OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH, O KTÓREJ MOWA W ART. 35 ROZPORZĄDZENIA PE I RADY (UE) 2016/679 (RODO) POWSZECHNEJ SPÓŁDZIELNI MIESZKANIOWEJ „PRZYMORZE" W GDAŃSKU.

Zał. nr 1 do Uchwały nr 600A

1. Systematyczny opis planowanych operacji przetwarzania danych osobowych i celów ich przetwarzania oraz prawnie uzasadnionych interesów realizowanych przez administratora.

a. Administrator przetwarza dane w formie papierowej oraz w formie elektronicznej. Dane w formie elektronicznej przetwarzane są w programach UNISOFT, PŁATNIK, SPÓŁDZIELCA - COMBIDATA, PEKAO BIZNES 24,EXCEL.

b. Dane przetwarzane są w celach:
   - zatrudniania pracowników,
   - wykonywania umów,
   - dochodzenia roszczeń (w tym postępowania egzekucyjne) oraz obrona przed roszczeniami,
   - przestrzegania podatkowych lub handlowych terminów przechowywania danych,
   - księgowości i rozliczeń publicznoprawnych, w tym podatki i składki.
   - realizacji celów statutowych administratora, w szczególności dotyczących zarządzania nieruchomościami stanowiącymi własność administratora i jego członków, a także lokatorów zamieszkujących w zasobach lokalowych administratora.

c. Dane pozyskiwane są od:
   - osób których dotyczą,
   - kontrahentów – w odniesieniu do ich pracowników i współpracowników,
   - z publicznie dostępnych rejestrów CEIDG – w odniesieniu do osób fizycznych prowadzących działalność gospodarczą.

d. Dane przekazywane są:
   - podmiotom realizującym zadania wyznaczone przez prawo pracy – wykonujące badania pracownicze – w zakresie wymaganym do realizacji,
   - kontrahentom – w zakresie danych pracowników, współpracowników i lokatorów (imię i nazwisko) w celu umożliwienia wejścia na miejsce realizacji umowy (np. plac budowy),
   - podmiotom świadczącym usługi prawne na rzecz administratora, organom państwowym i sądom,
   - zakładowi ubezpieczeń społecznych,
   - organom administracji, w tym podatkowej.

2. Ocena czy operacje przetwarzania są niezbędne i proporcjonalne w stosunku do celów.

Cel	Zakres danych	Niezbędne	Proporcjonalne.
Zatrudnianie pracowników.	Dane zgodne z art. 22 [1] par. 1 i 2 kodeksu pracy.	TAK	TAK
Wykonywanie umów.	a) W stosunku do pracowników i współpracowników własnych – jak wyżej. b) W stosunku do pracowników i współpracowników kontrahentów – imię i nazwisko, dane firmy w której pracuje, stanowisko służbowe, mail oraz numer telefonu. c) Rachunek bankowy w celach rozliczeń z pracownikami, współpracownikami oraz kontrahentami (osobami fizycznymi prowadzącymi działalność gospodarczą). d) Dane lokatorów zamieszkujących w zasobach mieszkaniowych administratora danych w zakresie niezbędnym do realizacji umów.	TAK	TAK
Dochodzenie roszczeń (w tym postępowania egzekucyjne) oraz obrona przed roszczeniami.	Imię i nazwisko, PESEL, adres, dane kontaktowe, dane ujawnione w rejestrach jawnych – CEIDG.	TAK	TAK
Przestrzeganie podatkowych lub handlowych terminów przechowywania danych.	Dane wymagane przez właściwe przepisy podatkowe lub handlowe.	TAK	TAK
Księgowość i rozliczenia publicznoprawne, w tym podatki i składki.	Dane wymagane przez właściwe przepisy podatkowe, rachunkowe i ubezpieczeniowe.	TAK	TAK
Realizacja celów statutowych administratora, w szczególności dotyczących zarządzania nieruchomościami stanowiącymi własność administratora i jego członków, a także lokator zamieszkujących w zasobach lokalowych administratora.	Dane wymagane przez właściwe przepisy prawa i statut administratora.	TAK	TAK

Ocenia się, że przetwarzane dane są niezbędne oraz proporcjonalne w stosunku do celów przetwarzania.

