarzać danych, które są mu zbędne). ADO może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administratora procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

l) Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych

Jeżeli ADO prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Administrator uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

m) Sprzeciw względem marketingu bezpośredniego

Jeżeli osoba uprawniona zgłosi sprzeciw względem przetwarzania jej danych przez ADO na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

n) Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.

Jeżeli ADO 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, ADO zapewni możliwość odwołania się do interwencji i decyzji człowieka po stronie ADO, chyba że taka automatyczna decyzja jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a ADO lub jest wprost dozwolona przepisami prawa lub opiera się o wyraźną zgodę odwołującej osoby.

7. Inspektor Ochrony Danych

Administrator zobowiązuje się do wyznaczenia Inspektora Ochrony Danych w razie zaktualizowania się obowiązku wynikającego z art. 37 RODO. W szczególności ADO zobowiązuje się do jego wyznaczenia, jeżeli główna działalność polegać będzie na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa. Administrator zobowiązuje się do wyznaczenia

Inspektora Ochrony Danych, jeżeli jego główna działalność polegać będzie na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę.

Administrator może powołać dobrowolnie Inspektora Ochrony Danych w celu podniesienia poziomu bezpieczeństwa danych osobowych. W razie podjęcia decyzji lub aktualizacji obowiązku wyznaczenia Inspektora Ochrony Danych Administrator zadba o weryfikację kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych osobowych, a także, żeby umiała wypełniać zadania, które nałoży na nią rozporządzenie.

W razie wyznaczenia Inspektora Ochrony Danych, Administrator niezwłocznie zawiadomi o danych kontaktowych organ nadzorczy. Administrator po wyznaczeniu Inspektora Ochrony Danych zadba o niezwłoczne włączenie go we wszystkie sprawy, które dotyczą ochrony danych osobowych. Administrator zapewni Inspektorowi Ochrony Danych zasoby niezbędne do wykonywania zadań z zakresu ochrony danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej. W zakresie swoich zadań Inspektor Ochrony Danych nie będzie otrzymywał instrukcji dotyczących wykonywania swoich zadań, nie będzie również karany ani odwoływany za wypełnianie swoich zadań.

Administrator zobowiąże Inspektora Ochrony Danych zachowania poufności co do wykonywania swoich zadań. Jeżeli Inspektor Ochrony Danych wykonywał będzie inne zadania i obowiązki Administrator zapewni, że nie będą one powodowały konfliktu interesów. Administrator zobowiąże Inspektora Ochrony danych do wypełniania swoich zadań z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania danych osobowych, mając na uwadze charakter, zakres, kontekst i cele przetwarzania danych osobowych. Administrator zobowiąże Inspektora Ochrony Danych do informowanie jego i personelu o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych osobowych i doradzanie w tej sprawie. Administrator zobowiąże Inspektora Ochrony Danych do monitorowania przestrzegania RODO, a także innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych osobowych oraz wewnętrznych polityk w dziedzinie ochrony danych osobowych, w tym podziału obowiązków, działań zwiększających świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania danych osobowych oraz prowadzenia powiązanych z tym audytów. Administrator zobowiąże Inspektora Ochrony Danych do udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowania jej wykonania. Administrator zobowiąże Inspektora Ochrony Danych do współpracy z organem nadzorczym. Administrator zobowiąże Inspektora Ochrony Danych do pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Rozdział IV - POLITYKA BEZPIECZEŃSTWA

1. **Środki organizacyjne zapewniające ochronę przetwarzanych danych osobowych:**

a) Do danych osobowych i ich przetwarzania dopuszczone są wyłącznie osoby upoważnione przez Administratora;

b) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;

c) Przetwarzając dane osobowe w systemach informatycznych, każda osoba upoważniona pracuje wyłącznie na swoim koncie użytkownika i na swoim komputerze;

d) Niedozwolone jest udostępnianie konta użytkownika przypisanego danej osobie, osobom trzecim;

e) Niedozwolone jest udostępnianie danych dostępowych do konta osobom postronnym lub innym osobom nieupoważnionym;

