ZARZĄDZENIE NR 114/2022
WÓJTA GMINY STARE BOGACZOWICE

z dnia 4 listopada 2022 r.

w sprawie wdrożenia dokumentacji dotyczącej ochrony danych osobowych w Urzędzie Gminy Stare Bogaczowice

Na podstawie 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 dyrektywy 95/46/WE, wprowadza się dokumentację ochrony danych osobowych dla Urzędu Gminy Stare Bogaczowice

Rozdział 1.
Zasady organizacji ochrony danych osobowych

§ 1. Ustala się Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącą do przetwarzania danych osobowych w Urzędzie Gminy Stare Bogaczowice, zwaną dalej dokumentacją ochrony danych osobowych.

§ 2. Zobowiązuje się pracowników oraz osoby współpracujące z Urzędem Gminy Stare Bogaczowice do stosowania zasad określonych w dokumentacji ochrony danych osobowych.

§ 3. 1. Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich ochrony w Urzędzie Gminy Stare Bogaczowice, z siedzibą przy ul. Głównej 132, 58-312 Stare Bogaczowice, zwanym dalej gminną jednostką samorządową.

2. W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając jednocześnie schematy postępowań na wypadek wystąpienia naruszenia bezpieczeństwa.

3. Dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi oraz w systemie informatycznym wyrażone w Polityce bezpieczeństwa oraz w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

4. Wszelkie zestawienia uzupełniające treść dokumentu zebrano w postaci załączników. Do najważniejszych należy ewidencja:

- zbiorów danych osobowych,
- miejsc ich przetwarzania,
- osób upoważnionych do przetwarzania danych, a także lista środków organizacyjnych i technicznych służących bezpieczeństwu danych.

Rozdział 2.
Podstawowe definicje

§ 4. 1. W dokumencie przyjmuje się następującą terminologię:

- Organ nadzorczy – oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 rozporządzenia.
- Dane osobowe – oznaczają 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.

- Przetwarzanie – oznacza operacje 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.
- Ograniczone przetwarzanie – oznacza oznaczenie przechowywanych danych w celu ograniczenia ich przyszłego przetwarzania.
- Profilowanie – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystywaniu 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.
- Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób, by nie można było już ich przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
- Zbiór danych – oznacza uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
- Dane szczególne - dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
- Dane genetyczne - oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.
- Dane biometryczne - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.
- Administrator - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państw członkowskich, to również w prawie Unii lub w prawie państw członkowskich może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
- Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
- Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców. Przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mających zastosowanie stosownie do celów przetwarzania.
- Strona trzecia - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe.
- Zgoda osoby – której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

- Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesłanych, przechowywanych lub w inny sposób przetwarzanych.
- Inspektor ochrony danych (IOD) – osoba realizująca zadania określone w art. 39 rozporządzenia, w tym nadzorująca stosowanie środków technicznych i organizacyjnych przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną. IOD jest powoływany przez Administratora lub organ prowadzący.
- Zastępca Inspektora ochrony danych – osoba zastępująca Inspektora ochrony danych osobowych w czasie jego nieobecności.
- Administrator systemu informatycznego, pomocnik Inspektora ochrony danych (ASI) – osoba lub osoby odpowiedzialna/e za prawidłowe funkcjonowanie systemu informatycznego. ASI pełni funkcję pomocnika IOD i jest powoływany przez Administratora.
- System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
- Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
- Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
- Rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
- Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
- Dokumentacja przetwarzania danych – dokumentacja opisująca sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
- Zagrożenia danych – polega z jednej strony na możliwości ich utraty, zniszczenia lub zafałszowania, z drugiej strony zaś na możliwości ich nieuprawnionego rozpowszechnienia.
- Zabezpieczenia – praktyki, procedury i mechanizmy zmniejszające ryzyko, chroniące przed zagrożeniami, ograniczające następstwa wykrywające niepożądane incydenty i ułatwiające odtworzenie prawidłowego stanu systemu.
- Pracownik – osoba zatrudniona na umowę o pracę, umowę cywilno - prawną, stażysta lub praktykant świadczący pracę dla Urzędu Gminy Stare Bogaczowice.
- Instytucja – Urząd Gminy Stare Bogaczowice.
- Instrukcja – instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Stare Bogaczowice.
- Sprawdzenie – czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, w szczególności w wyniku zwrócenia się o dokonanie sprawdzenia przez organ nadzorczy.
- Sprawozdanie – dokument opracowany przez IOD po dokonaniu sprawdzenia, którego celem jest zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
- Państwa trzecie – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego.

Rozdział 3.
Polityka Bezpieczeństwa

§ 1. Polityka bezpieczeństwa rozumiana jest jako wykaz praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz instytucji. Obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie, jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

Deklaracja

§ 2. 1. Administrator danych mając świadomość, iż przetwarza dane zwykłe i szczególne pracowników, dane zwykłe i szczególne osób fizycznych, którym Urząd Gminy Stare Bogaczowice świadczy usługi, deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.

2. W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem Administrator danych wprowadza określone niniejszym dokumentem zasady przetwarzania danych. Zasady te określa w szczególności Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Dokumenty te są uzupełniane załącznikami do dokumentacji, na które składają się m.in.: rejestr czynności przetwarzania danych osobowych, wykaz miejsc ich przetwarzania oraz osób upoważnionych do przetwarzania danych.

3. W celu zapewnienia prawidłowego monitorowania przetwarzania danych wprowadza się liczne ewidencje, które szczegółowo charakteryzują obszary objęte monitoringiem, umożliwiając pełną kontrolę nad tym, jakie dane i przez kogo są przetwarzane oraz komu udostępniane.

4. Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje stuprocentowej szczelności systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.

5. W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.

Charakterystyka instytucji

§ 3. Urząd Gminy Stare Bogaczowice realizuje zadania opisane w ustawie o samorządzie gminnym, będące zdaniami własnymi gmin lub też zadania zlecone z administracji rządowej, uprawniające Wójta Gminy Stare Bogaczowice do podejmowania stosownych działań, w tym do przetwarzania danych osobowych. Podstawowym obszarem działania są zadania związane z zaspokajaniem potrzeb mieszkańców Gminy Stare Bogaczowice, za których realizację odpowiada Urząd Gminy Stare Bogaczowice zgodnie z ustawą o samorządzie gminnym.

Rejestr czynności przetwarzania danych osobowych

§ 4. 1. Na podstawie art. 30 i 32 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 tworzy się:

- Rejestr kategorii oraz czynności przetwarzania danych osobowych – formularz nr 1,
- Wykaz pomieszczeń tworzących obszar fizyczny przetwarzania danych – formularz nr 2,
- Rejestr osób upoważnionych do przetwarzania danych osobowych – formularz nr 3.

Środki organizacyjne ochrony danych osobowych

§ 5. 1. W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

- Każdy pracownik upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z informacją kto w urzędzie pełni funkcję Inspektora ochrony danych osobowych oraz o jego zastępcy - formularz 6a,
- Przetwarzanie danych osobowych w instytucji może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań,

- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie. Wzór upoważnienia stanowi - formularz nr 4,
- Administrator prowadzi ewidencję osób upoważnionych oraz na jej podstawie przygotowuje upoważnienia do przetwarzania danych,
- Unieważnienie upoważnienia do przetwarzania danych następuje na piśmie, wg wzoru - formularz nr 5,
- Zabrania się przetwarzania danych poza obszarem określonym w formularzu nr 2, za wyjątkiem przypadków dopuszczonych przez Administratora,
- Każdy pracownik instytucji co najmniej raz na rok musi odbyć szkolenie z zakresu ochrony danych osobowych. Za organizację szkoleń odpowiedzialny jest IOD, który prowadzi w tym celu odpowiednią dokumentację. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych. Za przeprowadzenie szkolenia wstępnego odpowiada IOD.
- Każdy pracownik upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór oświadczenia stanowi formularz nr 6. Podpisany dokument jest dołączany do przedmiotowej dokumentacji.
- Obszar przetwarzania danych osobowych określony w formularzu nr 2 zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych poprzez zamknięcie pomieszczenia na klucz.
- Przebywanie osób nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej do przetwarzania danych osobowych. Wzory zgody na przebywanie w pomieszczeniach dla osób nieposiadających upoważnienia, a także odwołania tej zgody, stanowią odpowiednio formularz nr 7 oraz formularz nr 8.
- Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
- Monitory komputerów/laptopów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
- Przetwarzanie danych podawanych dobrowolnie może odbywać się tylko na podstawie pisemnej zgody podającego te dane, wg wzoru określonego w formularzu nr 9.
- Dokumenty zawierające dane osobowe należy niszczyć w specjalistycznych niszczarkach.
- Każdorazowe zbieranie danych od osoby właściciela tych danych lub o osobach trzecich, rodzi obowiązek informacyjny. Obowiązek należy realizować umieszczając odpowiednią treść informacyjną pod formularzem z danymi.
- Dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza obszar przetwarzania lub przesyłane pocztą elektroniczną, należy zabezpieczyć poprzez nadanie im haseł odczytu.
- Zbiory osobowe przetwarzane elektronicznie należy zabezpieczyć poprzez wykonywanie kopii bezpieczeństwa, zapisywanych na zewnętrznych nośnikach i przechowywanych pod zamknięciem.
- Komputery/laptopy, które przetwarzają zbiory osobowe wyszczególnione na formularzu nr 1 do dokumentacji, za wyjątkiem komputerów służących jedynie do edycji tekstu, należy wyposażyć w urządzenia podtrzymujące napięcie na wypadek braku zasilania.
- Pliki edytorów tekstu lub arkuszy kalkulacyjnych należy traktować jako kopie zbiorów, z których pochodzą przetwarzane w nich dane i odpowiednio zabezpieczyć stosując wytyczne zawarte w Instrukcji zarządzania systemem informatycznym, będącej częścią niniejszego dokumentu.
- W celu zapewnienia ochrony danych przetwarzanych elektronicznie należy zapewnić logowanie do systemu operacyjnego oraz bezpośrednio do specjalistycznych programów przetwarzających dane.
- Szczegółowe zasady postępowania ze zbiorami przetwarzanymi elektronicznie określa Instrukcja zarządzania systemem informatycznym, będąca częścią niniejszej dokumentacji.
- IOD do 31 stycznia każdego roku budżetowego sporządza na formularzu nr 10 Planu sprawdzeń z zakresu przestrzegania zasad ochrony danych osobowych. Plan sprawdzeń jest zatwierdzany przez Administratora.

- W oparciu o Plan sprawdzeń IOD dokonuje sprawdzeń stanu zabezpieczenia danych osobowych prowadzonych zarówno w zbiorach tradycyjnych, jak i w zbiorach elektronicznych. Fakt przeprowadzenia sprawdzenia IOD dokumentuje na formularzu nr 11 – Sprawozdanie ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
- IOD do 31 grudnia każdego roku budżetowego sporządza na formularzu nr 12 – Sprawozdanie roczne ze stanu zabezpieczenia danych osobowych. Sprawozdanie roczne ze stanu zabezpieczenia danych osobowych zatwierdzane jest przez ADO.
- IOD do 31 grudnia każdego roku budżetowego przeprowadza na formularzu nr 20 – audyt w ramach wprowadzonych Krajowych Ram Interoperacyjności.

Środki techniczne ochrony danych osobowych

§ 6. 1. Zbiory danych przetwarzane w instytucji zabezpiecza się poprzez:

1) Środki ochrony fizycznej.

- Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi.
- Zbiory danych osobowych przechowywane są w pomieszczeniach, w których okna częściowo zabezpieczone są kratami.
- Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej, niemetalowej szafie.
- Zbiory danych osobowych (akta osobowe) w formie papierowej przechowywane są w zamkniętej, metalowej szafie.
- Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są na przeznaczonym do tego serwerze.
- Pomieszczenia, w którym przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru wolno stojącymi gaśnicami.
- Dokumenty zawierające dane osobowe po ustaniu przydatności są przechowywane na okres archiwizacji w zakładowej Składnicy Akt, a po ustaniu okresu archiwizacji są niszczone poprzez spalenie. Natomiast dokumenty zawierające dane osobowe, które nie podlegają archiwizacji, po ich wykorzystaniu są niszczone w niszczarce.

2) Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej.

- Zbiory danych osobowych przetwarzane są przy użyciu komputerów stacjonarnych i na laptopach.
- Komputery i laptopy służące do przetwarzania danych osobowych są połączone z lokalną siecią komputerową.
- Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych, przetwarzanych przy użyciu systemów informatycznych.
- Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
- Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
- Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
- Zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak, np. robaki, wirusy, konie trojańskie, rootkity.
- Użyto system Firewall do ochrony dostępu do sieci komputerowej.

3) Środki ochrony w ramach systemowych narzędzi programowych i baz danych.

- Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbiorów danych osobowych.

- Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanych zbiorów danych osobowych.
- Dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
- Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbiorów danych osobowych.
- Zastosowano kryptograficzne środki ochrony danych osobowych.
- Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
- Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.
- Dodatkowe środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określa Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

4) Procedura bezpieczeństwa sprzętu poza siedzibą Instytucji.
- Użytkownik komputera przenośnego poza siedzibą instytucji ma obowiązek jego ochrony.
- Zabrania się pozostawiania komputerów przenośnych bez opieki w miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nim skutecznego nadzoru.
- Osoba używająca komputera przenośnego zawierającego dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania, przestrzegając jednocześnie zaleceń producentów dotyczących ochrony sprzętu.
- Korzystanie z komputera przenośnego w miejscach publicznych i innych niechronionych miejscach poza siedzibą instytucji wymaga ostrożności, by nie ujawnić danych osobom nieupoważnionym.
- Użytkowanie komputera przenośnego/dysku zewnętrznego/pendrive poza siedzibą instytucji dopuszczanie jest tylko za zgodą Administratora. Wzór zgody na użytkowanie komputera poza siedzibą instytucji stanowi formularz nr 13.
- Użytkownik komputera przenośnego/dysku zewnętrznego/pendrive jest zobowiązany złożyć oświadczenie, którego wzór stanowi formularz nr 14.
- W przypadku utraty komputera przenośnego/dysku zewnętrznego/pendrive użytkownik niezwłocznie powiadamia o tym fakcie swojego bezpośredniego przełożonego, a w przypadku kradzieży dokonuje również niezwłocznego zgłoszenia faktu popełnienia przestępstwa na Policji. W zawiadomieniu użytkownik, poza danymi ogólnymi, podaje okoliczności utraty komputera oraz opis charakteru utraconych danych wraz z podaniem ich znaczenia. W szczególności w zawiadomieniu należy określić, czy utracone dane miały charakter danych osobowych.

5) Szkolenie pracowników. IOD na polecenie Administratora, osobiście lub przy wykorzystaniu podmiotu zewnętrznego przeprowadza szkolenia pracowników w zakresie przepisów prawa oraz uregulowań wewnętrznych zgodnie z przyjętym harmonogramem stanowiącym formularz nr 21. Szkolenia:
- Pracownicy nowozatrudnieni przed przystąpieniem do pracy podlegają szkoleniu przez IOD z zakresu ochrony danych osobowych.
- Szkolenia okresowe odbywają się nie rzadziej niż raz w roku.
- Ze szkoleń grupowych sporządza się listę obecności pracowników biorących udział wraz z programem szkolenia, które przechowuje IOD.

6) Zasady aktualizacji Polityki bezpieczeństwa.

a) Aktualizację Polityki bezpieczeństwa przeprowadza się na wniosek IOD lub ASI.

b) Przyczynami prowadzącymi do aktualizacji Polityki bezpieczeństwa są następujące czynniki:

- Zgłoszenie ASI lub IOD przez pracownika ważnego problemu lub trudności w przestrzeganiu zasad zawartych w aktualnie obowiązującej Polityce bezpieczeństwa.
- Wykrycie przez ASI lub IOD nieprawidłowości w obowiązującej Polityce bezpieczeństwa.
- Wystąpienie zmian w obowiązujących przepisach związanych z Polityką bezpieczeństwa.
- Wejście w życie nowych przepisów, które mogą mieć wpływ na treść Polityki bezpieczeństwa.
- Likwidacja, utworzenie lub zmiany zawartości informacyjnej zbioru danych.

7) Następstwa grożące za nieprzestrzeganie Polityki bezpieczeństwa.

a) Pracownicy zobowiązani są do zapoznania i bezwzględnego stosowania wszystkich obowiązujących w instytucji przepisów i zarządzeń wewnętrznych dotyczących ochrony danych.

b) Za nieprzestrzeganie zasad Polityki bezpieczeństwa pracownik ponosi odpowiedzialność na zasadach określonych w Kodeksie Pracy, Kodeksie Karnym oraz ustawie o ochronie danych osobowych.

c) Nieprzestrzeganie Polityki bezpieczeństwa stanowi ciężkie naruszenie obowiązków pracowniczych.

8) Postępowanie z kluczami.

a) Klucze główne:

- Administrator wyznacza osoby, które są upoważnione do otwierania i zamykania głównych drzwi wejściowych przed rozpoczęciem i po zakończeniu pracy.
- Osoby upoważnione, którym zostały powierzone klucze do głównych drzwi są zobowiązane do wykorzystywania ich zgodnie z przeznaczeniem oraz nie kopiowania bez zgody Administratora oraz nie udostępniania osobom trzecim.

b) Klucze dostępowe do pomieszczeń wewnętrznych:

- Klucze zapasowe do poszczególnych pomieszczeń znajdują się w wyznaczonym pomieszczeniu.
- Osoby, które zostały upoważnione do dostępu w pomieszczeniu, o którym mowa wyżej, są zobowiązane do zabezpieczenia kluczy i wykorzystywania ich zgodnie z przeznaczeniem oraz nie kopiowania ich bez zgody Administratora oraz nie udostępniania osobom trzecim. Natomiast pracownicy posiadają swój komplet kluczy do zajmowanych pomieszczeń i są zobowiązani do ich odpowiedniego zabezpieczenia.

c) Klucze do biurek stanowiskowych i szaf:

- Do kluczy od biurek stanowiskowych, szaf biurowych, dostęp mają upoważnione przez Administratora osoby, które zobowiązane są do ich zabezpieczenia w indywidualny, właściwy do każdej sytuacji sposób, poprzez stosowanie odpowiednich środków technicznych i organizacyjnych.
- Osoby, które zostały upoważnione do kluczy od biurek stanowiskowych, szaf biurowych są zobowiązane do wykorzystywania ich zgodnie z przeznaczeniem oraz nie kopiowania bez zgody Administratora oraz nie udostępniania osobom trzecim.