3. Ocena ryzyka naruszenia praw i wolności osób, których dane dotyczą o którym mowa w art. 35 ust. 1 RODO.

Prawa i wolności osób, których dane dotyczą:

1) prawo do informacji, o którym mowa w art. 13 RODO (zbieranie danych od osoby, której dane dotyczą),
2) prawo do informacji, o którym mowa w art. 14 RODO (zbieranie danych w sposób inny niż od osoby, której dane dotyczą),
3) prawo dostępu do danych osobowych, o którym mowa w art. 15 RODO,
4) prawo do sprostowania danych osobowych, o którym mowa w art. 16 RODO,
5) prawo do usunięcia danych osobowych, o którym mowa w art. 17 RODO (tzw. prawo do bycia zapomnianym),
6) prawo do ograniczenia przetwarzania danych osobowych, o którym mowa w art. 18 RODO,
7) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
8) prawo do sprzeciwu, o którym mowa w art. 21 RODO,
9) prawo do niepodlegania decyzji opartej na zautomatyzowanym przetwarzaniu, w tym profilowaniu, o którym mowa w art. 22 RODO.

Stwierdzone ryzyka dla powyższych praw i wolności:

- utrata danych,
- wyciek danych osobowych (w tym kradzież lub nieuprawnione udostępnienie),
- modyfikacja danych,
- uniemożliwienie dostępu do danych (np. w skutek działania oprogramowania *ransomware*).

Powyższe ryzyka obejmują przyczyny o charakterze:

- ludzkim (w szczególności kradzież, zagubienie, nieuprawnione udostępnienie, modyfikację – również przypadkową)
- technicznym (w szczególności zagrożenia o charakterze informatycznym – w tym na skutek działania oprogramowania typu *malware*).

Ocenia się, że powyższe ryzyka są możliwe do wystąpienia ze względu na sposób przetwarzania danych. Ryzyko ocenia się jako nieznaczne.

4. Środki planowane w celu zaradzenia ryzyku, w tym mające zapewnić ochronę danych osobowych.

Administrator stosuje następujące środki bezpieczeństwa o charakterze zarówno organizacyjnym jak i technicznym, których celem jest zminimalizowanie zidentyfikowanych ryzyk oraz identyfikacja nowych ryzyk:

1) zabezpieczenia organizacyjne:
    a. dostęp do danych osobowych nadawany tylko upoważnionym osobom na podstawie pisemnego upoważnienia,
    b. szkolenia pracowników z zasad ochrony danych osobowych,
    c. dane osobowe w postaci papierowej przechowywane w szafie zamkniętej na klucz, w zamkniętym gabinecie, placówki Spółdzielni wyposażone w alarm oraz chroniona,
    d. dostęp do komputerów oraz oprogramowania zawierającego bazy danych osobowych chroniony hasłem,

e. prowadzenie bieżącego monitoringu ryzyka w celu identyfikacji nowych ryzyk,
f. stosowanie polityki korzystania z komputerów i innego sprzętu na którym znajdują się dane osobowe lub który umożliwia zdalny dostęp do danych osobowych – załącznik nr 1.
g. stosowanie procedury na wypadek naruszenia zasad ochrony danych osobowych – załącznik nr 2.

2) Zabezpieczenia techniczne:
   a. przetwarzanie danych osobowych, w tym poczty elektronicznej na serwerze profesjonalnego i zaufanego dostawcy domeny,
   b. wykonywanie kopii zapasowych baz danych osobowych,
   c. dostęp do danych na serwerze tylko dla osób uprawnionych, stosowanie loginu i hasła oraz różnego poziomu uprawnień, a co za tym idzie ograniczonego dostępu do danych,
   d. stosowanie oprogramowania antywirusowego w najnowszej wersji, ESET oraz firewall oraz bieżące aktualizowanie,
   e. brak korzystania z sieci wewnętrznej poza firmą (z wyjątkiem administratora sieci wewnętrznej),
   f. dostęp do sieci wewnętrznej spoza firmy ma tylko administrator sieci poprzez sieć typu Virtual Private Network.
   g. sieć Wi-Fi zabezpieczona szyfrowaniem WPA2,
   h. komputery firmowe połączone są do sieci lan kablowo, a sieć bezprzewodowa jest co do zasady nieużywana.

Gdańsk, dnia 25 maja 2018 r.