f) Wszelkie dokumenty zarówno w formie papierowej jak i w formie elektronicznej zawierające dane osobowe są odpowiednio zabezpieczane w przypadku, gdy w pomieszczeniu wchodzącym w skład obszaru przetwarzania danych osobowych nie znajduje się osoba upoważniona;

g) Podczas nieobecności osoby upoważnionej w pomieszczeniu, w którym przetwarzane są dane osobowe, w celu zabezpieczenia danych przetwarzanych elektroniczne, osoba upoważniona do przetwarzania danych zobowiązana jest wylogować się z konta użytkownika i wyłączyć komputer, lub jeżeli pomieszczenie jest opuszczane chwilowo - wylogowania się z konta użytkownika bez wyłączania komputera;

h) Podczas nieobecności osoby upoważnionej w pomieszczeniu, w którym przetwarzane są dane osobowe, w celu zabezpieczenia danych przetwarzanych elektroniczne za pomocą komputera przenośnego, osoba upoważniona do przetwarzania danych zobowiązana jest do umieszczenia ich w miejscu przechowywania, w taki sposób, aby uniemożliwić jego wyniesienie poza obszar przetwarzania danych;

i) Osoby pracujące przy przetwarzaniu danych osobowych zostały zapoznane z przepisami dotyczącymi przetwarzania danych osobowych i bezpieczeństwa systemów informatycznych;

j) Zabrania się eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych np. biurkach, ladach, półkach, parapetach itp.;

k) Wydruki i inne dokumenty zawierające dane osobowe są przechowywane w pomieszczeniach do tego wyznaczonych. Stosowana jest zasada tzw. czystego biurka;

l) Po zakończeniu pracy wszelka dokumentacja zawierająca dane osobowe jest przechowywana w szafach lub w pomieszczeniach o ograniczonym dostępie osób postronnych, do których dostęp jest utrudniony poprzez zastosowanie zabezpieczeń fizycznych takich jak: zamki w drzwiach, rolety, systemy kontroli dostępu itp. Dokumentacja zawierająca dane osobowe szczególnej kategorii przechowywana jest w szafach zamykanych na klucz;

m) Zaleca się zwrócenie szczególnej uwagi na sytuację przypadkowego pozostawienia dokumentów zawierających dane osobowe w miejscach ogólnodostępnych, przy kopiarkach, przy drukarkach itp.;

n) Administrator jest zobowiązany do corocznej weryfikacji posiadanych zbiorów danych osobowych, które mają na celu wyeliminowanie danych, do których ustały podstawy przetwarzania;

o) Osoby pracujące przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy;

p) Ekrany komputerów, tabletów i innych urządzeń (w tym przenośnych) muszą być ustawianie w ten sposób, aby uniemożliwić osobom nieuprawnionym wgląd w wyświetlane dane, dotyczy to zarówno stacjonarnych jak i przenośnych stanowisk pracy;

q) Użytkownicy systemów informatycznych służących do przetwarzania danych osobowych zobowiązani są do okresowej zmiany haseł (tam, gdzie nie jest to wymuszone przez system);

r) Niedopuszczalne jest używanie nośników danych niewiadomego pochodzenia.

Wykaz pomieszczeń, w których przetwarzane są dane osobowe:

Obszarem przetwarzania danych osobowych przez Administratora jest biuro w budynku zlokalizowanym pod adresem: ul. Królewska 65A, lok.1, 30-081 Kraków. Dodatkowym miejscem wykonywania działalności jest biuro zlokalizowane przy ul. Urzędniczej 20/11, 30-051 Kraków.

Dopuszcza się przetwarzanie danych osobowych w systemie informatycznym poza obszarem przetwarzania z użyciem urządzeń przenośnych.

2. **Środki fizyczne zapewniające ochronę przetwarzanych danych osobowych**

a) Obszar przetwarzania danych osobowych zabezpieczony jest za pomocą drzwi zamykanych na klucz;

b) Dokumenty zawierające dane osobowe przechowywane są w segregatorach układanych w zamykanych szafach, w części dostępnej tylko dla osób upoważnionych do przetwarzania danych osobowych;

c) Dostęp do pomieszczeń w których przetwarzane są dane osobowe objęty jest systemem kontroli dostępu;

d) Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są przed skutkami pożaru za pomocą gaśnicy wolnostojącej;

e) Dokumenty zawierające dane osobowe po ustaniu przydatności lub utracie podstawy do ich przetwarzania są niszczone w sposób mechaniczny za pomocą niszczarki dokumentów.

