Wójt Gminy Brzozie
woj. kujawsko-pomorskie

ZARZĄDZENIE Nr 39/2023
WÓJTA GMINY BRZOZIE
z dnia 13 czerwca 2023 r.

w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Gminy Brzozie

Na podstawie art. 24 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L 119 z 04.05.2016, str. 1, z późn. zm.) … zarządzam§, co następuje:

§ 1. Wprowadzam Politykę Ochrony Danych Osobowych w Urzędzie Gminy Brzozie zwaną dalej "Polityką", stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Polityka ma na celu dostosowanie środków technicznych i organizacyjnych do przepisów o ochronie danych osobowych, zapewnienie stosowania RODO, ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych oraz zapewnienie środków ochrony danych na poziomie adekwatnym do zidentyfikowanych ryzyk i zagrożeń dla ochrony danych.

§ 3. Politykę stosuje się do przetwarzania danych osobowych przez Urząd Gminy Brzozie, jako samodzielnego Administratora lub jako Współadministratora.

§ 4. Politykę stosuje się również do przetwarzania danych osobowych przez Urząd Gminy, jako podmiotu przetwarzającego w zakresie, w jakim umowa powierzenia przetwarzania danych osobowych go wiążąca (lub inny instrument prawny), nie stanowi inaczej.

§ 5. Zasady określone w Polityce obowiązują każdego pracownika, współpracownika, praktykanta, stażystę i wolontariusza, niezależnie od tego, czy będzie upoważniony do przetwarzania danych osobowych.

§ 6. Zobowiązuję pracowników Urzędu Gminy Brzozie do zapoznania się i ścisłego przestrzegania Polityki.

§ 7. Za dalsze monitorowanie adekwatności i aktualności Polityki odpowiada inspektor ochrony danych.

§ 8. Nadzór nad wykonaniem niniejszego zarządzenia powierzam inspektorowi ochrony danych.

§ 9. Traci moc zarządzenie Nr 17/2018 dnia 25 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Brzoziu oraz jednostkach organizacyjnych Gminy Brzozie.

§ 10. Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT

Danuta Kęckiarska-Cieszyńska

Wójt Gminy Brzozie
woj. kujawsko-pomorskie

Załącznik do zarządzenia Nr 39/2023
Wójta Gminy Brzozie
z dnia 13 czerwca 2023 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH W URZĘDZIE GMINY BRZOZIE

Rozdział 1
Postanowienie ogólne

§ 1. 1. Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych" („Polityka") ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Urzędzie Gminy Brzozie (dalej: Urząd) z siedzibą w Brzozie 50, 87-313 Brzozie, reprezentowanym przez Wójta Gminy Brzozie (dalej także jako "Administrator" lub "ADO").

2. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych lub RODO) (Dz. Urz. UE L 119, s. 1).

3. Celem wdrożenia niniejszej Polityki jest zapewnienie należytej, adekwatnej do zagrożeń i kategorii danych osobowych objętych ochroną ochrony danych osobowych będących w zasobach Administratora danych.

4. Wdrożenie Polityki ma zapewnić uzyskanie optymalnego dla działalności Urzędu i zgodnego z wymogami obowiązujących aktów prawnych sposobu przetwarzania informacji zawierających dane osobowe.

5. Urząd przetwarza dane osobowe oraz wytwarza i administruje dokumentacją zawierającą dane osobowe, dlatego podlega obowiązkowi zapewnienia zgodności z przepisami o ochronie danych osobowych.

6. Naruszenie ochrony danych osobowych może narazić na szkodę prawnie chroniony interes osób, których te dane dotyczą, a także Urząd odpowiedzialny za zapewnienie należytej ochrony tych danych.

7. Polityka ochrony danych osobowych określa sposób prowadzenia oraz zakres dokumentacji odnoszącej się do sposobu przetwarzania danych osobowych, a także określa środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych - odpowiednie do zagrożeń oraz kategorii danych objętych ochroną.

8. Zakres przedmiotowy stosowania niniejszej Polityki obejmuje wszystkie zbiory danych osobowych oraz czynności przetwarzania realizowane przez Administratora - odnosi się swoją treścią do informacji:

1) w formie papierowej - przetwarzanej w ramach tradycyjnego obiegu dokumentów;

2) w formie elektronicznej - przetwarzanej w ramach systemów informatycznych.

9. Zakres podmiotowy stosowania Polityki obejmuje wszystkich pracowników oraz inne osoby upoważnione przez Administratora do przetwarzania danych osobowych oraz uprawnione do przebywania w obszarach przetwarzania danych.

10. Niniejszy dokument stanowi najwyższej rangi dokument polityki ochrony danych osobowych w Urzędzie. Jest on wiążący dla wszystkich referatów Urzędu.

11. Z systemów przetwarzania danych osobowych znajdujących się w posiadaniu ADO mogą korzystać również inne podmioty, na podstawie odrębnych umów, porozumień lub stosunków prawnych, kształtowanych na podstawie przepisów szczególnych, określających zasady korzystania z tych systemów, w szczególności poprzez wyraźnie zdefiniowanie celu i zakresu takiego korzystania oraz wskazanie odpowiedzialności.

12. Polityka ma zastosowanie do przetwarzania danych osobowych niezależnie od:

1) sposobu przetwarzania (całkowicie zautomatyzowany, częściowo zautomatyzowany lub inny niż zautomatyzowany);

2) formy lub postaci przetwarzania (papierowa, elektroniczna lub inna);

3) kanałów przepływu danych osobowych;

4) narzędzi informatycznych służących do przetwarzania danych osobowych (systemów, aplikacji, programów);

5) celu przetwarzania;

6) źródła pochodzenia danych osobowych;

7) kategorii danych osobowych.

13. Administrator prowadzi i stosuje rejestry i szczegółowe procedury dotyczące ochrony danych osobowych, które stanowią integralną część Polityki.

Rozdział 2
Podstawy prawne

§ 2. W zakresie nieuregulowanym niniejszą Polityką stosuje się, przepisy:

1) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych lub RODO) (Dz.Urz. UE L 119, s. 1) [„RODO"];

2) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) [„Ustawa"];

3) ustawy o samorządzie gminnym;

4) kodeksu pracy;

5) kodeksu postępowania administracyjnego;

6) kodeksu cywilnego;

7) ustawy o zakładowym funduszu świadczeń socjalnych.

Rozdział 3

Skróty i definicje

§ 3. 1. Użyte w Polityce definicje i pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą Polityką oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte przez Administratora w zakresie ochrony danych osobowych.

2. Użyte w „Polityce ochrony danych osobowych" pojęcia, definicje i skróty oznaczają:

1) **Administrator danych osobowych** (Administrator, ADO) – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. W niniejszej Polityce przez Administratora rozumie się:

2) Urząd Gminy Brzozie;

3) Gminę Brzozie;

4) Wójta Gminy Brzozie;

5) Radę Gminy Brzozie;

6) Radnego Rady Gminy Brzozie;

7) Urząd Stanu Cywilnego.

Każdy z powyższych ADO w zakresie nadanych mu kompetencji przetwarza dane osobowe we własnych procesach, a więc każdy z osobna musi zrealizować wymóg przetwarzania danych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 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 z 2016 r. 119, s. 1 ze zm.) – dalej RODO.

2) **Administrator Systemu/Informatyk (AS)** – wyznaczona przez Administratora osoba odpowiedzialna za sprawne funkcjonowanie systemu informatycznego w Urzędzie. Rolę Administratora Systemu pełni informatyk lub osoba go zastępująca.

3) **Anonimizacja** – proces przetwarzania treści poprzez usunięcie informacji pozwalających na identyfikację osób fizycznych.

4) **Audyt bezpieczeństwa** – czynności formalne mające na celu sprawdzenie, czy dane dokumenty lub systemy przetwarzania informacji spełniają założenia Polityki ochrony danych osobowych

5) **Autentyczność informacji** – zasada, zgodnie z którą tożsamość osób lub zasobu jest taka, jak deklarowana; autentyczność dotyczy: użytkowników, procesów, systemów i informacji.

6) **Bezpieczeństwo informacji** – zapewnienie odpowiedniego poziomu poufności, integralności i dostępności informacji, ochrona informacji przed nieautoryzowanym dostępem, modyfikacją,

zatajeniem, kradzieżą i zniszczeniem.

7) **Bezpowrotne niszczenie informacji** – działania zapewniające, że (przy określonych założeniach pracochłonności) informacja nie może być odzyskana z nośników, na których była zapisana. Obejmuje to również zniszczenie poprzez fizyczne uszkodzenie nośników danych w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod.

8) **Dane osobowe** – oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, 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, w tym wizerunek, nagranie głosu, dane kontaktowe, dane o lokalizacji, informacje zawarte w korespondencji, informacje gromadzone za pośrednictwem sprzętu rejestrującego lub innej podobnej technologii.

9) **Dane dzieci** – dane osób poniżej 16 roku życia.

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

11) **Dane szczególnych kategorii** – 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.

12) **Dane wrażliwe** oznaczają dane szczególnych kategorii i dane karne.

13) **Dokument elektroniczny** – dokument utrwalony na nośnikach magnetycznych, optycznych lub w pamięci układów elektronicznych.

14) **Dostęp zdalny do sieci wewnętrznej Urzędu** – zapewnienie możliwości połączenia się do sieci określonym użytkownikom pracującym na komputerach podłączonych do sieci Internet poza siecią wewnętrzną Urzędu.

15) **Dostępność informacji** – informacja jest dostępna i możliwa do wykorzystania na każde autoryzowane żądanie, w założonym czasie.

16) **Dziennik ewidencji kopii bezpieczeństwa** – dokument zawierający opis wszystkich czynności związanych z tworzeniem oraz weryfikacją kopii bezpieczeństwa.

17) **Hasło użytkownika** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

18) **Incydent bezpieczeństwa** – sytuacja kryzysowa związana z nieautoryzowanym dostępem

do danych osobowych, ich zniszczeniem, modyfikacją, utratą lub innym celowym działaniem naruszającym bezpieczeństwo ochrony danych osobowych. Incydentem bezpieczeństwa jest również próba podjęcia wymienionych działań.

19) **Informacje** – treści wszelkiego rodzaju przechowywane na dowolnym nośniku informacji, w postaci tradycyjnej - dokumentacja papierowa jak i elektronicznej - układy elektroniczne oraz inne nośniki, np. magnetyczne lub optyczne. Informacja może być wyrażona za pomocą mowy, pisma, obrazu, rysunku, znaku, kodu, dźwięku lub w jakikolwiek inny sposób.

20) **Informacje chronione** – informacje prawnie chronione przetwarzane przez Administratora, w tym w szczególności dane osobowe. Mają jasno określone reguły dostępu i są chronione przed nieautoryzowanym dostępem, powielaniem, ujawnieniem, modyfikacją, zatajeniem, jak również zniszczeniem, utratą, nieprawidłowym wykorzystaniem lub kradzieżą.

21) **Informacje jawne** - informacje zabezpieczone przed modyfikacją i utratą (zniszczeniem), nie należące do informacji chronionych.

22) **Inspektor ochrony danych [IOD]** – osoba wyznaczona przez Administratora, nadzorująca przestrzeganie przepisów o ochronie danych osobowych w organizacji Administratora, wykonująca zadania określone w art. 39 RODO.

23) **Koordynator Ochrony Danych Osobowych (KODO)** – osoba wyznaczona przez Administratora, realizująca w organizacji Administratora zadania związane z zapewnieniem zgodności przetwarzania Danych osobowych z obowiązującym prawem.

24) **Integralność informacji** – zasada, zgodnie z którą system realizuje funkcję przetwarzania danych w sposób nienaruszony, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.

25) **Kopia bezpieczeństwa** (back-up) – kopia oprogramowania lub danych, pozwalająca na ich dokładne odtworzenie w wypadku utraty oryginału.

26) **Licencja dostępowa** – plik zawierający certyfikat użytkownika zabezpieczony hasłem, pozwalający na zestawianie szyfrowanego tunelu oprogramowaniem VPN pomiędzy komputerem zdalnym a siecią Urzędu.

27) **Login – identyfikator użytkownika** – nazwa użytkownika w systemie przetwarzania informacji.

28) **Logowanie** – proces uwierzytelniania użytkownika w systemie przetwarzania informacji.

29) **Kierownik referatu** – osoba określająca zakres, metody przetwarzania i dostęp do danych osobowych przetwarzanych w danym referacie.

30) **Modyfikacja informacji** – zmiana zapisu informacji w systemie przetwarzania.

31) **Nośnik informacji** – pamięć układów elektronicznych, medium magnetyczne, optyczne lub papierowe, na którym zapisuje się i przechowuje informacje.

32) **Nieautoryzowany dostęp** – wykonanie operacji w systemie przetwarzania danych, do której osoba nie została uprawniona (np. zapis, odczyt, udostępnienie lub usuwanie danych itp.).

33) **Niezawodność informacji** – spójne, powtarzalne, zamierzone zachowania i skutki.

34) **Ograniczenie przetwarzania** – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

35) **Osoba/Podmiot danych** – osoba, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

36) **Oprogramowanie VPN** – oprogramowanie zapewniającej dostęp zdalny do sieci Urzędu w postaci szyfrowanego tunelu.

37) **Organ nadzorczy** – Prezes Urzędu Ochrony Danych Osobowych lub ewentualnie właściwy organ nadzorczy w zakresie danych osobowych wyznaczony przez inne państwo członkowskie Unii Europejskiej.

38) **Podmiot przetwarzający/Przetwarzający** – organizacja lub osoba, której ADO powierzył przetwarzanie danych osobowych (np. usługodawca IT, obsługa prawna, obsługa informatyczna).

39) **Polityka ochrony danych osobowych/Polityka** – niniejszy dokument wraz z załącznikami.

40) **Poufność informacji** – informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom albo procesom.

41) **Prawa dostępu** – listy określające rodzaj operacji, jakie użytkownik może wykonać na udostępnionej informacji w systemie przetwarzania.

42) **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.

43) **Przetwarzanie danych** – oznacza operację 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.

44) **RCPD/Rejestr** – Rejestr Czynności Przetwarzania Danych Osobowych, prowadzony zgodnie z art. 30 ust. 1 RODO.

45) **RKCPD/Rejestr Kategorii Przetwarzania** – Rejestr Kategorii Czynności Przetwarzania Danych Osobowych, prowadzony zgodnie z art. 30 ust. 2 RODO.

46) **Rejestr zdarzeń systemowych** – pliki generowane przez system lub oprogramowanie dodatkowe, zawierające zapis zdarzeń związanych z pracą systemu komputerowego.

47) **Rola** – określony rodzaj praw dostępu do informacji, jakie nadaje się użytkownikom informacji. Każdy użytkownik informacji ma przyznane jasno określone role związane z dostępem do danych informacji.

48) **Rozliczalność** informacji – właściwość systemu pozwalająca przypisać określone działanie

w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie. Administrator jest odpowiedzialny za przestrzeganie zasad dotyczących przetwarzania danych osobowych i musi być w stanie wykazać ich przestrzeganie (udokumentować realizację zasad związanych z ochroną danych osobowych).

49) **Rozporządzenie/RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

50) **Serwer** - komputer świadczący usługi, sprowadzające się zazwyczaj do udostępniania pewnych zasobów innym komputerom lub pośredniczący w przekazywaniu danych między komputerami.

51) **Serwer VPN** – komputer w sieci Urzędu obsługujący dostęp zdalny do sieci Urzędu dla komputerów wyposażonych w oprogramowanie VPN.

52) **Serwerownia** – wydzielone i zabezpieczone pomieszczenie będące środowiskiem pracy komputerów pełniących rolę serwerów, a także aktywnych i pasywnych elementów sieci komputerowych.

53) **Sieć wewnętrzna Urzędu** – sieć telekomunikacyjna eksploatowana wyłącznie przez Urząd.

54) **System informatyczny** – system przetwarzania informacji składający się z urządzeń komputerowych, oprogramowania oraz zewnętrznych nośników informacji (płyta DVD-R, CD-R i inne).

55) **System przetwarzania** (informacji) – zespół określonych komponentów fizycznych i logicznych, współpracujących ze sobą według określonych reguł, służący do przetwarzania informacji.

56) **System zapasowy** – system przeznaczony do przejęcia zadań w razie awarii systemu przetwarzania informacji.

57) **Szyfrowanie** – proces polegający na takim przetworzeniu informacji chronionych, aby nie mogły być one odczytane przez osoby nieupoważnione.

58) **Tajemnica** – nie ujawnione do wiadomości publicznej informacje, których zakres regulowany jest ustawowo lub poprzez akty administracyjne wydawane przez Urząd lub jednostki nadrzędne, w szczególności: techniczne, finansowe, handlowe, organizacyjne.

59) **Transfer danych** – przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

60) **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych o ochronie danych osobowych.

61) **Uwierzytelnianie** – proces pozwalający na jednoznaczną identyfikację użytkownika w systemie przetwarzania informacji.

62) **Użytkownik systemu** – osoba upoważniona, która otrzymała uprawnienia do przetwarzania danych osobowych w ramach systemów informatycznych, wynikających z upoważnienia.

63) **Użytkownik zewnętrzny** – osoba nie będąca pracownikiem Urzędu lub podmiot, wykorzystujący

informacje chronione, których Administratorem jest Urząd.

64) **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

65) **Zasilanie awaryjne** – zapasowy system zasilania, umożliwiający czasowe dostarczenie zasilania do systemu przetwarzania informacji.

Rozdział 4

Ochrona danych osobowych w Urzędzie - zasady ogólne

§ 4. 1. Filary ochrony danych osobowych w Urzędzie:

1) **Legalność** – ADO dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
2) **Bezpieczeństwo** – ADO zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
3) **Prawa Jednostki** – ADO umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
4) **Rozliczalność** – ADO dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

2. Zasady ochrony danych

ADO przetwarza dane osobowe z poszanowaniem następujących zasad:

1) w oparciu o podstawę prawną i zgodnie z prawem **(legalizm);**
2) dane są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami **(ograniczenie celu);**
3) przetwarzanie jest realizowane rzetelnie i uczciwie (**rzetelność**);
4) dane przetwarzane są w sposób przejrzysty dla osoby, której dane dotyczą **(transparentność);**
5) dane są zbierane w konkretnych celach i nie "na zapas" **(minimalizacja);**
6) dane są przetwarzane tylko w celach w jakich zostały zebrane, nie więcej niż potrzeba **(adekwatność);**
7) przetwarzanie jest realizowane z dbałością o prawidłowość danych **(prawidłowość);**
8) dane są przechowywane nie dłużej niż potrzeba **(czasowość);**
9) Administrator zapewnia bezpieczeństwo danych **(bezpieczeństwo);**
10) Administrator jest odpowiedzialny za przestrzeganie obowiązujących przepisów prawa i musi być w stanie wykazać ich przestrzeganie **("rozliczalność").**

3. System ochrony danych

System ochrony danych osobowych w Urzędzie składa się z następujących elementów:

1) **Inwentaryzacja danych.**

Urząd dokonuje cyklicznej identyfikacji zasobów danych osobowych, klas danych, zależności między

zasobami danych, identyfikacji sposobów wykorzystania ewentualnych danych (inwentaryzacja), w tym:

a) przypadków ewentualnego przetwarzania danych wrażliwych (**dane wrażliwe**);

b) przypadków przetwarzania danych osób, których Urząd nie identyfikuje (**dane niezidentyfikowane**);

c) przypadków przetwarzania danych dzieci;

d) profilowania;

e) współadministrowania danymi.

2) **Rejestr.** ADO opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych w Urzędzie. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Urzędzie.

3) **Podstawy prawne.** Urząd zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych.

4) **Obsługa praw jednostki.** Urząd spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

a) **Obowiązki informacyjne.** ADO przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia dokumentowanie realizacji tych obowiązków.

b) **Możliwość wykonania żądań.** ADO weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

c) **Obsługa żądań.** ADO zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i ich dokumentowanie.

d) **Zawiadamianie o naruszeniach.** ADO stosuje procedury pozwalające na ustalenie konieczności zawiadomienia Prezesa UODO i osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5) **Minimalizacja.** Urząd posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

a) zasady zarządzania **adekwatnością** danych,

b) zasady reglamentacji i zarządzania **dostępem** do danych,

c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;

6) **Bezpieczeństwo.** ADO zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii,

b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie,

c) dostosowuje środki ochrony danych do ustalonego ryzyka,

d) posiada system zarządzania bezpieczeństwem informacji,

e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Prezesowi Urzędu Ochrony Danych Osobowych – zarządza incydentami.

7) **Przetwarzający.** ADO posiada zasady doboru przetwarzających dane na rzecz Urzędu, wymogów, co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

8) **Transfer danych.** ADO posiada zasady weryfikacji, czy Urząd nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodne z prawem warunki takiego przekazywania, jeśli ma ono miejsce.

9) ***Privacy by design.*** ADO zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Urzędzie uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

10) **Przetwarzanie transgraniczne.** Urząd posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

11) **Profilowanie.** ADO 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, ADO postępuje zgodnie z przyjętymi zasadami w tym zakresie.

12) **Współadministrowanie.** ADO identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

4. Rejestr Czynności Przetwarzania Danych (RCPD)

1) 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.

2) ADO prowadzi RCPD, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

3) RCPD jest jednym z podstawowych narzędzi umożliwiających ADO rozliczanie większości obowiązków ochrony danych.

4) ADO dokumentuje w RCPD podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

5) W Rejestrze, dla każdej czynności przetwarzania danych, którą ADO uznał za odrębną dla potrzeb Rejestru, odnotowuje się 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 ADO, jeśli podstawą jest uzasadniony

interes, (VI) opis kategorii odbiorców danych (w tym przetwarzających), (VII) informację o przekazaniu poza EU/EOG; (VIII) ogólny opis technicznych i organizacyjnych środków ochrony danych.

6) RCPD może zawierać informacje nieobowiązkowe - dodatkowe (rejestracja informacji w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść RCPD ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej).

5. Podstawy prawne przetwarzania danych osobowych

Referaty Urzędu przetwarzają dane osobowe utrwalone w postaci papierowej lub elektronicznej, w szczególności, w związku z realizacją zadań wynikających z przepisów prawa krajowego i Unii Europejskiej oraz zadań określonych w regulaminie organizacyjnym Urzędu:

1) Dane osobowe, z wyłączeniem danych osobowych określonych w ust. 2 i 3, są przetwarzane w Urzędzie na podstawie następujących przesłanek:

a) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze danych **(art. 6 ust. 1 lit. c RODO);**

b) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi **(art. 6 ust. 1 lit. e RODO)** *(stosowany, kiedy nie ma wyraźnego przepisu prawa, ale może być wykazany interes publiczny lub sprawowanie władzy publicznej w odpowiednim zakresie, wynikającym z przepisów);*

c) 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 **(art. 6 ust. 1 lit. b RODO)**;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej **(art. 6 ust. 1 lit. d RODO)**;

e) przetwarzanie jest niezbędne do celów, które wynikają z prawnie uzasadnionych interesów realizowanych przez Administratora **(art. 6 ust. 1 lit. f RODO)** *(przesłanki tej nie można stosować, kiedy Administrator wykonuje zadania organu);*

f) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów, jeżeli przetwarzanie nie odbywa się na podstawie przesłanek wskazanych w ppkt a-e **(art. 6 ust. 1 lit. a RODO)**.

W zakresie zgody:

— ADO wdraża metody zarządzania zgodami, umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, np. zgody na komunikację na odległość (e-mail, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

— Każdy pracownik odbierający zgodę osoby, której dane dotyczą, tworzy warunki, aby zgoda była udzielona dobrowolnie, świadomie i wobec konkretnego celu, a także w przypadku, kiedy zgoda

nie jest składana na piśmie, dokumentuje, w szczególności adnotacją, czy była złożona przez oświadczenie czy wyraźne działanie osoby, której dane dotyczą, potwierdzające przyzwolenie na przetwarzanie dotyczących jej danych osobowych.