Rozdział 4.
Charakterystyka systemu informatycznego

§ 1. 1. Sieć informatyczna, w której przetwarzane są dane osobowe stanowią wszystkie pracujące obecnie i przyszłe planowane serwery, komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.

2. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.

3. System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym stanowisku.

4. Serwer posiada zasilanie awaryjne utrzymujące stałe zasilanie oraz posiada oprogramowanie antywirusowe.

Ogólne zasady pracy w systemie informatycznym

§ 2. 1. IOD lub ASI odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych.

2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez ASI do eksploatacji licencjonowane oprogramowanie.

3. ASI prowadzi ewidencję oprogramowania.

4. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:

1) Mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika, z pominięciem narzędzi do edycji tekstu.

2) Mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej.

3) Mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii.

4) Urządzenia niwelujące zakłócenia i podtrzymujące zasilanie.

5) Mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie.

6) Mechanizmy zarządzania zmianami.

5. Użytkownikom zabrania się:

1) Korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy bez pisemnej zgody Administratora.

2) Udostępniania stanowisk roboczych osobom nieuprawnionym.

3) Wykorzystywania sieci komputerowej w celach innych niż wyznaczone przez Administratora.

4) Samowolnego instalowania i używania programów komputerowych.

5) Korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich.

6) Umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej oraz sieci Internetowej osobom nieuprawnionym.

7) Używania komputera bez zainstalowanego oprogramowania antywirusowego.

Procedura nadawania uprawnień do przetwarzania danych osobowych

§ 3. 1. Użytkowników systemu informatycznego tworzy oraz usuwa ASI na podstawie zgody IOD.

2. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym, jak również w rejestrach tradycyjnych, wymagane jest upoważnienie.

3. Wprowadza się rejestr osób upoważnionych do przetwarzania danych osobowych, który stanowi formularz nr 3.

4. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:

1) Nieobecności pracownika w pracy trwającej dłużej niż 30 dni kalendarzowych.

2) Zawieszenia w pełnieniu obowiązków służbowych.

5. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.

6. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

Metody i środki uwierzytelniania

§ 4. 1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.

2. Użytkownik posiadający upoważnienie do przetwarzania danych osobowych powinien posiadać hasło do systemu operacyjnego oraz osobne do baz danych osobowych i aplikacji.

3. Każdy użytkownik systemu informatycznego powinien posiadać odrębny identyfikator, którego nazwa składa się z pierwszych trzech liter imienia pisanych z małej litery oraz trzech pierwszych liter nazwiska pisanych z małej litery. Pomiędzy imieniem i nazwiskiem nie ma spacji ani kropki. Natomiast ASI to Administrator.

4. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika, IOD nadaje inny identyfikator odstępując od ogólnej zasady.

5. W identyfikatorze stosuje się polskie znaki diakrytyczne.

6. Hasło składa się z co najmniej ośmiu znaków, zawiera co najmniej jedną literę wielką, jedną cyfrę i jeden znak specjalny.

7. Hasło nie powinno zawierać żadnych informacji, które można skojarzyć z użytkownikiem komputera (imiona najbliższych, daty urodzenia, inicjały, itp.) i nie może być sekwencją kolejnych znaków klawiatury.

8. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieupoważniona, użytkownik zobowiązany jest do zgłoszenia tego faktu ASI i do natychmiastowej zmiany hasła.

9. Zmianę hasła należy dokonywać nie rzadziej niż co 30 dni.

10. Po zapoznaniu się z loginem i hasłem użytkownik zobowiązany jest do ich zniszczenia w odpowiednim urządzeniu niszczącym.

11. Hasło nie może być zapisywane i przechowywane.

12. Użytkownik nie może udostępniać identyfikatora oraz haseł osobom nieupoważnionym.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy

§ 5. 1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.

2. Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami niemającymi uprawnień.

3. Zawieszenie pracy polegające na opuszczeniu stanowiska pracy bez wylogowania się jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.

4. Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania się z systemu z zastrzeżeniem pkt 3.

5. Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.

6. Czas rozpoczęcia i zakończenia pracy w systemach sieciowych, w tym w systemach przetwarzania danych osobowych, określa Regulamin Pracy.

7. Konieczność pracy w aplikacjach sieciowych w godzinach innych niż określone w Regulaminie Pracy powinno być zgłoszone IOD.

8. ASI monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

Procedury tworzenia kopii awaryjnych

§ 6. 1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii zapasowych.

2. Ochronie podlegają także programy i narzędzia programowe służące przetwarzaniu danych poprzez wykonywanie kopii zapasowej plików instalacyjnych programów i narzędzi na wyznaczonej lokalizacji sieciowej.

3. Zabezpieczeniu poprzez wykonywanie kopii zapasowych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.

4. Za proces tworzenia kopii programów i narzędzi programowych oraz danych konfigurujących system odpowiedzialny jest ASI. Kopie przechowywane są przez ASI.

5. Kopie zapasowe mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.

6. Pliki edytorów tekstu lub arkuszy kalkulacyjnych traktowane są jako kopie zbiorów, z których pochodzą przetwarzane w nich dane i nie są objęte procedurami wykonywania kopii zapasowych.

7. Nośniki, na których są przechowywane kopie danych osobowych, powinny być wyraźnie oznaczone.

8. Za bezpieczeństwo kopii awaryjnych przetwarzanych lokalnie odpowiadają poszczególni użytkownicy systemu, którzy je wykonali. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności w sposób uniemożliwiający odtworzenie danych.

9. ASI zobowiązany jest do okresowego wykonywania testów odtworzenia kopii zapasowych.

10. Zewnętrzne nośniki kopii zapasowych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym.

11. Użytkownik tworzy wydruki związane z przetwarzaniem danych osobowych wyłącznie w zakresie i ilości niezbędnej dla celów służbowych w uzgodnieniu z przełożonym.

12. Wszystkie dokumenty, zestawienia i wydruki zawierające dane osobowe powinny być chronione przed dostępem osób nieupoważnionych. Użytkownik przechowuje je w zamkniętej szafie, w pomieszczeniu zabezpieczonym przed nieuprawnionym dostępem.

Przechowywanie elektronicznych nośników informacji

§ 7. 1. Nośniki danych oraz programów służących do przetwarzania danych osobowych, a także danych konfiguracyjnych systemu informatycznego, przechowuje ASI w odpowiednio zabezpieczonym pomieszczeniu.

2. Dane osobowe mogą być przetwarzane na serwerach, a także na dyskach lokalnych komputerów w lokalizacji ustalonej z IOD. Zabrania się gromadzenia danych osobowych na innych, nieautoryzowanych przez IOD nośnikach danych.

3. W uzasadnionych przypadkach, za zgodą IOD, dane osobowe można przetwarzać na zewnętrznych nośnikach informacji, autoryzowanych przez ASI.

4. Serwery oraz komputery, na których odbywa się przetwarzanie danych osobowych, powinny być zabezpieczone przed utratą danych spowodowaną awarią zasilania poprzez stosowanie specjalnych urządzeń podtrzymujących zasilanie i eliminujących zakłócenia sieci zasilającej.

5. Komputery przenośne oraz inne mobilne nośniki danych osobowych powinny być zabezpieczone ochroną kryptograficzną – powinny być zaszyfrowane.

6. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe, przeznaczone do:

1) Likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

2) Przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.

3) Naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem IOD.

7. Nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym przez IOD.

Zabezpieczenie systemu informatycznego przed złośliwym oprogramowaniem

§ 8. 1. ASI zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody.

2. System antywirusowy jest skonfigurowany w następujący sposób:

1) Skanowanie dysków zawierających potencjalnie niebezpieczne dane następuje automatycznie po włączeniu komputera.

2) Skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej jest realizowane na bieżąco.

3) Automatycznej aktualizacji wzorców wirusów.

3. W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie ASI.

4. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

1) Usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego.

2) Odtworzenie plików z kopii awaryjnych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane.

3) Samodzielną ingerencję w zawartość pliku - w zależności od posiadanych narzędzi i oprogramowania.

5. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.

Informacje o odbiorcach, których dane zostały udostępnione, dacie i zakresie tego udostępnienia

§ 9. 1. Dla każdej osoby, której dane są przetwarzane w systemie informatycznym powinny być automatycznie odnotowane następujące dane:

1) Dane o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba, że dane te traktuje się jako dane jawne.

2) Sprzeciwu osoby, której dane dotyczą w przypadku zamierzenia przetwarzania jej danych w celach marketingowych lub zamierzenia przekazania jej danych innemu administratorowi.

2. Zapis ust. 1 nie dotyczy systemów służących do przetwarzania danych ograniczonych do edycji teksu w celu udostępnienia go na piśmie i niezwłocznym usunięciu z systemu.

3. Dla każdej osoby, której dane są przetwarzane w systemie informatycznym, system powinien zapewniać sporządzenie i wydrukowanie raportu zawierającego w powszechnym rozumieniu formę informacji, o którym mowa w ust. 1.

4. W uzasadnionych przypadkach uniemożliwiających automatyczne odnotowywanie, o którym mowa w ust. 1, prowadzi się odrębny Rejestr udostępnień - formularz nr 15. Rejestr udostępnień jest prowadzony na każdym stanowisku oddzielnie, w wersji elektronicznej. Rejestr udostępnień jest drukowany przez pracownika na ostatni dzień roboczy roku kalendarzowego i przekazany do podpisu kierownikowi jednostki. Podpisane przez kierownika jednostki Rejestry udostępnień są przekazywane do IOD. Za prawidłowość i terminowość realizacji Rejestru udostępnień odpowiada pracownik.

5. Za udostępnianie danych zgodnie z przepisami prawa odpowiedzialny jest ADO.

Przesyłanie danych poza obszar przetwarzania

§ 10. 1. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.

2. W wypadku przesyłania danych osobowych przez sieć internetową pocztą elektroniczną należy każdy z załączników zabezpieczyć ochroną kryptologiczną poprzez nadanie hasła odczytu. Hasło należy przesłać lub podać odbiorcy w innej przesyłce, a najlepiej z wykorzystaniem innych metod komunikacji (telefon, fax, w bezpośredniej rozmowie).

3. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

4. Zabrania się przekazywania danych przez aplikacje internetowe niewykorzystujące odpowiedniego protokołu szyfrowania (adres internetowy musi być poprzedzony zapisem „https”).

Wykonywanie przeglądów i konserwacji systemów oraz nośników informacji

§ 11. 1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez Administratora lub posiadające umowy na powierzenie przetwarzania danych osobowych w zakresie konserwacji i napraw.

2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez IOD.

3. W przypadku uszkodzenia zestawu komputerowego, laptopa lub nośników danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez ASI.

4. W przypadku konieczności przeprowadzenia prac serwisowych poza instytucją, dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać usunięte w sposób trwały.

5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.

6. ASI wykonuje okresowy przegląd nośników danych osobowych, eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności.

Rozdział 5.
Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych

§ 1. 1. Analiza zagrożeń i ryzyka w instytucji określa środki zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Analiza ryzyka jest kluczowym elementem procesu bezpieczeństwa teleinformatycznego.

2. Ilekroć w analizie zagrożeń i ryzyka jest mowa o:

a) dostępności – należy przez to rozumieć właściwość określającą, że zasób systemu informatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym,

b) incydencie bezpieczeństwa teleinformatycznego – należy przez to rozumieć pojedyncze zdarzenie lub serię zdarzeń związanych z bezpieczeństwem informacji, które zagrażają ich poufności, dostępności lub integralności,

c) informatycznym nośniku danych – należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej,

d) integralności – należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony,

e) oprogramowaniu złośliwym – należy przez to rozumieć oprogramowanie, którego celem jest przeprowadzenie nieuprawnionych lub szkodliwych działań w systemie teleinformatycznym,

f) podatności - należy przez to rozumieć słabość zasobów lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie,

g) połączeniu międzysystemowym – należy przez to zrozumieć techniczne lub organizacyjne połączenie dwóch lub więcej systemów teleinformatycznych, umożliwiające ich współpracę, a w szczególności wymianę danych,

h) poufności – należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym,

i) przekazywaniu informacji – należy przez to rozumieć zarówno transmisję informacji, jak i przekazywanie informacji na informatycznych nośnikach danych, na których zostały utrwalone,

j) teście bezpieczeństwa – należy przez to rozumieć testy poprawności i skuteczności funkcjonowania zabezpieczeń w systemie teleinformatycznym,

k) zabezpieczeniu – należy przez to rozumieć środki o charakterze fizycznym, technicznym lub organizacyjnym, które zmniejszają ryzyko,

l) zagrożeniu – należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego,

m) zasobach systemu teleinformatycznego – należy przez to rozumieć informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych danych.

3. W czasie przetwarzania danych osobowych w instytucji informacje występują w postaci :

a) plików lub informacji przechowywanych na dysku twardym komputera stacjonarnego/laptopa,

b) plików lub informacji przechowywanych w pamięci operacyjnej komputera stacjonarnego/laptopa,

c) plików lub informacji zapisanych w nośnikach komputerowych,

d) wersji roboczych lub gotowych dokumentów wydrukowanych na papierze.

4. Bezpieczeństwo przetwarzanych i przechowywanych informacji zawierających dane osobowe wymaga:

a) zapewnienia ochrony fizycznej stanowiska komputerowego przed nieuprawnionym dostępem,

b) ochrony nośników technicznych i wydruków dokumentów wytworzonych przy pomocy sprzętu komputerowego, w tym określenia zasad postępowania z nimi w celu zabezpieczenia przed nieuprawnionym dostępem,

c) zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego,

d) zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz pamięci systemu informatycznego dla upoważnionych użytkowników,

e) zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywania na nich czynności,

f) zapewnienia możliwości kontroli nośników, na których przetworzono lub przechowywano dane osobowe.

Zagrożenia dla systemu (poufność)

§ 2. 1. Poufność to zapewnienie, że dane osobowe nie są udostępniane nieupoważnionym podmiotom.

2. Czynniki zagrażające poufności :

a) nieuprawniony dostęp do pomieszczeń, w których przetwarzane są dane osobowe,

b) ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe,

c) nieuprawnione przeniesienie informacji zawierającej dane osobowe na inny nośnik komputerowy,

d) utrata nośnika komputerowego zawierającego dane osobowe,

e) klęska żywiołowa, w wyniku której utracono poufność danych osobowych,

f) nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym.

3. Ocena ryzyka utraty poufności przetwarzanych danych osobowych polega na zwartościowaniu (przy pomocy skali punktowej) skutku i prawdopodobieństwa wystąpienia ryzyka.

4. Zasady określania skutku oraz prawdopodobieństwa wystąpienia ryzyka określa formularz nr 16.

5. Zidentyfikowane ryzyka utraty poufności przetwarzanych danych osobowych podlegają analizie pod kątem prawdopodobieństwa wystąpienia oraz jego wpływu (skutku) na przebieg procesów i wykonywanych zadań przez instytucję.

6. W ramach analizy dokonuje się punktowej oceny ryzyka podejmowanego w związku z realizowanym zadaniem zarówno przed, jak i po wprowadzeniu mechanizmów kontrolnych tj. Polityki bezpieczeństwa, instrukcji, czy też innych obowiązujących regulacji normatywnych.

7. Istotność ryzyka jest iloczynem wartości prawdopodobieństwa wystąpienia ryzyka oraz wartości skutku zaistnienia ryzyka.

8. Ocenę prawdopodobieństwa wystąpienia czynników zagrażających poufności dokonuje się w skali punktowej od 1 o 5, gdzie:

a) Bardzo małe – 1,

b) Małe prawdopodobne – 2,

c) Średnie – 3,

d) Prawdopodobne – 4,

e) Prawie pewne – 5.

9. Ocenę skutków zaistnienia ryzyka utraty poufności dokonywana jest w skali od 1 do 5, gdzie:

a) Oddziaływanie nieznaczne - 1,

b) Oddziaływanie małe - 2,

c) Oddziaływanie średnie -3,

d) Oddziaływanie poważne - 4,

e) Oddziaływanie katastrofalne - 5.

10. W celu określenia poziomu istotności ryzyka i reakcji na ryzyko, wyniki analizy ryzyka należy porównać z mapą ryzyka – formularz nr 16.

11. W zależności od poziomu istotności zidentyfikowanego ryzyka dla poufności danych osobowych, IOD rekomenduje działania mające na celu ograniczenie negatywnego wpływu ryzyka na poufność przetwarzanych danych osobowych.

12. Przyjmuje się następujące zasady akceptowalności ryzyka utraty poufności przetwarzania danych osobowych:

a) Ryzyko niskie - to ryzyko akceptowalne, należy je monitorować oraz poddawać systematycznej ocenie zgodnie z obowiązującymi zasadami (skala od 0,00 – 4,99),

b) Ryzyko średnie - to ryzyko akceptowalne, jeżeli podlega stałemu monitorowaniu, ale należy ograniczać jego wpływ na działalność instytucji poprzez wprowadzenie dodatkowych mechanizmów kontrolnych (skala od 5,00 – 12,99),

c) Ryzyko wysokie – stanowi realne zagrożenie dla poufności przetwarzanych danych osobowych przez instytucję, w żadnym wypadku nie podlega akceptacji i wymaga natychmiastowej interwencji ADO (skala od 13,00 – 25,00).

Zagrożenia dla systemu (rozliczalność)

§ 3. 1. Rozliczalność to właściwość zapewniająca, że działania podmiotu przetwarzającego dane osobowe mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

2. Czynniki zagrażające rozliczalności:

a) brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania,

b) wyparcie się pracy na stanowisku komputerowym, gdzie przetwarzane są dane osobowe,

c) wprowadzenie zmian w treści dokumentu zawierającego dane osobowe,

d) błędy oprogramowania lub sprzętu.

3. Ocena ryzyka utraty rozliczalności przetwarzanych danych osobowych polega na zwartościowaniu (przy pomocy skali punktowej) skutku i prawdopodobieństwa wystąpienia ryzyka.