3. **Środki sprzętowe, informatyczne i telekomunikacyjne zapewniające ochronę przetwarzanych danych osobowych**

a) Dokumenty, wydruki i inne nośniki w formie tradycyjnej, zawierające dane osobowe, a przeznaczone do usunięcia, niszczone są za pomocą niszczarki;

b) Nośniki w formie elektronicznej zawierające dane osobowe, a przeznaczone do usunięcia, niszczone są w niszczarce, jeśli niszczarka posiada możliwości zniszczenia danego nośnika. Jeśli brak jest takiej możliwości, należy dany nośnik uszkodzić fizycznie w sposób uniemożliwiający odzyskanie danych lub przekazać nośnik do utylizacji wyspecjalizowanej firmie, po uprzednim podpisaniu umowy powierzenia przetwarzania danych;

c) Urządzenie końcowe umożliwiające dostęp do danych osobowych zabezpieczone są identyfikatorem i hasłem;

d) Zastosowano system rejestracji dostępu do systemu, w którym przetwarzane są dane osobowe;

e) Zastosowano środki uniemożliwiające osobom postronnym wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemu informatycznego;

f) Bezpośredni dostęp do zbioru danych osobowych w formie elektronicznej wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;

g) W komputerach – urządzeniach końcowych zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł;

h) W urządzeniach końcowych stosowane są wygaszacze ekranów zabezpieczone hasłem, włączające się w przypadku dłuższej nieaktywności użytkownika;

i) Aktualizacje systemu operacyjnego i programów w komputerach działających pod kontrolą systemu Windows, w szczególności aktualizacje bezpieczeństwa, realizowane są przy wykorzystaniu funkcji Windows Update ustawionej w tryb automatyczny;

j) Użyto system Firewall do ochrony dostępu sieci komputerowej;

k) Skanowanie antywirusowe realizowane jest w sposób automatyczny, co najmniej raz w tygodniu;

l) Oprogramowanie antywirusowe (w tym w szczególności sygnatury wirusów) aktualizowane jest automatycznie.

Rozdział V - INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

1.Uprawnienia do przetwarzania danych osobowych w systemie informatycznym, zasady uwierzytelniania

a) Nadawanie uprawnień

I. ADO decyduje o zakresie uprawnień personelu w systemie informatycznym.
II. Identyfikator i pierwsze hasło do pracy w systemie informatycznym jest tworzone przez ADO lub osobę przez ADO upoważnioną.
III. Identyfikator i hasło należy przekazać użytkownikowi w sposób poufny.

IV. Użytkownik jest zobowiązany do niezwłocznej zmiany hasła otrzymanego od ADO
V. ADO aktualizuje spis identyfikatorów użytkowników przyznanych osobom uprawnionym do przetwarzania danych osobowych znajdujący się w Ewidencji osób upoważnionych do przetwarzania danych osobowych.
VI. w Ewidencji osób upoważnionych do przetwarzania danych osobowych, odnotowuje się również fakt przyznania uprawnień personelowi podmiotów, którym powierzono przetwarzanie danych osobowych, jeśli personel tego podmiotu korzysta z systemu informatycznego ADO.

b) Zmiana uprawnień

I. ADO decyduje o zakresie uprawnień personelu w systemie informatycznym.
II. ADO lub osoba przez ADO upoważniona aktualizuje spis identyfikatorów użytkowników przyznanych osobom uprawnionym do przetwarzania danych osobowych znajdujący się w Ewidencji osób upoważnionych do przetwarzania danych osobowych (o ile nastąpiła zmiana w tym zakresie) oraz informację o zakresie upoważnienia.

c) Odebranie uprawnień

I. ADO decyduje o odebraniu uprawnień do systemów informatycznych.
II. Odebranie uprawnień następuje w następujących sytuacjach:
    i. ustanie stosunku pracy lub zakończenie współpracy na podstawie umowy cywilnoprawnej,
    ii. wniosek podmiotu, któremu powierzono przetwarzanie danych osobowych, o ile odebranie uprawnień dotyczy pracownika tego podmiotu,
    iii. zmiana zakresu obowiązków,
    iv. uzasadnione ryzyko nadużycia,
    v. decyzja ADO podyktowana inną przyczyną niż w/w.