- Zgoda nie może być domniemana lub dorozumiana ani wywiedziona z oświadczenia woli o innej treści.
- Urząd, przetwarzając dane osobowe na podstawie zgody, zapewnia – przed wyrażeniem zgody przez osobę, której dane dotyczą – o poinformowaniu jej, że zgoda może być cofnięta w każdym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
- Odbieranie zgody odbywa się w formie możliwej do późniejszego udowodnienia (zasada rozliczalności), w szczególności w formie pisemnej.

2) **Dane osobowe szczególnych kategorii**, o których mowa w art. 9 RODO, są przetwarzane w na podstawie następujących przesłanek:

a) przetwarzanie jest niezbędne do wypełnienia obowiązku i wykonywania szczególnych praw przez Administratora danych lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej **(art. 9 ust. 2 lit. b RODO);**

b) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody **(art. 9 ust. 2 lit. c RODO)**;

c) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego **(art. 9 ust. 2 lit. g RODO)**;

d) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego lub leczenia **(art. 9 ust. 2 lit. h RODO)**;

e) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi **(art. 9 ust. 2 lit. i RODO)**;

f) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów **(art. 9 ust. 2 lit. a RODO)**.

Zgoda na przetwarzanie danych szczególnych musi być wyrażona na piśmie.

3) Dane osobowe dotyczące **wyroków skazujących i czynów zabronionych** są przetwarzane w Urzędzie, gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze danych **(art. 10 RODO)**.

Rozdział 5

Administrator Danych Osobowych

§ 5. Administrator dokłada należytej staranności w celu ochrony interesów osób, których dane dotyczą, w szczególności jest obowiązany zapewnić, aby dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych celów, merytorycznie poprawne i adekwatne do celów w jakich są zbierane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą oraz aby zapewniona była legalność, bezpieczeństwo, prawa jednostki i rozliczalność danych.

2. Administrator stosuje środki techniczne i organizacyjne zapewniające ochronę danych osobowych odpowiednią do zagrożeń oraz kategorii przetwarzanych danych oraz zabezpiecza posiadane dane przed: ich udostępnieniem, zmianą, utratą, uszkodzeniem, zniszczeniem lub przetwarzaniem przez osobę nieupoważnioną.

3. Administrator w szczególności zapewnia:

1) środki techniczne i organizacyjne niezbędne dla zapewnienia bezpiecznego przetwarzania danych w pomieszczeniach do tego przeznaczonych;
2) systemy i sprzęt informatyczny umożliwiające niezawodne i bezpieczne przetwarzanie danych;
3) dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie do przetwarzania danych osobowych;
4) zapoznanie z przepisami o ochronie danych osobowych każdej osoby upoważnionej do przetwarzania danych osobowych;
5) prowadzenie ewidencji osób upoważnionych;
6) należyte i terminowe udzielanie informacji na wniosek osób, których dane są przetwarzane i które zwróciły się z wnioskiem o udzielenie informacji zgodnie z RODO;
7) obligowanie do poufności osób upoważnionych do przetwarzania danych oraz uprawnionych do przebywania w obszarach przetwarzania danych;
8) przeprowadzanie oceny skutków dla ochrony danych, a gdy to konieczne przeprowadzenie niezbędnych konsultacji;
9) rejestrowanie czynności przetwarzania w rejestrach, o których mowa w art. 30 RODO;
10) podejmowanie niezwłocznych działań minimalizujących ryzyka dla ochrony danych osobowych;
11) zgłaszanie naruszeń, które mogą powodować negatywne skutki dla osoby, której dane dotyczą do organu nadzorczego;
12) w przypadku wysokiego ryzyka naruszenia, zawiadamianie osób, których dane dotyczą;
13) podnoszenie wiedzy osób przetwarzających dane osobowe;
14) korzystanie z podmiotów przetwarzających dających wystarczające gwarancje ochrony danych, na podstawie umowy powierzenia;
15) uwzględnianie prywatności w nowych procesach przetwarzania, a także stosowanie zasady domyślnej ochrony danych osobowych (**zasad Privacy by design i Privacy by default).**

4. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów o ochronie danych osobowych albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia.

5. Administrator jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił dane osobowe, o dokonanym uaktualnieniu lub sprostowaniu danych.

6. Administrator na bieżąco dostosowuje systemy informatyczne służące do przetwarzania danych i wszelkie systemy zabezpieczeń przetwarzania danych osobowych do wymogów określonych w obowiązujących przepisach prawa oraz ryzyk i zagrożeń dla przetwarzanych danych.

7. Zapewnia właściwe i niezwłoczne włączanie IOD we wszystkie sprawy dotyczące ochrony danych osobowych, począwszy od etapu ich projektowania oraz analizowania ryzyka dla ochrony danych osobowych, przez ich realizację, wdrożenie, aż do usunięcia danych osobowych, w szczególności konsultuje z IOD:

1) projekty aktów prawnych, regulacji wewnętrznych i innych dokumentów, w tym związanych z organizacją Urzędu, mających związek z przetwarzaniem lub ochroną danych osobowych;
2) planowane lub podejmowane przedsięwzięcia, w tym realizowane projekty, programy i inne inicjatywy, związane z przetwarzaniem danych osobowych;
3) szkolenia, konferencje i inne spotkania, w szczególności spotkania z udziałem przedstawicieli UODO lub dotyczące ochrony danych osobowych.

Rozdział 6
Inspektor ochrony danych oraz koordynator ochrony danych osobowych

§ 6. 1. Inspektor ochrony danych jest wyznaczany przez Administratora na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO.

2. Do zadań inspektora ochrony danych należy:

1) informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania RODO, innych przepisów o ochronie danych oraz polityk Administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;

4) współpraca z organem nadzorczym;

5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz, w stosownych przypadkach, prowadzenie konsultacji we wszelkich innych sprawach.

3. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

4. Status inspektora ochrony danych:

1) Administrator zapewnia, by inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;

2) Administrator wspiera inspektora w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby i przedsięwzięcia niezbędne do utrzymania właściwego poziomu oraz aktualizacji jego wiedzy fachowej;

3) Administrator zapewnia, aby inspektor nie otrzymywał instrukcji dotyczących wykonywania tych zadań;

4) Inspektor podlega bezpośrednio **Wójtowi Gminy Brzozie**;

5) Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw im przysługujących;

6) Inspektor jest zobowiązany do zachowania tajemnicy lub poufności, co do wykonywania swoich zadań.

5. Inspektor ochrony danych w szczególności:

1) nadzoruje przestrzeganie zasad ochrony;

2) jest umocowany do przetwarzania danych chronionych w ramach wykonywania swoich obowiązków;

3) akceptuje projekty dokumentów mających wpływ na bezpieczeństwo danych osobowych;

4) nadzoruje pod względem bezpieczeństwa danych osobowych pracę wszystkich pracowników Urzędu oraz Administratora Systemu;

5) prowadzi rejestr incydentów bezpieczeństwa (rejestr naruszeń ochrony danych osobowych, o którym mowa w Art. 33 ust. 5 RODO);

6) analizuje raporty wszelkich zdarzeń związanych z bezpieczeństwem danych osobowych;

7) przeprowadza szkolenia, o których mowa w art. 39 ust. 1 lit. a RODO;

8) weryfikuje podmioty przed zawarciem umowy powierzenia przetwarzania danych osobowych;

9) nadzoruje prowadzenie rejestru czynności przetwarzania danych osobowych w Urzędzie;

10) opiniuje żądania osób, których dane dotyczą kierowanych do Administratora na podstawie RODO;

11) sporządza projekty dokumentacji związanej z ochroną danych osobowych oraz aktualizuje niniejszą politykę.

6. **IOD** współpracuje z koordynatorem ochrony danych osobowych.

7. **Koordynator ochrony danych osobowych jest** wyznaczany przez Wójta Gminy Brzozie.

8. Do zadań koordynatora ochrony danych osobowych należy w szczególności:

1) wsparcie IOD w uzyskiwaniu niezbędnych informacji w obrębie organizacji (organizacyjno-technicznych);

2) prowadzenie komunikacji wśród pracowników;

3) monitorowanie realizacji obowiązków zleconych przez IOD-a;

4) wykonywania czynności techniczno-organizacyjne w zakresie prowadzenia dokumentacji ochrony danych osobowych;

5) prowadzenie ewidencji wydanych upoważnień do przetwarzania danych osobowych .

Rozdział 7

Odpowiedzialność kierowników referatów, administratora systemu oraz osób upoważnionych

§ 7. 1. Każdy **kierownik referatu** Urzędu, w którym przetwarzane są dane osobowe, sprawuje nadzór nad przetwarzaniem i ochroną danych osobowych w podległym referacie w celu zapewnienia zgodności ich przetwarzania z przepisami prawa i jest odpowiedzialny za:

1) zapewnienie, aby bieżące przetwarzanie danych osobowych, w szczególności przetwarzanych w zbiorach danych osobowych było zgodne z powszechnie obowiązującymi przepisami prawa i aktami wewnętrznymi Urzędu, w szczególności niniejszą Polityką;
2) współdziałanie z IOD w zakresie zapewnienia przestrzegania ochrony danych osobowych;
3) występowanie z wnioskiem o nadanie, zmianę lub odebranie uprawnień do przetwarzania danych osobowych, w tym do ich przetwarzania w systemie informatycznym, jeżeli dane przetwarzane są w formie elektronicznej, zgodnie z procedurą nadawania uprawnień ujętą w dokumencie określającym szczegółowe zasady zarządzania systemami informatycznymi;
4) zgłaszanie IOD zamiaru tworzenia, modyfikacji lub likwidacji zbioru/procesu, za który jest odpowiedzialny;
5) zgłaszanie IOD oraz Administratorowi zdarzeń zagrażających ochronie danych osobowych, mogących stanowić naruszenie ochrony danych osobowych i uczestniczenia w czynnościach wyjaśniających;
6) zawiadamianie, w uzgodnieniu z IOD, osoby, których dane zostały dotknięte naruszeniem ochrony danych osobowych,
7) zarządzanie wyznaczonym procesem przetwarzania danych osobowych w referacie;

8) poprawność merytoryczną danych osobowych przetwarzanych w danym procesie oraz ich aktualizację;
9) poinformowanie IOD o zmianach dotyczących danego procesu przetwarzania danych (zmiany w przepisach prawa, zakresie danych, okresu ich przechowywania, odbiorcach danych) w celu aktualizacji RCPD;
10) zgłaszanie do IOD informacji o zakończeniu przetwarzania danych osobowych w ramach danego procesu przetwarzania;
11) zgłaszanie do IOD zamiaru wprowadzenia nowego procesu przetwarzania danych osobowych
12) zgłaszanie do IOD wpływających zapytań i wniosków od osób, których dane dotyczą ;
13) określanie zakresu, metod przetwarzania i dostępu do danych osobowych,
14) dokonywanie przeglądu i usuwania danych osobowych;
15) zapewnienie właściwego i niezwłocznego włączania IOD we wszystkie sprawy dotyczące ochrony danych osobowych, w szczególności konsultuje z IOD:

a) projekty umów powierzenia przetwarzania danych osobowych,
b) projekty pism dotyczących ochrony danych osobowych kierowane do jednostek organizacyjnych podległych ADO albo przez niego nadzorowanych, w szczególności pism kierowanych do UODO,
c) środki ochrony praw i wolności osób, których dane osobowe dotyczą,
d) rozwiązania organizacyjne pod kątem właściwego wdrażania systemu ochrony danych osobowych;

16) przekazywanie do IOD dokumentacji i niezbędnych wyjaśnień na potrzeby kontroli zewnętrznych dotyczących ochrony danych osobowych.

2. Administrator Systemu (AS)/Informatyk w szczególności:

1) dba o poprawne, efektywne i bezpieczne działanie administrowanego systemu przetwarzania danych osobowych;
2) zapewnia ciągłość działania systemu;
3) inicjuje, koordynuje i nadzoruje działania mające na celu poprawę wydajności i bezpieczeństwa systemu;
4) instaluje i konfiguruje sprzęt i oprogramowanie;
5) zakłada, likwiduje oraz blokuje/odblokowuje konta użytkowników;
6) przyznaje/odbiera prawa dostępu do aplikacji służących do przetwarzania danych osobowych w systemie informatycznym;
7) zabezpiecza system teleinformatyczny, a także koordynuje działania związane z poprawnym funkcjonowaniem tego systemu;
8) współpracuje z właścicielem biznesowym w zakresie analizy ryzyka w odniesieniu do przetwarzania danych osobowych w systemie teleinformatycznym;
9) informuje ADO o wszelkich incydentach lub anomaliach związanych z systemem

teleinformatycznym służącym do przetwarzania danych osobowych;

10) w przypadku otrzymania informacji o naruszeniu lub podejrzeniu naruszenia zabezpieczeń, podejmuje natychmiastowe działania mające na celu zabezpieczenie stanu systemu teleinformatycznego, przeciwdziałanie skutkom naruszenia oraz podejmuje działania związane z wdrożeniem zabezpieczeń w systemie, a także współpracuje w ramach czynności wyjaśniających naruszenia;
11) nadzoruje funkcjonowaniem zabezpieczeń dotyczących przesyłania danych osobowych drogą teletransmisji;
12) wykonuje i zarządza kopiami zapasowymi.

3. Każda osoba (pracownik, stażysta, zleceniobiorca) upoważniona do przetwarzania danych osobowych jest obowiązana do należytego przestrzegania zasad ochrony danych osobowych określonych w RODO, ustawie - jeśli ma zastosowanie - oraz w Polityce, w szczególności do:

1) przetwarzania danych osobowych w zakresie swojego upoważnienia i zgodnie z celami przetwarzania;
2) przestrzegania zasad bezpieczeństwa dotyczących eksploatacji systemów teleinformatycznych i ochrony antywirusowej, a także korzystania z systemów teleinformatycznych służących do przetwarzania danych osobowych wyłącznie zgodnie z ich przeznaczeniem i w zakresie swoich zadań, a także do ochrony przed nieupoważnionym dostępem do tych systemów;
3) informowania przełożonego o wszelkich zauważonych nieprawidłowościach i zdarzeniach skutkujących lub mogących skutkować obniżeniem poziomu ochrony danych osobowych;
4) zgłaszania zdarzeń mogących stanowić naruszenie ochrony danych osobowych i uczestniczenia w czynnościach wyjaśniających;
5) zapewnienia poufności przetwarzanych danych osobowych oraz poufności sposobów zabezpieczenia danych osobowych, w trakcie wykonywania powierzonych zadań i po ich zakończeniu, w tym zapewnienia ochrony danych osobowych przed nieuprawnionym dostępem (w tym fizycznym), nieuzasadnioną modyfikacją, zniszczeniem, ujawnieniem lub pozyskaniem danych;
6) zapoznania się z Polityką i potwierdzenia tego w formie pisemnej.

4. Obowiązek zachowania w tajemnicy danych osobowych, które osoba upoważniona przetwarza w trakcie zatrudnienia/współpracy z Administratorem, nie gaśnie wraz z rozwiązaniem stosunku pracy lub innej umowy łączącej ją z Administratorem.

5. Osoba upoważniona przed przystąpieniem do przetwarzania danych osobowych jest zobligowana do odbycia wewnętrznego szkolenia dotyczącego ochrony danych osobowych. Odbycie szkolenia jest dokumentowane.

6. Naruszenie zasad ochrony danych osobowych wynikających z powszechnie obowiązujących przepisów prawa lub niniejszej Polityki oraz innych wewnętrznych aktów prawnych Urzędu mogą zostać potraktowane jako ciężkie naruszenie obowiązków pracowniczych. W przypadku

osób nie będących pracownikami może wiązać się z karą umowną. W każdych okolicznościach Urząd może dochodzić odpowiedzialności od osoby, która naruszyła obowiązujące zasady ochrony danych osobowych.

Rozdział 8
Organizacja systemu ochrony danych osobowych

§ 8. Zasady ogólne

1. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Administrator uwzględnia przy tym stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania.
2. Przy ocenie, czy stopień bezpieczeństwa jest odpowiedni, Administrator uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. W celu zapewnienia integralności i poufności danych osobowych Administrator zapewnia dostęp do danych osobowych jedynie osobom upoważnionym i wyłącznie w zakresie, w jakim jest to niezbędne ze względu na wykonywane przez nie zadania. Administrator stosuje rozwiązania organizacyjne i techniczne w celu zapewnienia, że wszystkie operacje na danych osobowych są rejestrowane i realizowane tylko przez osoby uprawnione.
4. Administrator prowadzi na bieżąco analizę ryzyka związanego z przetwarzaniem danych osobowych i monitoruje adekwatność stosowanych zabezpieczeń danych osobowych do identyfikowanych zagrożeń. W razie konieczności Administrator wdraża dodatkowe środki służące zwiększeniu bezpieczeństwa danych osobowych.
5. W przypadku gdy rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Jeżeli ocena skutków wskazuje, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator konsultuje się z Organem nadzorczym.
6. Jeżeli cele, w których Administrator przetwarza dane osobowe, nie wymagają zidentyfikowania przez niego Podmiotu danych, Administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania Podmiotu danych wyłącznie

po to, by zastosować się do wymogów RODO.

7. Sposoby osiągnięcia spójnej ochrony danych osobowych:

1) standaryzacja postępowania oraz opracowanie niezbędnej dokumentacji, tj. zasad, procedur, regulaminów;

2) wdrożenie rozwiązań technicznych, zapewniających wymagany niniejszym dokumentem poziom bezpieczeństwa przetwarzanych danych – inwestycje w infrastrukturę sieci i systemów informatycznych oraz fizyczne zabezpieczenie obszarów przetwarzania danych osobowych;

3) propagowanie zasad bezpieczeństwa przetwarzania danych osobowych wśród kierownictwa i pracowników/współpracowników Urzędu;

4) szkolenie wszystkich nowozatrudnionych pracowników, którzy będą mieć określone w zakresie obowiązków zadania, z którymi będzie wiązało się przetwarzanie danych osobowych;

5) szkolenia okresowe osób posiadających upoważnienie do przetwarzania danych chronionych.

8. Następujące rodzaje informacji zostały zidentyfikowane, jako informacje chronione:

1) dane osobowe zagregowane w procesach przetwarzania danych osobowych;

2) pozostałe dane, takie jak dane kontrahentów stanowiące tajemnicę handlową.

9. Urząd chroni zarówno dane własne jak i powierzone.

10. Bezpieczeństwo danych osobowych jest to również wynik wszystkich ludzkich postaw, akceptowanych wartości i norm postępowania, które tworzą wszyscy pracownicy.

11. Bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz w dokumentach powiązanych muszą być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez użytkowników zewnętrznych przetwarzających dane, których Administratorem jest Urząd.

12. **Zabrania się używania wszelkich systemów przetwarzania informacji w Urzędzie do celów prywatnych.**

13. Informacje przekazywane, w sytuacjach nieuregulowanych odrębnymi przepisami prawa, podmiotom zewnętrznym do celów statystycznych, badawczych, itp. mogą zostać udostępnione jedynie za wyraźną zgodą Administratora, po uprzednim ich zanonimizowaniu.

14. Dostęp do danych osobowych oraz możliwość ich przetwarzania mają tylko osoby upoważnione przez Administratora. Zakres przetwarzanych danych osobowych określony jest w treści Upoważnienia.

15. Wszystkie osoby, których praca będzie wiązała się z przetwarzaniem danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu z zakresu obowiązujących przepisów prawa oraz zasad dotyczących ochrony danych osobowych.

16. Inne podmioty są uprawnione do przetwarzania danych osobowych tylko i wyłącznie na podstawie zawartej umowy powierzenia danych (podwykonawcy) lub porozumienia o współadministrowaniu danymi (partnerzy).

17. Zabronione jest przetwarzanie danych poza zakresem upoważnienia.

18. Osoby upoważnione nie są uprawnione do udostępnienia danych osobowych osobom lub podmiotom nieupoważnionym. Decyzję w zakresie udostępnienia podejmuje Administrator

§ 9. Zarządzanie użytkownikami

1. Jakakolwiek zmiana w zakresie przyznanych uprawnień do przetwarzania danych osobowych podlega niezwłocznie odnotowaniu w ewidencji, o której mowa w § 6 ust. 8 pkt 5.
2. Kierownik referatu powiadamiany jest osobiście **przez Sekretarza Gminy lub osobę zajmującą się sprawami kadrowymi** o:

1) zatrudnieniu pracownika;
2) przeniesieniu pracownika do innego referatu;
3) czasowym oddelegowaniu do innego referatu oraz jego zakończeniu;
4) zmianie stanowiska pracownika;
5) ustaniu zatrudnienia pracownika;
6) zmianie nazwiska pracownika;
7) nieobecnościach pracowników trwających co najmniej 30 dni (np. zwolnienia lekarskie);
8) nieobecnościach pracowników, co do których wiadomo, że będą trwały co najmniej 30 dni (np. urlopy macierzyńskie, urlopy bezpłatne);
9) powrocie pracownika po okresie nieobecności, o których mowa w pkt 7 i 8.

§ 10. Nadawanie dostępu do danych osobowych

1. **Odpowiedzialność w zakresie upoważnień do przetwarzania danych osobowych/ dostępu do aplikacji:**

1) **Administrator** – w zakresie zatwierdzania upoważnień lub ich zmiany;
2) **Sekretarz Gminy** – w zakresie wydawania/zmiany/odwoływania upoważnień do przetwarzania danych osobowych dla kierowników referatów i stanowisk samodzielnych;
3) **IOD** – w zakresie weryfikowania przestrzegania procedury upoważniania do przetwarzania danych osobowych, przygotowania treści upoważnienia, zgodnie z wnioskiem kierownika referatu;
4) **Kierownicy referatów** – w zakresie występowania z wnioskiem o nadanie/zmianę/odwołanie upoważnienia do przetwarzania danych osobowych dla podległych pracowników oraz innych osób im podległych (stażystów, praktykantów, wolontariuszy oraz osób realizujących zadania na podstawie umowy cywilnoprawnej na rzecz danej komórki organizacyjnej);
5) **Osoba upoważniana** – w zakresie przyjęcia i przestrzegania upoważnienia.

§ 11. Środki organizacyjne ochrony danych osobowych

1. Dostęp do danych chronionych posiadają tylko i wyłącznie osoby z odpowiednim pisemnym, imiennym upoważnieniem, udzielonym przez Administratora.

2. Upoważnienie uprawnia osobę, o której mowa w ust. 1 do przetwarzania danych osobowych wyłącznie w obszarze określonym zakresem czynności pracowniczych lub wynikającym z zadań realizowanych na podstawie umów cywilnoprawnych lub odrębnych regulacji.
3. Każda osoba upoważniona jest zobowiązana zachować szczególną ostrożność przy przetwarzaniu wszelkich danych osobowych.
4. Należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych.
5. Nośników informacji (w formie papierowej i elektronicznej) z danymi nie można pozostawiać, w miejscach ogólnodostępnych i niezabezpieczonych oraz nie należy udostępniać osobom nieupoważnionym.
6. Pomieszczenia, w których są przetwarzane dane osobowe muszą być zamykane na klucz lub inny system umożliwiający blokadę wejścia.
7. W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą one przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
8. Miejsca (np. szafy) przeznaczone do przechowywania danych muszą być zamykane na klucz.
9. Klucze do tych miejsc posiadają tylko pracownicy upoważnieni przez kierownika referatu.
10. Miejsca z danymi są otwarte tylko na czas potrzebny na dostęp do danych, a następnie zostają zamknięte. Dotyczy to zwłaszcza danych osobowych szczególnej kategorii, o których mowa w art. 9 RODO.
11. Dane chronione w formie papierowej mogą znajdować się w miejscach ogólnodostępnych (np. na biurkach) tylko w trakcie wykonywania czynności służbowych, a następnie muszą być przechowywane w miejscach przeznaczonych do tego celu (np. zamykana szafa).
12. Wydruki robocze zawierające informacje chronione, błędne lub zdezaktualizowane muszą być niezwłocznie bezpowrotnie niszczone przy użyciu niszczarki do papieru lub w inny sposób, zapewniający skuteczne ich usunięcie lub zanonimizowanie.