4. Zasady określania skutku oraz prawdopodobieństwa wystąpienia ryzyka określa formularz nr 16.

5. Zidentyfikowane ryzyka utraty rozliczalności przetwarzanych danych osobowych podlegają analizie pod kątem prawdopodobieństwa wystąpienia oraz jego wpływu (skutku) na przebieg procesów i wykonywanych zadań przez instytucję.

6. W ramach analizy, dokonuje się punktowej oceny ryzyka podejmowanego w związku z realizowanym zadaniem zarówno przed, jak i po wprowadzeniu mechanizmów kontrolnych tj. Polityki bezpieczeństwa, instrukcji, czy też innych obowiązujących regulacji normatywnych.

7. Istotność ryzyka jest iloczynem wartości prawdopodobieństwa wystąpienia ryzyka oraz wartości skutku zaistnienia ryzyka.

8. Ocenę prawdopodobieństwa wystąpienia czynników zagrażających rozliczalności przetwarzanych danych osobowych dokonuje się w skali punktowej od 1 o 5, gdzie:

a) Bardzo małe – 1,

b) Małe prawdopodobne – 2,

c) Średnie – 3,

d) Prawdopodobne – 4,

e) Prawie pewne – 5.

9. Ocenę skutków zaistnienia ryzyka utraty rozliczalności przetwarzanych danych osobowych dokonywana jest w skali od 1 do 5, gdzie:

a) Oddziaływanie nieznaczne - 1,

b) Oddziaływanie małe - 2,

c) Oddziaływanie średnie -3,

d) Oddziaływanie poważne - 4,

e) Oddziaływanie katastrofalne - 5.

10. W celu określenia poziomu istotności ryzyka i reakcji na ryzyko, wyniki analizy ryzyka należy porównać z mapą ryzyka – formularz nr 16.

11. W zależności od poziomu istotności zidentyfikowanego ryzyka dla rozliczalności przetwarzanych danych osobowych, IOD rekomenduje działania mające na celu ograniczenie negatywnego wpływu ryzyka na rozliczalność przetwarzanych danych osobowych.

12. Przyjmuje się następujące zasady akceptowalności ryzyka utraty rozliczalności przetwarzania danych osobowych:

a) Ryzyko niskie - to ryzyko akceptowalne, należy je monitorować oraz poddawać systematycznej ocenie zgodnie z obowiązującymi zasadami (skala od 0 – 4,99),

b) Ryzyko średnie - to ryzyko akceptowalne, jeżeli podlega stałemu monitorowaniu, ale należy ograniczać jego wpływ na działalność instytucji poprzez wprowadzenie dodatkowych mechanizmów kontrolnych (skala od 5,00 – 12,99),

c) Ryzyko wysokie – stanowi realne zagrożenie dla rozliczalności przetwarzanych danych osobowych przez instytucję, w żadnym wypadku nie podlega akceptacji i wymaga natychmiastowej interwencji ADO (skala od 13,00 – 25,00).

Zagrożenia dla systemu (integralność)

§ 4. 1. Integralność to zapewnienie, aby wszelkie zmiany wykonywane w systemie informatycznym, w systemie jego katalogów oraz poszczególnych plikach zawierających dane osobowe były skutkiem zaplanowanych działań użytkowników systemu. Integralność to właściwość zawierająca zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

2. Czynniki zagrażające integralności:

a) nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego,

b) błędy, pomyłki,

c) brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika,

d) wadliwe działanie systemu operacyjnego,

e) wirus,

f) brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych.

3. Ocena ryzyka utraty integralności przetwarzanych danych osobowych polega na zwartościowaniu (przy pomocy skali punktowej) skutku i prawdopodobieństwa wystąpienia ryzyka.

4. Zasady określania skutku oraz prawdopodobieństwa wystąpienia ryzyka określa formularz nr 16.

5. Zidentyfikowane ryzyka utraty integralności przetwarzanych danych osobowych podlegają analizie pod kątem prawdopodobieństwa wystąpienia oraz jego wpływu (skutku) na przebieg procesów i wykonywanych zadań przez instytucję.

6. W ramach analizy, dokonuje się punktowej oceny ryzyka podejmowanego w związku z realizowanym zadaniem zarówno przed, jak i po wprowadzeniu mechanizmów kontrolnych tj. Polityki bezpieczeństwa, instrukcji, czy też innych obowiązujących regulacji normatywnych.

7. Istotność ryzyka jest iloczynem wartości prawdopodobieństwa wystąpienia ryzyka oraz wartości skutku zaistnienia ryzyka.

8. Ocenę prawdopodobieństwa wystąpienia czynników zagrażających integralności przetwarzanych danych osobowych dokonuje się w skali punktowej od 1 o 5, gdzie:

a) Bardzo małe – 1,

b) Małe prawdopodobne – 2,

c) Średnie – 3,

d) Prawdopodobne – 4,

e) Prawie pewne – 5.

9. Ocenę skutków zaistnienia ryzyka utraty integralności przetwarzanych danych osobowych dokonywana jest w skali od 1 do 5, gdzie:

a) Oddziaływanie nieznaczne - 1,

b) Oddziaływanie małe - 2,

c) Oddziaływanie średnie -3,

d) Oddziaływanie poważne - 4,

e) Oddziaływanie katastrofalne - 5.

10. W celu określenia poziomu istotności ryzyka i reakcji na ryzyko, wyniki analizy ryzyka należy porównać z mapą ryzyka – formularz nr 16.

11. W zależności od poziomu istotności zidentyfikowanego ryzyka dla integralności przetwarzanych danych osobowych, IOD rekomenduje działania mające na celu ograniczenie negatywnego wpływu ryzyka na integralność przetwarzanych danych osobowych.

12. Przyjmuje się następujące zasady akceptowalności ryzyka utraty integralności przetwarzania danych osobowych:

a) Ryzyko niskie - to ryzyko akceptowalne, należy je monitorować oraz poddawać systematycznej ocenie zgodnie z obowiązującymi zasadami (skala od 0 – 4,99),

b) Ryzyko średnie - to ryzyko akceptowalne, jeżeli podlega stałemu monitorowaniu, ale należy ograniczać jego wpływ na działalność instytucji poprzez wprowadzenie dodatkowych mechanizmów kontrolnych (skala od 5,00 – 12,99),

c) Ryzyko wysokie – stanowi realne zagrożenie dla integralności przetwarzanych danych osobowych przez instytucję, w żadnym wypadku nie podlega akceptacji i wymaga natychmiastowej interwencji ADO (skala od 13,00 – 25,00).

Zagrożenia dla stanowisk komputerowych

§ 5. 1. Źródłami zagrożeń dla stanowisk komputerowych, gdzie przetwarza się dane osobowe mogą być :

a) siły natury (zdarzenia, które nie wynikają z działalności człowieka):

- uderzenia pioruna,

- pożar będący konsekwencją uderzenia pioruna,

- starzenie się sprzętu,

- starzenie się nośników pamięci,

- smog, kurz,

- katastrofa budowlana,

- ulewny deszcz,

- huragan,
- ekstremalne temperatury, wilgotność,
- epidemia.

b) ludzie (mogą to być pracownicy lub osoby z zewnątrz, które działają w sposób celowy lub przypadkowy):

- błędy i pomyłki użytkowników,
- błędy i pomyłki administratorów,
- błędy utrzymania systemu w poufności, integralności i rozliczalności,
- zaniedbania użytkowników przy przesyłaniu, udostępnianiu lub kopiowaniu,
- zagubienie nośników zawierających dane osobowe,
- niewłaściwe zniszczenie nośnika,
- nielegalne użycie oprogramowania,
- choroba ważnych osób i nieuprawnione zastępstwo,
- epidemia kadry i brak osób upoważnionych do dostępu,
- podpalenie obiektu,
- zalanie wodą,
- katastrofa budowlana będąca konsekwencją przypadkowego działania człowieka,
- zakłócenia elektromagnetyczne, radiotechniczne,
- podłożenie i wybuch bomby, ładunku wybuchowego,
- użycie broni,
- zmiany napięcia w sieci,
- utrata prądu,
- zbieranie się ładunków elektrostatycznych,
- utrata kluczowych pracowników,
- niedobór pracowników,
- defekty oprogramowania,
- szpiegostwo,
- terroryzm,
- wandalizm,
- destrukcja zbiorów i programów impulsem elektromagnetycznym,
- kradzież,
- włamanie do systemu,
- wyłudzenie, fałszowanie dokumentów,
- podszycie się pod uprawnionego użytkownika,
- podsłuch,
- użycie złośliwego oprogramowania,
- wykorzystanie promieniowania ujawniającego.

2. Każde z wyżej wymienionych zagrożeń wynikających z działalności człowieka może być ograniczone poprzez :

a) rygorystyczne przestrzeganie zasad postępowania z danymi osobowymi,

b) fizyczne zabezpieczenie obiektu, w którym działa system,

c) wdrożenie systemu kontroli użytkowników,

d) brak połączenia stanowisk komputerowych systemu z siecią internetową.

3. Zagrożenia wynikające z działania sił natury można ograniczyć poprzez właściwe zabezpieczenie budynków i pomieszczeń, w których znajdują się stanowiska komputerowe, na których przetwarza się dane osobowe.

4. Potencjalne ataki mogą być wykonywane poprzez:

a) podsłuch,

b) wyłudzenie,

c) fałszowanie dokumentów,

d) wykorzystywanie promieniowania ujawniającego.

Zagrożenia dla systemu

§ 6. 1. Zagrożenia dla systemu to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentów, mogących mieć wpływ na ich ujawnienie bądź utratę tzn.:

a) poufność – właściwość polegająca na tym, że informacja nie jest dostępna lub wyjawiona nieuprawnionym osobom, podmiotom lub procesorom.

b) rozliczalność – właściwość pozwalająca na rozliczeniu osoby pracującej na stanowisku komputerowym systemu przetwarzającego dane osobowe w zakresie dostępu do pomieszczenia, w którym ono jest zainstalowane oraz rozliczenie czynności wykonywanych przy pomocy tego stanowiska komputerowego w systemie katalogów oraz pojedynczych zbiorów,

c) integralność – właściwość polegająca na zapewnieniu dokładności, kompletności aktywów.

Stopień ważności informacji

§ 7. 1. Stopień ważności informacji zawierających dane osobowe określa poziom ochrony oraz zastosowanie właściwych środków bezpieczeństwa.

2. W instytucji przetwarza się dane osobowe zwykłe i wrażliwe – merytorycznie związane z zakresem zadań realizowanych przez instytucję oraz zakresami obowiązków użytkowników.

3. Ponieważ przeważająca część danych osobowych w instytucji przetwarzana jest w sposób tradycyjny, a tylko nieznaczna część danych przetwarzana jest za pomocą komputerów, wielkość potencjalnych skutków ujawnienia lub utraty informacji w nich zawartych jest stosunkowo mała, dlatego też należy oszacować poziom utraty poufności, jako obarczone ryzykiem niskim (poziom – 1,498). Dotyczy to każdej kategorii w/w przetwarzanych zasobów danych osobowych.

4. Wytwarzane dokumenty zawierające dane osobowe są rejestrowane, przechowywane do wglądu, a następnie niszczone lub archiwizowane przez osoby posiadające stosowne uprawnienia.

5. Kopie zapasowe tworzone są na serwerze i dysku NAS. Można zatem określić wymagania związane z zachowaniem rozliczalności jako obarczone ryzykiem niskim (poziom – 1,166).

6. Dokładność i kompletność realizowanych czynności w zakresie realizowanych zadań statutowych przez instytucje są zapewnione poprzez odpowiednie usytuowanie stanowisk komputerowych, na których przetwarza się dane osobowe (stanowiska jednoosobowe).

7. Według oceny osób odpowiedzialnych za ochronę danych osobowych wymagania związane z potrzebą zachowania integralności informacji zawierających dane osobowe w systemie są obarczone ryzykiem niskim (wartość -1,000). Dotyczy to każdej kategorii w/w przetwarzanych zasobów danych osobowych.

Podatność systemu na zagrożenia

§ 8. 1. Podatność systemu na zagrożenia może wynikać z:

- dostępności systemu wynikającego np. z braku ochrony fizycznej budynku lub znacznej liczby pracowników mających potencjalny dostęp do systemu oraz wiedzę jak obsługiwać system,
- dostępność informacji znajdujących się w systemie za pośrednictwem połączeń zewnętrznych,

- możliwość celowego wprowadzenia luk w sprzęcie i oprogramowaniu lub wprowadzenia wirusów komputerowych,
- możliwość awarii sprzętu lub oprogramowania ze względu na uszkodzenia, błędy projektowe lub umyślną interwencję,
- przesłanie informacji przez niezabezpieczone łącze telekomunikacyjne.

2. Podatność systemu na zagrożenia została ograniczona poprzez:

- ochronę fizyczną stanowisk komputerowych,
- kontrolę dostępu do pomieszczeń, gdzie przetwarzane są dane osobowe,
- wydzielenie stref ochronnych,
- ograniczenie liczby pracowników mających potencjalnie dostęp do stanowisk komputerowych oraz wiedzę jak je obsługiwać,
- zbudowanie stabilnej sieci zasilającej,
- przeglądy okresowe nośników,
- kontrole zmian konfiguracji,
- testowanie oprogramowania,
- audyt teleinformatyczny,
- zabezpieczenie haseł,
- użycie oprogramowania komputerowego,
- backupy – kopie zapasowe.

3. W celu oszacowania potencjalnych strat wynikających z utraty lub ujawnienia danych osobowych przetwarzanych na stanowiskach komputerowych wykonano analizę ryzyka na podstawie przewidywanych zagrożeń dla zasobów.

4. Analiza ryzyka wykonywana jest nie rzadziej niż raz w roku przez IOD przy udziale ASI z wykorzystaniem formularza nr 17.

5. Analiza ryzyka wykonywana jest każdorazowo po zaistnieniu incydentu związanego z naruszeniem zasad ochrony danych osobowych. Analizą objęty jest obszar, w którym doszło do naruszenia zasad przetwarzania danych osobowych. Incydent związany z naruszeniem zasad ochrony danych osobowych jest dokumentowany przez IOD z wykorzystaniem formularza nr 18 na formularzu nr 19.

Analiza zagrożeń i ryzyka

§ 9. 1. Analiza zagrożeń i ryzyka polega na identyfikacji ryzyka wystąpienia niepożądanego czynnika, określenie jego wielkości, zidentyfikowania obszarów wymagających zabezpieczeń tak, aby to ryzyko zminimalizować lub całkowicie je zlikwidować.

2. Aby przeprowadzić poprawną analizę ryzyka, na początku należy określić:

- zasoby, które będziemy chronić,
- zagrożenia – czynnik, który może powodować wystąpienie incydentów,
- skutki – jaki wpływ będzie miał zaistniały incydent na system informatyczny.

3. Zasobami systemu są wszystkie elementy służące do przetwarzania, przechowywania lub przekazywania informacji oraz do zapewnienia im właściwego poziomu bezpieczeństwa, tzn.:

- sprzęt komputerowy przechowujący dane – dysk twardy,
- pracownicy przetwarzający dane osobowe,
- aplikacje, w których przetwarzane są dane osobowe,
- pomieszczenia, w których pracują osoby przetwarzające dane osobowe,
- koszty dodatkowych zabezpieczeń oraz odbudowy systemu po incydencie.

4. Podatność systemu to słabości zasobów, które mogą być wykorzystane do ujawnienia informacji lub ich utraty.

5. Skutki określają wysokość strat w systemie informatycznym po zaistnieniu incydentu.

Rozdział 6.
Postanowienia końcowe

§ 1. Traci moc Zarządzenie Nr 82/2021 Wójta Gminy Stare Bogaczowice z dnia 8 października 2021 r. w sprawie wdrożenia dokumentacji ochrony danych osobowych w Urzędzie Gminy Stare Bogaczowice.