d) Szczegółowe warunki dotyczące nadawania uprawnień do przetwarzania danych osobowych w zakresie czynności przetwarzania:

I. Dane przetwarzane są za pomocą oprogramowania (w szczególności): Pakiet Microsoft Office.
II. ADO tworząc konto nadaje uprawnienia przy wykorzystaniu wbudowanych narzędzi oprogramowań. Użytkownik, po otrzymaniu danych dostępowych, loguje się i niezwłocznie zmienia hasło na sobie tylko znane.
III. Użytkownik, po otrzymaniu danych dostępowych, loguje się do odpowiedniego oprogramowania i niezwłocznie zmienia hasło na sobie tylko znane.

e) Identyfikatory

I. Identyfikator użytkownika jest unikalny dla każdej upoważnionej osoby.
II. Identyfikator użytkownika, którego konto zostało usunięte nie może być przyznany innej osobie.
III. Zaleca się, aby identyfikator w łatwy sposób pozwalał zidentyfikować konkretnego użytkownika.

f) Polityka haseł

I. Hasło do systemu operacyjnego urządzeń na których przetwarzane są dane osobowe, musi posiadać co najmniej 8 znaków i musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;
II. Hasła do systemów i aplikacji z pomocą których przetwarzane są dane osobowe, muszą posiadać co najmniej 11 znaków i muszą zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;
III. Hasła powinno się zmieniać okresowo, nie rzadziej niż co 60 dni;
IV. W przypadku, gdy oprogramowanie nie wymusza długości, wykorzystywanego rodzaju znaków, czy częstotliwości zmiany haseł, użytkownik zobowiązany jest nadzorować prawidłowości hasła i częstotliwość jego zmiany samodzielnie;
V. Przekazywanie haseł musi odbywać się metodą zapewniającą poufność;
VI. Hasła wpisane z klawiatury muszą pojawiać się na ekranie w formie niejawnej;
VII. Użytkownik ma obowiązek zachowania hasła w tajemnicy;
VIII. Hasło przypisane do danego identyfikatora użytkownika jest znane wyłącznie osobie upoważnionej, której przydzielony został ten identyfikator;
IX. Użytkownik ma obowiązek zabezpieczenia hasła przed ujawnieniem osobom trzecim;
X. Zabronione jest w szczególności zapisywanie hasła w miejscach dostępnych dla osób trzecich;

2. Opis procesu tworzenia duplikatów plików zawierających dane osobowe i oprogramowania do ich przetwarzania, przetrzymywanie nośników informacji zawierających dane osobowe

a) Tworzenie kopii zapasowych

I. Za tworzenie kopii zapasowych zbiorów danych osobowych odpowiada ADO.
II. ADO może wyznaczyć osoby, które wykonują poszczególne kopie zapasowe.
III. Kopie zapasowe wykonywane są niezależnie od kopii wykonywanych przez podmioty, którym powierzono przetwarzanie danych osobowych.

IV. Częstotliwość wykonywania kopii zapasowych oraz minimalny czas ich przechowywania określa Harmonogram wykonywania kopii zapasowych przedstawiony w poniższej tabeli.
V. ADO ma prawo usunąć kopie, których minimalny czas utrzymywania minął.

Oprogramowanie	Lokalizacja oprogramowania	Częstotliwość wykonywania kopii	Rodzaj kopii	Czas utrzymywania kopii	Nośnik kopii bezpieczeństwa	Lokalizacja nośnika

b) Procedura tworzenia dodatkowych kopii zapasowych

I. Podłączenie dysku zewnętrznego przeznaczonego do przechowywania kopii zapasowej danych do urządzenia końcowego.
II. Zamontowanie kontenera z danymi, umieszczonego na dysku zewnętrzny.
III. Zalogowanie do oprogramowania
IV. Wykonanie zrzutu bazy danych i zapisanie go w odpowiedniej lokalizacji w kontenerze z danymi.
V. Wykonanie innych kopii zapasowych, jeśli konieczne.
VI. Odmontowanie kontenera z danymi.
VII. Odmontowanie i odłączenie dysku zewnętrznego.