ZAŁĄCZNIK NR 1 – POLITYKA KORZYSTANIA Z KOMPUTERÓW I INNEGO SPRZĘTU NA KTÓRYM ZNAJDUJĄ SIĘ DANE OSOBOWE LUB KTÓRY UMOŻLIWIA ZDALNY DOSTĘP DO DANYCH OSOBOWYCH

1. **Co określa polityka.**

   Polityka określa zasady posługiwania się komputerami i innym sprzętem na którym znajdują się dane osobowe lub który umożliwia dostęp do danych osobowych.

2. **Osoby których polityka dotyczy.**

   Polityka dotyczy każdej osoby, niezależnie od podstawy prawnej współpracy z administratorem danych osobowych (Powszechną Spółdzielnią Mieszkaniowa „PRZYMORZE" w Gdańsku), korzystającej z komputera lub innego sprzętu na którym znajdują się dane osobowe lub który umożliwia dostęp do danych osobowych.

3. **Cel polityki.**

   Celem niniejszej polityki jest dążenie do zapewnienia zgodności przetwarzania danych osobowych, znajdujących się lub dostępnych poprzez komputery i inne urządzenia elektroniczne, z przepisami prawa oraz eliminacja lub minimalizacja ryzyk zidentyfikowanych w ocenie skutków dla ochrony danych osobowych.

4. **Sposób realizacji celu polityki.**

   Cel polityki realizowany jest poprzez przyjęcie i stosowanie zasad posługiwania się komputerami oraz innym sprzętem na którym znajdują się dane osobowe lub dającym dostęp do danych osobowych opisanych w pkt. 5 poniżej.

5. **Zasady posługiwania się komputerami i innym sprzętem na którym znajdują się dane osobowe lub który umożliwia dostęp do danych osobowych:**

   a) korzystanie z komputerów wyłącznie w firmie; w wypadku posługiwania się komputerami poza firmą – dysponenci urządzeń są obowiązani nie udostępniać ich innym osobom, a także chronić przed kradzieżą, zagubieniem lub zniszczeniem,

   b) korzystanie wyłącznie z licencjonowanego oprogramowania od znanych dostawców,

   c) nieściąganie oraz nieinstalowanie oprogramowania nieznanego pochodzenia lub nieposiadającego licencji,

   d) instalowania oprogramowania mogą dokonywać tylko osoby upoważnione,

   e) korzystanie z zasobów sieciowych Internetu powinno być świadome i dążyć do minimalizacji ryzyka pobrania oprogramowania szkodliwego (malware), w tym szpiegującego (spyware) lub mogącego blokować dostęp (ransomware); należy unikać wejść na strony niezaufane, mogące być źródłem oprogramowania szkodliwego;

   f) korzystanie z poczty elektronicznej powinno być świadome i dążyć do minimalizacji ryzyka pobrania oprogramowania szkodliwego (malware), w tym szpiegującego (spyware) lub mogącego blokować dostęp (ransomware); w szczególności należy zwracać uwagę na zagrożenia w postaci wiadomości od nieznanych nadawców zawierające nieznane załączniki, których otwarcie może prowadzić do zainfekowania urządzenia;

   g) podczas pracy z danymi osobowymi należy dochowywać należytej staranności, aby zapewnić poprawność danych osobowych, w szczególności unikać ich przypadkowej modyfikacji.

ZAŁĄCZNIK NR 2 – PROCEDURA NA WYPADEK NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH.

1. **Cel procedury.**

Celem niniejszej procedury jest wprowadzenie zasad postępowania na wypadek naruszenia ochrony danych osobowych.

2. **Osoby których procedura dotyczy.**

Procedura dotyczy każdej osoby, niezależnie od podstawy prawnej współpracy z administratorem danych osobowych (Powszechną Spółdzielnią Mieszkaniowa „PRZYMORZE" w Gdańsku), która ma dostęp do danych osobowych lub stwierdzi naruszenie zasad ochrony danych osobowych.

3. **Definicje.**

a) administrator danych osobowych – Powszechna Spółdzielnia Mieszkaniowa „PRZYMORZE" z siedzibą w Gdańsku (80-365), przy ul. Czarny Dwór 12, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Gdańsk-Północ w Gdańsku, VII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000059746, e-mail: biuro.zao@przymorze.gda.pl, tel. 58 34612 57,

b) dane osobowe – 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 bądź społeczną tożsamość osoby fizycznej;

c) naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

d) organ nadzoru – Prezes Urzędu Ochrony Danych Osobowych (PUODO); Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa;

e) osoby decyzyjne administratora danych osobowych – członkowie zarządu lub prokurent;

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

4. **Sposób realizacji celu procedury.**

Cel procedury realizowany jest poprzez przyjęcie zasad postępowania na wypadek naruszenia ochrony danych osobowych.