§ 2. Wykonanie zarządzenia powierza się Inspektorowi ochrony danych.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Stare
Bogaczowice

Mirosław Lech

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Administrator danych, adres jego siedziby, numer REGON	Urząd Gminy Stare Bogaczowice, ul. Główna 132, 58-312 Stare Bogaczowice, REGON 000539319
Inspektor ochrony danych, adres jego siedziby, numer telefonu, adres e-mail	Gabriela Roszczyk, 58-312 Stare Bogaczowice, ul. Główna 132, tel. 74-8452220, e-mail urząd@starebogaczowice.ug.gov.pl

Lp.	Nazwa zbioru i cel przetwarzania danych w zbiorze	Podstawa prawna przetwarzania	Zakres danych przetwarzanych w zbiorze	Kategoria osób, którzy dane są przetwarzane	Podmiot, któremu powierzono przetwarzanie danych
1.	Akta osobowe – realizacja wymogu ustawowego	Kodeks pracy	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, daty urodzenia dzieci, imiona i nazwiska dzieci, stan zdrowia	Dane osobowe pracownika	Nie powierzono
2.	Dokumentacja płacowa – realizacja wymogu ustawowego	Ustawa o podatku dochodowym od osób fizycznych Ustawa o podatku dochodowym od osób prawnych	Imię i nazwisko, PESEL, adres zamieszkania, numer telefonu, dokument tożsamości	Dane osobowe pracownika	Nie powierzono
3.	Lista obecności w pracy- realizacja wymogu ustawowego	Regulamin organizacyjny	Imię i nazwisko	Dane osobowe pracownika	Nie powierzono
4.	Dokumentacja dotycząca zwolnień lekarskich pracowników – realizacja wymogu ustawowego	Kodeks pracy	Nazwisko i imię, data urodzenia, adres zamieszkania, PESEL	Dane osobowe pracownika	Nie powierzono

5.	Rejestr wydanych delegacji – realizacja wymogu ustawowego	Kodeks pracy	Nazwisko i imię	Dane osobowe pracownika	Nie powierzono
6.	Rejestr urlopów – realizacja wymogu ustawowego	Kodeks pracy	Imię i nazwisko	Dane osobowe pracownika	Nie powierzono
7.	Dokumentacja szkoleń – realizacja wymogu ustawowego	Kodeks pracy	Imię i nazwisko, data urodzenia i miejsce urodzenia, imię ojca	Dane osobowe pracownika	Firmy szkoleniowe
8.	Dokumentacja BHP pracowników- realizacja wymogu ustawowego	Kodeks pracy	Imię i nazwisko, data urodzenia i miejsce urodzenia	Dane osobowe pracownika	Firma BHP
9.	Dokumentacja wypadków pracowników – realizacja wymogu ustawowego	Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 19 grudnia 2002 r. w sprawie trybu uznawania zdarzenia powstałego w okresie ubezpieczenia wypadkowego za wypadek przy pracy, kwalifikacji prawnej zdarzenia, wzoru karty wypadku i terminu jej sporządzenia Rozporządzenia Ministra Gospodarki i Pracy z 16.9.2004 r. w sprawie wzoru protokołu ustalenia okoliczności i przyczyn wypadku przy pracy	Nazwiska i imiona, imię ojca, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, seria i nr dowodu osobistego, stan zdrowia	Dane osobowe pracownika	Firma BHP
10.	Dokumentacja KZP– realizacja wymogu ustawowego	Ustawa o związkach zawodowych	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu	Dane osobowe pracownika lub emeryci	Komisja KZP- podmiot zewnętrzny
11.	Badania okresowe– realizacja wymogu ustawowego	Kodeks pracy	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL	Dane osobowe pracownika	NZOZ
12.	Ubezpieczenie pracowników-	Zgoda pracownika	Imię i nazwiska, adres zamieszkania, imię ojca i matki, adres zamieszkania, miejsce urodzenia,	Dane osobowe pracownika	Firmy ubezpieczeniowa

	realizacja wymogu własnego		PESEL, dane osobowe osoby uposażonej , stan zdrowia		
13.	Dokumentacja wydanych zaświadczeń o zatrudnieniu i wynagrodzeniu – realizacja wymogu ustawowego	Ustawa o podatku dochodowym od osób fizycznych	Nazwiska i imiona, imię ojca, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, seria i nr dowodu osobistego	Dane osobowe pracownika	Nie powierzono
14.	Strona internetowa i BIP- realizacja wymogu ustawowego	Zgoda osób	Imię i nazwisko, numer telefonu, adres e-mailowy, adres zamieszkania, wizerunek	Dane osobowe	Nie powierzono
15.	Tablica ogłoszeń– realizacja wymogu własnego	Zgoda pracownika	Imię i nazwisko	Dane osobowe pracownika	Nie powierzono
16.	Dziennik korespondencyjny – realizacja wymogu ustawowego	Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (tekst jednolity Rozporządzenie Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych	Imię i nazwisko, adres zamieszkania	Dane osobowe	Nie powierzono
17.	Rejestr pieczęci, pieczątek i stempli – realizacja wymogu ustawowego	Ustawa o Rachunkowości	Imię i nazwisko	Dane osobowe pracownika	Nie powierzono
18.	Księga inwentarzowa– realizacja wymogu ustawowego	Ustawa o Rachunkowości	Imię i nazwisko	Dane osobowe pracownika	Nie powierzono
19.	Umowy cywilno-prawne - realizacja wymogu ustawowego	Kodeks Cywilny	Nazwiska i imiona, adres zamieszkania lub pobytu, PESEL, NIP, REGON, seria i nr dowodu osobistego, nr telefonu, e-mail	Dane osobowe	Nie powierzono

20.	Faktury - realizacja wymogu ustawowego	Ustawa o podatku dochodowym od osób fizycznych Ustawa o podatku dochodowym od osób prawnych	Nazwisko, imię, adres zamieszkania, NIP, REGON	Dane osobowe	Nie powierzono
21.	Druki ścisłego zarachowania- realizacja wymogu ustawowego	Ustawa o rachunkowości	Imię i nazwisko	Dane osobowe pracownika	Nie powierzono
22.	Książka kontroli – realizacja wymogu ustawowego	Upoważnienie do kontroli organu kontrolującego	Imię i nazwisko	Dane osobowe	Nie powierzono
23.	Rejestr skarg i wniosków, petycji- realizacja wymogu ustawowego	Kodeks postępowania administracyjnego	Imię i nazwisko, adres zamieszkania lub pobytu	Dane osobowe	Nie powierzono
24.	Dokumentacja dot. zamówień publicznych poniżej 30 tyś. Euro i powyżej 30 tyś. Euro - realizacja wymogu ustawowego	Ustawa Prawo zamówień publicznych	Imię i nazwisko, adres zamieszkania, PESEL, NIP, adres e-mail, numer telefonu	Dane osoby	Nie powierzono
25.	Dokumentacja odbywanych staży, praktyk, robót publicznych oraz prac społeczno-użytecznych -realizacja wymogu ustawowego	Umowa	Imię i nazwisko, imię ojca i matki, data i miejsce urodzenia, adres zamieszkania, PESEL, NIP, dokument tożsamości, numer telefonu, adres e-mail	Dane osoby	Powiatowy Urząd Pracy
26.	Dokumentacja osób chcących zatrudnić się w instytucji - realizacja wymogu własnego	Zgoda osób	Imię i nazwisko, adres zamieszkania, data urodzenia i miejsce urodzenia, wizerunek PESEL, NIP, adres e-mail, numer l	Dane osoby	Nie powierzono

27.	Rejestr wyjść służbowych i prywatnych – realizacja wymogu własnego	Regulamin pracy	Imię i nazwisko	Dane osobowe pracownika	Nie powierzono
28.	Oświadczenia majątkowe osób zobowiązanych do złożenia na podstawie art. 24h ustawy o samorządzie gminnym – realizacja wymogu ustawowego	Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym	Imię i nazwisko, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, miejsce pracy, zawód	Dane osoby	Nie powierzono
29.	Ewidencja Obrony Cywilnej - realizacja wymogu ustawowego	Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej	Imię i nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania lub pobytu, miejsce pracy	Dane osoby	Nie powierzono
30.	Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania terenu -realizacja wymogu ustawowego	Ustawa z dnia 7 lipca 1994 r. o zagospodarowaniu przestrzennym	Imię i nazwisko, adres zamieszkania lub pobytu	Dane osoby	Firma zewnętrzna
31.	Ewidencja dodatków mieszkaniowych - realizacja wymogu ustawowego	Ustawa z dnia 2 lipca 1994 r. o najmie lokali mieszkalnych i dodatkach mieszkaniowych	Imię i nazwisko, data urodzenia, adres zamieszkania lub pobytu, miejsce pracy, seria i numer dowodu osobistego	Dane osoby	Nie pwierzono
32.	Dodatek energetyczny- realizacja wymogu ustawowego	Ustawa z dnia 2 lipca 1994 r. o najmie lokali mieszkalnych i dodatkach mieszkaniowych	Imię i nazwisko, data urodzenia, adres zamieszkania lub pobytu, miejsce pracy, seria i numer dowodu osobistego	Dane osoby	Nie powierzono

33.	Ewidencja podatników, płatników, dłużników- realizacja wymogu ustawowego	Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji Ustawa z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych	Imię i nazwisko, adres zamieszkania lub pobytu, PESEL, miejsce pracy	Dane osoby	Nie powierzono
34.	Księgowość – budżet – realizacja wymogu ustawowego	Ustawa z dnia 29 września 1994 r. o rachunkowości Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych	Imię i nazwisko, adres zamieszkania lub pobytu, NIP, seria i numer dowodu osobistego	Dane osoby	Nie powierzono
35.	Rejestr dzierżawnych gruntów i opłat za użytkowanie - realizacja wymogu ustawowego	Ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami	Imię i nazwisko, adres zamieszkania lub pobytu,	Dane osoby	Nie powierzono
36.	Rejestr przedpoborowych, lista poborowych i rejestr świadczeń- realizacja wymogu ustawowego	Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej	Imię i nazwisko, imiona rodziców, adres zamieszkania lub pobytu,	Dane osoby	Nie powierzono
37.	Wykaz osób przeznaczonych i odpowiedzialnych za akcję kurierską - realizacja wymogu ustawowego	Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej	Imię i nazwisko, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu	Dane osoby	Nie powierzono
38.	Wymiar podatku rolnego - realizacja wymogu ustawowego	Ustawa z dnia 15 listopada 1984 r. o podatku rolnym Ustawa z dnia 28 września 1991 r. o lasach	Imię i nazwisko, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, PESEL	Dane osoby	Nie powierzono
39.	Koncesje na sprzedaż napojów alkoholowych- realizacja wymogu	Ustawa z dnia 26 października 1982 o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi	Imię i nazwisko, adres zamieszkania lub pobytu	Dane osoby	Nie powierzono

	ustawowego				
40.	Ewidencja ludności- realizacja wymogu ustawowego	Ustawa z dnia 10 kwietnia 1974 r o ewidencji ludności i dowodach osobistych	Imię i nazwisko, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, PESEL, zawód, wykształcenia, seria i numer dowodu osobistego, Nazwisko: panieńskie, z poprzedniego małżeństwa, rodowe Nazwisko i imię: ojca, matki, współmałżonka Stan cywilny Miejsce i godzina urodzenia Miejsce wystawienia i numer aktu urodzenia żony, męża Data zawarcia związku małżeńskiego Wystawca dowodu osobistego Obowiązek wojskowy Stopień wojskowy Nazwa i numer wojskowego dokumentu osobistego Wystawca dokumentu wojskowego Data rozwodu	Dane osoby	Nie powierzono
41.	Zbiór wydanych i utraconych dowodów osobistych w systemie Źródło– realizacja wymogów ustawowych	Ustawa z dnia 10 kwietnia 1974 r o ewidencji ludności i dowodach osobistych	Imię i nazwisko, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, PESEL, seria i numer dowodu osobistego	Dane osoby	Nie powierzono
42.	Zbiór decyzja związanych z wycinką drzew i krzewów- realizacja wymogu ustawowego	Ustawa z dnia 16 kwietnia 2004r. o ochronie przyrody	Imię i nazwisko, adres zamieszkania lub pobytu, numer telefonu,	Dane osoby	Nie powierzono

43.	Pozwolenie na posiadanie psa rasy uznanej za agresywną- realizacja wymogu ustawowego	Ustawa z dnia 21 sierpnia 1997r. o ochronie zwierząt	Imię i nazwisko, adres zamieszkania lub pobytu	Dane osoby	Nie powierzono
44.	Gminna Komisja Rozwiązywania Problemów Alkoholowych i Narkomanii - realizacja wymogu ustawowego	Ustawa z dnia 26 października 1982r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi	Imię i nazwisko, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, PESEL, miejsce pracy, wykształcenie, nałogi, inne orzeczenia	Dane osoby	Nie powierzono
45.	Zbiór opinii urbanistycznych – realziacja wymogu ustawowego	Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym	Imię i nazwisko, adres zamieszkania lub pobytu	Dane osoby	Starostwo Powiatowe/Firma zewnętrzna
46.	Zbiór decyzja o środowiskowych uwarunkowaniach zgody na realizację przedsięwzięcia- realizacja wymogu ustawowego	Ustawa z dnia 27 kwietnia 2001r. Prawo ochrony środowiska	Imię i nazwisko, adres zamieszkania lub pobytu, numer telefonu	Dane osoby	Firma zewnętrzna
47.	Decyzja o ustaleniu lokalizacji inwestycji celu publicznego i warunków zabudowy- realizacja wymogu ustawowego	Ustawa z dnia 27 marca 2003r. o planowaniu i zagospodarowaniu przestrzennym	Imię i nazwisko, adres zamieszkania lub pobytu, numer telefonu	Dane osoby	Firma zewnętrzna
48.	Zbiór wypisów, wyrysów oraz opinii z miejscowego planu zagospodarowania przestrzennego- realizacja wymogu ustawowego	Ustawa z dnia 27 marca 2003r. o planowaniu i zagospodarowaniu przestrzennym	Imię i nazwisko, adres zamieszkania lub pobytu	Dane osoby	Nie powierzono

49.	Zbiór oraz rejestr podań i decyzji w sprawie umorzenia odsetek, rozłożenia na raty, odroczenia terminów płatności podatków: rolnego, leśnego i od nieruchomości, opłata od wywozu nieczystości- realizacja wymogu ustawowego	Ustawa z dnia 29 sierpnia 1997r. Ordynacja podatkowa	Imię i nazwisko, adres zamieszkania lub pobytu, NIP, miejsce pracy, numer telefonu	Dane osoby	Nie powierzono
50.	Ewidencja numeracji porzadkowej nieruchomości– realizacja wymogu ustawowego	Ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne	Imię i nazwisko, adres zamieszkania lub pobytu	Dane osoby	Nie powierzono
51.	Postanowienia i decyzje o rozgraniczeniu nieruchomości– realizacja wymogu ustawowego	Ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne	Imię i nazwisko, adres zamieszkania lub pobytu	Dane osoby	Nie powierzono
52.	Decyzję zatwierdzające podział nieruchomości– realizacja wymogu ustawowego	Ustawa o gospodarce nieruchomościami	Imię i nazwisko, adres zamieszkania lub pobytu, numer telefonu	Dane osoby	Nie powierzono
53.	Opłaty adiacenckie -realizacja wymogu ustawowego	Ustawa o gospodarce nieruchomościami	Imię i nazwisko, imiona rodziców, adres zamieszkania lub pobytu, PESEL, seria i numer dowodu osobistego	Dane osoby	Nie powierzono
54.	Ewidencja osób podlegających obowiązkowi stawienia się do kwalifikacji wojskowej– realizacja wymogu ustawowego	Ustawa z dnia 21 listopada 1967r. o powszechnym obowiązku obrony Rzeczpospolitej Polskiej	Imię i nazwisko, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, PESEL, seria i numer dowodu osobistego	Dane osoby	Nie powierzono

55.	Dokumentacja Ochotniczych Straży Pożarnych– realizacja wymogu ustawowego	Ustawa z dnia 24 sierpnia 1991r. o ochronie przeciwpożarowej	Imię i nazwisko, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, PESEL, miejsce pracy	Dane osoby	Nie powierzono
56.	Oświadczenia majątkowe Radnych– realizacja wymogu ustawowego	Ustawa z dnia 8 marca 1990r. o samorządzie gminnym	Imię i nazwisko, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, zawód	Dane osoby	Nie powierzono
57.	Ewidencja Radnych I Sołtysów– realizacja wymogu ustawowego	Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym	Imię i nazwisko, data urodzenia, data urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, zawód, numer telefonu	Dane osoby	Nie powierzono
58.	Decyzje i zezwolenia na lokalizację w pasie drogowym urządzeń infrastruktury technicznej– realizacja wymogu ustawowego	Ustawa z dnia 21 marca 1985 r. o drogach publicznych	Imię i nazwisko, adres zamieszkania lub pobytu, NIP, numer telefonu	Dane osoby	Nie powierzono
59.	Ewidencja gruntów– realizacja wymogu ustawowego	Ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne	Imię i nazwisko, imiona rodziców, adres zamieszkania lub pobytu, powierzchnia i numer nieruchomości, Numer księgi wieczystej, tytuł własności nieruchomości nazwiska i imiona współwłaścicieli nieruchomości	Dane osoby	Starostwo Powiatowe
60.	Dofinansowanie kształcenia uczniów w celu przygotowanie zawodowe - realizacja wymogu ustawowego	Ustawa z dnia 7 września 1991r. o systemie oświaty Ustawa Prawo Oświatowe	Imię i nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, miejsce pracy, zawód, wykształcenie	Dane osoby	Nie powierzono

61.	Rejestr decyzji o urządzenie zjazdu indywidualnego z drogi gminnej i wewnętrznej– realizacja wymogu ustawowego	Ustawa z dnia 21 marca 1985 r. o drogach publicznych	Imię i nazwisko, adres zamieszkania lub pobytu, numer telefonu	Dane osoby	Nie powierzono
62.	Zbiór decyzji zezwalających na zajęcie pasa drogowego– realizacja wymogu ustawowego	Ustawa z dnia 21 marca 1985 r. o drogach publicznych	Imię i nazwisko, adres zamieszkania lub pobytu	Dane osoby	Nie powierzono
63.	Pocztowa książka nadawcza– realizacja wymogu ustawowego	Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach Rozporządzenie Prezesa RM z dn. 18.01.2011 w sprawie instrukcji kancelaryjnej i jednolitego rzeczowego wykazu akt oraz instrukcji w sprawie organizacji zakresu działania archiwów zakładowych Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym	Imię i nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, NIP, seria i numer dowodu osobistego, numer telefonu	Dane osoby	Nie powierzono
64.	Rejestr kontrahentów– realizacja wymogu ustawowego	Ustawa z dnia 29 września 1994 r. o rachunkowości Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym	Imię i nazwisko, adres zamieszkania lub pobytu, PESEL, NIP, numer telefonu	dane osoby	Nie powierzono
65.	Przydział gminnego lokalu mieszkalnego– realizacja wymogu ustawowego	Ustawa z dnia 21 czerwca 2001 r. o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym	Imię i nazwisko, adres zamieszkania lub pobytu, seria i numer dowodu osobistego	Dane osoby	Nie powierzono
66.	Inwestycje Gminne– realizacja wymogu ustawowego	Ustawa z 7 lipca 1994 r Prawo budowlane Ustawa z 27 marca 2003r. o planowaniu i zagospodarowaniu przestrzennym Ustawa z 23 kwietnia 1964 r. Kodeks Cywilny Ustawa z 29 stycznia 2004r. Prawo zamówień publicznych	Imię i nazwisko, adres zamieszkania lub pobytu, PESEL, NIP, seria i numer dowodu osobistego	Dane osoby	Nie powierzono
67.	Sprzedaż nieruchomościami komunalnych- realizacja wymogu ustawowego	Ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami Ustawa z dnia 4 września 1997 r. o przekształceniu prawa użytkowania wieczystego przysługującego osobom fizycznym w prawo własności	Imię i nazwisko, imiona rodziców, adres zamieszkania lub pobytu, PESEL	Dane osoby	Nie powierzono