3. Praca w systemie informatycznym

Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest do sprawdzenia urządzenia końcowego i stanowiska pracy w szczególności pod kątem okoliczności wskazujących na możliwość naruszenia ochrony danych osobowych.

a) Rozpoczęcie pracy

I. Uruchomić urządzenie końcowe i zalogować się podając swój identyfikator i hasło dostępu do systemu operacyjnego (lub dane dostępowe na innych poziomach logowania);
II. Należy zapewnić warunki do dyskretnego podania danych dostępowych;
III. Należy uruchomić aplikację, wpisując swój identyfikator i hasło dostępu;
IV. Można rozpocząć pracę.

b) Wstrzymanie pracy

I. Przy opuszczeniu stanowiska pracy dopilnować, aby dane osobowe nie wyświetlały się na ekranie. W takiej sytuacji sugeruje się zablokowanie urządzenia końcowego poprzez wyświetlenie ekranu logowania zabezpieczonego hasłem;
II. Przy opuszczeniu stanowiska pracy na dłuższy czas, należy wylogować się z aplikacji oraz zablokować urządzenie końcowe.

Niezależnie od powyższych każde urządzenie końcowe ma skonfigurowany wygaszacz ekranu zabezpieczony hasłem, włączający się w przypadku 5 minutowej nieaktywności użytkownika.

c) Zakończenie pracy

I. Wylogować się z aplikacji i zamknąć aplikację.
II. Zamknąć system.
III. Wyłączyć monitor, jeśli korzysta z monitora z niezależnym zasilaniem
IV. Zabezpieczyć stanowisko pracy, w szczególności nośniki danych, dokumenty i wydruki zawierające dane osobowe.

d) Sposoby postępowania w zakresie komunikacji w sieci komputerowej

a) Wszelkie pliki zawierające kopie danych osobowych zawartych w systemie, wysyłanych poza system, myszą być zabezpieczone hasłem.

b) W miarę możliwości, dane osobowe zawarte na serwerze sieciowym nie mogą być przechowywane na stacjach roboczych. Należy dane te umieszczać na dysku sieciowym.

c) Nieuzasadnione kopiowanie danych z serwera na stacje robocze bądź na nośniki informatyczne jest zabronione.

4. Zabezpieczenie systemu przed złośliwym oprogramowaniem

Administrator zapewnia zabezpieczenie systemu informatycznego przed działaniem szkodliwego oprogramowania oraz zagrożeniami pochodzącymi z sieci publicznej. Niniejsze zadanie realizowane jest poprzez:

— zobowiązanie podmiotów, którym powierzono dane osobowe do stosowania odpowiednich zabezpieczeń;
— stosowanie następujących zabezpieczeń we własnych systemach informatycznych:

- oprogramowanie antywirusowe
- firewall
- zabezpieczenia kryptograficzne
- zabezpieczenia organizacyjne
- zabezpieczenie sieci Wi-Fi hasłem, ukrycie SSID i szyfrowanie protokołem WPA2-PSK

d) **Aktualizacja oprogramowania**

Aktualizacje systemu operacyjnego i programów, w szczególności aktualizacje bezpieczeństwa, realizowane są przy wykorzystaniu funkcji aktualizacji oprogramowania wbudowanej w system operacyjny ustawionej w tryb automatyczny.

e) **Oprogramowanie antywirusowe**

Na stacjach końcowych działających pod kontrolą systemu Windows, każdy użytkownik posiada zainstalowany system antywirusowy. ADO kontroluje na bieżąco oprogramowanie jakie jest zainstalowane na komputerach osób przetwarzających dane osobowe. Oprogramowanie antywirusowe należy skonfigurować w taki sposób, aby wykonywało ciągłe skanowanie zasobów (skanowanie w tle). Przynajmniej raz w miesiącu należy wykonać w sposób automatyczny pełne skanowanie systemu. Definicje antywirusowe programu aktualizowane są automatycznie.