Rozdział 9

Realizacja praw osób, których dane osobowe są przetwarzane w Urzędzie (Podmiotów danych)

§ 12. 1. Administrator zapewnia, że realizuje uprawnienia Podmiotów danych na zasadach określonych w RODO, w tym:

1) **prawo do informacji o przetwarzaniu danych** – Administrator przekazuje osobie zgłaszającej żądanie informację o przetwarzaniu danych osobowych, w tym przede wszystkim o celach i podstawach prawnych przetwarzania, zakresie posiadanych danych osobowych, podmiotach, którym są ujawniane i planowanym terminie usunięcia danych osobowych;

2) **prawo uzyskania kopii danych** – Administrator przekazuje osobie zgłaszającej żądanie kopię danych osobowych, które jej dotyczą;

3) **prawo do sprostowania danych** – Administrator usuwa na żądanie ewentualne niezgodności lub błędy przetwarzanych danych osobowych oraz uzupełnia je, jeśli są niekompletne;
4) **prawo do usunięcia danych** – Administrator na żądanie usuwa albo anonimizuje dane osobowe, których przetwarzanie nie jest już niezbędne do realizowania żadnego z celów, dla których zostały zebrane;
5) **prawo do ograniczenia przetwarzania danych** – Administrator na żądanie zaprzestaje wykonywania operacji na danych osobowych – z wyjątkiem operacji, na które Podmiot danych wyraził zgodę – oraz ich przechowywania, zgodnie z przyjętymi zasadami retencji lub dopóki nie ustaną przyczyny ograniczenia przetwarzania danych osobowych (np. zostanie wydana decyzja Organu nadzorczego zezwalająca na dalsze przetwarzanie);
6) **prawo do przenoszenia danych** – w zakresie, w jakim dane osobowe są przetwarzane w sposób zautomatyzowany w związku z zawartą umową lub wyrażoną zgodą, Administrator na żądanie wydaje dane osobowe dostarczone przez osobę, której dotyczą, w formacie pozwalającym na odczyt danych osobowych przez komputer;
7) **prawo sprzeciwu wobec przetwarzania danych w celach marketingowych** – Podmiot danych może w każdym momencie sprzeciwić się przetwarzaniu danych osobowych w celach marketingowych, bez konieczności uzasadnienia takiego sprzeciwu;
8) **prawo sprzeciwu wobec innych celów przetwarzania danych** – Podmiot danych może w każdym momencie sprzeciwić się – z przyczyn związanych z jego szczególną sytuacją – przetwarzaniu danych osobowych, które odbywa się na podstawie prawnie uzasadnionego interesu Administratora;
9) **prawo wycofania zgody** – jeśli dane osobowe przetwarzane są na podstawie wyrażonej zgody, Podmiot danych ma prawo wycofać ją w dowolnym momencie, co jednak nie wpływa na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem.

2. Kontakty z Podmiotem danych

1) Administrator wdraża odpowiednie środki, aby komunikacja z Podmiotem danych odbywała się w zwięzłej, przejrzystej i łatwo dostępnej formie, jasnym i prostym językiem.
2) Administrator udziela Podmiotom danych informacji na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli Podmiot danych tego zażąda, Administrator udziela informacji ustnie.
3) Z wyjątkiem prawa do informacji, realizacja praw osób, których dane dotyczą, jeżeli jest możliwa, odbywa się na podstawie pisemnego wniosku osoby, której dane osobowe dotyczą.
4) W przypadku wątpliwości, co do tożsamości osoby zwracającej się z wnioskiem o realizację jej praw, tożsamość osoby jest weryfikowana, w szczególności poprzez uzyskanie informacji, która została podana we wcześniejszych kontaktach, a co do której można mieć pewność, że będzie ją posiadać jedynie osoba, której dane osobowe dotyczą.

5) Wpływające zapytania i wnioski dotyczące przetwarzanych w Urzędzie danych osobowych osób, których te dane dotyczą, są rejestrowane w ***prowadzonym przez IOD "Rejestrze wniosków i zapytań osób, których dane osobowe są przetwarzane w Urzędzie".***

6) **Administrator ułatwia Podmiotom danych wykonywanie praw przysługujących** im na gruncie RODO, w tym uprawnień przewidzianych w art. 15–22 RODO.

7) Administrator bez zbędnej zwłoki udziela Podmiotom danych informacji o działaniach podjętych w związku z żądaniem zgłoszonym na podstawie art. 15–22 RODO.

3. Realizacja wniosków osób, których dane dotyczą

1) Rozpatrywanie wniosków osób, których dane dotyczą, związanych z realizacją ich praw, wpływających do Urzędu, koordynuje IOD.

2) Odpowiedź na wniosek udzielana jest w terminie nie dłuższym niż miesiąc.

3) Za realizację merytoryczną wniosku odpowiedzialni są kierownicy referatów.

4) Inspektor weryfikuje kompletność danych adresowych oraz identyfikuje referat, w którym przetwarzane są dane osoby wnioskującej o realizację jej praw.

5) W sytuacji braku wystarczających informacji, umożliwiających zidentyfikowanie referatu, do którego wniosek powinien być przekazany, IOD występuje do osoby, która zwróciła się z wnioskiem o realizację jej praw, o uszczegółowienie informacji.

6) Po otrzymaniu informacji z referatu, realizującego przetwarzanie danych osobowych, dotyczących otrzymanego wniosku, Inspektor udziela w formie pisemnej odpowiedzi osobie wnioskującej.

7) W przypadku braku możliwości realizacji wniosku, informację o przyczynach braku możliwości jego realizacji, Inspektor przesyła osobie, która wystąpiła z wnioskiem o realizację jej praw.

8) Jeżeli wniosek osoby w zakresie przysługujących jej praw związanych z ochroną danych osobowych został przesłany bezpośrednio do referatu, kierownik tego referatu jest zobowiązany do niezwłocznego przekazania wniosku Inspektorowi.

4. Realizacja obowiązków informacyjnych

1) Realizacja obowiązku informacyjnego może odbywać się:

a) jednoetapowo - wszystkie informacje wskazane w art. 13 ust. 1 i 2 lub art. 14 ust. 1 i 2 RODO przekazywane są jednocześnie;

b) wieloetapowo (warstwowo) - najważniejsze informacje **(nazwa i dane kontaktowe ADO, kontakt do IOD, cel i podstawa prawna przetwarzania danych)** przekazywane są w momencie pierwszego kontaktu z osobą, której dane dotyczą, natomiast informacje szczegółowe o zasadach przetwarzania, przekazywane są poprzez stronę internetową Urzędu, BIP, tablice informacyjne znajdujące się w siedzibie Urzędu oraz pracownika merytorycznego.

2) Informacje podaje się w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, a zakres przekazywanych informacji należy dostosować do sposobu pozyskania danych osobowych.

3) Pozyskując dane osobowe od osoby, której dane dotyczą, Administrator danych przekazuje tej osobie informacje wskazane w art. 13 ust. 1 i 2 RODO w momencie pozyskania danych.
4) Jeżeli dane osobowe pozyskano z innego źródła niż od osoby, której dane dotyczą, Administrator danych podaje osobie informacje wskazane w art. 14 ust. 1 i 2 RODO.
5) Obowiązek, o którym mowa w pkt 3) i 4), jest realizowany przez udostępnienie w odpowiedni sposób klauzuli informacyjnej.
6) Informacje, o których mowa w pkt 4 podaje się w terminie:
a) nie później niż jednego miesiąca od momentu pozyskania danych osobowych, biorąc pod uwagę konkretne okoliczności przetwarzania danych osobowych;
b) najpóźniej przy pierwszej komunikacji z osobą, której dane dotyczą, jeżeli dane osobowe mają być stosowane do komunikacji z tą osobą;
c) najpóźniej przy pierwszym ujawnieniu danych osobowych, jeżeli planuje się je ujawnić innemu odbiorcy.
7) Za realizację obowiązków informacyjnych, o których mowa w pkt. 3) i 4) odpowiedzialni są kierownicy referatów, w których dane osobowe będą przetwarzane.
8) Informacje te mogą zostać przekazane ustnie, na piśmie, w tym drogą elektroniczną, a w szczególnych przypadkach – telefonicznie.
9) Zgodnie z zasadą rozliczalności, Urząd ma obowiązek wykazać spełnienie obowiązku informacyjnego (przekazanie klauzuli osobie, której dane dotyczą).

§ 13. Powierzenie przetwarzania danych osobowych

1. Urząd Gminy Brzozie, Gmina Brzozie, Wójt Gminy Brzozie, Rada Gminy Brzozie, Radny Rady Gminy Brzozie, Urząd Stanu Cywilnego, realizując swoje zadania związane z przetwarzaniem danych osobowych:

1) **jako administrator danych** – może powierzyć przetwarzanie danych osobowych w swoim imieniu innemu podmiotowi;
2) **jako podmiot przetwarzający** – może na zlecenie i w imieniu innego podmiotu, będącego administratorem danych, przetwarzać powierzone dane osobowe.

2. Administrator danych może powierzyć innemu podmiotowi przetwarzanie danych osobowych, w drodze odrębnej umowy zawartej w formie pisemnej lub elektronicznej albo poprzez uwzględnienie w umowie głównej postanowień zawierających uregulowania analogiczne, jak w odrębnej umowie powierzenia przetwarzania danych osobowych.
3. Podmiot przetwarzający powinien zapewniać gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych osobowych chroniło prawa osób, których dane dotyczą – **obowiązkowa weryfikacja podmiotu przed nawiązaniem współpracy.**
4. W przypadku, gdy Administrator danych przyjmie dane osobowe do przetwarzania od innego podmiotu będącego administratorem danych, za realizację obowiązków wynikających z umowy

powierzenia przetwarzania danych osobowych odpowiada, w imieniu Administratora danych, kierownik referatu realizującego zadania, z którymi wiąże się przetwarzanie powierzonych danych osobowych.

5. Kierownik referatu zobowiązany jest do informowania Inspektora, co najmniej z dwutygodniowym wyprzedzeniem, o zamiarze powierzenia przetwarzania danych osobowych i przekazania mu niezbędnych informacji w tym zakresie, w szczególności opisu, na czym ma polegać przetwarzanie danych osobowych przez podmiot przetwarzający, aby umożliwić Inspektorowi zajęcie stanowiska w przedmiotowej kwestii, i dokonać z nim uzgodnienia kryteriów powierzenia.
6. Informacje o zawartych umowach powierzenia przetwarzania danych osobowych są ujęte w "Rejestrze czynności przetwarzania danych osobowych".
7. Kategorie czynności przetwarzania, które zostały powierzone do przetwarzania do Urzędu, ujęte są w "Rejestrze kategorii czynności przetwarzania danych osobowych".
8. **Kopie zawartych umów powierzenia przetwarzania danych są przekazywane do Inspektora niezwłocznie po ich podpisaniu.**
9. Każda umowa lub postanowienia w sprawie powierzenia danych osobowych do przetwarzania w Urzędzie przez innego administratora danych muszą być uzgodnione i zatwierdzone przez Inspektora.

§ 14. Udostępnienie danych osobowych

1. Udostępnienie danych osobowych stanowi przekazanie danych osobowych odbiorcy, który sam decyduje o celach i sposobach przetwarzania danych.
2. Administrator udostępnia dane osobowe tylko osobom lub podmiotom uprawnionym.
3. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.
4. Dane osobowe udostępnia się na pisemny lub elektroniczny (np. poprzez ePUAP), umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej.
5. Wniosek powinien zawierać informacje umożliwiające weryfikację tożsamości wnioskodawcy, cel udostępnienia, podstawę prawną udostępnienia, kategorie udostępnianych danych oraz ich zakres w sposób umożliwiający ich odnalezienie i przygotowanie do udostępnienia.
6. Wnioski w sprawie udostępnienia danych osobowych rozpatrywane są przez osobę odpowiedzialną merytorycznie za dostęp do przetwarzanych zasobów.
7. W przypadku, kiedy wniosek o udostępnienie danych nie zawiera podstawy prawnej lub zawiera wadliwą podstawę prawną osoba odpowiedzialna merytorycznie wzywa wnioskodawcę do uzupełnienia lub odmawia udostępnienia danych osobowych.

8. W przypadku wniosku osoby fizycznej, pracownik dokłada starań w celu ustalenia właściwej podstawy prawnej udostępnienia.
9. Pracownik merytoryczny weryfikuje żądanie udostępnienia danych osobowych, z którym występują organy publiczne, w szczególności pod kątem tego, czy ma formę pisemną, jest uzasadnione, ma charakter wyjątkowy i nie prowadzi do udostępniania wszystkich danych osobowych zawartych w określonym zbiorze lub systemie oraz czy nie prowadzi do łączenia zbiorów danych osobowych.
10. Pracownik może udostępniać dane osobowe na podstawie wniosku podmiotu w sprawie stałego udostępnienia określonych danych osobowych drogą elektroniczną, zgodnie z przepisami prawa. W takim przypadku zawiera się porozumienie określające podstawy udostępnienia, a także ustalenia techniczne zapewniające współpracę dwóch systemów teleinformatycznych w taki sposób, aby była zapewniona rozliczalność działań oraz wykazanie trybu wnioskowego.
11. Informacje zawierające dane osobowe pracownik przekazuje uprawnionym podmiotom lub osobom w następujący sposób:
    1) w postaci papierowej - przesyłką pocztową;
    2) w postaci elektronicznej - za pomocą teletransmisji danych, w postaci zabezpieczonej;
    3) w inny sposób - określony konkretnym wymogiem prawnym, umową lub porozumieniem.
12. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych, jeżeli:

1) spowodowałoby to istotne naruszenia prywatności lub dóbr osobistych osób, których dane te dotyczą lub innych osób;
2) wniosek o udostępnienie dotyczy całego zbioru danych;
3) niemożliwa jest weryfikacja tożsamości wnioskodawcy;
4) nie został wskazany cel i podstawa prawna udostępnienia lub wskazane informacje nie stanowią podstawy do udostępnienia danych;
5) niemożliwe jest ustalenie czyich danych dotyczy udostępnienie;
6) nie wskazano zakresu danych niezbędnych do zrealizowania celu udostępnienia;
7) dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

13. Każde udostępnienie jest w referacie ewidencjonowane/dokumentowane.

§ 15. Przekazywanie danych do państw trzecich lub organizacji międzynarodowej

1. Poziom ochrony Danych osobowych poza Europejskim Obszarem Gospodarczym (EOG) różni się od tego zapewnianego przez prawo europejskie. Z tego powodu Administrator przekazuje Dane osobowe do państwa trzeciego tylko wtedy, gdy jest to konieczne i z zapewnieniem odpowiedniego stopnia ochrony, przede wszystkim poprzez:

1) współpracę z podmiotami przetwarzającymi dane osobowe w państwach, w odniesieniu do

których została wydana stosowna decyzja Komisji Europejskiej dotycząca stwierdzenia zapewnienia odpowiedniego stopnia ochrony danych osobowych (jeżeli dane państwo zostało uznane przez Komisję Europejską za zapewniające odpowiedni stopień ochrony danych, to zgodnie z art. 45 RODO takie przekazywanie danych nie wymaga dodatkowych zezwoleń - w tym przypadku dodatkowych mechanizmów transferu danych),

2) stosowanie standardowych klauzul umownych wydanych przez Komisję Europejską.

2. Inwentaryzacja:

1) Test transferu danych - weryfikacja czy dochodzi do transferu danych poza EOG oraz analiza konieczności przeprowadzenia TIA np. w ramach wykorzystywania narzędzi marketingowych, wykonywania umowy,

2) Inwentaryzacja umów – weryfikacja jakie umowy obecnie mamy podpisane z dostawcami,

3) Transfer Impact Assessment (TIA) - czyli ocena ryzyka transferu danych na co składa się:

a) identyfikacja przedmiotu transferu,

b) identyfikacja możliwej podstawy prawnej transferu poza EOG,

c) identyfikacja przepisów w danym państwie trzecim poza EOG pod kątem poziomu ochrony danych osobowych,

d) określenie dodatkowych zabezpieczeń technicznych, organizacyjnych i prawnych.

§ 16. Zasady dotyczące rozwiązywania sytuacji kryzysowych - naruszenia

1. Poniższe postanowienia mają zastosowanie zarówno w przypadku wystąpienia lub podejrzenia wystąpienia incydentu bezpieczeństwa, z wyłączeniem zautomatyzowanych (nieautoryzowanych) prób dostępu do zasobów serwerów zewnętrznych, na które Administrator z racji specyfiki sieci Internet nie ma wpływu.

2. Przed przystąpieniem do pracy użytkownicy informacji zobowiązani są dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na wystąpienie bądź podejrzenie wystąpienia incydentu bezpieczeństwa.

3. Za okoliczności, które uznaje się za wystąpienie incydentu bezpieczeństwa uważa się w szczególności:

1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują;

2) nieuprawnione naruszenie lub próby naruszenia poufności, integralności i rozliczalności danych i systemu;

3) niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych;

4) nieuprawniony dostęp do danych osobowych (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu);

5) udostępnienie danych osobowych osobom nieupoważnionym;

6) inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy - jeżeli wskazuje na próbę nieuprawnionego dostępu;
7) zdarzenia losowe, obniżające poziom ochrony systemu (np. pożar);
8) kradzież sprzętu informatycznego lub nośników informacji zawierających dane osobowe (np. wydruków komputerowych, płyt CD-R, dysków twardych, pamięci zewnętrznych, itp.).

4. W przypadku stwierdzenia wystąpienia incydentu bezpieczeństwa lub możliwości jego wystąpienia, użytkownicy informacji zobowiązani są do bezzwłocznego powiadomienia o tym fakcie bezpośredniego przełożonego, IOD oraz AS/Informatyka – w przypadku podejrzenia/ wystąpienia incydentu bezpieczeństwa systemu informatycznego.
5. Jeżeli konieczna jest ocena sytuacji na miejscu przez IOD, do czasu jego przybycia zgłaszający:

1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;
2) zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;
3) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

6. W przypadku stwierdzenia wystąpienia incydentu bezpieczeństwa kierownik referatu:

1) ocenia zaistniałą sytuację, biorąc pod uwagę okoliczności jej wystąpienia, a także szacuje poziom negatywnych następstw incydentu;
2) sprawdza relację osoby, która dokonała powiadomienia oraz innych osób związanych z incydentem;
3) sporządza raport z przebiegu zdarzenia, w którym powinny się znaleźć w szczególności:
   a) data zaistnienia incydentu,
   b) data i godzina powiadomienia o incydencie,
   c) informacja o osobie zgłaszającej incydent,
   d) opis incydentu,
   e) informacja o podjętych działaniach wraz z uzasadnieniem,
   f) wnioski w sprawie ograniczenia możliwości ponownego wystąpienia naruszenia bezpieczeństwa informacji chronionych.

7. IOD odnotowuje zaistniałe zdarzenie w rejestrze incydentów.
8. W przypadku stwierdzenia wystąpienia incydentu bezpieczeństwa, użytkownik informacji może kontynuować pracę dopiero po otrzymaniu pozwolenia od AS lub IOD.
9. W przypadku, gdy incydent bezpieczeństwa jest wynikiem uchybienia obowiązującej w Urzędzie dyscypliny pracy, IOD oraz AS wyjaśniają wszystkie okoliczności incydentu, o czym informują ADO.
10. Po zakończeniu czynności naprawczych system przetwarzający dane osobowe musi utrzymać

poziom ochrony, nie niższy niż przed wystąpieniem incydentu bezpieczeństwa.

§ 17. Audyt zgodności przetwarzania danych

1. Audyty, kontrole i sprawdzenia prowadzone przez IOD dotyczą oceny zgodności przetwarzania danych osobowych z RODO, innymi przepisami prawa oraz z wewnętrznymi regulacjami dotyczącymi ochrony danych osobowych, a także oceny realizacji działań naprawczych.
2. W celu realizacji audytów, kontroli i sprawdzeń, o których mowa w ust. 1, IOD może korzystać ze wsparcia odpowiedniej komórki organizacyjnej.
3. IOD informuje Administratora o zaplanowanych audytach, kontrolach i sprawdzeniach.
4. Audyt i kontrola w zakresie ochrony danych osobowych mogą być częścią składową odpowiednio audytu lub kontroli z innych obszarów działalności Urzędu, pod warunkiem, że w zakresie dotyczącym ochrony danych osobowych audyt lub kontrolę prowadzi IOD.
5. W przypadku pozyskania przez IOD informacji o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia, IOD ma prawo do przeprowadzenia kontroli doraźnej przedmiotowego obszaru.

§ 18. Realizacja szkoleń i prowadzenie działań zwiększających świadomość w zakresie ochrony danych osobowych

1. W Urzędzie organizowane są szkolenia z zakresu ochrony danych osobowych dla pracowników oraz osób wykonujących zadania na podstawie umów (np. cywilnoprawnych), w zakresie obowiązujących przepisów oraz zagrożeń związanych z przetwarzaniem danych osobowych, zwane dalej "szkoleniami".
2. Szkolenia prowadzi IOD lub kierownik referatu.
3. Szkolenia przeprowadza się dla każdego nowego pracownika oraz osób wykonujących zadania na podstawie innych umów (np. cywilnoprawnych).
4. W przypadku braku możliwości przeprowadzenia szkolenia w trybie stacjonarnym lub on - line, IOD lub kierownik referatu, przekazuje pracownikowi do zapoznania się materiały szkoleniowe w postaci elektronicznej.
5. Szkolenia obejmują co najmniej następujące zagadnienia:

1) przepisy o ochronie danych osobowych;
2) zasady przetwarzania danych osobowych w Urzędzie;
3) regulacje dotyczące bezpiecznego przetwarzania danych osobowych, w tym w systemach teleinformatycznych;
4) zagrożenia związane z przetwarzaniem danych osobowych;
5) sposób postępowania w razie zaistnienia zagrożenia dla bezpieczeństwa przetwarzanych danych osobowych lub naruszenia zasad przetwarzania danych osobowych;
6) odpowiedzialność za niezgodne z prawem przetwarzanie danych osobowych.

6. Przeprowadzenie szkoleń w trybie stacjonarnym lub on - line jest odpowiednio dokumentowane listą obecności oraz oświadczeniem uczestników o zapoznaniu się z przepisami o ochronie danych osobowych.
7. W Urzędzie prowadzone są działania mające na celu zwiększenie świadomości pracowników w zakresie ochrony danych osobowych, poprzez publikowanie za pomocą służbowych adresów e-mail treści dotyczących ochrony i bezpiecznego przetwarzania danych osobowych. Pracownik ma obowiązek potwierdzić fakt zapoznania się z materiałem.

§ 19. Strefy bezpieczeństwa

1. W budynku użytkowanym przez Urząd wyznacza się następujące strefy bezpieczeństwa:
1) strefa publiczna;
2) strefa ograniczonego dostępu;
3) strefa ścisłej kontroli dostępu.
2. Strefa publiczna:
1) strefę publiczną stanowią pomieszczenia ogólnodostępne oraz ciągi komunikacyjne;
2) dostęp do strefy publicznej nie jest ograniczony.
3. Strefa ograniczonego dostępu:
1) strefę ograniczonego dostępu stanowią pomieszczenia, w których są przetwarzane dane osobowe, za wyjątkiem pomieszczeń, o których mowa w ust. 4 pkt 1);
2) dostęp do strefy ograniczonego dostępu posiadają osoby upoważnione;
3) osoby postronne mogą przebywać w strefie ograniczonego dostępu wyłącznie w obecności osób, o których mowa w pkt 2) powyżej.
4. Strefa ścisłej kontroli dostępu:
1) strefę ścisłej kontroli dostępu stanowią pomieszczenia serwerowni;
2) pomieszczenie z serwerami (serwerownia), w którym mogą przebywać wyłącznie Wójt, Z-ca Wójta, Sekretarz, Skarbnik, pracownicy zatrudnieni na stanowiskach właściwych ds. informatyki oraz pracownicy firm zajmujących się serwisem sprzętu i ochroną budynku tylko w obecności tych pracowników. Osoby postronne obowiązuje zakaz wstępu do serwerowni. Klucz do tego pomieszczenia jest przechowywany w sekretariacie.
3) zasady dostępu do strefy ścisłej kontroli dostępu zostaną określone w odrębnych aktach wewnętrznych wydanych przez ADO.