68.	Ewidencja nazw ulic i placów– realizacja wymogu ustawowego	Ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne	Imię i nazwisko, adres zamieszkania lub pobytu, PESEL, numer telefonu	Dane osoby	Nie powierzono
69.	Karta Dużej Rodziny– realizacja wymogu ustawowego	Rozporządzenie Rady Ministrów z dnia 27 maja 2014 r. w sprawie szczegółowych warunków realizacji rządowego programu dla rodzin wielodzietnych	Imię i nazwisko, data i miejsce urodzenia, PESEL, adres zamieszkania lub pobytu	Dane osoby	GOPS
70.	Program 500 +– realizacja wymogu ustawowego	Ustawa z dnia 11 lutego 2016 r. o pomocy państwa w wychowaniu dzieci Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 18 lutego 2016 r. w sprawie sposobu i trybu postępowania w sprawach o świadczenie wychowawcze	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, numer telefonu, adres –e-mail, płeć, nr i seria dokumentu tożsamości, inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym	Dane osoby	GOPS
71.	Profil zaufany ePUAP– realizacja wymogu ustawowego	Ustawa z dnia 17 lutego 2015 r. o informacji podmiotów realizujących zadania publiczne Rozporządzenie MAiC z dnia 5 czerwca 2014 r. w sprawie zasad potwierdzania, przedłużania ważności, unieważniania oraz wykorzystywania i unieważniania profilu zaufania elektronicznego platformy usług administracji publicznej	Imię i nazwisko, PESEL, numer telefonu, e-mail, identyfikator użytkownika na koncie ePUAP	Dane osoby	Nie powierzono
72.	Rejestr mieszkańców oraz Rejestr zamieszkania cudzoziemców - realizacja wymogu ustawowego	Ustawa o ewidencji ludności z dnia 24.09.2010 r. (	Imię i nazwisko, nazwisko rodowe, imiona i nazwiska rodowe rodziców, data urodzenia, miejsce urodzenia, kraj urodzenia, stan cywilny, numer aktu urodzenia, płeć, PESEL, obywatelstwo lub statut bezpaństwowca, imię i nazwisko rodowe małżonka, data zawarcia związku, adres zamieszkania lub pobytu, kraj miejsca zamieszkania, kraj poprzedniego miejsca zamieszkania, data wymeldowania z pobytu stałego, adres zameldowania na pobyt czasowy, seria i numer, data ważności dowodu osobistego lub paszportu obywatela polskiego	Dane osoby	Nie powierzono

73.	Ewidencja osób posiadających wyroby zawierające azbest – realizacja wymogu ustawowego	Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska	Imię i nazwisko, adres zamieszkania lub pobytu, numer telefonu	Dane osoby	Nie powierzono
74.	Ewidencja właścicieli nieruchomości zobowiązanych do złożenia deklaracji o wysokości opłaty za gospodarowanie odpadami komunlanymi – realizacja wymogu ustawowego	Ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach	Imię i nazwisko, adres zamieszkania lub pobytu, PESEL, numer telefonu	Dane osoby	Nie powierzono
75.	Zwrot podatku akcyzowego dla rolników-realizacja obowiązku ustawowego	Ustawa z dnia 10 marca 2006 r. o zwrocie podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej	Imię i nazwisko, adres zamieszkania lub pobytu, PESEL, NIP, seria i numer dowodu osobistego	Dane osoby	Nie powierzono
76.	Zbiór i rejestr wniosków o wpis do hipoteki przymusowej w Księdze wieczystej – realizacja wymogu ustawowego	Ustawa z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa	Imię i nazwisko, adres zamieszkania lub pobytu,	Dane osoby	Nie powierzono
77.	System Informacji Oświatowej - realizacja wymogu ustawowego	Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej	Imię i nazwisko, data urodzenia, adres zamieszkania lub pobytu, PESEL, miejsce pracy, wykształcenie, seria i numer dowodu osobistego	Dane osoby	Nie powierzono
78.	Archiwum zakładowe –realizacja wymogu ustawowego	Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach	Imię i nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, miejsce pracy, zawód, wykształcenie, seria i numer	Dane osoby	Nie powierzono

			dowodu osobistego, numer telefonu		
79.	Fundusz alimentacyjny- dłużnicy alimentacyjni – realizacja wymogów ustawowych	Ustawia z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów	Imię i nazwisko, data i miejsce urodzenia, adres zamieszkania, PESEL, orzeczenie o niepełnosprawności, numer telefonu	Dane osoby	GOPS
80.	Dokumentacja dotycząca stypendiów szkolnych i socjalnych– realizacja wymogów ustawowych	Uchwała Rady Gminy	Imię i nazwisko, adres zamieszkania	Dane osobowe	GOPS
81.	Dokumentacja dot. wniosków Gminnego Programu Odnowy Wsi- realizacja wymogu własnego	Uchwała Rady Gminy	Imię i nazwisko, adres zamieszkania, numer telefonu, adres e-mail	Dane osoby	Nie powierzono
82.	Dokumentacja kadrowo-płacowa Dyrektorów placówek oświatowych – realizacja wymogu ustawowego	Ustawa Prawo Oświatowe	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, daty urodzenia dzieci, imiona i nazwiska dzieci, stan zdrowia	Dane osoby	Nie powierzono
83.	Dokumentacja dotycząca kontroli obowiązku nauki przez młodzież zamieszkałą na terenie gminy– realizacja wymogów ustawowych	Rozporządzenia MEN z 19 lutego 2002 r. w sprawie prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji	Imię i nazwisko, data urodzenia, adres zamieszkania, PESEL, imiona rodziców	Dane osobowe	Nie powierzono
84.	Dokumentacja projektowa –	Umowa	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres	Dane osobowe dzieci, rodziców lub opiekunów prawnych, nauczycieli	Koordynator projektu

	realizacja wymogu ustawowego		zamieszkania lub pobytu, PESEL, wykształcenie, przebieg dotychczasowego zatrudnienia, daty urodzenia dzieci, imiona i nazwiska dzieci, stan zdrowia		
85.	Dokumentacja opłat za ścieki i wodę– realizacja wymogu ustawowego	Ustawa z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowymi odprowadzaniu ścieków	Imię i nazwisko, data urodzenia, adres zamieszkania	Dane osobowe	Nie powierzono
86.	Dokumentacja dotycząca gospodarki wodnej i ściekowej- warunki przyłączenia do sieci, zatwierdzanie dokumentacji projektowej, dokumentacja usuwanych awarii- realizacja wymogu ustawowego	Ustawa z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowymi odprowadzaniu ścieków	Imię i nazwisko i adres zamieszkania, imię ojca i matki, imiona dzieci, PESEL, NIP, dokument tożsamości, nr telefonu, adres e-mail	Dane osoby	WZWiK Wałbrzych
87.	Dokumentacja postępowań egzaminacyjnych na awans zawodowy nauczycieli – realizacja wymogów ustawowych	Ustawa Karta Nauczyciela	Imiona, nazwisko, nazwisko rodowe, data urodzenia, adres zamieszkania, przebieg zatrudnienia, wykształcenie, stan zdrowia	Dane osobowe	Nie powierzono
88.	Dokumentacja postępowań konkursowych na dyrektora placówki lub powierzenie obowiązków – realizacja wymogów ustawowych	Rozporządzenie MEN z dnia 08.04.2010 r. w sprawie regulaminu konkursu na stanowisko dyrektora publicznej szkoły lub publicznej placówki oraz trybu prac komisji konkursowej (	Imiona, nazwisko, nazwisko rodowe, data urodzenia, adres zamieszkania ,p przebieg zatrudnienia, wykształcenie, składniki wynagrodzenia, zapytanie o karalność, stan zdrowia, ocena pracy dyrektora	Dane osobowe	Nie powierzono
89.	Dokumentacja dotycząca oceny pracy dyrektorów placówek –	Rozporządzenie MEN z dnia 21.12.2012r. w sprawie kryteriów i trybu dokonywania oceny pracy nauczyciela, trybu postepowania	Imiona, nazwisko, nazwisko rodowe, data urodzenia, adres zam. Przebieg zatrudnienia,	Dane osobowe	Nie powierzono

	realizacja wymogów ustawowych	odwoławczego i sposobu powoływania zespołu odwoławczego	wykształcenie		
90.	Dokumentacja dotycząca wniosków o nagrody i odznaczenia MEN i KO– realizacja wymogów ustawowych	Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 24.12.2013 r. zmieniający rozporządzenie w sprawie szczegółowego trybu postępowania w sprawie o nadanie orderów i odznaczeń oraz wzorów odpowiednich dokumentów	Imię i nazwisko, stopień awansu zawodowego, staż pracy, stanowisko	Dane osobowe	Nie powierzono
91.	Dokumentacja dotycząca wyprawki szkolnej – realizacja wymogów ustawowych	Rządowy Program dotyczący wyprawki szkolnej	Imię i nazwisko, adres zamieszkania, orzeczenia o niepełnosprawności	Dane osobowe	GOPS
92.	Doskonalenie zawodowe nauczycieli – realizacja wymogów ustawowych	Ustawa Karta Nauczyciela	Imię i nazwisko, stopień awansu zawodowego, staż pracy, stanowisko	Dane osobowe	Nie powierzono
93.	Dokumentacja dotycząca rozliczenia subwencji i dotacji oświatowych i innych – realizacja wymogów ustawowych	Ustawo Prawo Oświatowe Ustawa o opiece nad dziećmi do lat 3	Imię i nazwisko, adres zamieszkania, stan zdrowia, orzeczenia o niepełnosprawności, opinie z PPP, dane osobowe rodziców i opiekunów prawnych	Dane osobowe	Nie powierzono
94.	Dokumentacja nauczania indywidualnego i rewalidacji– realizacja wymogów ustawowych	Rozporządzeniem MEN w sprawie indywidualnego obowiązkowego rocznego przygotowania przedszkolnego i indywidualnego nauczania dzieci i młodzieży Rozporządzenia Ministra Edukacji Narodowej w sprawie ramowych planów nauczania w szkołach publicznych	Imię i nazwisko dziecka i rodzica, adres zamieszkania, data i miejsce urodzenia, orzeczenie o niepełnosprawności, orzeczenie o potrzebie kształcenia specjalnego, PESEL	Dane osobowe	Nie powierzono
95.	Arkusz organizacyjny- realizacja wymogu ustawowego	Rozporządzenia MEN z dnia 29 sierpnia 2014 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i	Imię i nazwisko	Dane osobowe pracowników	Nie powierzono

		opiekuńczej oraz rodzajów tej dokumentacji			
96.	Opinie i Orzeczenia Poradni Psychologiczno-Pedagogicznej- realizacja wymogu ustawowego	Rozporządzenie Ministra Edukacji Narodowej z dnia 30 kwietnia 2013 r. w sprawie zasad udzielania i organizacji pomocy psychologiczno-pedagogicznej w publicznych przedszkolach, szkołach i placówkach	Imię i nazwisko, PESEL, imiona i nazwisko rodziców/prawnych opiekunów, telefon kontaktowy, data i miejsce urodzenia, adres zamieszkania, stan zdrowia	Dane osobowe dzieci i ich rodziców/opiekunów prawnych	Nie powierzono
97.	Dokumentacja związane z dofinansowaniem dożywiania - realizacja zadań własnych szkoły	Zgoda rodziców	Imię i nazwisko	Dane osobowe dzieci	GOPS
98.	Dokumentacja dot. dotacji do niepublicznych przedszkoli	Ustawa Prawo Oświatowe	Imię i nazwisko, adres zamieszkania, PESEL, opinie i orzeczenia, dane osobowe rodziców/opiekunów prawnych	Dane osobowe dzieci i ich rodziców/opiekunów prawnych	Edugrands
99.	Platforma dot. tworzenia arkuszy organizacyjnych szkoły- realizacja dania własnego	Ustawa Prawo Oświatowe	Imię i nazwiska, PESEL , wykształcenie, stopień awansu zawodowego	Dane osobowe	Wolter Kluwer
100.	Ewidencja uczniów dojeżdżających do szkoły – realizacja wymogu ustawowego	Ustawa Prawo Oświatowe	Imię i nazwisko, adres zamieszkania	Dane osobowe dzieci	Nie powierzono
101.	Noty księgowe z tytułu uczęszczania dziecka poza obwodem – realizacja wymogu ustawowego	Ustawa Prawo Oświatowe	Imię i nazwisko, adres zamieszkania	Dane osobowe dzieci	Nie powierzono

102.	Dokumentacja dot. utylizacji azbestu- realizacja wymogu własnego	Uchwała Rady Gminy	Imię i nazwisko, adres zamieszkania, numer telefonu	Dane osobowe	Nie powierzono
103.	Dokumentacja dot. konsultacji społecznych -realizacja wymogu własnego	Uchwała Rady Gminy	Imię i nazwisko, adres zamieszkania, data urodzenia, numer telefonu	Dane osobowe	Nie powierzono
104.	Dokumentacja dot. podatku od środków transportu-realizacja wymogu ustawowego	Ustawa o środkach transportu	Imię i nazwisko, adres zamieszkania, PESEL	Dane osobowe	Nie powierzono
105.	Monitoring- realizacja wymogu ustawowego	Ustawa o ochronie danych osobowych	Wizerunek	Dane osobowe	Nie powierzono
106.	Dokumentacja dot. programu profilaktyki zdrowotnej- realizacja wymogu ustawowego	Ustawa o zdrowiu publicznym Ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych	Imię i nazwisko, adres zamieszkania, imiona rodziców, PESEL,	Dane osobowe	Nie powierzono
107.	Dokumentacja dot. współpracy z organizacjami pozarządowymi - realizacja wymogów ustawowych	Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie	Imię i nazwisko, adres zamieszkania, PESEL, NIP, Seria i numer dowodu osobistego, rachunek bankowy	Dane osobowe	Nie powierzono
108.	Dokumentacja dot. likwidacji szkód łowieckich – realizacja wymogu ustawowego	Ustawa Prawo łowieckie	Imię i nazwisko, adres zamieszkania, numer działki	Dane osobowe	Nie powierzono

109.	Dokumentacja dot. realizacji programu niskiej emisji – realizacja wymogu własnego	Uchwała Rady Gminy	Imię i nazwisko, adres zamieszkania, PESEL, seria i numer dowodu osobistego	Dane osobowe	Nie powierzono
110.	Dokumentacja dot. przetwarzania danych osobowych – realizacja wymogu ustawowego	Ustawa o ochronie danych osobowych	Imię i nazwisko adres udzielającego zgodę	Dane osobowe pracownika	Nie powierzono
111.	Dokumentacja dot. spisu rolnego	Ustawa o powszechnym spisie rolnym	Imię i nazwisko	Dane osobowe	Nie powierzono
112.	Dokumentacja dot. spisu powszechnego	Ustawa o narodowym spisie powszechnym ludności i mieszkań	Imię i nazwisko	Dane osobowe	Nie powierzono

……
(data, podpis ADO)

Formularz nr 2

Wykaz miejsc przetwarzania danych

Lp.	Nazwa pomieszczeń	Adres
1	Pokój Wójta	ul. Główna 132, 58-312 Stare Bogaczowice
2	Pokój Zastępcy Wójta	ul. Główna 132, 58-312 Stare Bogaczowice
3	Pokój Sekretarza Gminy	ul. Główna 132, 58-312 Stare Bogaczowice
4	Pokój Skarbnika Gminy	ul. Główna 132, 58-312 Stare Bogaczowice
5	Pokoje Referatu Organizacyjnego i Spraw Obywatelskich	ul. Główna 132, 58-312 Stare Bogaczowice
6	Pokoje Referatu Inwestycji, Ochrony Środowiska i Gospodarki Mieniem	ul. Główna 132, 58-312 Stare Bogaczowice
7	Pokoje Referatu Finansowo-Budżetowego	ul. Główna 132, 58-312 Stare Bogaczowice
8	Pokój Insp. d/s infrastruktury technicznej i dróg	ul. Główna 132, 58-312 Stare Bogaczowice
9	Archiwum Zakładowe	ul. Główna 132, 58-312 Stare Bogaczowice
10	Serwerownia	ul. Główna 132, 58-312 Stare Bogaczowice

……

(data, podpis Wójta)

Formularz nr 3

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr upoważnienia	Imię i nazwisko	Nr zbiorów	Okres upoważnienia		Program/identyfikator	Nr unieważnienia
			OD	DO		

.....
(data, podpis ADO)

Formularz nr 4
Stare Bogaczowice, dn. 24.05.2018 r.

……..

(sygnatura)

WAŻNOŚĆ
od:
do:

UPOWAŻNIENIE

Na podstawie art. 32 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) upoważniam Pana/ią:

do przetwarzania, w ramach wykonywanych obowiązków służbowych, następujących zbiorów danych osobowych:

Nr zbiorów z ewidencji zbiorów	Nazwa programu / identyfikator

……

(data, podpis ADO)

Formularz nr 5

Stare Bogaczowice, dn.

…….

(sygnatura)

UNIEWAŻNIENIE UPOWAŻNIENIA

Na podstawie art. 32 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) unieważniam upoważnienie do przetwarzania danych osobowych wydane dnia o sygnaturze dla Pani/Pana:

……

(data, podpis ADO)

Formularz nr 6

OŚWIADCZENIE

o zaznajomieniu się z przepisami dotyczącymi ochrony danych osobowych

Ja, niżej podpisany(a)

....

(imię i nazwisko) (instytucja)

…..…….

(stanowisko)

Oświadczam, że:

1. Zapoznałam /em* się z treścią Zarządzenia Wójta Gminy Stare Bogaczowice sprawie wprowadzenia Polityki bezpieczeństwa i instrukcji przetwarzania danych w Urzędzie Gminy Stare Bogaczowice,
2. Zostałam/em/* przeszkolona/ny/* w zakresie przepisów prawa oraz uregulowań wewnętrznych w zakresie bezpieczeństwa danych osobowych.
3. Zobowiązuję się do bezwzględnego zachowania w tajemnicy wszelkich informacji uzyskanych w związku z wykonywanym zakresem czynności na stanowisku pracy oraz przyjmuję do wiadomości, że dane osobowe przetwarzane w Urzędzie Gminy Stare Bogaczowice objęte są ochroną - zgodnie z Rozporządzeniem 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).
4. Zobowiązuję się do zachowania tajemnicy danych osobowych po ustaniu zatrudnienia w Urzędzie Gminy Stare Bogaczowice,
5. Zobowiązuję się do bezwzględnego zachowania w tajemnicy informacji związanych ze sposobem zabezpieczenia danych osobowych.
6. Zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem się/zapoznałam się z racji wykonywanej pracy, a w szczególności nie będę:
   a. Ujawniać danych zawartych w eksploatowanych systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
   b. Ujawniać szczegółów technologicznych używanych w systemów oraz oprogramowania,
   c. Udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych,
   d. Kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą dokumentacją.