Użytkownik jest zobowiązany do każdorazowego wykonania skanowania programem antywirusowym wszelkich nośników danych (płyty CD, DVD, pendrive, itp.) podłączanych do stacji roboczych systemu informatycznego.

f) **Firewall**

Na stacjach końcowych działających pod kontrolą systemu Windows działa firewall.

e) Nośniki zewnętrzne

Zabrania się korzystania z nośników danych niewiadomego pochodzenia.

5. Systemy i nośniki informacji, konserwacja i przeglądy

a) Przeglądy i konserwacje prowadzone przez ADO

Administrator zapewnia przeglądy i konserwacje systemu w szczególności poprzez cykliczne:

I. sprawdzanie konfiguracji systemu operacyjnego pod kątem wykonywania automatycznych aktualizacji.
II. sprawdzanie konfiguracji oprogramowania antywirusowego pod kątem wykonywania automatycznych aktualizacji.
III. kontrole oprogramowania używanego w urządzeniach końcowych pod kątem jego aktualizacji. W przypadku pojawienia się nowej wersji oprogramowania należy przeanalizować, czy nowa wersja posiada aktualizację luk bezpieczeństwa w stosunku do aktualnie używanej. W przypadku pojawienia się poprawek luk bezpieczeństwa, aktualizacja jest wymagana. W przypadku niepojawienia się poprawek luk bezpieczeństwa, aktualizacja jest opcjonalna.
IV. skanowanie oraz monitorowanie parametrów prac dysku zewnętrznego służącego do przechowywania kopii zapasowych zbiorów danych osobowych i innych kopii zapasowych.

Administrator może wyznaczyć osobę odpowiedzialną za realizację przeglądów i konserwacji systemu.

b) Przeglądy i konserwacje prowadzone przez podmioty zewnętrzne

Administrator zapewnia nadzór nad prowadzonymi przez osoby nieposiadające upoważnienia do przetwarzania danych osobowych pracami konserwacyjnymi, przeglądami lub naprawami systemu informatycznego wykorzystywanego do przetwarzania danych osobowych. Konserwacja, przeglądy lub naprawy powinny odbywać się w strefie przetwarzania danych osobowych. Jeżeli istnieje konieczność wydania do podmiotu zewnętrznego urządzeń, będących składnikiem systemu informatycznego, Administrator zobowiązany jest zapewnić usunięcie danych osobowych z tych urządzeń w sposób nieumożliwiający odzyskanie tych danych (np. za pomocą dedykowanego oprogramowania lub poprzez demontaż nośników danych). W przypadku braku możliwość skutecznego usunięcia danych lub demontażu nośników, należy z podmiotem dokonującym konserwacji podpisać umowę powierzenia danych osobowych.

c) Przechowywanie nośników informacji zawierających dane osobowe

I. Nośniki, zawierające dane osobowe przechowywane są w miejscach uniemożliwiających dostęp do nich osobom nieupoważnionym.
II. Po ustaniu przydatności danych osobowych zawartych na nośnikach, dane są trwale usuwane z użyciem oprogramowania powodującego wielokrotne nadpisanie danych (bez możliwości odtworzenia ich treści).

III. Urządzenia, dyski lub inne nośniki informacji, zawierające zapis danych osobowych przeznaczonych do likwidacji są pozbawiane zapisu (programowe wymazywanie danych oraz formatowanie nośnika), a w przypadku, gdy jest to niemożliwe uszkodzone mechanicznie w sposób uniemożliwiający jego odczyt.
IV. Urządzenia, dyski lub inne nośniki informacji zawierające zapis danych osobowych przeznaczone do naprawy są pozbawiane zapisu (programowe wymazywanie danych oraz formatowanie nośnika). Jeśli nie ma możliwości pozbawienia nośnika zapisu, naprawa jest dokonywana przez podmiot, z którym podpisano umowę powierzenia.
V. Urządzenia, dyski lub inne nośniki informacji zawierające dane osobowe, których naprawa nie jest możliwa są niszczone w sposób uniemożliwiający odczytanie zapisanych na nich informacji.