§ 20. Kontrole zewnętrzne dotyczące przetwarzania danych osobowych

1. Administrator niezwłocznie włącza IOD w działania wykonywane w ramach kontroli prowadzonych przez zewnętrzne organy kontrolne w Urzędzie, dotyczące ochrony danych osobowych, w szczególności w zakresie:

1) uczestnictwa IOD w spotkaniach z przedstawicielami organu kontrolnego lub czynnościach kontrolnych;
2) opiniowania treści odpowiedzi na zapytania organu kontrolnego, w tym zakresu i treści dokumentów przekazywanych organowi kontrolnemu;
3) przedstawiania organowi kontrolnemu stanowiska IOD w kwestiach ochrony danych osobowych;
4) zapoznania się z projektem protokołu z czynności kontrolnych, możliwości przedstawienia Administratorowi uwag IOD do jego treści, a także zapoznania się z ostateczną wersją protokołu;
5) zapoznania się z projektem wystąpienia pokontrolnego, a także możliwości przedstawienia Administratorowi uwag IOD do jego treści;
6) zapoznania IOD z ostateczną wersją wystąpienia pokontrolnego oraz opiniowania treści odpowiedzi na zarzuty stawiane przez organ kontrolny;
7) ustalania sposobu realizacji zaleceń organu kontrolnego, terminów oraz osób lub referatów zobowiązanych do ich realizacji.

§ 21. Odpowiedzialność (sankcje)

Odpowiedzialność karną, dyscyplinarną lub służbową za naruszenie przepisów dotyczących ochrony danych osobowych określają przepisy odrębne.

§ 22. Przeglądy i aktualizacja Polityki oraz powiązanych dokumentów

1. Polityka podlega okresowym przeglądom pod kątem jej adekwatności, nie rzadziej niż raz do roku.
2. **Przeglądu Polityki dokonuje IOD** we współpracy z właścicielami biznesowymi danych i właścicielami biznesowymi systemów informatycznych.
3. Przegląd obejmuje w szczególności ocenę adekwatności Polityki do:

1) obowiązujących przepisów prawa w zakresie ochrony danych osobowych, którym podlega Administrator;
2) procesów funkcjonujących w Urzędzie.

4. Przegląd Polityki jest wykonywany niezwłocznie w każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany organizacyjne, a także na skutek zaleceń i rekomendacji wynikających z kontroli, audytów, sprawdzeń oraz z wykrytych naruszeń ochrony danych osobowych.
5. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej przepisów, IOD podejmuje niezwłocznie działania mające na celu aktualizację Polityki w wymaganym zakresie.
6. Regulacje określone w ust. 1-5 stosuje się odpowiednio do powiązanych polityk szczegółowych, procedur i instrukcji i ich właścicieli biznesowych, chyba że regulują one inaczej kwestię ich aktualizacji.

§ 23. Administrator prowadzi i stosuje następujące rejestry i procedury dotyczące ochrony danych osobowych, które stanowią integralną część Polityki:

1) Procedura sporządzania rejestru czynności przetwarzania danych osobowych oraz rejestru kategorii czynności przetwarzania w Urzędzie Gminy Brzozie – zał. nr 1;
2) Procedura stosowania zasad Privacy by design i Privacy by default w Urzędzie Gminy Brzozie – zał. nr 2;
3) Procedura upoważniania do przetwarzania danych osobowych w Urzędzie Gminy Brzozie – zał. nr 3;
4) Procedura obsługi żądań podmiotów danych w Urzędzie Gminy Brzozie – zał. nr 4;
5) Procedura wyboru dostawcy przetwarzającego dane osobowe oraz postępowania w zakresie zawierania umów lub porozumień w sprawie powierzenia przetwarzania danych osobowych w Urzędzie Gminy Brzozie – zał. nr 5;
6) Procedura postępowania w przypadku naruszenia ochrony danych osobowych w Urzędzie Gminy Brzozie – zał. nr 6;
7) Procedura regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania w Urzędzie Gminy Brzozie – zał. nr 7;
8) Metodologia analizy ryzyka – zał. nr 8.

§ 24. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz Ustawy.

WÓJT

Danuta Kądziorska-Cieszyńska

Załącznik nr 1
do Polityki Ochrony Danych Osobowych
w Urzędzie Gminy Brzozie

Procedura sporządzania rejestru czynności przetwarzania danych osobowych oraz rejestru kategorii czynności przetwarzania w Urzędzie Gminy Brzozie

CEL PROCEDURY

Zapewnienie przez Administratora zgodności z RODO (art. 30 RODO), czyli ze wskazanymi w tym akcie prawnym zasadami i warunkami przetwarzania danych osobowych.

ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

Kierownicy Referatów – w zakresie aktualności i poprawności informacji zawartych w rejestrach cząstkowych w ramach realizowanych procesów przetwarzania danych osobowych w zarządzanym referacie. W przypadku przetwarzania danych powierzonych przez innych administratorów, Kierownicy referatów odpowiadają za prowadzenie rejestru kategorii czynności przetwarzania realizowanych przez ich referat.

Sekretarz Gminy – w zakresie koordynowania oraz prowadzenia nadzoru nad prowadzeniem rejestru czynności przetwarzania dla stanowisk samodzielnych.

Inspektor ochrony danych – w zakresie okresowej weryfikacji rejestrów oraz aktualizacji rejestrów w przypadku otrzymania stosownych informacji od kierowników referatów.

POSTANOWIENIA OGÓLNE PROCEDURY

1. **Rejestr czynności przetwarzania (RCP)** i **rejestr kategorii czynności przetwarzania (RKCP)** tworzy się na podstawie rejestrów cząstkowych tworzonych przez każdy referat oraz stanowiska jednoosobowe.
2. Za sporządzenie rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania odpowiada Kierownik referatu oraz pracownik merytoryczny obsługujący proces, w którym przetwarzane są dane osobowe.
3. RCP i RKCP sporządza się i aktualizuje na podstawie przeprowadzonej inwentaryzacji czynności przetwarzania danych, w oparciu o przekazane przez IOD lub Sekretarza do poszczególnych referatów projekty rejestrów, o których mowa w ust. 1, zgodnie z właściwością, celem ponownego uzgodnienia zapisów oraz ewentualnego uaktualnienia.
4. Inspektor ochrony danych co najmniej raz w roku występuje do komórek organizacyjnych o zweryfikowanie aktualności RCP i RKCP. W przypadku zmian, dokonuje aktualizacji RCP i RKCP.

5. Kierownicy referatów mają obowiązek na bieżąco informować IOD o wszelkich zmianach w procesach przetwarzania danych osobowych realizowanych w swoich komórkach, w szczególności dotyczących:

1) celów i podstaw przetwarzania danych;
2) kategorii osób, których dane są przetwarzane;
3) zakresu przetwarzania danych;
4) podmiotów przetwarzających, którym dane są powierzane;
5) odbiorców danych, którym dane są udostępnione, w tym odbiorców w państwach trzecich lub będących organizacją międzynarodową.

6. Kierownicy referatów prowadzą RKCP, poprzez wprowadzenie do nich danych z zawartych umów powierzenia przetwarzania danych w imieniu innych administratorów. W RKCP zamieszcza się w szczególności:

1) imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie - przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
2) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
3) gdy ma to zastosowanie - przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
4) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

WÓJT
Danuta Kędziorska-Cieszyńska

Załącznik nr 2
do Polityki Ochrony Danych Osobowych
w Urzędzie Gminy Brzozie

Procedura stosowania zasad Privacy by design i Privacy by default
w Urzędzie Gminy Brzozie

Rozdział 1
Zagadnienia ogólne

1. Niniejsza Procedura ma na celu wdrożenie do Polityki Bezpieczeństwa Danych Osobowych zasadę privacy by design, stosownie do art. 25 ust. 1 Rozporządzenia oraz zasadę privacy by default, stosownie do art. 25 ust. 2 Rozporządzenia.
2. Użyte zwroty i definicje są tożsame ze wskazanymi w Polityce Bezpieczeństwa przyjętej u Administratora.
3. Niniejszy dokument dotyczy zarówno procesów już wdrożonych, jak i tych dopiero wdrażanych. Bez znaczenia pozostaje również fakt, czy zmiany wynikają z decyzji Administratora, podpisanej umowy, czy spowodowane są nowelizacją przepisów.
4. Nadrzędnym celem niniejszego dokumentu jest zapobieżenie wystąpienia naruszenia przetwarzania danych osobowych oraz należyta realizacja praw osób fizycznych.
5. Procedura ma zastosowanie do:
   1) zadań własnych;
   2) zleconych - o ile zlecający zadanie nie dostarcza oprogramowania, sprzętu.
6. Analizy wykonywane w związku z realizacją niniejszej Procedury są dokumentowane w formie pisemnej.
7. Zmiany w procesie przetwarzania danych osobowych są okolicznością szczególnie obarczającą Administratora odpowiedzialnością za zmaterializowanie się zagrożeń związanych z niedopełnieniem powyższych obowiązków.
8. Względy natury organizacyjno - finansowej nie powinny być traktowane jako podstawy do sprzecznego z prawem przetwarzania danych osobowych.
9. Procedura ma na celu zapewnienie, że dane osobowe będą chronione przez cały cykl istnienia określonego procesu, poprzez jego etapy: projektowania, wdrażania, sprawdzania i korekt.
10. Niniejsza procedura powinna być uwzględniona, gdy Administrator dokonuje zmiany w funkcjonującym procesie przetwarzania, która wiąże się ze zmianą zasad lub sposobów przetwarzania danych osobowych, w szczególności związanych z działaniami:
    1) rekrutacyjnymi, działaniami kadrowymi, a zwłaszcza monitorowaniem działalności pracowników;

2) organizacją urzędu;
3) promocyjnymi, w szczególności poprzez:
a) publikowanie na portalach społecznościowych,
b) wykorzystanie wizerunku na banerach i innych akcesoriach reklamowych;
4) księgowymi;
5) monitoringiem;
6) procesem uchwałodawczym, który związany jest z potrzebą przetwarzania danych mieszkańców;
7) wprowadza nową czynność przetwarzania, które wiążą się z przetwarzaniem danych osobowych.

Rozdział 2

Privacy by design

Wdrożenie nowego procesu należy poprzedzić etapem projektowania.

1. Wdrażając nowy proces Administrator stosuje następujące zasady:
   1) podejście proaktywne, niereaktywne i zaradcze, nie naprawcze;
   2) prywatność jako ustawienie domyślne;
   3) prywatność włączona w projekt;
   4) ochrona od początku do końca cyklu życia informacji;
   5) widoczność i przejrzystość;
   6) poszanowanie dla prywatności użytkowników.
2. Administrator przedstawia zamiar nowego proces przetwarzania lub jego modyfikacji kierownikowi referatu, IOD, ASI oraz sekretarzowi/skarbnikowi/innym pracownikom posiadającym wiedzę merytoryczna w sprawie.
3. W sytuacji gdy produkt bądź usługa znajduje się w etapie rozwoju, ADO i pracownicy merytoryczni rozważają procedury gromadzenia, przechowywania i używania danych, aby móc zaprojektować najlepszy sposób ochrony danych osobowych.
4. ASI wskazuje optymalne technologie służące zabezpieczeniu procesu oraz określa możliwe koszty zabezpieczenia informatycznego.
5. IOD dokonuje oceny nowego procesu poprzez jej konfrontację z zasadą legalności, rzetelności i przejrzystości, zasadą ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, integralności i poufności.
6. IOD dokonuje oceny na temat możliwości zrobienia DPIA.
7. W przypadku gdy proces nowy proces odbywa się wyłącznie poprzez przyjęcie uchwały nakładającej obowiązek podania danych osobowych IOD oraz radca prawny przedstawiają

opinie na temat zasad legalności, szczególnie uwzględniając standard art. 51 (ust. 1-4) Konstytucji.

8. **Etap wdrożenia** rozpoczyna się, gdy IOD dokona weryfikacji procesu przetwarzania przez pryzmat zasad przetwarzania określonych w art. 5 RODO.
9. ASI przedstawia opinie na temat wiedzy technicznej - jeśli przetwarzanie odbywa się w sposób automatyczny.
10. IOD tak opracowuje proces przetwarzania, aby zapewnić respektowanie praw podmiotów danych określonych w art. 12-22 RODO.
11. IOD dokonuje identyfikacji i pomiaru ryzyka.
12. Obowiązkiem Administratora wobec już zidentyfikowanego i ocenionego ryzyka będzie podjęcie działań zmierzających do zmniejszenia ryzyka jego wystąpienia.
13. Wszyscy pracownicy zaangażowani oceniając procedurę powinni wskazać:
    1) zdarzenia zwiększające wystąpieniu naruszeniu danych osobowych w ramach wskazanego procesu;
    2) potencjalne możliwości naruszenia praw i wolności osób fizycznych;
    3) dotychczas stosowane środki zabezpieczające wraz z opinią, czy były one wystarczające;
    4) możliwość realizacji praw osób, których dane dotyczą;
    5) konieczność przeprowadzenia zmian w sytuacji, gdy dotychczas było to niewystarczające.
14. Administrator w każdym momencie posiada możliwość wdrożenia dodatkowych środków w celu dostosowania ich do potencjalnego wzrostu ryzyka.
15. Do analizy należy uwzględnić środki organizacyjne oraz techniczne. Środki techniczne i organizacyjne oraz niezbędne zabezpieczenia mogą być rozumiane w szerokim znaczeniu jako dowolna metoda lub środek, które administrator może zastosować w procesie przetwarzania. Zaleca się stosowanie pisemnego wykazu stosowanych środków. Wykaz ten może ulegać zmianie ze względu na potrzeby Administratora, zmieniające się uwarunkowania technologiczne oraz przepisy prawa.
16. Ustalając niezbędne środki, administratorzy muszą brać pod uwagę charakter, zakres, kontekst i cel przetwarzania danych.
17. Pracownicy powinni zostać przeszkoleni w zakresie obsługi technicznej oraz związanej z zakresu postępowania z naruszeniami danych osobowych.
18. Ochrona danych osobowych powinna następować na każdym etapie.
19. Odpowiedzialność Administratora nie kończy się na zastosowaniu odpowiednich środków bezpieczeństwa przy gromadzeniu danych: ochrona danych i ochrona prywatności trwa od momentu pozyskania danych, aż do momentu ich zniszczenia.

Rozdział 3

Privacy by default

1. Administrator powinien wybrać i odpowiadać za wdrożenie domyślnych ustawień ochrony danych i opcji w taki sposób, aby jedynie przetwarzanie, które jest ściśle niezbędne do osiągnięcia określonego, zgodnego z prawem celu, było realizowane domyślnie.
2. Administrator zbiera tylko taką ilość danych jaką potrzebuje, zgodnie z zasadą minimalizacji.
3. Oceniając proces przetwarzania danych pracownicy biorą pod uwagę :
   1) zakres przetwarzanych danych, w kontekście minimalizacji danych, w tym zasadę minimalizmu z art. 5 RODO oraz standard art. 51 Konstytucji;
   2) okres przechowywania danych;
   3) okres upublicznienia poprzez BIP danych osobowych;
   4) w sytuacji wpłynięcia wniosków o udostępnienie informacji publicznej - zakres udostępnionych danych osobowych w trybie wnioskowym.
4. Administrator stosując system upoważnień do przetwarzania danych osobowych wprowadza ograniczenia dotyczące dostępu do danych osobowych oraz rodzaju tego dostępu na podstawie oceny konieczności, a także sprawdzić, czy dane osobowe są rzeczywiście dostępne dla podmiotów, którym są one potrzebne w razie potrzeby, na przykład w sytuacjach nadzwyczajnych. Kontroli dostępu należy przestrzegać podczas całego przepływu danych w ramach przetwarzania.
5. IOD raportuje Administratorowi błędy oraz uchybienia, a także z własnej inicjatywy przedstawia wnioski, gdy zauważy taka potrzebę.
6. W sytuacji gdy wprowadzono nową czynność przetwarzania, lub w sposób istotny zmodyfikowano już istniejącą pracownicy są zobligowani do przeszkolenia się.
7. Administrator nadając upoważnienia do przetwarzania danych ogranicza dostęp do danych zgodnie z zasadą najmniejszych przywilejów.
8. Użytkując program ASI zwraca uwagę aby:
   1) ilość zbieranych i przetwarzanych danych osobowych powinna być ograniczona do tego, co jest zgodne z prawem i bezwzględnie konieczne;
   2) przetwarzane dane były anonimizowane lub pseudonimizowane we wszystkich możliwych sytuacjach;
   3) przetwarzane szczególne kategorie danych były oddzielone od pozostałych przetwarzanych danych;
   4) w oprogramowaniu własnym lub podmiotu przetwarzającego:
      a) wszystkie konfiguracje przyjazne dla prywatności były domyślnie włączone,
      b) śledzenie urządzeń powinno być domyślnie wyłączone,
      c) Bluetooth powinien być domyślnie wyłączony,

d) ASI stara się usunąć wychwycone słabości i luki w oprogramowaniu również w sytuacji gdy jest to oprogramowanie zewnętrzne,

5) w sytuacji, gdy zakupiony program posiada dodatkowe funkcjonalności, które mogą stanowić niebezpieczeństwo dla prywatności, stara się wyłączyć te funkcje.

9. Wdrożony proces przetwarzania podlega sprawdzaniu przez wyznaczonych pracowników.
10. Po rozpoczęciu czynności przetwarzania IOD sprawdza, czy wymagane jest ponowne przeprowadzenie ocen zagrożeń bezpieczeństwa i wpływu na ochronę danych, które zostały ukończone w fazie wymagań. IOD dokumentuje przeprowadzoną analizę.
11. ASI monitoruje bezpieczeństwo serwerów, punktów końcowych i sieci w celu wykrycia podejrzanej aktywność, która może wykorzystać luki w oprogramowaniu, skutkujące incydentami związanymi z ochroną i bezpieczeństwem danych.
12. W przypadku incydentów teleinformatycznych ASI analizuje, przegląda logi, uzyskuje przegląd tego, co się stało, oraz określa zakres incydentu.
13. W przypadku skargi, która wpłynęła od podmiotu danych, IOD kontaktuje się z ASI (jeśli naruszenie jest związane z działaniem systemów teleinformatycznych) oraz pracownikiem merytorycznym.
14. W pełni wdrożona czynność przetwarzana powinna przechodzić korekty.
15. O wykrytych incydentach mających związek z naruszeniem przetwarzanych danych ASI informuje IOD. Incydentom związanym z bezpieczeństwem należy nadać wysoki priorytet.
16. ASI sprawdza, czy zagrożenia stanowią rzeczywiste naruszenia bezpieczeństwa, czy są fałszywymi alarmami.
17. W przypadku incydentów należy stosować procedury związane z planem ciągłości działania i odtwarzania systemów po awarii.
18. W przypadku stale powtarzających się incydentów, które kwalifikowane są jako naruszenie danych osobowych należy rozważyć zmianę czynności przetwarzania – w zakresie niezbędnym (zmianę oprogramowania, uprawnień, etc.)
19. W ramach cyklicznych szkoleń IOD oraz ASI przeprowadza szkolenie w zakresie reagowania na incydenty obejmujące incydenty teleinformatyczne.

Rozdział 4

Szczególne obowiązki związane z poszczególnymi czynnościami przetwarzania danych

I. Upublicznianie danych w BIP związanych z nowym procesem

1. W sytuacji zamieszczenia danych w BIP administrator uwzględnia przepisy Polityki Retencji przyjętej w urzędzie.
2. Danych osobowych nie zamieszcza się, a upublicznione uchyla, jeżeli nie jest to niezbędne do celów ich przetwarzania oraz jeżeli nie istnieje inny zgodny cel i podstawa prawna zgodna z art. 6 bądź art. 9 RODO.

3. Każde upubliczniane danych poprzez BIP powinno być w razie potrzeby obiektywnie uzasadnione przez administratora danych zgodnie z zasadą rozliczalności.
4. Brak jednak określonych przepisami prawa okresów przetwarzania udostępnionych informacji (zawierających dane osobowe) nie powoduje, że informacje takie można przetwarzać bezterminowo.
5. Szczegóły upubliczniania znajdują się w polityce retencji.

II. Podpisanie umowy cywilnoprawnej

1. Jeżeli administrator korzysta z oprogramowania osób trzecich lub oprogramowania dostępnego na rynku, powinien przeprowadzić ocenę ryzyka związanego z produktem i upewnić się, że jego funkcje, które nie mają podstawy prawnej lub nie są zgodne z zamierzonymi celami przetwarzania, zostaną wyłączone.
2. W sytuacji gdy realizacja czynności przetwarzania związana jest podpisywanie umów cywilnoprawnych, w których zachodzić będzie powierzenie przetwarzania danych osobowych wyznaczony pracownik przed podpisaniem umowy zwraca się do:
   1) IOD w celu uzyskania opinii na temat danych, które są niezbędne dla zrealizowania zadania i wymagają powierzenia przetwarzania;
   2) ASI w celu uzyskania opinii o wymaganych funkcjonalnościach- informuje o kosztach.
3. W sytuacji gdy zachodzi powierzenie przetwarzania danych osobowych administrator określa:
   1) wdrożenie odpowiednich środków technicznych i organizacyjnych, takich jak np. pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych;
   2) w momencie podpisywania umowy głównej - administrator wskaże podstawowe warunki dotyczące zabezpieczania danych osobowych, które następnie zostaną doprecyzowane w umowie powierzenia. Powyższe dotyczy w szczególności zagadnień przekazywania danych poza obszar EOG;
   3) W przypadku migracji danych osobowych należy włączyć podmiotu przetwarzającego w proces. Administrator zwraca uwagę na dostarczenie mu pełnych informacji o podejmowanych czynnościach i oczekiwanych rezultatach, administrator

III. Udostępnianie danych

1. Pracownicy są zobligowania do sprawdzania, a w razie wątpliwości konsultowania z IOD udostępniania danych innym podmiotom. W szczególności dotyczy to innych organów administracji, komorników, poczty polskiej, itd. pod względem legalizmu.

WÓJT
Danuta Kędziorska-Cieszyńska

Załącznik nr 3
do Polityki Ochrony Danych Osobowych
w Urzędzie Gminy Brzozie

Procedura upoważniania do przetwarzania danych osobowych w Urzędzie Gminy Brzozie

§1.

Wstęp

1. Procedura obowiązuje każdą osobę, która jest dopuszczana do przetwarzania danych osobowych.
2. Za realizowanie niniejszej procedury odpowiadają:
   1) **Administrator**, zatwierdzający upoważnienia lub ich zmiany;
   2) **Sekretarz Gminy** – w zakresie wydawania/zmiany/odwoływania upoważnień do przetwarzania danych osobowych dla stanowisk samodzielnych; uprawniony przez Administratora do zatwierdzania w jego imieniu upoważnień lub ich zmian;
   3) **Kierownicy referatów** – w zakresie występowania z wnioskiem o nadanie/zmianę/odwołanie upoważnienia do przetwarzania danych osobowych dla podległych pracowników oraz innych osób im podległych (stażystów, praktykantów, wolontariuszy oraz osób realizujących zadania na podstawie umowy cywilnoprawnej na rzecz danej komórki organizacyjnej);
   4) **Osoba upoważniana** zobligowana do przyjęcia i przestrzegania upoważnienia lub jego zmiany;
   5) **IOD** – w zakresie weryfikowania przestrzegania procedury upoważniania do przetwarzania danych osobowych.
3. Do przetwarzania danych osobowych mogą zostać dopuszczone tylko i wyłącznie osoby, które otrzymały pisemne upoważnienie od Administratora lub uprawnionej przez niego osoby. Upoważnienia są nadawane w formie pisemnej i wymagają zatwierdzenia przez Administratora oraz potwierdzenia przyjęcia przez osobę upoważnioną.