Stare Bogaczowice, dnia ....

(data, podpis)

Formularz nr 6a

……..
(imię i nazwisko)

Stare Bogaczowice, dnia.....

OŚWIADCZENIE

Oświadczam, iż zostałam/zostałem poinformowana/poinformowany o imieniu, nazwisku i danych kontaktowych Inspektora danych osobowych oraz jego zastępcy, możliwości konsultacji w zakresie przetwarzania danych osobowych i współpracy z Inspektorem danych osobowych oraz jego zastępcą.

……
podpis pracownika

Formularz nr 7

Stare Bogaczowice, dn.

……..

(sygnatura)

WAŻNOŚĆ
od:
do:

ZGODA

NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH

Na podstawie art.32 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) **wyrażam zgodę Pani/Panu:**

na przebywanie w pomieszczeniach, w których przetwarzane są dane osobowe w zakresie niezbędnym do wykonywania obowiązków służbowych.

……

(data, podpis ADO)

Formularz nr 8

Stare Bogaczowice, dn.

……

(sygnatura)

ODWOŁANIE ZGODY

NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH

Na podstawie art.32 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) **odwołuję zgodę** z dnia o sygnaturze udzieloną **Pani/Panu:**

do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe.

……

(data, podpis ADO)

Formularz nr 9

……., dn. ……

……
(imię i nazwisko)

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Na podstawie art. 6 ust. 1 lit. a 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 **wyrażam zgodę** na przetwarzanie niżej wymienionych moich danych osobowych.

Zgoda udzielona jest tylko do przetwarzania danych oraz ich udostępniania w podanym niżej zakresie.

Lp.	Zakres danych – zgoda	Cel przetwarzania	Odbiorcy lub kategorie odbiorców danych
1			
2			
3			

Jednocześnie zgodnie z art. 13 ust. 1 i 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 przyjmuję do wiadomości, że:

- Administratorem danych jest Urząd Gminy Stare Bogaczowice z siedzibą w przy ul. Głównej 132, 58-312 Stare Bogaczowice reprezentowany przez Wójta,
- Urząd Gminy Stare Bogaczowice powołał Inspektora ochrony danych, kontakt: tel. 74-8452220, e-mail urzad@starebogaczowice.ug.gov.pl
- Dane będą przetwarzane wyłączenie zgodnie z określonym celem,
- Dane będą udostępniane wyłącznie podanym odbiorcom,
- Pani/Pana dane będą przechowywane przez okres określony w JRWA Urzędu Gminy Stare Bogaczowice,
- Przysługuje mi prawo dostępu do treści danych oraz ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, (jeżeli

przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem,

- Ma Pan/Pani prawo wniesienia skargi do UODO, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza 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,
- Pani /Pana dane będą przetwarzane w sposób zautomatyzowany oraz tradycyjny i nie będą profilowane,
- Dane podaję dobrowolnie.

……

(data, podpis)

Formularz nr 10

PLAN SPRAWDZEŃ NA ROK

Zatwierdzam:

……..
(pieczęć i podpis ADO)

Nazwa Administratora danych, adres siedziby, numer REGON	Urząd Gminy Stare Bogaczowice, ul. Główna 132, 58-312 Stare Bogaczowice, REGON 000539319

L.p.	Wymaganie	Pytanie audytowe	Zakres audyty	
			Miejsce audytu (stanowisko, osoba audytowana)	Termin audytu
1	Przetwarzanie danych osobowych jest dopuszczalne wtedy, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba, że przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a uzyskanie jej zgody jest niemożliwe. Dane można przetwarzać do czasu, gdy uzyskanie zgody tej osoby będzie możliwe.	Czy osoba, której dane dotyczą, wyraziła zgodę na ich przetwarzanie, lub przetwarzanie tych danych jest niezbędne dla ochrony żywotnych interesów tej osoby?		
2	Przetwarzanie danych osobowych jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.	Czy przetwarzanie danych osobowych jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa?		
3	Przetwarzanie danych osobowych jest konieczne do realizacji umowy, gdy osoba, której te dane dotyczą jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.	Czy są realizowane umowy, z udziałem osoby będącej stroną w umowie lub przetwarzanie danych jest niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą?		
4	Przetwarzanie danych osobowych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.	Czy przetwarzanie danych osobowych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego?		
5	Przetwarzanie danych osobowych jest niezbędne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza prawa i wolności osoby, której dane dotyczą.	Czy przetwarzanie danych osobowych jest niezbędne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza prawa i wolności osoby, której dane dotyczą?		

6	Administrator poinformował osobę o adresie swojej siedziby i pełnej nazwie, a w przypadku, gdy administratorem jest osoba fizyczna - o miejscu swego zamieszkania oraz imieniu i nazwisku.	Czy administrator poinformował osobę o adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem jest osoba fizyczna - o miejscu swego zamieszkania oraz imieniu i nazwisku?		
7	Administrator poinformował osobę o celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych.	Czy administrator poinformował osobę o celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych?		
8	Administrator poinformował osobę o prawie dostępu do swoich danych oraz ich poprawiania.	Czy administrator poinformował osobę o prawie dostępu do swoich danych oraz ich poprawiania?		
9	Administrator poinformował osobę o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.	Czy administrator poinformował osobę o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej?		
10	Administrator poinformował osobę bezpośrednio po utrwaleniu zebranych danych o źródle danych.	Czy administrator poinformował osobę o źródle danych?		
11	Administrator poinformował osobę bezpośrednio po utrwaleniu zebranych danych o uprawnieniu do wniesienia w określonych ustawowo przypadkach pisemnie umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację	Czy administrator poinformował osobę o uprawnieniu do wniesienia w określonych ustawowo przypadkach pisemnie umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację?		
12	Administrator poinformował osobę bezpośrednio po utrwaleniu zebranych danych o prawie wniesienia sprzeciwu wobec przetwarzania jej danych w określonych ustawowo przypadkach, gdy administrator ma zamiar przetwarzać je w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.	Czy administrator poinformował osobę o prawie wniesienia sprzeciwu wobec przetwarzania jej danych w określonych ustawowo przypadkach, gdy administrator ma zamiar przetwarzać je w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych?		
13	Administrator zapewnia przetwarzanie danych zgodnie z prawem.	Czy administrator zapewnia przetwarzanie danych zgodnie z prawem?		
14	Administrator zapewnia, że dane są zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.	Czy administrator zapewnia, że dane są zbierane dla oznaczonych, zgodnych z prawem celów i dane nie są poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami?		
15	Administrator zapewnia merytoryczną poprawność danych i adekwatność w stosunku do celów, w jakich są przetwarzane.	Czy administrator zapewnia merytoryczna poprawność danych i adekwatność w stosunku do celów, w jakich są przetwarzane?		
16	Administrator zapewnia, że dane przechowywane są w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.	Czy administrator zapewnia, że dane przechowywane są w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania?		
17	Administrator danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.	Czy administrator danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną?		

18	Administrator danych zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.	Czy administrator danych zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem?		
19	Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz ich środki ochrony.	Czy administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz ich środki ochrony?		
20	Dokumentacja Administratora danych zawiera Politykę bezpieczeństwa.	Czy dokumentacja zawiera Politykę bezpieczeństwa?		
21	Polityka bezpieczeństwa zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.	Czy Polityka bezpieczeństwa zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe?		
22	Polityka bezpieczeństwa zawiera Rejestr czynności przetwarzania danych osobowych przez Administratora danych	Czy Polityka bezpieczeństwa zawiera Rejestr czynności przetwarzania danych osobowych przez Administratora danych?		
23	Polityka bezpieczeństwa zawiera opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi.	Czy Polityka bezpieczeństwa zawiera opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi?		
24	Polityka bezpieczeństwa zawiera opis sposobu przepływu danych pomiędzy poszczególnymi systemami.	Czy Polityka bezpieczeństwa zawiera opis sposób przepływu danych pomiędzy poszczególnymi systemami?		
25	Polityka bezpieczeństwa zawiera określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.	Czy Polityka bezpieczeństwa zawiera w szczególności określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych?		
26	Dokumentacja Administratora danych zawiera instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.	Czy dokumentacja Administratora danych zawiera instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych?		
27	Instrukcja zawiera w szczególności procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie Informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.	Czy instrukcja zawiera w szczególności procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności?		
28	Instrukcja zawiera opis metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem	Czy instrukcja zawiera opis metod i środków uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem?		
29	Instrukcja zawiera procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.	Czy instrukcja zawiera procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu?		
30	Instrukcja zawiera procedury tworzenia kopn zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.	Czy instrukcja zawiera procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania?		
31	Instrukcja zawiera opis sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe.	Czy instrukcja zawiera opis sposobu, miejsca i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe?		

32	Instrukcja zawiera informacje o sposobie, miejscu i okresie przechowywania kopii zapasowych.	Czy instrukcja zawiera informacje o sposobie, miejscu i okresie przechowywania kopii zapasowych?		
33	Instrukcja zawiera informacje o sposobie zabezpieczania systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.	Czy instrukcja zawiera informacje o sposobie zabezpieczania systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego?		
34	Instrukcja zawiera informacje o sposobie realizacji wymogów dotyczących odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.	Czy instrukcja zawiera informacje o sposobie realizacji wymogów dotyczących odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia?		
35	Instrukcja zawiera procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.	Czy instrukcja zawiera procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych?		
36	Dokumentacja dot. ochrony danych jest prowadzona przez Administratora danych w formie pisemnej.	Czy dokumentacja dot. ochrony danych jest prowadzona w formie pisemnej przez Administratora danych?		
37	Dokumentację dot. ochrony danych wdraża Administrator danych.	Czy dokumentację dot. ochrony danych wdrażał Administrator danych?		
38	Do przetwarzania danych dopuszczane są wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych.	Czy do przetwarzania danych dopuszczane są wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych?		
39	Administrator danych zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane.	Czy Administrator danych zapewnia kontrolę nad tym, jakie dane osobowe i kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane?		
40	Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania.	Czy Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania?		
41	Ewidencja zawiera imię i nazwisko osoby upoważnionej.	Czy ewidencja zawiera imię i nazwisko osoby upoważnionej?		
42	Ewidencja zawiera datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych.	Czy ewidencja zawiera datę nadania ustania oraz zakres upoważnienia do przetwarzania danych osobowych?		
43	Ewidencja zawiera identyfikator, jeżeli dane są przetwarzane w systemie Informatycznym.	Czy ewidencja zawiera identyfikator, gdy dane są przetwarzane w systemie informatycznym?		
44	Obszar(budynki, pomieszczenia lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe), zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.	Czy obszar, w którym przetwarzane są dane osobowe, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych?		
45	Przebywanie osób nieuprawnionych w obszarze (budynki, pomieszczenia lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe) jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.	Czy przebywanie osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych?		

46	W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.	Czy w systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych?		
47	Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają, co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator.	Czy zapewnia się, aby w systemie informatycznym rejestrowany był dla każdego użytkownika odrębny identyfikator?		
48	Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają, co najmniej dwie osoby, wówczas zapewnia się, aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.	Czy zapewnia się, aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia?		
49	System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego	Czy system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego?		
50	System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.	Czy system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej?		
51	Identyfikator użytkownika, który utraci uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.	Czy identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie?		
52	W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej, niż co 30 dni.	Czy w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej, niż co 30 dni?.		
53	Hasło składa się, co najmniej z 8 znaków.	Czy hasło składa się, co najmniej z 8 znaków?		
54	Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.	Czy dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych?		
55	Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem	Czy kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem?		
56	Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.	Czy kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności?		
57	Osoba użytkują komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania	Czy osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe?		
58	Osoba użytkująca komputer przenośny zawierający dane osobowe, podczas jego transportu stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.	Czy osoba użytkująca komputer przenośny zawierający dane osobowe, podczas jego transportu stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych?		

59	Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku, g d y nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;	Czy urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku, g d y nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie?		
60	Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie	Czy urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych- pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie?		
61	Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy- pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.	Czy urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych?		
62	Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego	Czy Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego?		
63	W przypadku stosowania haseł do uwierzytelniania użytkowników, hasła te składają się, co najmniej z 8 znaków, zawierają małe i wielkie litery oraz cyfry lub znaki specjalne.	Czy w przypadku stosowania haseł do uwierzytelniania użytkowników, hasła te składają się, co najmniej z 8 znaków, zawierają małe i wielkie litery oraz cyfry lub znaki specjalne?		
64	Urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar, w którym przetwarzane są dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.	Czy urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar, w którym przetwarzane są dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych?		
65	Wdrożono fizyczne lub logiczne zabezpieczenia chroniące, przed nieuprawnionym dostępem z sieci publicznej, system informatyczny służący do przetwarzania danych osobowych.	Czy wdrożono fizyczne lub logiczne zabezpieczenia chroniące, przed nieuprawnionym dostępem z sieci publicznej, system informatyczny służący do przetwarzania danych osobowych?		
66	W przypadku zastosowania logicznych zabezpieczeń obejmują one kontrolę przepływu informacji pomiędzy systemem informatycznym Administratora danych, a siecią publiczną.	Czy w przypadku zastosowania logicznych zabezpieczeń obejmują one kontrolę przepływu informacji pomiędzy systemem informatycznym Administratora danych, a siecią publiczną?		
67	W przypadku zastosowania logicznych zabezpieczeń obejmują one kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego Administratora baz danych?	Czy w przypadku zastosowania logicznych zabezpieczeń obejmują one kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora baz danych?		
68	Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej.	Czy Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej?		
69	System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie daty pierwszego wprowadzenia danych do systemu.	Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie daty pierwszego wprowadzenia danych do systemu?		
70	System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie identyfikatora użytkownika wprowadzającego dane do systemu.	Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie identyfikatora użytkownika wprowadzającego dane do		

		systemu?		
71	System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie źródła, w przypadku zbierania danych nie od osoby, której owe dane dotyczą.	Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie źródła, w przypadku zbierania danych nie od osoby, której owe dane dotyczą?		
72	System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie informacji o odbiorcach, którem dane zostały udostępnione, dacie i zakresie tego udostępniania, chyba, że system informatyczny używany jest w zakresie przetwarzania danych w zbiorach jawnych.	Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie informacji o odbiorcach, którem dane zostały udostępnione, dacie i zakresie tego udostępniania, chyba, że system informatyczny używany jest w zakresie przetwarzania danych w zbiorach jawnych?		
73	System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie sprzeciwu wobec przetwarzania danych przez osobę, której te dane dotyczą.	Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie sprzeciwu wobec przetwarzania danych przez osobę, której te dane dotyczą?		
74	Odnotowanie informacji dotyczących daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego te dane następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzania danych.	Czy odnotowanie informacji dotyczących daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego te dane następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzania danych?		
75	System umożliwia tworzenie i drukowanie raportów zawierających odnotowane informacje w przystępnej formie dla każdej osoby, której dane są przetwarzane.	Czy system umożliwia tworzenie i drukowanie raportów zawierających odnotowane informacje w przystępnej formie, dla każdej osoby, której dane są przetwarzane?		
76	Przestrzeganie wymagań określonych przez Administratora danych w Polityce bezpieczeństwa i instrukcji przetwarzania danych osobowych.	1. Czy powołano Administratora Bezpieczeństwa Informacji/inspektora ochrony danych?		
		2. Czy określono zakres obowiązków Administratora Bezpieczeństwa Informacji/ Inspektora ochrony danych?		
		3. Czy określono sposób postępowania w przypadku naruszenia ochrony danych osobowych?		
		4. Czy korespondencja w zakresie procedur kadrowo-płacowych prowadzona jest za pomocą listów poleconych?		
		5. Czy pracownicy (użytkownicy) dopuszczeni do przetwarzania danych osobowych zapoznali się w sposób udokumentowany z Polityką bezpieczeństwa i Instrukcją przetwarzania danych osobowych?		
		6. Czy pracownicy zachowują ostrożność udzielając informacji dot. danych osobowych przez telefon i poza instytucją?		
		7. Czy pracownicy zachowują ostrożność udzielając informacji osobom nieuprawnionym?		
		8. Czy pracownicy reagują na obecność nieznanych osób przebywających w pobliżu miejsca przetwarzania danych i zachowujące się podejrzanie?		
		9. Czy pracownicy są świadomi konieczności zgłaszania incydentów bezpieczeństwa Administratorowi bezpieczeństwa informacji/ inspektorowi ochrony danych?		

		10. Czy pracownicy podpisali oświadczenia o ochronie danych osobowych, do których przetwarzania zostali upoważnieni?		
		11. Czy zakres udostępnionych danych osobowych osobie upoważnionej do przetwarzania danych osobowych jest pisemnie potwierdzony przez Administratora danych?		
		12. Czy przestrzegany jest zakaz niepodawania swojego hasła, pod rygorem naruszenia zasad bezpieczeństwa informacji?		
		13. Czy hasło posiada ilość znaków, zgodnie z poziomem bezpieczeństwa?		
		14. Czy hasła nie są zapisywane na kartkach, w pobliżu komputera, w innych widocznych miejscach?		
		15. Czy użytkownik jest świadom zakazu udostępniania swojego hasła innym użytkownikom?		
		16. Czy sprawdzane jest podczas logowania się, czy ktoś się nie próbował włamać do systemu?		
		17. Czy użytkownik loguje się zawsze na swój login i hasło?		
		18. Czy użytkownik blokuje dostęp do swojego komputera po odejściu od stanowiska pracy za pomocą wygaszacza z hasłem?		
		19. Czy po zakończeniu pracy użytkownik wylogowuje się a następnie zamyka komputer?		
		20. Czy w razie awarii komputera lub sprzętu przetwarzającego dane osobowe, użytkownik powiadamia informatyka, do którego kontakt jest znany?		
		21. Czy laptop pozostawiany jest bez opieki w pomieszczeniu, jeśli pomieszczenie nie jest zamknięte na klucz?		
		22. Czy ekrany monitorów ustawiono w taki sposób, żeby uniemożliwić odczyt wyświetlanych danych osobowych osobom nieupoważnionym?		
		23. Czy określono politykę korzystania z Internetu?		
		24. Czy określono politykę korzystania z poczty firmowej?		
		25. Czy osoby reprezentujące Administratora danych są świadome odpowiedzialności karnej i finansowej za naruszenie ochrony danych osobowych?		
		26. Czy dokumenty w postaci papierowej lub elektronicznej zawierające dane osobowe po zakończeniu pracy są zamknięte (klucze w szafach)?		
		27. Czy dokumenty papierowe i nośniki informacji (płyty CD) zawierające dane osobowe niszczone są w niszczarkach?		
		28. Czy stosuje się system kontroli dostępu do obszarów przetwarzania danych osobowych?		