Rozdział VI – PLAN CIĄGŁOŚCI DZIAŁANIA

1. Informacje ogólne:

a) Administrator wyznaczył następujące obszary krytyczne dla organizacji systemu ochrony danych osobowych:

I. brak zasilania w siedzibie firmy;
II. awaria systemu informatycznego;
III. awaria sprzętu do przetwarzania danych osobowych;
IV. brak dostępu do sieci internetowej;
V. brak dostępu do pomieszczeń, w których przetwarzane są dane osobowe;

b) Wobec zdefiniowanych obszarów krytycznych opracowano Plan ciągłości działania, który znajduje się w niniejszym rozdziale.

c) Dla przedsiębiorstwa ADO przewidziano konieczność zabezpieczenia możliwości ciągłości działania dla następujących elementów - z wykorzystaniem systemów informatycznych oraz bez udziału systemów informatycznych.

2. Zapewnienie ciągłości pracy systemu przetwarzania danych osobowych z udziałem systemów informatycznych

a) Zapewnienie ciągłości pracy systemów informatycznych

I. Wprowadza się procedurę zgłaszania awarii systemów informatycznych wykorzystywanych do przetwarzania danych osobowych w przedsiębiorstwie ADO.

II. Każdy z użytkowników systemu informatycznego, w sytuacji wystąpienia awarii tego systemu, ma obowiązek niezwłocznego zgłoszenia awarii tego systemu Administratorowi.

III. Administrator zawiadamia niezwłocznie o wystąpieniu awarii osobę obsługującą firmę pod względem informatycznym.

IV. Czas reakcji i czas naprawy określa umowa pomiędzy ADO a osobą wykonującą naprawy, z zastrzeżeniem, że podjęcie czynności naprawczych nie powinno zostać podjęte później niż 2 godziny od zgłoszenia awarii.

V. Do czasu usunięcia awarii systemu informatycznego, ADO wykorzystuje dokumentację papierową, która po usunięciu awarii systemu informatycznego jest niezwłocznie wprowadzana przez upoważnioną osobę do systemu.

VI. Wzór dokumentacji papierowej wykorzystywanej alternatywnie w trakcie awarii systemu informatycznego nie musi być ściśle określony. Powinien jednak zawierać elementy niezbędne do kompletnego wprowadzenia danych osobowych do systemu informatycznego. Jeśli dostawca oprogramowania informatycznego przewidział taką sytuację, stosuje się szablony dokumentów papierowych dostarczonych przez dostawcę oprogramowania.

VII. Po usunięciu awarii osoba obsługująca podmiot pod względem informatycznym weryfikuje prawidłowość baz danych, która jest uzupełniana o informacje wytworzone za pomocą zastępczej dokumentacji papierowej.

VIII. W przypadku uszkodzenia bazy danych należy wykorzystać kopię zapasową w celu przywrócenia poprawności systemu informatycznego.

IX. Z czynności mających na celu przywrócenie pracy systemu Administrator sporządza stosowną notatkę.

b) Zapewnienie ciągłości pracy sprzętu, na którym przetwarzane są dane osobowe

I. Wprowadza się procedurę zgłaszania awarii urządzeń wykorzystywanych do przetwarzania danych osobowych w przedsiębiorstwie ADO.

II. Każdy z użytkowników, w sytuacji wystąpienia awarii sprzętu służącego do przetwarzania danych osobowych ma obowiązek niezwłocznego zgłoszenia awarii tego sprzętu Administratorowi.

III. Administrator zawiadamia niezwłocznie o wystąpieniu awarii osobę obsługującą przedsiębiorstwo ADO pod względem informatycznym.

IV. Podjęcie diagnostyki w celu eliminacji awarii powinno nastąpić nie później niż w ciągu 2 godzin od zgłoszenia awarii, a sama awaria powinna zostać usunięta w ciągu 24 godzin od daty jej wystąpienia.

V. Do czasu usunięcia awarii, personel ADO wykorzystuje dokumentację papierową, która po usunięciu awarii jest niezwłocznie wprowadzana przez upoważnioną osobę do systemu lub wykorzystywany jest inny sprzęt ADO.

VI. Jeżeli awarii nie da się usunąć w ciągu 24 godzin, Administrator zapewnia przy udziale osoby obsługującej przedsiębiorstwie ADO pod względem informatycznym zapasowe urządzenie spełniające wymogi przepisów prawa i umożliwiające realizowanie usług świadczonych przez ADO.

c) Zapewnienie ciągłości pracy w przypadku braku zasilania elektrycznego w sieci energetycznej

I. Każdy użytkownik systemu ma obowiązek niezwłocznego zgłoszenia braku zasilania sieci energetycznej w przedsiębiorstwie ADO po jej wystąpieniu z wykorzystaniem numeru alarmowego, który jest dostępny w biurze.