§2.

Wniosek o nadanie upoważnienia

1. W momencie otrzymania informacji o zatrudnieniu lub rozpoczęciu współpracy w ramach zlecenia, wolontariatu, stażu, praktyk, które będą wymagały przetwarzania danych osobowych, przed dopuszczeniem tej osoby do przetwarzania danych osobowych, należy przygotować wniosek o nadanie upoważnienia.
2. Wniosek o nadanie upoważnienia należy złożyć również w związku:

1) ze zmianą zakresu obowiązków;
2) ze zmianą stanowiska pracy lub komórki organizacyjnej;
3) organizacją stażu lub praktyki lub wolontariatu;
4) z realizacją umowy cywilnoprawnej;

– jeżeli realizowane przez nich zadania wiążą się z przetwarzaniem danych osobowych.

3. Za przygotowanie wniosku są odpowiedzialni:

1) Kierownik referatu, bezpośredni przełożony lub opiekun nowego pracownika/współpracownika;

2) Sekretarz Gminy dla osoby zatrudnianej na samodzielnym stanowisku.

4. Osoba odpowiedzialna za przygotowanie wniosku o upoważnienie wskazuje w nim swoje dane (jako wnioskodawcy), dane osoby upoważnianej oraz zakres upoważnienia i okres jego obowiązywania.
5. Prawidłowo wypełniony wniosek wnioskodawca niezwłocznie przekazuje do IOD.

§ 3.

Nadanie upoważnienia

1. IOD na podstawie wniosku przygotowuje treść upoważnienia.
2. Nadanie upoważnienia odbywa się poprzez jego zatwierdzenie przez Administratora lub uprawnioną przez niego osobę.
3. Upoważnienie jest niezwłocznie przekazywane przez wnioskodawcę do osoby upoważnionej.
4. Osoba upoważniona przyjmuje upoważnienie oraz zobowiązuje się do zachowania poufności zgodnie z treścią upoważnienia, co potwierdza złożeniem podpisu na upoważnieniu.
5. Jeżeli upoważnienie uprawnia także do przetwarzania danych w systemach informatycznych, wnioskodawca przekazuje do administratorów odpowiednich systemów informację o zakresie upoważnienia do tych systemów w celu nadania osobie upoważnionej niezbędnych uprawnień.
6. Upoważnienie jest przechowywane w dziale kadr wraz z umową osoby upoważnionej (teczka akt osobowych).

§4.

Zmiana zakresu upoważnienia

1. Upoważnienie jest zmieniane niezwłocznie po zmianie zakresu obowiązków osoby upoważnionej w zakresie zgodnym ze zmianą, która nastąpiła, poprzez wydanie nowego upoważnienia.
2. Zmiana zakresu upoważnienia odbywa się poprzez zatwierdzenie przez Administratora lub uprawnioną przez niego osobę wniosku o nadanie upoważnienia, zgodnie z procedurą nadawania upoważnień.
3. Nowe upoważnienie zastępuje stare.
4. Za przygotowanie wniosku są odpowiedzialni:
   a) Kierownik referatu, bezpośredni przełożony lub opiekun nowego pracownika/współpracownika,
   b) Sekretarz Gminy dla osoby zatrudnianej na samodzielnym stanowisku.
5. Osoba odpowiedzialna za przygotowanie wniosku o upoważnienie wskazuje w nim swoje dane (jako wnioskodawcy), dane osoby upoważnianej, której upoważnienie ma ulec zmianie, nowy zakres upoważnienia i okres jego obowiązywania.
6. Prawidłowo wypełniony wniosek wnioskodawca niezwłocznie przekazuje do Sekretarza Gminy.
7. Dalsza część procedury jest realizowana zgodnie z §3 Nadanie upoważnienia.

§ 5.

Odwołanie upoważnienia

1. Za odwołanie upoważnień odpowiedzialny jest Administrator lub osoby przez niego do tego uprawnione.
2. Upoważnienie jest odwoływanie niezwłocznie:

a) po zakończeniu współpracy z osobą upoważnioną, jeżeli nastąpiła przed końcem okresu obowiązywania upoważnienia lub w upoważnieniu nie wskazano, że wygasa w dniu zakończenia współpracy,

b) zmianie obowiązków osoby upoważnionej, w zakresie takim, że dalsze przetwarzanie danych nie będzie miało miejsca,

c) odejścia pracownika na dłuższe zwolnienie lekarskie lub bezpłatny urlop (jeżeli przekracza 3 miesiące).

3. Odwołanie odbywa się w trybie wnioskowym.
4. Za przygotowanie wniosku są odpowiedzialni:

a) kierownik referatu, bezpośredni przełożony lub opiekun nowego pracownika/współpracownika,

b) Sekretarz Gminy dla osoby zatrudnianej na samodzielnym stanowisku.

5. Osoba odpowiedzialna za przygotowanie wniosku wskazuje w nim swoje dane (jako wnioskodawcy), dane osoby upoważnianej, której upoważnienie ma zostać odwołane, przyczynę odwołania oraz datę obowiązywania odwołania.
6. Prawidłowo wypełniony wniosek wnioskodawca niezwłocznie przekazuje do Administratora danych lub osoby uprawnionej przez niego do nadawania i zmiany upoważnień.
7. Odwołanie upoważnienia odbywa się poprzez zatwierdzenie przez Administratora lub uprawnioną przez niego osobę wniosku o odwołanie upoważnienia.
8. Zatwierdzony wniosek stanowi odwołanie upoważnienia do przetwarzania danych, które jest niezwłocznie przekazywane przez wnioskodawcę do:

a) administratorów systemów informatycznych,

b) osób współpracujących z osobą upoważnioną,

c) osoby upoważnionej, o ile takie przekazanie jest możliwe.

9. Wnioskodawca przekazuje odwołanie upoważnienia do działu kadr.
10. Odwołanie upoważnienia jest przechowywane w dziale kadr wraz z umową osoby upoważnionej.
11. Wzór wniosku o nadanie/modyfikację/odwołanie upoważnienia oraz wzór upoważnienia i wzór oświadczenia o zachowaniu poufności i przestrzegania przepisów o ochronie danych osobowych stanowią załączniki nr 1-3 do niniejszej procedury.

WÓJT
Danuta Kędziorska-Cieszyńska

Załącznik nr 1
do Procedury upoważniania do przetwarzania
danych osobowych w Urzędzie Gminy Brzozie

Brzozie, dnia .....

Wniosek

o nadanie/modyfikację/odwołanie* upoważnienia do przetwarzania danych osobowych

w Urzędzie Gminy Brzozie

(wypełnia bezpośredni przełożony)

1) Imię i nazwisko osoby, której wniosek dotyczy:

_____

2) Referat: _____

3) Nazwa zbioru/ów danych osobowych – kategorie osób, zakres danych:

_____

_____

_____

4) System informatyczny/systemy informatyczne:

_____

_____

5) Okres obowiązania upoważnienia do przetwarzania danych osobowych:

_____

.....
(data i podpis osoby wnioskującej)

.....
(pieczęć, data i podpis AD lub osoby działającej w jego imieniu)*

Egz. nr 1 - osoba wydająca upoważnienie
* niepotrzebne skreślić

WÓJT
Danuta Kędziorska-Tuczyńska

Załącznik nr 2
do Procedury upoważniania do przetwarzania
danych osobowych w Urzędzie Gminy Brzozie

Brzozie, dnia .....

Upoważnienie
do przetwarzania danych osobowych

Działając w imieniu **Administratora Danych Osobowych**
.....
na podstawie art. 29 i art. 32 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej RODO (GDPR)

upoważniam Panią/Pana:

.....
(imię i nazwisko osoby upoważnionej)

do przetwarzania danych osobowych w **zakresie pełnionych obowiązków służbowych na stanowisku:** ..... w celach związanych wyłącznie z wykonywaniem obowiązków.

Niniejsze upoważnienie obowiązuje od dnia ..... i traci moc najpóźniej z dniem odwołania albo rozwiązania umowy zawartej między osobą upoważnioną a Administratorem – o ile nie zostanie wypowiedziana wcześniej i dotyczy przetwarzania danych osobowych w formie **tradycyjnej i elektronicznej**.

Upoważnienie do przetwarzania danych osobowych obejmuje wyłącznie czynności przetwarzania konieczne do realizacji zadań powierzonych przez Administratora w ramach wykonywania obowiązków wynikających z umowy, w tym indywidualnego zakresu zadań pracownika.

Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, w trakcie zatrudnienia, jak również po jego ustaniu oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.
Osoba upoważniona jest zobowiązana do niezwłocznego zgłaszania wszystkich przypadków naruszeń ochrony danych osobowych Administratorowi lub inspektorowi ochrony danych.
Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych u Administratora.

.....
Data/czytelny podpis osoby upoważnionej

.....
Podpis Administratora

.....
(pieczęć i podpis AD lub osoby działającej w jego imieniu)

WÓJT
Danuta Kędziorska-Cieszyńska

Załącznik nr 3
do Procedury upoważniania do przetwarzania
danych osobowych w Urzędzie Gminy Brzozie

.....
(imię i nazwisko)

.....
(stanowisko)

Oświadczenie o zachowaniu poufności i przestrzeganiu przepisów o ochronie danych osobowych

1. Ja niżej podpisana/y oświadczam, iż zobowiązuję się do zachowania w tajemnicy i poufności danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miała/miał dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających z zawartej umowy, zarówno w czasie trwania umowy, jak i po jej ustaniu.

2. Zobowiązuję się do zachowania w poufności informacji uzyskanych w związku z pełnioną funkcją i wykonywaną pracą.

3. Oświadczam, że zapoznałem/am się z powszechnie obowiązującymi przepisami prawa w zakresie ochrony danych osobowych, w tym w szczególności z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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) oraz przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych i zobowiązuję się do ich przestrzegania.

4. W szczególności zobowiązuję się – w razie konieczności wynikającej z wykonywanych przeze mnie obowiązków służbowych – do pozyskiwania wiedzy i informacji na temat prawidłowości i zgodności z prawem przetwarzania danych osobowych m. in. od Administratora lub Inspektora.

5. Zobowiązuję się do niezwłocznego zgłaszania przełożonemu wszelkich przypadków naruszeń ochrony danych osobowych, zagrożeń, jak również wszelkich zaobserwowanych prób lub faktów naruszenia zabezpieczeń pomieszczeń lub systemów informatycznych.

6. Zobowiązuję się do zapewnienia ochrony, poufności oraz integralności przetwarzanych danych osobowych, w szczególności do zapewnienia należytego zabezpieczania danych osobowych przed ich ujawnieniem lub udostępnieniem (nawet przypadkowym) osobom trzecim.

7. Oświadczam, że powierzone mi dane osobowe będę wykorzystywała wyłącznie dla celów, związanych z wykonywaniem zadań służbowych, w zakresie określonym w nadanym mi imiennie upoważnieniu.

8. Mam świadomość grożącej mi odpowiedzialności, stosownie do przepisów art. 107 Ustawy o ochronie danych osobowych.

.....
Data / Czytelny podpis Pracownika

WÓJT
Danuta Kędziorska-Cieszyńska

Załącznik nr 4
do Polityki Ochrony Danych Osobowych
w Urzędzie Gminy Brzozie

Procedura obsługi żądań podmiotów danych w Urzędzie Gminy Brzozie

Zapewnienia

Administrator danych (ADO) weryfikuje i zapewnia możliwość efektywnego wykonania praw podmiotu, zapewniając jednocześnie odpowiednie warunki, aby prawa podmiotu były realizowane terminowo, w sposób wymagany przez RODO oraz dokumentowane.

Transparentność

ADO ma obowiązek podejmować odpowiednie środki, aby z osobą, której dane dotyczą, prowadzić wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania dotyczących jej danych osobowych.

Ułatwianie realizacji praw

ADO będzie ułatwiać podmiotowi danych realizację ich praw wskazanych w art. 15-22 RODO. Przyjmuje się następujące sposoby przekazywania informacji służące ułatwianiu zgłaszania żądań z art. 15-22 RODO, a także wniosków o wycofanie zgody.

CEL PROCEDURY

Sprecyzowanie i wdrożenie w jednolitej i przejrzystej procedury postępowania w przypadku złożenia przez osobę, której dane dotyczą wniosku w zakresie przysługujących jej na mocy przepisów o ochronie danych osobowych praw.

ZASADY REALIZACJI PRAW OSÓB, WYNIKAJĄCE Z RODO

1. Każdej osobie, której dane osobowe są przetwarzane przysługują prawa określone w art. 15-22 RODO, w tym:

1) prawo dostępu do danych jej dotyczących;
2) prawo do sprostowania danych;
3) prawo do usunięcia danych;
4) prawo do ograniczenia przetwarzania;
5) prawo do przenoszenia danych;
6) prawo do sprzeciwu na przetwarzanie jej danych;
7) prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu;
8) prawo do uzyskania kopii danych.

2. Rozpatrywanie żądań osoby, której dane dotyczą odbywa się po zweryfikowaniu tożsamości tej osoby.

3. Jeżeli istnieją uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15-21, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

4. Jeżeli nie można jednoznacznie potwierdzić tożsamości wnoszącego żądanie, odmawia się realizacji żądania.

5. W sytuacji powierzania danych podmiotom przetwarzającym lub udostępniania danych innym administratorom danych należy ich powiadamiać o każdym sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, które było wynikiem realizacji wniosku otrzymanego od osoby, której dane dotyczą.

6. Na wnioski dotyczące żądań realizacji praw osób należy udzielać odpowiedzi niezwłocznie, w terminie nie przekraczającym miesiąca od otrzymania żądania.

7. W razie potrzeby termin udzielenia odpowiedzi można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W takim wypadku w terminie miesiąca od otrzymania żądania należy poinformować osobę, której dane dotyczą o przedłużeniu terminu, z podaniem przyczyn opóźnienia.

8. Jeśli żądanie zostało przekazane elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

9. W przypadku nie podjęcia działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje się osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do Prezesa UODO oraz skorzystania ze środków ochrony prawnej przed sądem.

10. Informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15-22 i 34 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, można:

a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, albo
b) odmówić podjęcia działań w związku z żądaniem.

11. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

12. Informacje, których udziela się osobom, których dane dotyczą, na mocy art. 13 i 14, można opatrzyć standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego.

13. W imieniu małoletniego wniosek składa jego rodzic lub opiekun prawny.

ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

1. Kierownicy komórek organizacyjnych – w zakresie realizacji wniosku kierowanego do ich komórki organizacyjnej.

2. Inspektor ochrony danych [IOD] w zakresie konsultowania sposobu realizacji wniosku.

POSTANOWIENIA OGÓLNE PROCEDURY

1. Inspektor ochrony danych jest odpowiedzialny za przyjmowanie, rejestrowanie.

2. Korespondencję pisemną lub przesłaną elektronicznie za pośrednictwem poczty e-mail lub poprzez system e-PUAP, której treść wskazuje na wniosek obywatela w zakresie praw związanych z ochroną danych osobowych, należy niezwłocznie przekazać do IOD.

3. IOD po zarejestrowaniu wniosku weryfikuje tożsamość wnioskodawcy oraz czy informacje podane we wniosku umożliwiają udzielenie odpowiedzi na przesłany wniosek. Jeżeli nie zostało to zrealizowane wcześniej, przekazuje wnioskodawcy klauzulę informacyjną dotyczącą przetwarzania na potrzeby realizacji praw osoby, której dane dotyczą.

4. W przypadku braku możliwości potwierdzenia tożsamości, IOD wzywa wnioskodawcę do podania informacji, które umożliwią weryfikację tożsamości. Brak odpowiedzi lub uznanie, że dodatkowe informacje są niewystarczające, skutkuje przekazaniem wnioskodawcy informacji o odmowie zrealizowania wniosku. W takim wypadku należy wskazać sposób ponownego złożenia wniosku.

5. Po skutecznym zweryfikowaniu tożsamości wnioskodawcy, IOD przekazuje treść wniosku do właściwego pracownika merytorycznego, w celu uzyskania informacji o możliwości zrealizowania wniosku.

6. Pracownik merytoryczny niezwłocznie weryfikuje możliwość zrealizowania wniosku i przekazuje do IOD informacje o działaniach, które zostały zrealizowane w związku z otrzymanym wnioskiem.

7. W przypadku, gdy korespondencja, której treść wskazuje na wniosek obywatela w zakresie przysługujących mu praw wynikających z przepisów RODO, została przesłana bezpośrednio do pracownika merytorycznego, jest on zobowiązany do niezwłocznego przekazania wniosku do IOD.

8. IOD odnotowuje informację o sposobie załatwienia sprawy.

9. Skargi i wnioski realizowane na podstawie Kodeksu postępowania administracyjnego obsługiwane są zgodnie z odrębną procedurą obowiązującą w Urzędzie Gminy Brzozie.

ZASADY REALIZACJI POSZCZEGÓLNYCH PRAW, PRZYSŁUGUJĄCYCH OSOBIE, KTÓREJ DANE DOTYCZĄ

Prawo do uzyskania informacji

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania potwierdzenia, czy w Urzędzie Gminy Brzozie przetwarzane są jej dane osobowe. Jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz pozyskania następujących informacji:

1) w jakim celu są przetwarzane;
2) jakich kategorii danych osobowych dotyczy przetwarzanie;
3) o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
4) o planowanym okresie przechowywania danych osobowych, a gdy nie jest możliwe wskazanie konkretnego czasu przechowywania, o kryteriach ustalania tego okresu;
5) o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6) o prawie wniesienia skargi do organu nadzorczego;
7) o źródle danych, jeżeli nie zostały zebrane od osoby, której dotyczą.

2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej osoba, której dane dotyczą ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.

3. Jeżeli osoba, której dane dotyczą zwróci się z wnioskiem o dostarczenie kopii jej danych osobowych podlegających przetwarzaniu, żądanie takie realizuje się bezpłatnie. Za wszelkie kolejne kopie, można pobrać opłatę. Opłata powinna obejmować jedynie faktyczne koszty sporządzenia kopii, tj. koszt papieru, koszty kserowania. Cennik może być ustalony odrębnie dla każdej komórki organizacyjnej lub sporządzony dla całej jednostki.

4. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się drogą elektroniczną po jednoznacznej weryfikacji tożsamości osoby, np. podaniu daty urodzenia, podaniu innej informacji, która była podana we wcześniejszej korespondencji, a co do której można mieć pewność, że będzie ją posiadać jedynie osoba, którego dane dotyczą.

5. Kopię danych, o której mowa w ust. 3, wydaje się w postaci wydruku po ich przepisaniu lub skopiowaniu do ustrukturyzowanego powszechnie używanego formatu nadającego się do odczytu maszynowego (informacja maszynowa). Nie wydaje się skanów dokumentów ani ich kserokopii, które mogą zawierać dodatkowe dane niedotyczące osoby występującej z wnioskiem.

6. Prawo do uzyskania kopii, nie może niekorzystnie wpływać na prawa i wolności innych.

7. Inspektor ochrony danych wraz z pracownikiem merytorycznym, realizującym wniosek, podejmują decyzję, czy kopię danych wydać w postaci zanonimizowanych kopii dokumentów i/lub plików, czy informacji przetworzonej o kategoriach przetwarzanych danych. Prawo do uzyskania kopii

danych, nie jest równoważne z prawem do uzyskania kopii dokumentów lub plików, w których te dane są zawarte.

Prawo do sprostowania danych

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.

2. Ponadto osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

3. Pracownik merytoryczny, który w ramach wykonywanych zadań przetwarza dane osoby wnioskującej i otrzymał od IOD wniosek o sprostowanie danych, obowiązany jest dokonać weryfikacji przetwarzanych danych. Uzupełnienie danych następuje z uwzględnieniem celów przetwarzania.

4. Prawo do sprostowania danych nie znajduje zastosowania do danych osobowych, w odniesieniu do których tryb ich sprostowania lub uzupełnienia określają odrębne przepisy, np. procedura sprostowania błędów i omyłek zawartych w decyzji administracyjnej w trybie art. 113 Kodeksu postępowania administracyjnego.

Prawo do żądania usunięcia danych

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego usunięcia dotyczących jej danych osobowych. Należy bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

2) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;

3) dane osobowe były przetwarzane niezgodnie z prawem;

4) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie państwa członkowskiego, któremu podlega administrator.

2. Jeżeli dane osobowe zostały upublicznione, a na mocy ust. 1 istnieje obowiązek usunięcia tych danych osobowych, to (biorąc pod uwagę dostępną technologię i koszt realizacji) podejmuje się niezbędne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, że obywatel, którego dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

3. Przepisy ust. 1 i 2 nie mają zastosowania w zakresie, w jakim przetwarzanie jest niezbędne:

1) do korzystania z prawa do wolności wypowiedzi i informacji lub

2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii Europejskiej lub prawa państwa członkowskiego, któremu podlega administrator lub do wykonania

zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, lub

3) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania, lub

4) do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do żądania ograniczenia przetwarzania

1. Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania jej danych osobowych.

2. Ograniczenie przetwarzania oznacza, że dane osobowe można jedynie przechowywać. Inne formy przetwarzania mogą mieć miejsce wyłącznie za zgodą osoby, której dane dotyczą, lub 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 Unii Europejskiej lub państwa członkowskiego.

3. Do ograniczenia może dojść w następujących przypadkach:

1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych; w tym przypadku ogranicza się przetwarzanie na okres pozwalający sprawdzić prawidłowość danych;

2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

3) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

4) osoba, której dane dotyczą, wobec przetwarzania wniósł sprzeciw. W tym przypadku ogranicza się przetwarzanie do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu.

4. Ograniczenia przetwarzania dokonuje się poprzez odpowiednie oznaczenie danych osobowych, których dotyczy żądanie, przetwarzanych zarówno w formie tradycyjnej, jak i elektronicznej tak, aby każdy pracownik administratora, który jest upoważniony do przetwarzania tych danych był świadomy, że dane te można jedynie przechowywać.

5. Przed uchyleniem ograniczenia przetwarzania informuje się o tym osobę, która żądała ograniczenia.

Prawo do przeniesienia danych

1. Jeżeli przetwarzanie odbywa się na podstawie umowy, której stroną jest osoba, której dane dotyczą, oraz w sposób zautomatyzowany ma ona prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego swoje dane osobowe.

2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

3. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.

4. Wykonanie prawa, o którym mowa w ust. 1 pozostaje bez uszczerbku dla prawa do usunięcia danych.

5. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Prawo do wniesienia sprzeciwu wobec przetwarzania danych

1. Jeżeli przetwarzanie oparte jest na przesłance wykonania zadania realizowanego w interesie publicznym lub prawnie uzasadnionym interesie administratora osoba, której dane dotyczą z przyczyn związanych z jej szczególną sytuacją, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania jej danych osobowych.

2. Administratorowi nie wolno już przetwarzać danych osobowych, względem których wniesiono sprzeciw, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

3. W momencie złożenia sprzeciwu wobec przetwarzania administrator niezwłocznie ogranicza przetwarzanie i weryfikuje czy istnieją ważniejsze uzasadnione podstawy do przetwarzania niż interes osoby wnioskującej. Jeżeli administrator posiada podstawę prawną, o której mowa powyżej, informuje osobę wnioskującą o odmowie realizacji prawa wraz z uzasadnieniem decyzji. W przypadku, gdy uzasadniona jest przesłanka do zrealizowania żądania, postępuje się zgodnie z ust. 2.

4. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

5. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

Prawo do niepodlegania decyzjom na podstawie zautomatyzowanego przetwarzania

1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

2. Prawo to nie ma zastosowania, jeżeli ta decyzja:

1) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;

2) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą;

3) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

WÓJT
Danuta Kędzierska-Cieszyńska

Wójt Gminy Brzozie
woj. kujawsko-pomorskie

Załącznik nr 4
do Polityki Ochrony Danych Osobowych
w Urzędzie Gminy Brzozie

Procedura obsługi żądań podmiotów danych w Urzędzie Gminy Brzozie

Zapewnienia

Administrator danych (ADO) weryfikuje i zapewnia możliwość efektywnego wykonania praw podmiotu, zapewniając jednocześnie odpowiednie warunki, aby prawa podmiotu były realizowane terminowo, w sposób wymagany przez RODO oraz dokumentowane.

Transparentność

ADO ma obowiązek podejmować odpowiednie środki, aby z osobą, której dane dotyczą, prowadzić wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania dotyczących jej danych osobowych.

Ułatwianie realizacji praw

ADO będzie ułatwiać podmiotowi danych realizację ich praw wskazanych w art. 15-22 RODO. Przyjmuje się następujące sposoby przekazywania informacji służące ułatwianiu zgłaszania żądań z art. 15-22 RODO, a także wniosków o wycofanie zgody.

CEL PROCEDURY

Sprecyzowanie i wdrożenie w jednolitej i przejrzystej procedury postępowania w przypadku złożenia przez osobę, której dane dotyczą wniosku w zakresie przysługujących jej na mocy przepisów o ochronie danych osobowych praw.

ZASADY REALIZACJI PRAW OSÓB, WYNIKAJĄCE Z RODO

1. Każdej osobie, której dane osobowe są przetwarzane przysługują prawa określone w art. 15-22 RODO, w tym:

1) prawo dostępu do danych jej dotyczących;
2) prawo do sprostowania danych;
3) prawo do usunięcia danych;
4) prawo do ograniczenia przetwarzania;
5) prawo do przenoszenia danych;
6) prawo do sprzeciwu na przetwarzanie jej danych;
7) prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu;
8) prawo do uzyskania kopii danych.

2. Rozpatrywanie żądań osoby, której dane dotyczą odbywa się po zweryfikowaniu tożsamości tej osoby.

3. Jeżeli istnieją uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15-21, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

4. Jeżeli nie można jednoznacznie potwierdzić tożsamości wnoszącego żądanie, odmawia się realizacji żądania.

5. W sytuacji powierzania danych podmiotom przetwarzającym lub udostępniania danych innym administratorom danych należy ich powiadamiać o każdym sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, które było wynikiem realizacji wniosku otrzymanego od osoby, której dane dotyczą.

6. Na wnioski dotyczące żądań realizacji praw osób należy udzielać odpowiedzi niezwłocznie, w terminie nie przekraczającym miesiąca od otrzymania żądania.

7. W razie potrzeby termin udzielenia odpowiedzi można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W takim wypadku w terminie miesiąca od otrzymania żądania należy poinformować osobę, której dane dotyczą o przedłużeniu terminu, z podaniem przyczyn opóźnienia.

8. Jeśli żądanie zostało przekazane elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

9. W przypadku nie podjęcia działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje się osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do Prezesa UODO oraz skorzystania ze środków ochrony prawnej przed sądem.

10. Informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15-22 i 34 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, można:

a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, albo
b) odmówić podjęcia działań w związku z żądaniem.

11. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

12. Informacje, których udziela się osobom, których dane dotyczą, na mocy art. 13 i 14, można opatrzyć standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego.

13. W imieniu małoletniego wniosek składa jego rodzic lub opiekun prawny.

ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

1. Kierownicy komórek organizacyjnych – w zakresie realizacji wniosku kierowanego do ich komórki organizacyjnej.

2. Inspektor ochrony danych [IOD] w zakresie konsultowania sposobu realizacji wniosku.

POSTANOWIENIA OGÓLNE PROCEDURY

1. Inspektor ochrony danych jest odpowiedzialny za przyjmowanie, rejestrowanie.

2. Korespondencję pisemną lub przesłaną elektronicznie za pośrednictwem poczty e-mail lub poprzez system e-PUAP, której treść wskazuje na wniosek obywatela w zakresie praw związanych z ochroną danych osobowych, należy niezwłocznie przekazać do IOD.

3. IOD po zarejestrowaniu wniosku weryfikuje tożsamość wnioskodawcy oraz czy informacje podane we wniosku umożliwiają udzielenie odpowiedzi na przesłany wniosek. Jeżeli nie zostało to zrealizowane wcześniej, przekazuje wnioskodawcy klauzulę informacyjną dotyczącą przetwarzania na potrzeby realizacji praw osoby, której dane dotyczą.

4. W przypadku braku możliwości potwierdzenia tożsamości, IOD wzywa wnioskodawcę do podania informacji, które umożliwią weryfikację tożsamości. Brak odpowiedzi lub uznanie, że dodatkowe informacje są niewystarczające, skutkuje przekazaniem wnioskodawcy informacji o odmowie zrealizowania wniosku. W takim wypadku należy wskazać sposób ponownego złożenia wniosku.

5. Po skutecznym zweryfikowaniu tożsamości wnioskodawcy, IOD przekazuje treść wniosku do właściwego pracownika merytorycznego, w celu uzyskania informacji o możliwości zrealizowania wniosku.

6. Pracownik merytoryczny niezwłocznie weryfikuje możliwość zrealizowania wniosku i przekazuje do IOD informacje o działaniach, które zostały zrealizowane w związku z otrzymanym wnioskiem.

7. W przypadku, gdy korespondencja, której treść wskazuje na wniosek obywatela w zakresie przysługujących mu praw wynikających z przepisów RODO, została przesłana bezpośrednio do pracownika merytorycznego, jest on zobowiązany do niezwłocznego przekazania wniosku do IOD.

8. IOD odnotowuje informację o sposobie załatwienia sprawy.

9. Skargi i wnioski realizowane na podstawie Kodeksu postępowania administracyjnego obsługiwane są zgodnie z odrębną procedurą obowiązującą w Urzędzie Gminy Brzozie.

ZASADY REALIZACJI POSZCZEGÓLNYCH PRAW, PRZYSŁUGUJĄCYCH OSOBIE, KTÓREJ DANE DOTYCZĄ

Prawo do uzyskania informacji

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania potwierdzenia, czy w Urzędzie Gminy Brzozie przetwarzane są jej dane osobowe. Jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz pozyskania następujących informacji:

1) w jakim celu są przetwarzane;
2) jakich kategorii danych osobowych dotyczy przetwarzanie;
3) o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
4) o planowanym okresie przechowywania danych osobowych, a gdy nie jest możliwe wskazanie konkretnego czasu przechowywania, o kryteriach ustalania tego okresu;
5) o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6) o prawie wniesienia skargi do organu nadzorczego;
7) o źródle danych, jeżeli nie zostały zebrane od osoby, której dotyczą.

2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej osoba, której dane dotyczą ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.

3. Jeżeli osoba, której dane dotyczą zwróci się z wnioskiem o dostarczenie kopii jej danych osobowych podlegających przetwarzaniu, żądanie takie realizuje się bezpłatnie. Za wszelkie kolejne kopie, można pobrać opłatę. Opłata powinna obejmować jedynie faktyczne koszty sporządzenia kopii, tj. koszt papieru, koszty kserowania. Cennik może być ustalony odrębnie dla każdej komórki organizacyjnej lub sporządzony dla całej jednostki.

4. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się drogą elektroniczną po jednoznacznej weryfikacji tożsamości osoby, np. podaniu daty urodzenia, podaniu innej informacji, która była podana we wcześniejszej korespondencji, a co do której można mieć pewność, że będzie ją posiadać jedynie osoba, którego dane dotyczą.

5. Kopię danych, o której mowa w ust. 3, wydaje się w postaci wydruku po ich przepisaniu lub skopiowaniu do ustrukturyzowanego powszechnie używanego formatu nadającego się do odczytu maszynowego (informacja maszynowa). Nie wydaje się skanów dokumentów ani ich kserokopii, które mogą zawierać dodatkowe dane niedotyczące osoby występującej z wnioskiem.

6. Prawo do uzyskania kopii, nie może niekorzystnie wpływać na prawa i wolności innych.

7. Inspektor ochrony danych wraz z pracownikiem merytorycznym, realizującym wniosek, podejmują decyzję, czy kopię danych wydać w postaci zanonimizowanych kopii dokumentów i/lub plików, czy informacji przetworzonej o kategoriach przetwarzanych danych. Prawo do uzyskania kopii

danych, nie jest równoważne z prawem do uzyskania kopii dokumentów lub plików, w których te dane są zawarte.

Prawo do sprostowania danych

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.

2. Ponadto osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

3. Pracownik merytoryczny, który w ramach wykonywanych zadań przetwarza dane osoby wnioskującej i otrzymał od IOD wniosek o sprostowanie danych, obowiązany jest dokonać weryfikacji przetwarzanych danych. Uzupełnienie danych następuje z uwzględnieniem celów przetwarzania.

4. Prawo do sprostowania danych nie znajduje zastosowania do danych osobowych, w odniesieniu do których tryb ich sprostowania lub uzupełnienia określają odrębne przepisy, np. procedura sprostowania błędów i omyłek zawartych w decyzji administracyjnej w trybie art. 113 Kodeksu postępowania administracyjnego.

Prawo do żądania usunięcia danych

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego usunięcia dotyczących jej danych osobowych. Należy bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

2) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;

3) dane osobowe były przetwarzane niezgodnie z prawem;

4) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie państwa członkowskiego, któremu podlega administrator.

2. Jeżeli dane osobowe zostały upublicznione, a na mocy ust. 1 istnieje obowiązek usunięcia tych danych osobowych, to (biorąc pod uwagę dostępną technologię i koszt realizacji) podejmuje się niezbędne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, że obywatel, którego dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

3. Przepisy ust. 1 i 2 nie mają zastosowania w zakresie, w jakim przetwarzanie jest niezbędne:

1) do korzystania z prawa do wolności wypowiedzi i informacji lub

2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii Europejskiej lub prawa państwa członkowskiego, któremu podlega administrator lub do wykonania

zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, lub

3) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania, lub

4) do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do żądania ograniczenia przetwarzania

1. Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania jej danych osobowych.

2. Ograniczenie przetwarzania oznacza, że dane osobowe można jedynie przechowywać. Inne formy przetwarzania mogą mieć miejsce wyłącznie za zgodą osoby, której dane dotyczą, lub 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 Unii Europejskiej lub państwa członkowskiego.

3. Do ograniczenia może dojść w następujących przypadkach:

1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych; w tym przypadku ogranicza się przetwarzanie na okres pozwalający sprawdzić prawidłowość danych;

2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

3) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

4) osoba, której dane dotyczą, wobec przetwarzania wniósł sprzeciw. W tym przypadku ogranicza się przetwarzanie do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu.

4. Ograniczenia przetwarzania dokonuje się poprzez odpowiednie oznaczenie danych osobowych, których dotyczy żądanie, przetwarzanych zarówno w formie tradycyjnej, jak i elektronicznej tak, aby każdy pracownik administratora, który jest upoważniony do przetwarzania tych danych był świadomy, że dane te można jedynie przechowywać.

5. Przed uchyleniem ograniczenia przetwarzania informuje się o tym osobę, która żądała ograniczenia.

Prawo do przeniesienia danych

1. Jeżeli przetwarzanie odbywa się na podstawie umowy, której stroną jest osoba, której dane dotyczą, oraz w sposób zautomatyzowany ma ona prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego swoje dane osobowe.

2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

3. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.

4. Wykonanie prawa, o którym mowa w ust. 1 pozostaje bez uszczerbku dla prawa do usunięcia danych.

5. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Prawo do wniesienia sprzeciwu wobec przetwarzania danych

1. Jeżeli przetwarzanie oparte jest na przesłance wykonania zadania realizowanego w interesie publicznym lub prawnie uzasadnionym interesie administratora osoba, której dane dotyczą z przyczyn związanych z jej szczególną sytuacją, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania jej danych osobowych.

2. Administratorowi nie wolno już przetwarzać danych osobowych, względem których wniesiono sprzeciw, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

3. W momencie złożenia sprzeciwu wobec przetwarzania administrator niezwłocznie ogranicza przetwarzanie i weryfikuje czy istnieją ważniejsze uzasadnione podstawy do przetwarzania niż interes osoby wnioskującej. Jeżeli administrator posiada podstawę prawną, o której mowa powyżej, informuje osobę wnioskującą o odmowie realizacji prawa wraz z uzasadnieniem decyzji. W przypadku, gdy uzasadniona jest przesłanka do zrealizowania żądania, postępuje się zgodnie z ust. 2.

4. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

5. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

Prawo do niepodlegania decyzjom na podstawie zautomatyzowanego przetwarzania

1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

2. Prawo to nie ma zastosowania, jeżeli ta decyzja:

1) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;

2) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą;

3) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

Załącznik nr 6
do Polityki Ochrony Danych Osobowych
w Urzędzie Gminy Brzozie

Procedura postępowania w przypadku naruszenia ochrony danych osobowych w Urzędzie Gminy Brzozie

I. Cel procedury

Celem procedury jest zapewnienie szybkiej i skutecznej reakcji na naruszenie ochrony danych osobowych, w tym spełnienie obowiązków wynikających z art. 33 i 34 RODO oraz wytycznych UODO.

II. Definicje

1. **Naruszenie ochrony danych osobowych** – zgodnie z art. 4 pkt 12 RODO oznacza naruszenie bezpieczeństwa prowadzące do:
   1) zniszczenia;
   2) utracenia;
   3) zmodyfikowania;
   4) nieuprawnionego ujawnienia;
   5) nieuprawnionego dostępu.
2. **Administratorem danych osobowych** jest, zgodnie z artykułem 4 punkt 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
3. Jeśli w postanowieniach zarządzenia nie zostanie wskazane inaczej, Administratorem Danych Osobowych jest Wójt Gminy.

III. Klasyfikacja naruszeń ochrony danych osobowych

1. **Naruszenia poufności danych** rozumie się jako każde zdarzenie prowadzące do:
   1) nieuprawnionego ujawnienia danych osobowych osobom nieupoważnionym;
   2) nieautoryzowanego dostępu do danych objętych obowiązkiem ochrony;
   3) utraty kontroli nad danymi w wyniku działania osób trzecich lub niewłaściwych zabezpieczeń.
2. **Naruszenia integralności danych** oznaczają zdarzenia skutkujące:
   1) nieautoryzowaną lub przypadkową modyfikacją danych osobowych;

2) nieprawidłowym przetworzeniem prowadzącym do zmiany treści danych;
3) uszkodzeniem danych uniemożliwiającym ustalenie ich pierwotnej wersji.

3. **Naruszenia dostępności danych** obejmują sytuacje, w których:
   1) dane osobowe stają się niedostępne dla uprawnionych podmiotów w wymaganym czasie;
   2) dochodzi do trwałej utraty danych w wyniku zdarzeń losowych lub celowych działań;
   3) systemy przetwarzania uniemożliwiają realizację praw osób, których dane dotyczą.

IV. Stwierdzenie naruszenia

1. Wystąpienie naruszenia ochrony danych osobowych nie oznacza, że administrator lub podmiot przetwarzający dopuścił się naruszenia przepisów RODO.
2. Naruszenie przepisów RODO wynika z postępowania niezgodnego z określonymi wymogami przewidzianymi w tym akcie prawnym.

V. Obowiązki administratora

1. W przypadku „stwierdzenia" naruszenia ochrony danych osobowych administrator musi zrealizować następujące obowiązki. Należą do nich:
   1) zaradzenie naruszeniu ochrony danych osobowych oraz jego ewentualnym negatywnym skutkom;
   2) ocenienie ryzyka naruszenia praw lub wolności osób fizycznych, jakie może wynikać z naruszenia ochrony danych osobowych;
   3) zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu (w przypadku ryzyka naruszenia praw lub wolności osób fizycznych);
   4) zawiadamianie osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych (w przypadku wysokiego ryzyka naruszenia praw lub wolności tych osób);
   5) dokumentowanie naruszenia ochrony danych osobowych. Każde takie zdarzenie stanowi okazję do poprawy zabezpieczeń i minimalizowania ryzyka występowania podobnych incydentów w przyszłości.

VI. Działania IOD

1. Działania IOD w sprawie naruszeń ochrony danych osobowych obejmują w szczególności:
   1) pomoc w zapobieganiu naruszeniom, w szczególności poprzez promowanie w organizacji wiedzy o ochronie danych osobowych, organizowanie szkoleń oraz formułowanie zaleceń dotyczących bezpieczeństwa przetwarzania danych;
   2) udzielanie wskazówek dotyczących odpowiedniego reagowania na naruszenia ochrony danych osobowych, w tym zaradzania im;
   3) doradztwo w zakresie dokumentowania naruszeń i zarządzania dokumentacją;

4) przekazywanie dodatkowych informacji o naruszeniach organowi nadzorczemu i osobom, których dane dotyczą.

2. IOD nie powinien:
   a) zgłaszać naruszeń ochrony danych osobowych Prezesowi UODO w imieniu administratorów ani podpisywać i wysyłać takich zgłoszeń;
   b) zawiadamiać w imieniu administratorów osób, których dane dotyczą, o naruszeniach ochrony danych osobowych;
   c) dokumentować naruszeń ochrony danych osobowych w imieniu administratorów (w szczególności jeśli wiązałoby się to z ustalaniem celów i sposobów przetwarzania danych osobowych albo określeniem działań zaradczych);
   d) podejmować zobowiązań dotyczących bezpieczeństwa przetwarzania w imieniu administratorów lub podmiotów przetwarzających;
   e) działać na podstawie pełnomocnictwa w sprawach dotyczących ochrony danych osobowych.

VII. Odpowiedzialność administratorów w zakresie ochrony danych osobowych

1. Administrator danych osobowych ponosi odpowiedzialność za przestrzeganie przepisów o ochronie danych osobowych, zgodnie z zasadą rozliczalności, o której mowa w art. 5 ust. 2 RODO.
2. Zasada rozliczalności oznacza obowiązek wykazania, że działania podejmowane przez administratora są zgodne z przepisami RODO.
3. Administrator jest zobowiązany do dokumentowania swoich działań w zakresie ochrony danych osobowych oraz do przechowywania dowodów potwierdzających zgodność tych działań z obowiązującymi przepisami, w szczególności na potrzeby kontroli lub postępowania przed organem nadzorczym.
4. Dokumentacja potwierdzająca zgodność z RODO obejmuje w szczególności:
   1) dokumenty tradycyjne, takie jak notatki służbowe, instrukcje, procedury, decyzje wewnętrzne, korespondencję e-mailową;
   2) wyciągi i raporty z systemów informatycznych;
   3) raporty z audytów, testów bezpieczeństwa lub przeglądów zgodności.
5. Brak możliwości wykazania zgodności z RODO może zostać uznany za naruszenie przepisów o ochronie danych osobowych, niezależnie od rzeczywistego przebiegu zdarzeń.

VIII. Obowiązek zgłaszania incydentów ochrony danych osobowych

1. Każdy pracownik, który powezmie podejrzenie lub stwierdzi naruszenie ochrony danych osobowych (tzw. incydent), jest zobowiązany niezwłocznie poinformować o tym swojego bezpośredniego przełożonego oraz Inspektora Ochrony Danych.

2. W przypadku, gdy incydent dotyczy funkcjonowania jednostki organizacyjnej, pracownik zobowiązany jest również powiadomić organ wykonawczy (np. wójta, burmistrza, prezydenta miasta, dyrektora), przekazując możliwie pełne informacje na temat zdarzenia.
3. Zgłoszenie powinno nastąpić niezwłocznie, nie później niż w ciągu 24 godzin od momentu powzięcia informacji o incydencie, w formie ustnej (do wiadomości przełożonego) oraz pisemnej (e-mail, notatka służbowa lub formularz zgłoszeniowy).
4. Niedopełnienie obowiązku zgłoszenia może zostać potraktowane jako naruszenie obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

IX. Moment rozpoczęcia biegu terminu zgłoszenia naruszenia ochrony danych osobowych

1. Administrator danych osobowych stwierdza naruszenie ochrony danych osobowych w momencie, gdy uzyskuje wiedzę, że wykryte zdarzenie:
   1) stanowi incydent bezpieczeństwa informacji;
   2) dotyczy przetwarzanych danych osobowych;
   3) może skutkować przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub dostępem do tych danych.
2. Stwierdzenie naruszenia przez Administratora stanowi moment początkowy dla biegu terminu 72 godzin na dokonanie ewentualnego zgłoszenia do organu nadzorczego, zgodnie z art. 33 ust. 1 RODO.
3. Za moment uzyskania uzasadnionych podstaw uznaje się także sytuację, w której Inspektor Ochrony Danych, działając z upoważnienia Wójta, poinformuje go o potwierdzonym naruszeniu ochrony danych osobowych.
4. W przypadku wątpliwości co do charakteru zdarzenia, Wójt podejmuje niezwłoczne działania w celu ustalenia, czy wystąpiło naruszenie wymagające zgłoszenia do organu nadzorczego.
5. Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania wiąże się ryzyko lub wysokie ryzyko.

X. Zasady zgłaszania incydentów w ramach współpracy z podmiotami przetwarzającymi

1. Ze względu na fakt, że incydenty ochrony danych osobowych mogą występować zarówno po stronie administratora, jak i podmiotów przetwarzających, strony zobowiązane są do uzgodnienia jednoznacznych zasad wymiany informacji na temat potencjalnych lub potwierdzonych naruszeń ochrony danych osobowych.
2. W umowie powierzenia przetwarzania danych osobowych należy określić:
   1) kto jest odpowiedzialny za zgłoszenie naruszenia organowi nadzorczemu i osobom, których dane dotyczą;

2) sposób i formę powiadamiania pozostałych stron o incydencie (np. e-mail, telefon, dedykowany formularz);
3) maksymalny termin na zgłoszenie incydentu drugiej stronie (np. nie później niż w ciągu 12 godzin od wykrycia);
4) zakres przekazywanych informacji, w tym co najmniej: opis naruszenia, kategorie danych i osób, potencjalne skutki oraz podjęte lub planowane środki zaradcze.

3. Celem powyższych ustaleń jest umożliwienie administratorowi niezwłocznego podjęcia działań zaradczych oraz realizacja obowiązków wynikających z RODO, w szczególności w zakresie zgłaszania naruszeń organowi nadzorczemu w terminie 72 godzin.
4. Brak współpracy lub opóźnienie w przekazaniu informacji przez podmiot przetwarzający może zostać uznane za naruszenie postanowień umowy i skutkować odpowiedzialnością kontraktową.

XI. Zasady oceny ryzyka naruszenia ochrony danych osobowych

1. Administrator danych osobowych jest zobowiązany do dokonania niezwłocznej oceny ryzyka naruszenia ochrony danych osobowych w przypadku zaistnienia incydentu bezpieczeństwa.
2. Aby prawidłowo ocenić ryzyko, należy oszacować:
   1) wagę potencjalnych konsekwencji dla osób, których dane dotyczą;
   2) prawdopodobieństwo wystąpienia tych konsekwencji.
   3)
3. Ocena ryzyka powinna uwzględniać w szczególności następujące okoliczności danego zdarzenia:
   1) rodzaj naruszenia ochrony danych osobowych (np. utrata, ujawnienie, dostęp nieuprawniony);
   2) charakter, wrażliwość i zakres danych osobowych objętych naruszeniem;
   3) łatwość identyfikacji osób, których dane dotyczą;
   4) dotkliwość możliwych konsekwencji dla osób, których dane dotyczą (np. utrata reputacji, szkoda majątkowa, dyskryminacja);
   5) cechy szczególne osób, których dane dotyczą (np. dzieci, osoby starsze, osoby w trudnej sytuacji życiowej);
   6) cechy szczególne administratora (np. skala przetwarzania danych, profil działalności publicznej);
   7) liczbę osób, których dane dotyczą.
4. Ocena ryzyka powinna być odpowiednio udokumentowana i przechowywana na wypadek kontroli organu nadzorczego.
5. Administrator musi ustalić, czy naruszenie ochrony danych osobowych może wiązać się z:
   1) brakiem ryzyka;

2) ryzykiem, co wymaga zgłoszenia go Prezesowi UODO;
3) wysokim ryzykiem, co oznacza obowiązek zgłoszenia go Prezesowi UODO oraz zawiadomienia osób, których dane dotyczą.