		29. Czy konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji?		
		30. Czy używane jest tylko licencjonowane oprogramowanie do przetwarzania danych osobowych?		
		31. Czy urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej?		
		32. Czy sieć lokalna podłączona jest do Internetu za pomocą odrębnego komputera?		

.....

(data, podpis IOD)

Sprawozdanie ze sprawdzenia zgodności przetwarzania danych osobowych

Nazwa Administratora danych, adres siedziby, numer REGON	Inspektor ochrony danych/Administrator Bezpieczeństwa Informacji	Miejsce audytu (stanowisko, osoba audytowana)	Termin audytu
Urząd Gminy Stare Bogaczowice, ul. Główna 132, 58-312 stare Bogaczowice, REGON 0005393319			

L.p.	Wymaganie	Pytanie audytowe	Stan przestrzegania wymagania		
			Tak	Częściowo	Nie
1	Przetwarzanie danych osobowych jest dopuszczalne wtedy, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba, że przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a uzyskanie jej zgody jest niemożliwe. Dane można przetwarzać do czasu, gdy uzyskanie zgody tej osoby będzie możliwe.	Czy osoba, której dane dotyczą, wyraziła zgodę na ich przetwarzanie, lub przetwarzanie tych danych jest niezbędne dla ochrony żywotnych interesów tej osoby?			
2	Przetwarzanie danych osobowych jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.	Czy przetwarzanie danych osobowych jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa?			
3	Przetwarzanie danych osobowych jest konieczne do realizacji umowy, gdy osoba, której te dane dotyczą jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.	Czy są realizowane umowy, z udziałem osoby będącej stroną w umowie lub przetwarzanie danych jest niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą?			
4	Przetwarzanie danych osobowych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.	Czy przetwarzanie danych osobowych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego?			
5	Przetwarzanie danych osobowych jest niezbędne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza prawa i wolności osoby, której dane dotyczą.	Czy przetwarzanie danych osobowych jest niezbędne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza prawa i wolności osoby, której dane dotyczą?			
6	Administrator poinformował osobę o adresie swojej siedziby i pełnej nazwie, a w przypadku, gdy administratorem jest osoba fizyczna - o miejscu swego zamieszkania oraz imieniu i nazwisku.	Czy administrator poinformował osobę o adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem jest osoba fizyczna - o miejscu swego zamieszkania oraz imieniu i nazwisku?			
7	Administrator poinformował osobę o celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych.	Czy administrator poinformował osobę o celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych?			
8	Administrator poinformował osobę o prawie dostępu do	Czy administrator poinformował osobę o prawie dostępu do			

	swoich danych oraz ich poprawiania.	swoich danych oraz ich poprawiania?			
9	Administrator poinformował osobę o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.	Czy administrator poinformował osobę o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej?			
10	Administrator poinformował osobę bezpośrednio po utrwaleniu zebranych danych o źródle danych.	Czy administrator poinformował osobę o źródle danych?			
11	Administrator poinformował osobę bezpośrednio po utrwaleniu zebranych danych o uprawnieniu do wniesienia w określonych ustawowo przypadkach pisemnie umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację	Czy administrator poinformował osobę o uprawnieniu do wniesienia w określonych ustawowo przypadkach pisemnie umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację?			
12	Administrator poinformował osobę bezpośrednio po utrwaleniu zebranych danych o prawie wniesienia sprzeciwu wobec przetwarzania jej danych w określonych ustawowo przypadkach, gdy administrator ma zamiar przetwarzać je w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.	Czy administrator poinformował osobę o prawie wniesienia sprzeciwu wobec przetwarzania jej danych w określonych ustawowo przypadkach, gdy administrator ma zamiar przetwarzać je w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych?			
13	Administrator zapewnia przetwarzanie danych zgodnie z prawem.	Czy administrator zapewnia przetwarzanie danych zgodnie z prawem?			
14	Administrator zapewnia, że dane są zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.	Czy administrator zapewnia, że dane są zbierane dla oznaczonych, zgodnych z prawem celów i dane nie są poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami?			
15	Administrator zapewnia merytoryczną poprawność danych i adekwatność w stosunku do celów, w jakich są przetwarzane.	Czy administrator zapewnia merytoryczna poprawność danych i adekwatność w stosunku do celów, w jakich są przetwarzane?			
16	Administrator zapewnia, że dane przechowywane są w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.	Czy administrator zapewnia, że dane przechowywane są w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania?			
17	Administrator danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.	Czy administrator danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną?			
18	Administrator danych zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.	Czy administrator danych zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem?			
19	Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz ich środki ochrony.	Czy administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz ich środki ochrony?			
20	Dokumentacja Administratora danych zawiera Politykę	Czy dokumentacja zawiera Politykę bezpieczeństwa?			

	bezpieczeństwa.				
21	Polityka bezpieczeństwa zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.	Czy Polityka bezpieczeństwa zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe?			
22	Polityka bezpieczeństwa zawiera Rejestr czynności przetwarzania danych osobowych przez Administratora danych	Czy Polityka bezpieczeństwa zawiera Rejestr czynności przetwarzania danych osobowych przez Administratora danych?			
23	Polityka bezpieczeństwa zawiera opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi.	Czy Polityka bezpieczeństwa zawiera opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi?			
24	Polityka bezpieczeństwa zawiera opis sposobu przepływu danych pomiędzy poszczególnymi systemami.	Czy Polityka bezpieczeństwa zawiera opis sposób przepływu danych pomiędzy poszczególnymi systemami?			
25	Polityka bezpieczeństwa zawiera określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.	Czy Polityka bezpieczeństwa zawiera w szczególności określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych?			
26	Dokumentacja Administratora danych zawiera instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.	Czy dokumentacja Administratora danych zawiera instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych?			
27	Instrukcja zawiera w szczególności procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie Informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.	Czy instrukcja zawiera w szczególności procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności?			
28	Instrukcja zawiera opis metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem	Czy instrukcja zawiera opis metod i środków uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem?			
29	Instrukcja zawiera procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.	Czy instrukcja zawiera procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu?			
30	Instrukcja zawiera procedury tworzenia kopn zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.	Czy instrukcja zawiera procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania?			
31	Instrukcja zawiera opis sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe.	Czy instrukcja zawiera opis sposobu, miejsca i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe?			
32	Instrukcja zawiera informacje o sposobie, miejscu i okresie przechowywania kopii zapasowych.	Czy instrukcja zawiera informacje o sposobie, miejscu i okresie przechowywania kopii zapasowych?			
33	Instrukcja zawiera informacje o sposobie zabezpieczania systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.	Czy instrukcja zawiera informacje o sposobie zabezpieczania systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego?			
34	Instrukcja zawiera informacje o sposobie realizacji wymogów dotyczących odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione,	Czy instrukcja zawiera informacje o sposobie realizacji wymogów dotyczących odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie			

	dacie i zakresie tego udostępnienia.	tego udostępnienia?			
35	Instrukcja zawiera procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.	Czy instrukcja zawiera procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych?			
36	Dokumentacja dot. ochrony danych jest prowadzona przez Administratora danych w formie pisemnej.	Czy dokumentacja dot. ochrony danych jest prowadzona w formie pisemnej przez Administratora danych?			
37	Dokumentację dot. ochrony danych wdraża Administrator danych.	Czy dokumentację dot. ochrony danych wdrażał Administrator danych?			
38	Do przetwarzania danych dopuszczane są wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych.	Czy do przetwarzania danych dopuszczane są wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych?			
39	Administrator danych zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane.	Czy Administrator danych zapewnia kontrolę nad tym, jakie dane osobowe i kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane?			
40	Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania.	Czy Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania?			
41	Ewidencja zawiera imię i nazwisko osoby upoważnionej.	Czy ewidencja zawiera imię i nazwisko osoby upoważnionej?			
42	Ewidencja zawiera datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych.	Czy ewidencja zawiera datę nadania ustania oraz zakres upoważnienia do przetwarzania danych osobowych?			
43	Ewidencja zawiera identyfikator, jeżeli dane są przetwarzane w systemie Informatycznym.	Czy ewidencja zawiera identyfikator, gdy dane są przetwarzane w systemie informatycznym?			
44	Przestrzeganie wymagań określonych przez Administratora danych w Polityce bezpieczeństwa i instrukcji przetwarzania danych osobowych	1. Czy powołano Administratora Bezpieczeństwa Informacji/inspektora ochrony danych?			
		2. Czy określono zakres obowiązków Administratora Bezpieczeństwa Informacji/ Inspektora ochrony danych?			
		3. Czy osoby reprezentujące Administratora danych są świadome odpowiedzialności karnej i finansowej za naruszenie ochrony danych osobowych?			

.....

(data, podpis IOD)

Treść ustaleń z audytu	Dowody potwierdzające ustalenia z audytu

1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

.....
(data, podpis IOD)

Rekomendacje		
Lp.	Rekomendacja osoby przeprowadzającej audyt	Decyzja osoby reprezentującej Administratora danych w sprawie rekomendacji
1		
2		
3		
4		
5		
6		
7		

.....
(data, podpis ADO)

Formularz nr 12

Sprawozdanie roczne
ze sprawdzenia stanu ochrony danych osobowych
w Urzędzie Gminy Stare Bogaczowice za rok 2018

Zatwierdzam:

……..
(pieczęć i podpis Wójta)

1. Oznaczenie administratora danych osobowych i adres jego siedziby:
2. Imię i nazwisko Inspektora ochrony danych:
3. Imię i nazwisko administratora sieci informatycznej:
4. Wykaz czynności objętych sprawozdaniem.

L.p.	Czynności	Stan faktyczny	Rekomendacje
1	Analiza dokumentacji		
2	Analiza upoważnień do przetwarzania danych osobowych		
3	Analiza odbytych szkoleń		
4	Analiza spełnienia obowiązku rejestracji IOD w UODO		
5	Analiza przypadków naruszeń przepisów		
6	Analiza umów powierzenia danych		
7	Analiza działań podjętych dla bezpieczeństwa przetwarzania danych		
8	Analiza zabezpieczeń		

	systemu informatycznego (antywirus, firewall)		

5. Plan czynności do realizacji w celu zapewnienia bezpieczeństwa danych i spełnienia wymogów ustawowych.

L.p.	Czynności do wykonania	Data zakończenia czynności	Osoba odpowiedzialna
1	Dokonanie ponownego przejrzenia Polityki Bezpieczeństwa i Instrukcji służącej do przetwarzania danych osobowych pod kątem zgodności z aktualnym stanem prawnym		IOD
2	Dokonanie sprawdzeń stanu działania systemu antywirusowego na skrzynce e-mail oraz komputerach służących do przetwarzania danych osobowych		ASI
3	Weryfikacja wydanych upoważnień oraz unieważnień wydanych upoważnień pod kątem zmian kadrowych		Wójt/IOD

……

(data, podpis IOD)

6. Rekomendacje przyjęte do realizacji.

.....
(data, podpis Wójta)

Formularz nr 13

Stare Bogaczowice, dn.

…….

(sygnatura)

Zgoda na użytkowanie pendrive/dysku zewnętrznego/laptopa poza siedzibą instytucji

Wyrażam zgodę na użytkowanie komputera przenośnego/pendrive/dysku zewnętrznego poza siedzibą instytucji.

Nazwisko i imię pracownika:

Numer ewidencyjny lub seryjne komputera przenośnego/pendrive/dysku zewnętrznego: ……

Czas użytkowania od do

Zakres danych osobowych udostępnionych pracownikowi - …….

……

(data, podpis ADO)

Miejscowość, dn.

…….

(sygnatura)

OŚWIADCZENIE UŻYTKOWNIKA PENDRIVE/DYSKU ZEWNĘTRZNEGO/LAPTOPA

.....

(Imię i nazwisko)

Oświadczam, że przekazany sprzęt

o numerze ewidencyjnym:

i numerze seryjnym
będzie wykorzystany wyłącznie do celów służbowych. Na wyżej wymienionym komputerze nie będę samodzielnie instalował(a) żądnego oprogramowania.

Jednocześnie oświadczam, że zostałem poinformowany(a), Administrator danych nie ponosi odpowiedzialności za nieprawidłowe funkcjonowanie komputera/pendrive/dysku zewnętrznego spowodowane samodzielnym zainstalowaniem oprogramowania na wyżej wymienionym komputerze oraz o konsekwencjach prawnych i służbowych grożących w przypadku samodzielnej instalacji oprogramowania.

Przyjmuję do wiadomości, iż dane zgromadzone na powierzonym mi komputerze/pendrive/dysku zewnętrznym oraz dostępne w wewnętrznej sieci Urzędu Gminy Stare Bogaczowice objęte są tajemnicą służbową i w związku z powyższym zobowiązuję się do przestrzegania odpowiednich procedur mających na celu ochronę danych osobowych, jak i tych stanowiących tajemnicę służbową przed nieuprawnionym udostępnieniem zgodnie z Polityką bezpieczeństwa

……

(data, podpis użutkownika sprzętu)

Formularz nr 15

REJESTR CZYNNOŚCI UDOSTĘPNIEŃ na rok

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Lp.	**Nazwa czynności przetwarzania**	**Jednostka organizacyjna (departament, dział itp.)**	**Cel przetwarzania**	**Kategorie osób**	**Kategorie danych**	**Podstawa prawna**	**Źródło danych**	**Planowany termin usunięcia kategorii danych** *(jeżeli jest to możliwe)*	**Nazwa współadministratora i dane kontaktowe** *(jeśli dotyczy)*	**Nazwa podmiotu przetwarzającego i dane kontaktowe** *(jeśli dotyczy)*	**Kategorie odbiorców** *(innych niż podmiot przetwarzający)*	**Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1** ***(jeżeli jest to możliwe)***	Transfer do kraju trzeciego lub org. międzynarodowej	
													Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	**Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń**
			Art.. 30 ust. 1 pkt b	**Art.. 30 ust. 1 pkt c**	**Art.. 30 ust. 1 pkt c**			**Art.. 30 ust. 1 pkt f**	**Art.. 30 ust. 1 pkt a**	**Art.. 30 ust. 1 pkt d**	**Art.. 30 ust. 1 pkt d**	**Art.. 30 ust. 1 pkt g**	**Art. 30 ust. 1 pkt e**	**Art. 30 ust. 1 pkt e**
1.														
2.														
3.														

.....

(data, podpis Wójta)

MAPA RYZYKA

Oddziaływanie						
	Katastrofalne (5)	5	10	15	20	25
	Poważne (4)	4	8	12	16	20
	Średnie (3)	3	6	9	12	15
	Małe (2)	2	4	6	8	10
	Nieznaczne (1)	1	2	3	4	5
		Bardzo małe (1)	Mało prawdopodobne (2)	Średnie (3)	Prawdopodobne (4)	Prawie pewne (5)
	Prawdopodobieństwo					

	Ryzyko niskie
	Ryzyko średnie
	Ryzyko wysokie

Formularz nr 17

ANALIZA RYZYKA

…… Stare Bogaczowice, dnia

(nazwa jednostki organizacyjnej)

Numer ident. ryzyka	Potencjalne zagrożenie	Oddziaływanie	Prawdopodobieństwo	Punktowa ocena ryzyka	Oddziaływanie	Prawdopodobieństwo	Punktowa ocena ryzyka	Oddziaływanie	Prawdopodobieństwo	Punktowa ocena ryzyka	Średnie ryzyko	Rekomendacje
1	2	3	4	5	6	7	8	9	10	11	12	13
Zasoby : 1. Sprzęt		1. Poufność			2. Rozliczalność			3. Integralność				
1	Awarie sprzęty ze względu na ich wyeksploatowanie											
2	Utrata nośnika komputerowego zawierającego dane osobowe											
3	Nieuprawnione przeniesienie informacji zawierającej dane osobowe na inny nośnik komputerowy											
4	Klęska żywiołowa, w wyniku, której utracono poufność danych osobowych											
5	Nie zgłoszenie błędów w oprogramowaniu lub awarii sprzętu											
6	Brak kont użytkowanika i haseł dostępowych na komputerach											
Wartość średnia												
Zasoby : 2. Ludzie		1. Poufność			2. Rozliczalność			3. Integralność				
1	Brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania											
2	Wyparcie się pracy na stanowisku komputerowym, gdzie przetwarzane są dane osobowe											

3	Wprowadzenie zmian w treści dokumentu zawierającego dane osobowe											
4	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe											
5	Samowolne instalowanie oprogramowania lub wyłączenie oprogramowania antywirsowego											
6	Niezgłoszenie incydentów informatycznych											
Wartość średnia												
Zasoby : 3. Aplikacje		1. Poufność			2. Rozliczalność			3. Integralność				
1	Nieuprawniony dostęp do poszczególnych programów specjalistycznych											
2	Brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego uzytkownika											
3	Atak wirusa											
4	Wadliwe działanie systemu operacyjnego											
5	Brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych											
6	Brak umów powierzenia danych w przypadku korzystania ze zdalnego serwisu oprogramowania											
Wartość średnia												
Zasoby : 4. Pomieszczenia		1. Poufność			2. Rozliczalność			3. Integralność				
1	Nieuprawniony dostęp do pomieszczeń, w których przetwarzane są dane osobowe											
2	Brak polityki dostępu do kluczy											
3	Brak wydzielonych stref dostępu do serwerowni i archiwum											
4	Brak mechanizmu dopuszczenia do stref przetwarzania danych dla osób nie posiadajacych uprawnień do przetwarzania danych											
5	Brak dodatkowego zasilania dla urzadzeń przetwarzajacych dane osobowe											
6	Brak zabezpiecznia ppoż. pomieszczeń, w których przetwarzanie są dane osobowe											
Wartość średnia												
Zasoby : 5. Dodatkowe zabezpieczenia		1. Poufność			2. Rozliczalność			3. Integralność				

1	Alarm											-
2	Monitoring											-
3	Umowy powierzenia danych											-
4	Odcięcie zasilania, w przypadku zdarzeń losowych np. pożary, przepięcia energetyczne											-
5	Powołanie ASI lub zawarcie umowy cywilno-prawnej na świadczenie usługi ASI											-
6	Powołąnie IOD lub zawarcie umowy cywilno-prawnej na świadczenie usługi IOD											-
Wartość średnia												
Ogółem (średnia)												

Stare Bogaczowice, dnia ……

(data, podpis IOD)

Formularz nr 18

RAPORT
z naruszenia bezpieczeństwa zasad ochrony danych osobowych
w …….