II. Komputery, na których przetwarzane są dane osobowe są w miarę możliwości komputerami przenośnymi.

III. Jeżeli komputery, na których przetwarzane są dane osobowe są komputerami przenośnymi, użytkownik takiego komputera, jest zobowiązany do takiej organizacji pracy, aby zapewnić przez cały jej okres maksymalny poziom naładowania baterii, która umożliwi jego pracę bez zasilania, co najmniej przez 2 godziny.

IV. Jeżeli użytkownik podejrzewa, że naprawa dostawy prądu może wydłużyć się ponad czas naładowania baterii jest zobowiązany do bezpiecznego przerwania pracy i wyłączenia sprzętu komputerowego.

V. Do czasu przywrócenia napięcia w sieci elektrycznej stosuje się bezpośrednio zapisy, o których mowa w ust. 2 pkt a ppkt V i VI Planu Ciągłości Działania.

VI. Jeżeli do przetwarzania danych osobowych użytkowane są komputery stacjonarne wyposażone są one w urządzenia UPS.

VII. W przypadku braku zasilania użytkownik komputera stacjonarnego ma niezwłoczny obowiązek bezpiecznego zakończenia pracy i wyłączenia stacji roboczej.

VIII. W przypadku wyłączenia serwera bazy danych w przedsiębiorstwie ADO stosuje się zapisy, o których mowa w ust. 2 pkt a ppkt V i VI Planu Ciągłości Działania.

d) Zapewnienie ciągłości pracy w przypadku braku dostępu do sieci internetowej

I. Jeżeli użytkownik stwierdzi brak dostępu do sieci internetowej należy to zgłosić niezwłocznie na numer pomocy technicznej dostawcy, który jest wywieszony w biurze.

II. W przypadku konieczności użytkowania sieci i przedłużającej się awarii należy skorzystać z internetu mobilnego dostępnego w siedzibie firmy jako alternatywne źródło.

III. Za uruchomienie łącza alternatywnego odpowiada Administrator lub wskazana przez niego osoba.

3. Zapewnienie ciągłości pracy systemu przetwarzania danych osobowych bez udziału systemów informatycznych

a) Sytuacjami, które mogą uniemożliwiać przetwarzanie danych osobowych w przedsiębiorstwie ADO bez wykorzystania systemów informatycznych mogą być:

I. Brak możliwości dostępu do pomieszczeń, w których przetwarzane są dane osobowe,

II. Brak możliwości wykorzystania pomieszczeń, w których przetwarzane są dane osobowe ze względu na awarię np. zalanie pomieszczenia, awaria ogrzewania.

b) W przypadku wystąpienia sytuacji, o których mowa w niniejszym rozdziale każdy z użytkowników przetwarzających dane osobowe ma obowiązek niezwłocznego kontaktu telefonicznego i zgłoszenia tego faktu Administratorowi.

c) Administrator według najlepszej wiedzy i uznania niezwłocznie zgłasza zaistniałe usterki kompetentnym podmiotom według właściwości ich działania.

d) W przypadku braku możliwości wykorzystania pomieszczeń do przetwarzania danych osobowych z powodu awarii, Administrator jest zobowiązany wskazać użytkownikowi inne, spełniające wszystkie normy pomieszczenie, w którym będzie on mógł kontynuować swoje obowiązki.

Rozdział VII – POSTANOWIENIA KOŃCOWE

a) Niniejsza dokumentacja jest regularnie analizowana i aktualizowana w miarę konieczności przez ADO.

b) Niniejsza polityka jest dokumentem wewnętrznym i nie może być, bez zgody ADO, udostępniana osobom postronnym żadnej formie.

c) ADO ma obowiązek zapoznać z treścią niniejszej Polityki personel.

d) Personel zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.

e) W sprawach nieuregulowanych w niniejszej Polityce zastosowanie mają właściwe przepisy RODO.

Załącznik:

- Regulamin korzystania z poczty elektronicznej