XII. Przypadki niewystępowania ryzyka naruszenia praw i wolności

1. Administrator, dokonując oceny ryzyka związanego z incydentem ochrony danych osobowych, może uznać, że ryzyko naruszenia praw lub wolności osób fizycznych nie występuje, jeżeli spełnione są określone przesłanki.
2. Do typowych przypadków, w których brak jest ryzyka naruszenia, należą w szczególności:
   1) ujawnienie danych, które są już publicznie dostępne, a ich ponowne rozpowszechnienie nie powoduje dodatkowego zagrożenia dla osób, których dane dotyczą;
   2) ujawnienie lub utrata danych osobowych zaszyfrowanych w sposób zapewniający ich nieczytelność dla osób nieupoważnionych – pod warunkiem, że:
      a)dane są zabezpieczone silnym mechanizmem kryptograficznym,
      b) klucz szyfrujący nie został naruszony,
      c)administrator posiada dostęp do integralnej kopii zapasowej danych;
   3) incydenty, którym administrator skutecznie i definitywnie zaradził przed powstaniem realnego zagrożenia dla osób, których dane dotyczą (np. przywrócenie kontroli nad kontem zanim doszło do odczytu danych przez osobę nieuprawnioną).
3. W przypadkach takich incydentów nie zachodzi obowiązek zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych, ani zawiadamiania osób, których dane dotyczą – pod warunkiem, że administrator posiada dokumentację potwierdzającą brak ryzyka.
4. Każdy incydent związany z naruszeniem ochrony danych osobowych wymaga indywidualnej analizy z uwzględnieniem charakteru zdarzenia oraz jego potencjalnych skutków dla osób, których dane dotyczą.

XIII. Okoliczności świadczące o wysokim ryzyku naruszenia praw lub wolności osób fizycznych

1. Administrator danych osobowych, powinien w szczególności zwrócić uwagę na następujące okoliczności, które mogą świadczyć o wysokim ryzyku naruszenia praw lub wolności osób fizycznych. Powyższe dotyczy w szczególności objęcie incydentem szczególnych kategorii danych osobowych, takich jak:
   1) informacje ujawniające pochodzenie rasowe lub etniczne,
   2) poglądy polityczne,
   3) przekonania religijne lub światopoglądowe,
   4) przynależność do związków zawodowych,
   5) dane genetyczne i biometryczne,

6) dane dotyczące zdrowia, seksualności i orientacji seksualnej,
7) informacje o wyrokach skazujących oraz czynach zabronionych,
8) dane finansowe oraz dane powszechnie wykorzystywane do potwierdzania tożsamości lub zawierania umów (takie jak numer PESEL, seria i numer dowodu osobistego);

2. Szeroki zakres danych osobowych objętych incydentem – im większy zakres, tym większe ryzyko;
3. Szczególna dotkliwość potencjalnych skutków incydentu, w tym:
   1) kradzież tożsamości;
   2) oszustwa finansowe;
   3) poważne straty finansowe;
   4) problemy zawodowe;
   5) uszczerbek na zdrowiu psychicznym lub fizycznym;
   6) silny stres, lęk lub obniżone poczucie bezpieczeństwa.
4. Szczególny charakter osób objętych incydentem – np. dzieci, osoby starsze, osoby z niepełnosprawnością lub znajdujące się w trudnej sytuacji życiowej;
5. Duża liczba osób objętych incydentem – im większa skala naruszenia, tym wyższe prawdopodobieństwo wystąpienia szkód. W przypadku wystąpienia jednej lub kilku z wyżej wymienionych okoliczności, administrator powinien rozważyć konieczność niezwłocznego poinformowania osób, których dane dotyczą, zgodnie z art. 34 RODO.

XIV. Zaufany odbiorca danych osobowych

1. Zaufanym odbiorcą może zostać uznany taki podmiot, który przypadkowo otrzymał dane osobowe, lecz z uwagi na dotychczasową, pozytywną współpracę z administratorem danych osobowych można uznać go za godnego zaufania, a więc takiego, który prawidłowo zareaguje na zaistniały incydent i przyczyni się do ograniczenia ryzyka naruszenia praw lub wolności osób, których dane dotyczą.
2. Aby możliwe było uznanie nieuprawnionego odbiorcy danych osobowych za „zaufanego", muszą zostać spełnione łącznie następujące warunki:
   1) podmiot ten pozostaje z administratorem w stałych relacjach organizacyjnych lub współpracy biznesowej, np. jako:
      a) inny dział w strukturze urzędu,
      b) długoletni, sprawdzony dostawca usług,
      c) podmiot przetwarzający działający na podstawie umowy powierzenia, który wykazuje się wysokim poziomem profesjonalizmu i rzetelności;
   2) administrator danych osobowych zna istotne szczegóły dotyczące tego podmiotu, w szczególności:
      a) jego procedury bezpieczeństwa,

b) historię współpracy, w tym wcześniejsze, prawidłowe reakcje na incydenty lub sytuacje wymagające podjęcia działań ochronnych.

3. Uznanie danego odbiorcy za „zaufanego" następuje w ramach indywidualnej oceny ryzyka związanego z danym naruszeniem poufności danych osobowych. Oznacza to, że:
   1) decyzja o nadaniu statusu „zaufanego odbiorcy" nie ma charakteru stałego;
   2) każdorazowo należy przeprowadzić ocenę ryzyka naruszenia praw lub wolności osób fizycznych;
   3) status ten należy monitorować i okresowo weryfikować, w tym również w kontekście nowych okoliczności lub incydentów.
4. Jeżeli zmiana okoliczności (np. zmiana praktyk odbiorcy, incydent po jego stronie, naruszenie warunków umowy) prowadzi do utraty zaufania, administrator powinien ponownie ocenić ryzyko i ewentualnie uznać, że dany podmiot nie spełnia już kryteriów „zaufanego odbiorcy".

XV. Obowiązek dokumentowania naruszeń ochrony danych osobowych

1. Administrator danych osobowych ma obowiązek dokumentować wszystkie stwierdzone naruszenia ochrony danych osobowych.
2. W ramach zasady rozliczalności administrator powinien również dokumentować przypadki incydentów bezpieczeństwa, które zostały zaklasyfikowane jako niebędące naruszeniami danych osobowych, ze szczególnym uwzględnieniem przyczyn takiej decyzji.
3. Dokumentacja może być prowadzona w formie wewnętrznego rejestru naruszeń ochrony danych osobowych. Prowadzenie odrębnej ewidencji nie jest obowiązkowe, jednak wszelkie informacje muszą być:
   1) wyraźnie oznaczone;
   2) dostępne do wglądu na żądanie.
4. Dokumentacja naruszeń powinna obejmować co najmniej następujące elementy:

   1) okoliczności naruszenia ochrony danych osobowych, w tym:
      a) data i czas wystąpienia naruszenia,
      b) moment stwierdzenia naruszenia oraz jego zakończenia,
      c) sposób wykrycia naruszenia,
      d) przyczyny naruszenia,
      e) rodzaj i przebieg naruszenia,
      f) rodzaj i zakres danych osobowych objętych naruszeniem,
      g) liczba i kategorie osób, których dane dotyczą;

   2) skutki naruszenia, jeśli wystąpiły, oraz możliwe konsekwencje dla osób, których dane dotyczą;

   3) uzasadnienie oceny ryzyka związanego z naruszeniem;

   4) podjęte działania:

a) zaradcze, mające na celu powstrzymanie i ograniczenie skutków naruszenia,
b) zapobiegawcze, mające na celu minimalizowanie ryzyka wystąpienia podobnych naruszeń w przyszłości;

5) szczegóły dotyczące zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych (UODO), w tym:
a) data zgłoszenia,
b) ewentualne przyczyny opóźnienia w zgłoszeniu,
c) inne istotne informacje zawarte w zgłoszeniu,
d) lub w przypadku braku zgłoszenia – uzasadnienie decyzji o niezgłoszeniu naruszenia Prezesowi UODO,

6) szczegóły dotyczące zawiadomienia osób, których dane dotyczą, o naruszeniu, w tym:
a) data zawiadomienia,
b) treść zawiadomienia,
c) metoda powiadomienia,
d) liczba osób powiadomionych,
e) lub – w razie braku zawiadomienia – uzasadnienie decyzji o niezawiadomieniu osób, których dane dotyczą.

5. Dokumentacja naruszeń ochrony danych osobowych powinna być regularnie aktualizowana. Każda nowa informacja dotycząca incydentu, jego skutków lub podjętych działań może wpływać na ocenę ryzyka i wymagać korekty rejestru.

XVI. Techniczna realizacja obowiązku zgłaszania naruszeń ochrony danych osobowych na podstawie art. 33 RODO

1. Techniczna realizacja obowiązku zgłaszania naruszeń ochrony danych osobowych na podstawie art. 33 RODO odbywa się za pośrednictwem kanałów komunikacji wskazanych przez Prezesa Urzędu Ochrony Danych Osobowych (UODO).
2. W ramach realizacji obowiązku zgłaszania naruszeń ochrony danych osobowych wyróżnia się trzy rodzaje zgłoszeń:
   1) zgłoszenia wstępne – pozwalają na przekazanie podstawowych informacji o incydencie w wymaganym terminie (72 godziny od stwierdzenia naruszenia), z jednoczesnym obowiązkiem późniejszego uzupełnienia danych;
   2) zgłoszenia uzupełniające – umożliwiają aktualizowanie oraz rozszerzanie informacji o naruszeniu w miarę pozyskiwania nowych danych i szczegółów dotyczących incydentu;
   3) zgłoszenia kompletne – zawierają wszystkie wymagane informacje już przy pierwszym zgłoszeniu, co pozwala na pełne i wyczerpujące przedstawienie sytuacji bez konieczności późniejszych uzupełnień.

3. Zgłoszenie powinno zawierać:
    1) podstawowe informacje o administratorze oraz innych podmiotach powiązanych z incydentem, takich jak współadministratorzy, podmioty przetwarzające lub podmioty trzecie;
    2) okoliczności naruszenia ochrony danych osobowych, w tym m. in. datę i czas wystąpienia naruszenia, moment jego stwierdzenia i zakończenia, sposób wykrycia, przyczyny, rodzaj i przebieg naruszenia oraz rodzaj i zakres danych objętych naruszeniem, a także liczbę i kategorie osób, których dane dotyczą;
    3) skutki naruszenia lub możliwe skutki dla osób, których dane dotyczą;
    4) uzasadnienie oceny ryzyka związanego z naruszeniem;
    5) podjęte działania zaradcze, jeśli zostały wdrożone, lub zaplanowane działania wraz z deklarowaną datą ich realizacji, gdy nie zostały jeszcze podjęte;
    6) wdrożone środki bezpieczeństwa zapobiegające podobnym incydentom w przyszłości lub zaplanowane środki z deklaracją terminu ich wdrożenia;
    7) szczegóły dotyczące zawiadomienia osób, których dane dotyczą o naruszeniu – w tym datę, treść, metodę oraz liczbę zawiadomionych osób, albo, jeśli osoby te nie zostały zawiadomione, uzasadnienie takiej decyzji zgodnie z art. 34 ust. 3 RODO;
    8) imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych (IOD) lub informacji o innym wyznaczonym w organizacji punkcie kontaktowym.

XVII. Zawiadamianie osób, których dane dotyczą

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Administrator nie jest zobowiązany do zawiadamiania osób, których dane dotyczą, o naruszeniach ochrony danych osobowych, nawet jeśli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności tych osób, jeżeli zachodzą przynajmniej jedno z następujących warunków:
    1) przed wystąpieniem naruszenia zastosowano odpowiednie środki ochrony, które całkowicie eliminują wysokie ryzyko – przykładem może być sytuacja ujawnienia lub utraty danych zaszyfrowanych w sposób zapewniający ich nieczytelność dla osób nieupoważnionych pod warunkiem, że klucz szyfrujący nie został naruszony, a administrator dysponuje kopią zapasową tych danych;
    2) po wystąpieniu naruszenia administrator natychmiast podjął działania ochronne, które skutecznie wyeliminowały wysokie ryzyko naruszenia praw lub wolności osób, czyli incydent został definitywnie opanowany i zarządzony;

3) zawiadomienie osób wymagałoby niewspółmiernie dużego wysiłku, jednakże ten wyjątek obowiązuje tylko wtedy, gdy administrator wyda publiczny komunikat lub w inny, równie skuteczny sposób poinformuje osoby fizyczne o naruszeniu – w takim przypadku zwolnienie dotyczy wyłącznie indywidualnego zawiadomienia.

WÓJT
Danuta Kędzierska-Cieszyńska

Wójt Gminy Brzozie
woj. kujawsko-pomorskie

Załącznik nr 6
do Polityki Ochrony Danych Osobowych
w Urzędzie Gminy Brzozie

Procedura postępowania w przypadku naruszenia ochrony danych osobowych w Urzędzie Gminy Brzozie

I. Cel procedury

Celem procedury jest zapewnienie szybkiej i skutecznej reakcji na naruszenie ochrony danych osobowych, w tym spełnienie obowiązków wynikających z art. 33 i 34 RODO oraz wytycznych UODO.

II. Definicje

1. **Naruszenie ochrony danych osobowych** – zgodnie z art. 4 pkt 12 RODO oznacza naruszenie bezpieczeństwa prowadzące do:
   1) zniszczenia;
   2) utracenia;
   3) zmodyfikowania;
   4) nieuprawnionego ujawnienia;
   5) nieuprawnionego dostępu.
2. **Administratorem danych osobowych** jest, zgodnie z artykułem 4 punkt 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
3. Jeśli w postanowieniach zarządzenia nie zostanie wskazane inaczej, Administratorem Danych Osobowych jest Wójt Gminy.

III. Klasyfikacja naruszeń ochrony danych osobowych

1. **Naruszenia poufności danych** rozumie się jako każde zdarzenie prowadzące do:
   1) nieuprawnionego ujawnienia danych osobowych osobom nieupoważnionym;
   2) nieautoryzowanego dostępu do danych objętych obowiązkiem ochrony;
   3) utraty kontroli nad danymi w wyniku działania osób trzecich lub niewłaściwych zabezpieczeń.
2. **Naruszenia integralności danych** oznaczają zdarzenia skutkujące:
   1) nieautoryzowaną lub przypadkową modyfikacją danych osobowych;

2) nieprawidłowym przetworzeniem prowadzącym do zmiany treści danych;
3) uszkodzeniem danych uniemożliwiającym ustalenie ich pierwotnej wersji.

3. **Naruszenia dostępności danych** obejmują sytuacje, w których:
   1) dane osobowe stają się niedostępne dla uprawnionych podmiotów w wymaganym czasie;
   2) dochodzi do trwałej utraty danych w wyniku zdarzeń losowych lub celowych działań;
   3) systemy przetwarzania uniemożliwiają realizację praw osób, których dane dotyczą.

IV. Stwierdzenie naruszenia

1. Wystąpienie naruszenia ochrony danych osobowych nie oznacza, że administrator lub podmiot przetwarzający dopuścił się naruszenia przepisów RODO.
2. Naruszenie przepisów RODO wynika z postępowania niezgodnego z określonymi wymogami przewidzianymi w tym akcie prawnym.

V. Obowiązki administratora

1. W przypadku „stwierdzenia" naruszenia ochrony danych osobowych administrator musi zrealizować następujące obowiązki. Należą do nich:
   1) zaradzenie naruszeniu ochrony danych osobowych oraz jego ewentualnym negatywnym skutkom;
   2) ocenienie ryzyka naruszenia praw lub wolności osób fizycznych, jakie może wynikać z naruszenia ochrony danych osobowych;
   3) zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu (w przypadku ryzyka naruszenia praw lub wolności osób fizycznych);
   4) zawiadamianie osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych (w przypadku wysokiego ryzyka naruszenia praw lub wolności tych osób);
   5) dokumentowanie naruszenia ochrony danych osobowych. Każde takie zdarzenie stanowi okazję do poprawy zabezpieczeń i minimalizowania ryzyka występowania podobnych incydentów w przyszłości.

VI. Działania IOD

1. Działania IOD w sprawie naruszeń ochrony danych osobowych obejmują w szczególności:
   1) pomoc w zapobieganiu naruszeniom, w szczególności poprzez promowanie w organizacji wiedzy o ochronie danych osobowych, organizowanie szkoleń oraz formułowanie zaleceń dotyczących bezpieczeństwa przetwarzania danych;
   2) udzielanie wskazówek dotyczących odpowiedniego reagowania na naruszenia ochrony danych osobowych, w tym zaradzania im;
   3) doradztwo w zakresie dokumentowania naruszeń i zarządzania dokumentacją;

4) przekazywanie dodatkowych informacji o naruszeniach organowi nadzorczemu i osobom, których dane dotyczą.

2. IOD nie powinien:
   a) zgłaszać naruszeń ochrony danych osobowych Prezesowi UODO w imieniu administratorów ani podpisywać i wysyłać takich zgłoszeń;
   b) zawiadamiać w imieniu administratorów osób, których dane dotyczą, o naruszeniach ochrony danych osobowych;
   c) dokumentować naruszeń ochrony danych osobowych w imieniu administratorów (w szczególności jeśli wiązałoby się to z ustalaniem celów i sposobów przetwarzania danych osobowych albo określeniem działań zaradczych);
   d) podejmować zobowiązań dotyczących bezpieczeństwa przetwarzania w imieniu administratorów lub podmiotów przetwarzających;
   e) działać na podstawie pełnomocnictwa w sprawach dotyczących ochrony danych osobowych.

VII. Odpowiedzialność administratorów w zakresie ochrony danych osobowych

1. Administrator danych osobowych ponosi odpowiedzialność za przestrzeganie przepisów o ochronie danych osobowych, zgodnie z zasadą rozliczalności, o której mowa w art. 5 ust. 2 RODO.
2. Zasada rozliczalności oznacza obowiązek wykazania, że działania podejmowane przez administratora są zgodne z przepisami RODO.
3. Administrator jest zobowiązany do dokumentowania swoich działań w zakresie ochrony danych osobowych oraz do przechowywania dowodów potwierdzających zgodność tych działań z obowiązującymi przepisami, w szczególności na potrzeby kontroli lub postępowania przed organem nadzorczym.
4. Dokumentacja potwierdzająca zgodność z RODO obejmuje w szczególności:
   1) dokumenty tradycyjne, takie jak notatki służbowe, instrukcje, procedury, decyzje wewnętrzne, korespondencję e-mailową;
   2) wyciągi i raporty z systemów informatycznych;
   3) raporty z audytów, testów bezpieczeństwa lub przeglądów zgodności.
5. Brak możliwości wykazania zgodności z RODO może zostać uznany za naruszenie przepisów o ochronie danych osobowych, niezależnie od rzeczywistego przebiegu zdarzeń.

VIII. Obowiązek zgłaszania incydentów ochrony danych osobowych

1. Każdy pracownik, który powezmie podejrzenie lub stwierdzi naruszenie ochrony danych osobowych (tzw. incydent), jest zobowiązany niezwłocznie poinformować o tym swojego bezpośredniego przełożonego oraz Inspektora Ochrony Danych.

2. W przypadku, gdy incydent dotyczy funkcjonowania jednostki organizacyjnej, pracownik zobowiązany jest również powiadomić organ wykonawczy (np. wójta, burmistrza, prezydenta miasta, dyrektora), przekazując możliwie pełne informacje na temat zdarzenia.
3. Zgłoszenie powinno nastąpić niezwłocznie, nie później niż w ciągu 24 godzin od momentu powzięcia informacji o incydencie, w formie ustnej (do wiadomości przełożonego) oraz pisemnej (e-mail, notatka służbowa lub formularz zgłoszeniowy).
4. Niedopełnienie obowiązku zgłoszenia może zostać potraktowane jako naruszenie obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

IX. Moment rozpoczęcia biegu terminu zgłoszenia naruszenia ochrony danych osobowych

1. Administrator danych osobowych stwierdza naruszenie ochrony danych osobowych w momencie, gdy uzyskuje wiedzę, że wykryte zdarzenie:
   1) stanowi incydent bezpieczeństwa informacji;
   2) dotyczy przetwarzanych danych osobowych;
   3) może skutkować przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub dostępem do tych danych.
2. Stwierdzenie naruszenia przez Administratora stanowi moment początkowy dla biegu terminu 72 godzin na dokonanie ewentualnego zgłoszenia do organu nadzorczego, zgodnie z art. 33 ust. 1 RODO.
3. Za moment uzyskania uzasadnionych podstaw uznaje się także sytuację, w której Inspektor Ochrony Danych, działając z upoważnienia Wójta, poinformuje go o potwierdzonym naruszeniu ochrony danych osobowych.
4. W przypadku wątpliwości co do charakteru zdarzenia, Wójt podejmuje niezwłoczne działania w celu ustalenia, czy wystąpiło naruszenie wymagające zgłoszenia do organu nadzorczego.
5. Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania wiąże się ryzyko lub wysokie ryzyko.

X. Zasady zgłaszania incydentów w ramach współpracy z podmiotami przetwarzającymi

1. Ze względu na fakt, że incydenty ochrony danych osobowych mogą występować zarówno po stronie administratora, jak i podmiotów przetwarzających, strony zobowiązane są do uzgodnienia jednoznacznych zasad wymiany informacji na temat potencjalnych lub potwierdzonych naruszeń ochrony danych osobowych.
2. W umowie powierzenia przetwarzania danych osobowych należy określić:
   1) kto jest odpowiedzialny za zgłoszenie naruszenia organowi nadzorczemu i osobom, których dane dotyczą;

2) sposób i formę powiadamiania pozostałych stron o incydencie (np. e-mail, telefon, dedykowany formularz);
3) maksymalny termin na zgłoszenie incydentu drugiej stronie (np. nie później niż w ciągu 12 godzin od wykrycia);
4) zakres przekazywanych informacji, w tym co najmniej: opis naruszenia, kategorie danych i osób, potencjalne skutki oraz podjęte lub planowane środki zaradcze.

3. Celem powyższych ustaleń jest umożliwienie administratorowi niezwłocznego podjęcia działań zaradczych oraz realizacja obowiązków wynikających z RODO, w szczególności w zakresie zgłaszania naruszeń organowi nadzorczemu w terminie 72 godzin.
4. Brak współpracy lub opóźnienie w przekazaniu informacji przez podmiot przetwarzający może zostać uznane za naruszenie postanowień umowy i skutkować odpowiedzialnością kontraktową.

XI. Zasady oceny ryzyka naruszenia ochrony danych osobowych

1. Administrator danych osobowych jest zobowiązany do dokonania niezwłocznej oceny ryzyka naruszenia ochrony danych osobowych w przypadku zaistnienia incydentu bezpieczeństwa.
2. Aby prawidłowo ocenić ryzyko, należy oszacować:
   1) wagę potencjalnych konsekwencji dla osób, których dane dotyczą;
   2) prawdopodobieństwo wystąpienia tych konsekwencji.
   3)
3. Ocena ryzyka powinna uwzględniać w szczególności następujące okoliczności danego zdarzenia:
   1) rodzaj naruszenia ochrony danych osobowych (np. utrata, ujawnienie, dostęp nieuprawniony);
   2) charakter, wrażliwość i zakres danych osobowych objętych naruszeniem;
   3) łatwość identyfikacji osób, których dane dotyczą;
   4) dotkliwość możliwych konsekwencji dla osób, których dane dotyczą (np. utrata reputacji, szkoda majątkowa, dyskryminacja);
   5) cechy szczególne osób, których dane dotyczą (np. dzieci, osoby starsze, osoby w trudnej sytuacji życiowej);
   6) cechy szczególne administratora (np. skala przetwarzania danych, profil działalności publicznej);
   7) liczbę osób, których dane dotyczą.
4. Ocena ryzyka powinna być odpowiednio udokumentowana i przechowywana na wypadek kontroli organu nadzorczego.
5. Administrator musi ustalić, czy naruszenie ochrony danych osobowych może wiązać się z:
   1) brakiem ryzyka;

2) ryzykiem, co wymaga zgłoszenia go Prezesowi UODO;
3) wysokim ryzykiem, co oznacza obowiązek zgłoszenia go Prezesowi UODO oraz zawiadomienia osób, których dane dotyczą.