1. Data: ……. …… Godzina: ……
(dd.mm.rr) (gg:mm)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……..
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

……..
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
……
……
……..

5. Przyczyny wystąpienia zdarzenia:
……
……
……..

6. Podjęte działania:
……
……
……..

7. Postępowanie wyjaśniające:
……
……
……..

……

(data, podpis ADO)

Formularz nr 19

REJESTR INCYDENTÓW NA ROK 2021

L.p.	Rodzaj incydentu	Opis incydentu	Osoba zgłaszająca	Data ujawnienia incydentu	Wynik postępowania wyjaśniającego	Czy incydent zgłoszona do UODO	IOD (data, podpis)	ADO (data, podpis)

……
(data, podpis Wójta)

Formularz nr 20

AUDYT KRI NA ROK

Zatwierdzam:

……..
(pieczęć i podpis Wójta)

Nazwa Administratora danych, adres siedziby	
Audytowany	

L.p.	Wymaganie	Pytanie audytowe	Zakres spełnienia wymagania			
			TAK	NIE	CZĘŚCIOWO	NIE DOTYCZY
I	**Minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej**					
	A. Dostęp do rejestru systemu SIO					
1		Czy Urząd zobowiązany jest do prowadzenia rejestrów publicznych				
2		Czy Urząd zobowiązany jest do wprowadzania danych do istniejących rejestrów publicznych SIO				
3		Czy administrator rejestru publicznego SIO nadał uprawnienia dostępu do rejestru				
4		Czy pracownicy Urzędu mają stosowne upoważnienie dostępu do systemu SIO				
5		Czy pracownik Urzędu upoważniony do pracy w systemie SIO zmienia hasło dostępowe umożliwiające zalogowanie się do systemu SIO				
6		Czy osoby upoważnione znają procedurę nadania nowego hasła dostępowego w przypadku utraty hasła poprzedniego uprawniającego do dostępu do systemu SIO				
7		Czy pracownicy znają procedurę zgłaszania incydentu nieuprawnionego dostępu do systemu SIO				
8		Czy Urząd w roku 2020 odnotował incydenty dostępu do systemu SIO przez osobę nieuprawnioną				
9		Czy w Urzędzie określono miejsce przechowywania upoważnień dostępu do systemu SIO				
10		Czy określono z poziomu ilu komputerów lokalnych możliwy jest				

		dostęp do systemu SIO				
11		Czy komputery lokalne, z który możliwy jest dostęp do rejestrów systemu SIO posiadają UPS				
	B. Dostęp do rejestru systemu Empatia					
12		Czy Urząd zobowiązany jest do wprowadzania danych do istniejących rejestrów publicznych Empatia				
13		Czy administrator rejestru publicznego SIO nadał uprawnienia dostępu do rejestru				
14		Czy pracownicy Urzędu mają stosowne upoważnienie dostępu do systemu Empatia				
15		Czy pracownik Urzędu upoważniony do pracy w systemie Empatia zmienia hasło dostępowe umożliwiające zalogowanie się do systemu Empatia				
16		Czy osoby upoważnione znają procedurę nadania nowego hasła dostępowego w przypadku utraty hasła poprzedniego uprawniającego do dostępu do systemu Empatia				
17		Czy pracownicy znają procedurę zgłaszania incydentu nieuprawnionego dostępu do systemu Empatia				
18		Czy Urząd w roku 2020 odnotował incydenty dostępu do systemu Empatia przez osobę nieuprawnioną				
19		Czy w Urzędzie określono miejsce przechowywania upoważnień dostępu do systemu Empatia				
20		Czy określono z poziomu ilu komputerów lokalnych możliwy jest dostęp do systemu Empatia				
21		Czy komputery lokalne, z który możliwy jest dostęp do rejestrów systemu Empatia posiadają UPS				
	C. Dostęp do rejestru systemu CEDIG					
22		Czy Urząd zobowiązany jest do wprowadzania danych do istniejących rejestrów publicznych CEDIG				
23		Czy administrator rejestru publicznego CEDIG nadał uprawnienia dostępu do rejestru				
24		Czy pracownicy Urzędu mają stosowne upoważnienie dostępu do systemu CEDIG				
25		Czy pracownik Urzędu upoważniony do pracy w systemie CEDIG zmienia hasło dostępowe umożliwiające zalogowanie się do systemu CEDIG				
26		Czy osoby upoważnione znają procedurę nadania nowego hasła dostępowego w przypadku utraty hasła poprzedniego uprawniającego do dostępu do systemu CEDIG				
27		Czy pracownicy znają procedurę zgłaszania incydentu nieuprawnionego dostępu do systemu CEDIG				
28		Czy Urząd w roku 2020 odnotował incydenty dostępu do systemu CEDIG przez osobę nieuprawnioną				
29		Czy w Urzędzie określono miejsce przechowywania				

		upoważnień dostępu do systemu CEDIG				
30		Czy określono z poziomu ilu komputerów lokalnych możliwy jest dostęp do systemu CEDIG				
31		Czy komputery lokalne, z który możliwy jest dostęp do rejestrów systemu CEDIG posiadają UPS				
	D. Dostęp do rejestru systemu Źródło					
32		Czy Urząd zobowiązany jest do wprowadzania danych do istniejących rejestrów publicznych Źródło				
33		Czy administrator rejestru publicznego Źródło nadał uprawnienia dostępu do rejestru				
34		Czy pracownicy Urzędu mają stosowne upoważnienie dostępu do systemu Źródło				
35		Czy pracownik Urzędu upoważniony do pracy w systemie Selwin zmienia hasło dostępowe umożliwiające zalogowanie się do systemu Źródło				
36		Czy osoby upoważnione znają procedurę nadania nowego hasła dostępowego w przypadku utraty hasła poprzedniego uprawniającego do dostępu do systemu Źródło				
37		Czy pracownicy znają procedurę zgłaszania incydentu nieuprawnionego dostępu do systemu Źródło				
38		Czy Urząd w roku 2020 odnotował incydenty dostępu do systemu Selwin przez osobę nieuprawnioną				
39		Czy w Urzędzie określono miejsce przechowywania upoważnień dostępu do systemu Źródło				
40		Czy określono z poziomu ilu komputerów lokalnych możliwy jest dostęp do systemu Źródło				
41		Czy komputery lokalne, z który możliwy jest dostęp do rejestrów systemu Źródło posiadają UPS				
	E. Dostęp do rejestru systemu ePUAP					
42		Czy Urząd posiada założony profil w systemie ePUAP				
43		Czy administrator ePUAP nadal login i hasło pracownikom Urzędu uprawniające do pracy na założonym przez Urząd profilu ePUAP. Ile osób dostało uprawnienia				
44		Czy zapewniono by pracownik posiadający uprawnienia do systemu ePUAP w przypadku wpłynięcia na jego konto wiadomości z podpisem kwalifikowalnym otrzymywał na swój komputer lokalny powiadomienie o wpływie na jego konto informacji.				
45		Czy Urząd określiła w sposób udokumentowany, kto jest odpowiedzialny za odbiór i wydruk wiadomości wpływających na skrzynkę poczty e-PUAP				
46		Czy Urząd określiła obowiązek wpisywani wiadomości otrzymywanych pocztą ePUAP jako wpływu do dziennika korespondencji				
47		Czy Urząd posiada aktualna i zatwierdzoną przez Archiwum				

		Państwowe w Opolu instrukcję kancelaryjno-archiwalną				
48		Czy odpowiedzi udzielane za pośrednictwem poczty ePUAP są rejestrowane w dzienniku korespondencji jako wypływ				
II	**Minimalne wymagania dla systemów teleinformatycznych**					
	A. Dostęp do skrzynki poczty służbowej					
49		Czy skrzynka poczty służbowej Urzędu jest zainstalowana na wykupionej przez Urząd domenie.				
50		Czy Urząd ustaliła w sposób udokumentowany, kto jest odpowiedzialny za sprawdzenie wiadomości wpływających na skrzynkę poczty służbowej Urzędu, wstępną selekcję wiadomości i wydruk wiadomości mających istotne znaczenie dla funkcjonowania Urzędu.				
51		Czy Urząd ustanowił indywidualne skrzynki poczty służbowej dla pracowników				
52		Czy wiadomości mające istotne znaczenie dla Urzędu wpływające na skrzynkę poczty służbowej są drukowane i wpisywane do Dziennika korespondencji.				
53		Czy dokumenty zwierające dane osobowe są szyfrowane				
54		Czy Urząd określiła jaki program będzie wykorzystywane do szyfrowania plików tekstowych				
55		Czy Urząd określiła jaki program będzie wykorzystywane do szyfrowania plików wizualnych, audio i graficznych				
56		Czy ustalono w jaki sposób pracownicy mogą wysłać na skrzynkę poczty służbowej dokumenty zawierające dane osobowe				
	B. Dostęp do Internetu i sieci Wi-Fi					
57		Czy Urząd ma podpisaną umowę z dostawcą Internetu				
58		Czy sygnał Internetu przechodzi przez ruter lub serwer				
59		Czy Urząd posiada wewnętrzną sieć Wi – Fi				
60		Czy sieć wewnętrzna Wi-Fi jest zabezpieczona hasłem dostępowym				
61		Czy hasło dostępu do sieci Wi-Fi jest znane wszystkim pracownikom Urzędu				
62		Czy klientom Urzędu udostępnia się hasło do sieci Wi-Fi				
63		Czy Urząd stosuje oprogramowanie do monitorowania dostępu do stron internetowych i ich blokowania				
64		Czy ustalono miejsce przechowywania kodów dostępowych do sieci Wi-Fi				
	C. Dostęp do monitoringu					
65		Czy Urząd posiada monitoring wizyjny				
66		Czy monitoring wizyjny został wprowadzony zgodnie z wymogami prawnymi				
67		Czy ustalono kto ma prawo wglądu w zapis rejestratora				

		monitoringu wizyjnego				
68		Czy ustalono kto ma prawo udostępniania zapisu z rejestratora monitoringu wizyjnego podmiotom zewnętrznym				
69		Czy w 2020 r. odnotowano wniosek organu uprawnionego o udostępnienie zapisu z monitoringu wizyjnego				
70		Czy w 2020 r. odnotowano wnioski pisemne lub ustne klientów Urzędu o udostępnienie zapisu z monitoringu wizyjnego				
	D Dostęp do BIP					
71		Czy Urząd posiada swoją stronę BIP				
72		Czy Urząd w sposób udokumentowany wskazał osobę odpowiedzialna za prowadzenie strony BIP i jej aktualizację				
73		Czy strona BIP Urzędu odpowiada wymogą prawnym w zakresie jej zawartości				
74		Czy akty prawa miejscowego zamieszczone na stronie BIP są stale aktualizowane.				
75		Czy na stronie BIP znajdują się dane adresowego Administratora danych, dane kontaktowe do IOD oraz pełna treść klauzuli informacyjnej				
76		Czy strona BIP zawiera wykaz wszystkich aktów prawnych wytworzonych przez Urząd				
77		Czy Urząd w roku 2020 r. odnotował jakikolwiek incydent z próbą ataku teleinformatycznego na swoją stronę BIP				
	System Zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji					
78		Czy Urząd posiada dokumentacje ochrony danych osobowych zgodną z wymaganiami RODO				
79		Czy dokumentacja ochrony danych osobowych jest stale aktualizowana				
80		Czy Urząd posiada spis sprzętu i oprogramowania służącego do przetwarzania danych osobowych				
81		Czy Urząd dokonuje analizy stanu sprzętu i oprogramowania pod katem stanu technicznego i dalszej przydatności				
82		Czy Urząd posiada aktualne licencje na użytkowane oprogramowanie				
83		Czy Urząd korzysta ze wsparcia zdalnego dla użytkowanego oprogramowania oraz czy posiada stosowne umowy powierzenia danych				
84		Czy Urząd dokonuje analizy ryzyka pod kątem utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyka				
85		Czy podjęto działania zmierzające do zapewnienia, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia				
86		Czy uprawnienia osób do przetwarzania danych osobowych są				

		adekwatne do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji				
87		Czy w przypadku zmiany zadań i obowiązków pracownik ma zmiennie upoważnienie				
88		Czy Urząd przeprowadza coroczne szkolenia pracowników zaangażowanych w proces przetwarzania danych				
89		Czy Urząd określił zasady pracy na urządzeniach mobilnych oraz pracy na odległość				
90		Czy laptopy, dyski zewnętrzne oraz pendrive posiadają zabezpieczenia uniemożliwiające ich nieuprawnione ujawnienie, modyfikacje, usunięcie lub zniszczenie				
91		Czy Urząd zawarła umowę na obsługę serwisowa sprzętu informatycznego oraz stosowanego oprogramowania				
92		Czy Urząd ma zawarte umowy serwisowe na użytkowny przez siebie sprzęt informatyczny				
	Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych					
	A. Zabezpieczenie posiadanego serwera					
93		Czy Urząd dba o aktualizację posiadanego oprogramowania i sprzętu w serwerowni				
94		Czy Urząd zapewnił odpowiednie zabezpieczenie pomieszczenia serwerowni				
95		Czy Urząd określił wykaz osób mających prawo wstępu do serwerowni.				
96		Czy Urząd stosuje odpowiednie oprogramowanie zabezpieczające serwer przed wrogi atakiem osób nieuprawnionych				
	B. Zabezpieczenie posiadanego oprogramowania					
97		Czy Urząd posiada aktualne licencje na stosowane przez Urząd oprogramowanie				
98		Czy posiadane oprogramowanie wymaga wspomagania zdalnego przez twórców oprogramowania. Czy zawarto umowy powierzenia danych				
99		Czy upoważnienia pracowników wskazują do jakich programów maja dostęp poprzez hasła i login				
100		Czy informatyk prowadzi wykaz haseł dostępowych i loginów				
101		Czy Urząd odnotował w 2020 r. próby nieuprawnionego włamania na programy użytkowane przez Urząd				
102		Czy istniejący mechanizm reakcji na zidentyfikowany incydent umożliwia podjęcie szybkiej decyzji o wszczęciu działań korygujących				
103		Czy szkoła zapewnia możliwość przeprowadzenia okresowego audytu wewnętrznego w zakresie bezpieczeństwa , nie rzadziej niż raz w roku				

	Zapewnienie odpowiedniego poziomu dostępności do zasobów informatycznych instytucji dla osób niepełnosprawnych					
104		Czy instytucja posiada własną stronę internetową				
105		Czy instytucja określiła w sposób udokumentowany kto odpowiada za prowadzenie strony internetowej instytucji				
106		Czy strona internetowa instytucji jest dostosowana dla osób niedowidzących lub słabo widzących				
107		Czy instytucja sporządza coroczne sprawozdanie o dostępności strony internetowej dla osób niepełnosprawnych.				

Treść ustaleń z audytu		Dowody potwierdzające ustalenia z audytu

.....
(data, podpis IOD)

Rekomendacje		
Lp.	Rekomendacja osoby przeprowadzającej audyt	Decyzja osoby reprezentującej Administratora danych w sprawie rekomendacji
95	Należy określić wykaz osób uprawnionych do wejścia do serwerowni.	Zrealizowane

.....
(data, podpis Wójta)

Formularz nr 21

Harmonogram szkoleń pracowników Urzędu Gminy w Starych Bogaczowicach

l.p	Szkolenie			Zakres
1.	Pierwsze	w związku z rozpoczęciem zatrudnienia	Wszyscy pracownicy	- przepisy powszechnie obowiązujące, - przepis wewnętrzne jednostki, - przepisy w zakresie dotyczącym zajmowanego stanowiska.
2.	Okresowe	min. 1 raz w roku	Wszyscy pracownicy	- zmiany przepisów wewnętrznych jednostki - zmiany przepisów prawnych dotyczących RODO, - zmiany przepisów branżowych,
3.	Incydentalne	w przypadku wystąpienia naruszenia przepisów RODO	Wszyscy pracownicy	- przepisy powszechnie obowiązujące, - przepis wewnętrzne jednostki, - przepisy w zakresie dotyczącym zajmowanego stanowiska

DOKUMENT PODPISANY ELEKTRONICZNIE

Dane podpisywanego dokumentu

Typ dokumentu	Zarządzenie
Numer dokumentu	114/2022
Data dokumentu	2022-11-04
Organ wydający	Wójt Gminy Stare Bogaczowice
Przedmiot regulacji	w sprawie wdrożenia dokumentacji dotyczącej ochrony danych osobowych w Urzędzie Gminy Stare Bogaczowice
Identyfikator dokumentu	8E0AEF24-B575-4C45-A958-F8DC9A6FEBEE

Informacje o złożonych podpisach elektronicznych

Podpis:	
Sygnatura	Signature-1364884785
Numer seryjny	787319D55B400933097C85A81A1FDD13
Osoba podpisująca	MIROSŁAW LECH\; GMINA STARE BOGACZOWICE
Instytucja	GMINA STARE BOGACZOWICE
Miejscowość	STARE BOGACZOWICE
Województwo	dolnośląskie
Kraj	PL
Data złożenia podpisu	2022-11-04 11:03:00
Zakres podpisu	Cały dokument
Wystawca certyfikatu	VATPL-5170359458 Certum QCA 2017 Asseco Data Systems S.A. PL