XII. Przypadki niewystępowania ryzyka naruszenia praw i wolności

1. Administrator, dokonując oceny ryzyka związanego z incydentem ochrony danych osobowych, może uznać, że ryzyko naruszenia praw lub wolności osób fizycznych nie występuje, jeżeli spełnione są określone przesłanki.
2. Do typowych przypadków, w których brak jest ryzyka naruszenia, należą w szczególności:
   1) ujawnienie danych, które są już publicznie dostępne, a ich ponowne rozpowszechnienie nie powoduje dodatkowego zagrożenia dla osób, których dane dotyczą;
   2) ujawnienie lub utrata danych osobowych zaszyfrowanych w sposób zapewniający ich nieczytelność dla osób nieupoważnionych – pod warunkiem, że:
      a)dane są zabezpieczone silnym mechanizmem kryptograficznym,
      b) klucz szyfrujący nie został naruszony,
      c)administrator posiada dostęp do integralnej kopii zapasowej danych;
   3) incydenty, którym administrator skutecznie i definitywnie zaradził przed powstaniem realnego zagrożenia dla osób, których dane dotyczą (np. przywrócenie kontroli nad kontem zanim doszło do odczytu danych przez osobę nieuprawnioną).
3. W przypadkach takich incydentów nie zachodzi obowiązek zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych, ani zawiadamiania osób, których dane dotyczą – pod warunkiem, że administrator posiada dokumentację potwierdzającą brak ryzyka.
4. Każdy incydent związany z naruszeniem ochrony danych osobowych wymaga indywidualnej analizy z uwzględnieniem charakteru zdarzenia oraz jego potencjalnych skutków dla osób, których dane dotyczą.

XIII. Okoliczności świadczące o wysokim ryzyku naruszenia praw lub wolności osób fizycznych

1. Administrator danych osobowych, powinien w szczególności zwrócić uwagę na następujące okoliczności, które mogą świadczyć o wysokim ryzyku naruszenia praw lub wolności osób fizycznych. Powyższe dotyczy w szczególności objęcie incydentem szczególnych kategorii danych osobowych, takich jak:
   1) informacje ujawniające pochodzenie rasowe lub etniczne,
   2) poglądy polityczne,
   3) przekonania religijne lub światopoglądowe,
   4) przynależność do związków zawodowych,
   5) dane genetyczne i biometryczne,

6) dane dotyczące zdrowia, seksualności i orientacji seksualnej,
7) informacje o wyrokach skazujących oraz czynach zabronionych,
8) dane finansowe oraz dane powszechnie wykorzystywane do potwierdzania tożsamości lub zawierania umów (takie jak numer PESEL, seria i numer dowodu osobistego);

2. Szeroki zakres danych osobowych objętych incydentem – im większy zakres, tym większe ryzyko;
3. Szczególna dotkliwość potencjalnych skutków incydentu, w tym:
   1) kradzież tożsamości;
   2) oszustwa finansowe;
   3) poważne straty finansowe;
   4) problemy zawodowe;
   5) uszczerbek na zdrowiu psychicznym lub fizycznym;
   6) silny stres, lęk lub obniżone poczucie bezpieczeństwa.
4. Szczególny charakter osób objętych incydentem – np. dzieci, osoby starsze, osoby z niepełnosprawnością lub znajdujące się w trudnej sytuacji życiowej;
5. Duża liczba osób objętych incydentem – im większa skala naruszenia, tym wyższe prawdopodobieństwo wystąpienia szkód. W przypadku wystąpienia jednej lub kilku z wyżej wymienionych okoliczności, administrator powinien rozważyć konieczność niezwłocznego poinformowania osób, których dane dotyczą, zgodnie z art. 34 RODO.

XIV. Zaufany odbiorca danych osobowych

1. Zaufanym odbiorcą może zostać uznany taki podmiot, który przypadkowo otrzymał dane osobowe, lecz z uwagi na dotychczasową, pozytywną współpracę z administratorem danych osobowych można uznać go za godnego zaufania, a więc takiego, który prawidłowo zareaguje na zaistniały incydent i przyczyni się do ograniczenia ryzyka naruszenia praw lub wolności osób, których dane dotyczą.
2. Aby możliwe było uznanie nieuprawnionego odbiorcy danych osobowych za „zaufanego", muszą zostać spełnione łącznie następujące warunki:
   1) podmiot ten pozostaje z administratorem w stałych relacjach organizacyjnych lub współpracy biznesowej, np. jako:
      a) inny dział w strukturze urzędu,
      b) długoletni, sprawdzony dostawca usług,
      c) podmiot przetwarzający działający na podstawie umowy powierzenia, który wykazuje się wysokim poziomem profesjonalizmu i rzetelności;
   2) administrator danych osobowych zna istotne szczegóły dotyczące tego podmiotu, w szczególności:
      a) jego procedury bezpieczeństwa,

b) historię współpracy, w tym wcześniejsze, prawidłowe reakcje na incydenty lub sytuacje wymagające podjęcia działań ochronnych.

3. Uznanie danego odbiorcy za „zaufanego" następuje w ramach indywidualnej oceny ryzyka związanego z danym naruszeniem poufności danych osobowych. Oznacza to, że:
   1) decyzja o nadaniu statusu „zaufanego odbiorcy" nie ma charakteru stałego;
   2) każdorazowo należy przeprowadzić ocenę ryzyka naruszenia praw lub wolności osób fizycznych;
   3) status ten należy monitorować i okresowo weryfikować, w tym również w kontekście nowych okoliczności lub incydentów.
4. Jeżeli zmiana okoliczności (np. zmiana praktyk odbiorcy, incydent po jego stronie, naruszenie warunków umowy) prowadzi do utraty zaufania, administrator powinien ponownie ocenić ryzyko i ewentualnie uznać, że dany podmiot nie spełnia już kryteriów „zaufanego odbiorcy".

XV. Obowiązek dokumentowania naruszeń ochrony danych osobowych

1. Administrator danych osobowych ma obowiązek dokumentować wszystkie stwierdzone naruszenia ochrony danych osobowych.
2. W ramach zasady rozliczalności administrator powinien również dokumentować przypadki incydentów bezpieczeństwa, które zostały zaklasyfikowane jako niebędące naruszeniami danych osobowych, ze szczególnym uwzględnieniem przyczyn takiej decyzji.
3. Dokumentacja może być prowadzona w formie wewnętrznego rejestru naruszeń ochrony danych osobowych. Prowadzenie odrębnej ewidencji nie jest obowiązkowe, jednak wszelkie informacje muszą być:
   1) wyraźnie oznaczone;
   2) dostępne do wglądu na żądanie.
4. Dokumentacja naruszeń powinna obejmować co najmniej następujące elementy:

   1) okoliczności naruszenia ochrony danych osobowych, w tym:
      a) data i czas wystąpienia naruszenia,
      b) moment stwierdzenia naruszenia oraz jego zakończenia,
      c) sposób wykrycia naruszenia,
      d) przyczyny naruszenia,
      e) rodzaj i przebieg naruszenia,
      f) rodzaj i zakres danych osobowych objętych naruszeniem,
      g) liczba i kategorie osób, których dane dotyczą;

   2) skutki naruszenia, jeśli wystąpiły, oraz możliwe konsekwencje dla osób, których dane dotyczą;

   3) uzasadnienie oceny ryzyka związanego z naruszeniem;

   4) podjęte działania:

a) zaradcze, mające na celu powstrzymanie i ograniczenie skutków naruszenia,
b) zapobiegawcze, mające na celu minimalizowanie ryzyka wystąpienia podobnych naruszeń w przyszłości;

5) szczegóły dotyczące zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych (UODO), w tym:
a) data zgłoszenia,
b) ewentualne przyczyny opóźnienia w zgłoszeniu,
c) inne istotne informacje zawarte w zgłoszeniu,
d) lub w przypadku braku zgłoszenia – uzasadnienie decyzji o niezgłoszeniu naruszenia Prezesowi UODO,

6) szczegóły dotyczące zawiadomienia osób, których dane dotyczą, o naruszeniu, w tym:
a) data zawiadomienia,
b) treść zawiadomienia,
c) metoda powiadomienia,
d) liczba osób powiadomionych,
e) lub – w razie braku zawiadomienia – uzasadnienie decyzji o niezawiadomieniu osób, których dane dotyczą.

5. Dokumentacja naruszeń ochrony danych osobowych powinna być regularnie aktualizowana. Każda nowa informacja dotycząca incydentu, jego skutków lub podjętych działań może wpływać na ocenę ryzyka i wymagać korekty rejestru.

XVI. Techniczna realizacja obowiązku zgłaszania naruszeń ochrony danych osobowych na podstawie art. 33 RODO

1. Techniczna realizacja obowiązku zgłaszania naruszeń ochrony danych osobowych na podstawie art. 33 RODO odbywa się za pośrednictwem kanałów komunikacji wskazanych przez Prezesa Urzędu Ochrony Danych Osobowych (UODO).
2. W ramach realizacji obowiązku zgłaszania naruszeń ochrony danych osobowych wyróżnia się trzy rodzaje zgłoszeń:
   1) zgłoszenia wstępne – pozwalają na przekazanie podstawowych informacji o incydencie w wymaganym terminie (72 godziny od stwierdzenia naruszenia), z jednoczesnym obowiązkiem późniejszego uzupełnienia danych;
   2) zgłoszenia uzupełniające – umożliwiają aktualizowanie oraz rozszerzanie informacji o naruszeniu w miarę pozyskiwania nowych danych i szczegółów dotyczących incydentu;
   3) zgłoszenia kompletne – zawierają wszystkie wymagane informacje już przy pierwszym zgłoszeniu, co pozwala na pełne i wyczerpujące przedstawienie sytuacji bez konieczności późniejszych uzupełnień.

3. Zgłoszenie powinno zawierać:
    1) podstawowe informacje o administratorze oraz innych podmiotach powiązanych z incydentem, takich jak współadministratorzy, podmioty przetwarzające lub podmioty trzecie;
    2) okoliczności naruszenia ochrony danych osobowych, w tym m. in. datę i czas wystąpienia naruszenia, moment jego stwierdzenia i zakończenia, sposób wykrycia, przyczyny, rodzaj i przebieg naruszenia oraz rodzaj i zakres danych objętych naruszeniem, a także liczbę i kategorie osób, których dane dotyczą;
    3) skutki naruszenia lub możliwe skutki dla osób, których dane dotyczą;
    4) uzasadnienie oceny ryzyka związanego z naruszeniem;
    5) podjęte działania zaradcze, jeśli zostały wdrożone, lub zaplanowane działania wraz z deklarowaną datą ich realizacji, gdy nie zostały jeszcze podjęte;
    6) wdrożone środki bezpieczeństwa zapobiegające podobnym incydentom w przyszłości lub zaplanowane środki z deklaracją terminu ich wdrożenia;
    7) szczegóły dotyczące zawiadomienia osób, których dane dotyczą o naruszeniu – w tym datę, treść, metodę oraz liczbę zawiadomionych osób, albo, jeśli osoby te nie zostały zawiadomione, uzasadnienie takiej decyzji zgodnie z art. 34 ust. 3 RODO;
    8) imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych (IOD) lub informacji o innym wyznaczonym w organizacji punkcie kontaktowym.

XVII. Zawiadamianie osób, których dane dotyczą

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Administrator nie jest zobowiązany do zawiadamiania osób, których dane dotyczą, o naruszeniach ochrony danych osobowych, nawet jeśli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności tych osób, jeżeli zachodzą przynajmniej jedno z następujących warunków:
    1) przed wystąpieniem naruszenia zastosowano odpowiednie środki ochrony, które całkowicie eliminują wysokie ryzyko – przykładem może być sytuacja ujawnienia lub utraty danych zaszyfrowanych w sposób zapewniający ich nieczytelność dla osób nieupoważnionych pod warunkiem, że klucz szyfrujący nie został naruszony, a administrator dysponuje kopią zapasową tych danych;
    2) po wystąpieniu naruszenia administrator natychmiast podjął działania ochronne, które skutecznie wyeliminowały wysokie ryzyko naruszenia praw lub wolności osób, czyli incydent został definitywnie opanowany i zarządzony;

3) zawiadomienie osób wymagałoby niewspółmiernie dużego wysiłku, jednakże ten wyjątek obowiązuje tylko wtedy, gdy administrator wyda publiczny komunikat lub w inny, równie skuteczny sposób poinformuje osoby fizyczne o naruszeniu – w takim przypadku zwolnienie dotyczy wyłącznie indywidualnego zawiadomienia.

WÓJT
Danuta Kędzierska-Cieszyńska

Wójt Gminy Brzozie
woj. kujawsko-pomorskie

Załącznik nr 7
do Polityki Ochrony Danych Osobowych
w Urzędzie Gminy Brzozie

Procedura regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania w Urzędzie Gminy Brzozie

1. Procedura zostaje wprowadzona w celu zapewnienia właściwego wywiązywania się przez Administratora z obowiązku wynikającego z przepisów art 32 RODO.
2. Zgodnie z przepisami RODO wybór właściwych środków bezpieczeństwa ochrony danych powinien być determinowany przez okoliczności i warunki ich przetwarzania, a także prawdopodobieństwo i powagę zdarzeń, które mogą doprowadzić do naruszenia praw i wolności osób, których dane są przetwarzane.
3. Za monitorowanie realizowania przez Administratora oraz jego personel postanowień niniejszej Procedury odpowiada inspektor ochrony danych.
4. Ocenę skuteczności przyjętych środków ochrony dokonuje się okresowo dla każdego procesu przetwarzania.
5. Oceny dokonuje się dla każdego procesu oddzielnie we współpracy z osobami odpowiedzialnymi za przetwarzanie danych w ramach danego procesu przetwarzania, w odniesieniu do ich subiektywnej oceny skuteczności ochrony danych w ramach danego procesu, a także wiedzy o możliwych naruszeniach procedur i technicznych środków ochrony danych.
6. Mierzenie skuteczności zastosowanych środków ochrony jest realizowane w odniesieniu do procesów przetwarzania u Administratora, tj. m. in.:
    1) rekrutacji pracowników;
    2) świadczenia pracy przez pracowników;
    3) korzystania z usług zleceniobiorców;
    4) przyznawania środków z ZFŚS;
    5) marketingu produktów i usług;
    6) realizowania umów z klientami;
    7) prowadzenia korespondencji;
    8) realizowania reklamacji;
    9) archiwizacji/niszczenia danych;
    10) ochrony mienia z wykorzystaniem monitoringu wizyjnego.
7. Podczas oceny skuteczności przyjętych dla danego procesu przetwarzania środków technicznych oraz organizacyjnych dokonuje się wyliczenia zastosowanych rozwiązań, w szczególności:
    1) obowiązujące dla procesu polityki i procedury;

2) zapewnianie zobowiązania do poufności personelu;
3) przeszkolenie personelu;
4) podział odpowiedzialności za dane osobowe;
5) inwentaryzacja Systemów oraz nośników służących do przetwarzania danych;
6) postępowanie z nośnikami (szyfrowanie, przekazywanie, niszczenie);
7) środki ochrony w ramach systemów informatycznych oraz aplikacji, w których są przetwarzane dane;
8) środki ochrony dla urządzeń służących do przetwarzania danych;
9) zabezpieczenia sieci internetowej;
10) kontrola dostępu do pomieszczeń;
11) kontrola dostępu do systemów i nośników danych;
12) uprawnienia użytkowników;
13) zapewnianie ciągłości działania i przywracania danych;
14) fizyczne środki ochrony danych;
15) bezpieczeństwo danych przetwarzanych przez podwykonawców;
16) zarządzanie naruszeniami;
17) legalność przetwarzanych danych;
18) realizowanie praw osób;
19) zapewnianie rozliczalności danych.

8. Dla każdego procesu przetwarzania należy określić zagrożenia, w odniesieniu do kontekstu i charakteru przetwarzania w ramach tego procesu.
9. Dla każdego procesu dokonuje się oceny skutków materializacji wskazanych zagrożeń oraz prawdopodobieństwa materializacji tego zagrożenia, a następnie, dokonuje się jego oszacowania.
10. Na podstawie ustalonych informacji dokonuje się oceny skuteczności przyjętych rozwiązań służących zapewnieniu ochrony danych, poprzez odniesienie się do możliwego ryzyka naruszenia dla danych w ramach każdego z procesów przetwarzania.
11. Ocena skuteczności w zależności od oszacowanego ryzyka:
    1) **Niskie ryzyko- przyjęte środki są skuteczne**, można ale nie trzeba podjąć działania które ulepszą system ochrony danych;
    2) **Średnie ryzyko- przyjęte środki mogą być niewystarczające**, należy podjąć działania minimalizujące ryzyko;
    3) **Wysokie ryzyko- przyjęte środki są niewystarczające**, należy niezwłocznie podjąć działania minimalizujące ryzyko.
12. W zależności od dokonanej oceny Administrator podejmuje działania mające na celu ulepszenie zastosowanych środków ochrony danych w celu minimalizacji ryzyka.

WÓJT
Danuta Kędziorska-Cieszyńska

Załącznik nr 8
do Polityki Ochrony Danych Osobowych
w Urzędzie Gminy Brzozie

METODOLOGIA ANALIZY RYZYKA

Art. 35 RODO ust. 1 RODO wskazuje, że jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków dla ochrony danych (DPIA). Art. 35 ust. 4 RODO nałożył na Urząd ochrony Danych Osobowych obowiązek ustanowienia i podania do publicznej wiadomości wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych. Prezes UODO w Komunikacie z dnia 17.06.2019 r. wskazał rodzaje operacji przetwarzania wymagających oceny skutków. Administrator oceniając, czy dany rodzaj operacji będzie podlegał obowiązkowi przeprowadzenia DPIA, musi wziąć pod uwagę, wskazane na wstępie przesłanki. Jeżeli jakakolwiek z nich zostanie spełniona, dokonanie DPIA jest obligatoryjne.

I. ETAP 1: Ustalenie stanu faktycznego – analiza wymogu przeprowadzenia oceny skutków dla ochrony danych

Lp.	Dane do identyfikacji procesu przetwarzania	Opis
	Opis czynności przetwarzania	*Opis procesu, w ramach, którego będzie dochodziło przetwarzanie danych*
	Podstawa prawna przetwarzania	
	Administrator danych	
	Podmioty przetwarzające	
	Umowy powierzenia przetwarzania danych osobowych	
	Systemy wspierające przetwarzanie	
	Planowane przepływy danych	

II. ETAP 2 Opis celu, charakteru, zakresu i kontekstu przetwarzania danych

	Cel czynności przetwarzania	*Należy opisać:* • *Co administrator chce osiągnąć przez planowanie przetwarzanie* • *Jaki jest skutek przetwarzania – wpływ na osoby fizyczne* • *Jakie są korzyści z przetwarzania dla administratora i osób fizycznych, których dotyczy przetwarzanie*
	Charakter przetwarzania	*Należy opisać:* • *Sposób gromadzenia, wykorzystywania, przechowywania i usuwania danych* • *Źródło danych* • *Czy dane będą komuś udostępniane*
	Zakres przetwarzania:	*Należy opisać:* • *Jakie dane są przetwarzane (zwykłe, szczególnej kategorii)?* • *Ile danych będzie gromadzonych i wykorzystywanych?* • *Jak często?*

		• *Ilu osób dotyczy przetwarzanie?* • *Określenie retencji danych* • *Określenie obszar przetwarzania danych np. województwo, miasto itp.*
	Kontekst przetwarzania:	*Należy opisać:* • *Kontekst wewnętrzny – obejmujący czynniki wewnętrzne podmiotu, firmy, jej organizacji* • *Kontekst zewnętrzny – obejmujący czynniki zewnętrzne, w których działa podmiot* • *Kontekst powinien definiować elementy związane ze środowiskiem prawnym, geograficznym, politycznym oraz społecznym, w jakim funkcjonuje firma i przetwarzane są dane osobowe. Należy określić takie elementy jak: lokalne lub branżowe regulacje prawne na podstawie, których działa firma, zakres terytorialny przetwarzania danych (EOG lub poza EOG), inwentaryzacja aktywów dla dokładności oraz skuteczności procesu szacowania ryzyka.* • *Czy operacje w ramach przetwarzania danych są wymienione w Komunikacie Prezesa Urzędu Ochrony Danych Osobowych z dnia 17.06.2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony*

III. ETAP 3 - Identyfikacja i ocena ryzyka w celu określenia konieczności przeprowadzenia oceny skutków dla ochrony danych osobowych

Etap ten jest niezbędny do określenia czy wprowadzana operacja przetwarzania danych wymaga dokonania oceny skutków.

METODA OCENY RYZYKA POTENCJALNEGO ORAZ SZCZĄTKOWEGO					
ISTOTNOŚĆ (WAGA) ZAGROŻENIA	PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA				
	pomijalne (1)	niskie (2)	średnie (3)	wysokie (4)	krytyczne (5)
pomijalna (1)	1	2	3	4	5
niska (2)	2	4	6	8	10
średnia (3)	3	6	9	12	15
wysoka (4)	4	8	12	16	20
krytyczna (5)	5	10	15	20	25
STOPIEŃ RYZYKA	niski (1-7)	średni (8-14)	wysoki (15-25)		

Poziom ryzyka wyznaczono według wzoru: **R = P x S**
gdzie:

R –poziom ryzyka

P – wartość przypisana prawdopodobieństwu materializacji zagrożenia

S – wartość skutków

Analiza ryzyka						
Źródło ryzyka i charakter potencjalnego wpływu na osoby	**Prawdopodobieństwo**	**Skutek - dotkliwość dla osób fizycznych**	**Poziom ryzyka**	**Identyfikacja negatywnych skutków zdarzenia**	**Wpływ zdarzenia na atrybuty bezpieczeństwa informacji**	**Wpływ na osobę fizyczną**

Identyfikacja środków redukujących ryzyko

Środki zmniejszające ryzyko				
Ryzyko	**Środki zaradzenia ryzyku**	**Wpływ na ryzyko**	**Ryzyko szczątkowe**	**Środek zatwierdzony**
		Ocena czy ryzyko zostało: • wyeliminowane • zredukowane • zaakceptowane	Wskazanie poziomu ryzyka: • niski • średni • wysoki	TAK/NIE
		Ocena czy ryzyko zostało: • wyeliminowane • zredukowane • zaakceptowane	Wskazanie poziomu ryzyka: • niski • średni • wysoki	TAK/NIE

Wynik wstępnej weryfikacji procesu przetwarzania danych osobowych: Przeprowadzenie oceny skutków dla ochrony (jest/nie jest*) wymagane.

***W przypadku odpowiedzi twierdzącej należy przejść do kolejnego etapu, który wymaga zawarcia pozostałych elementów wskazanych w art. 35 ust. 7 RODO tj. określenie niezbędności oraz proporcjonalności danych w stosunku do celów, weryfikację środków przyczyniających się do zachowania praw osób, których dane dotyczą. Pozostałe elementy z art. 35 ust. 7 RODO wyczerpuje ocena z etapów I – III**

WÓJT
Danuta Kędzierska-Cieszyńska