5. **Postępowanie na wypadek naruszenia ochrony danych osobowych.**

a) osoba, która stwierdza naruszenie ochrony danych osobowych jest zobowiązana do niezwłocznego pisemnego (w tym e-mail) poinformowania osób decyzyjnych administratora danych osobowych, w szczególności podając rodzaj naruszenia oraz jego czas jego powstania oraz czas jego stwierdzenia;

b) osoby decyzyjne administratora danych osobowych (działając wspólnie) niezwłocznie zarządzają ustalenie charakteru naruszenia, jego możliwych konsekwencji, a także innych danych wymaganych do zgłoszenia naruszenia do organu nadzoru (pkt 4 lit. e) niniejszej Procedury), a po ich ustaleniu decydują o środkach naprawczych (np. zastosowaniu dodatkowych zabezpieczeń) mających na celu zaradzenie naruszeniu ochrony danych osobowych, w tym w stosownych

przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków; wzór protokołu stanowi załącznik A do niniejszej procedury;

c) osoby decyzyjne administratora danych osobowych (działając wspólnie) dokonują oceny prawdopodobieństwa czy naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, których dane dotyczą; wzór protokołu stanowi załącznik A do niniejszej procedury;

d) zgodnie z art. 33 ust. 1 RODO administrator danych osobowych bez zbędnej zwłoki – w miarę możliwości, nie później niż w ciągu 72 godzin od stwierdzenia naruszenia – zgłasza naruszenie organowi nadzoru, chyba że jest mało prawdopodobne by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W razie przekazania zgłoszenie po 72 godzinach, należy załączyć wyjaśnienie przyczyn opóźnienia.

e) zgłoszenie naruszenia ochrony danych osobowych do organu nadzoru powinno zawierać co najmniej (załącznik B do procedury):
   - opis charakteru naruszenia danych osobowych, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą oraz kategorię i przybliżoną liczbę wpisów danych osobowych, których naruszenie dotyczy;
   - zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych osobowych lub oznaczenie innego punktu kontaktowego od którego można uzyskać informację; w wypadku braku inspektora ochrony danych osobowych należy podać jako punkt kontaktowy osobę, która będzie w stanie podać organowi nadzoru informację dotyczącą naruszenia;
   - opis możliwych konsekwencji naruszenia ochrony danych osobowych;
   - opis środków zastosowanych lub proponowanych przez administratora danych osobowych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

f) administrator danych osobowych dokumentuje wszelkie naruszenia danych osobowych, w tym okoliczności naruszenia i jego skutki oraz podjęte działania zaradcze w sposób pozwalający organowi nadzoru na weryfikację przestrzegania art. 33 RODO. W związku z naruszeniem należy uzyskać i zachować co najmniej:
   - zawiadomienie osób decyzyjnych administratora danych osobowych o stwierdzonym naruszeniu (pkt 4 lit. a) niniejszej procedury),
   - protokół z którego będzie wynikało ustalenia okoliczności i środków, o których mowa w pkt 4 lit b) i c) niniejszej procedury, wzór protokołu stanowi załącznik A do niniejszej procedury;
   - zgłoszenie do organu nadzoru, wzór zgłoszenia stanowi załącznik B do niniejszej procedury,
   - zawiadomienie osoby, której dane dotyczą, o którym mowa w art. 34 RODO (jeżeli ma zastosowanie), wzór zawiadomienia stanowi załącznik C do niniejszej procedury;

g) zgodnie z art. 34 RODO, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator danych osobowych zawiadamia osobę (załącznik C do procedury), której dane dotyczą o takim naruszeniu, chyba że zachodzi jedna z poniższych okoliczności, wskazanych w art. 34 ust. 3 RODO:

- administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do danych osobowych,
- administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dotyczą,
- wymagałoby ono niewspółmiernie dużego wysiłku; w takim wypadku należy wydać publiczny komunikat lub zastosować podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

ZAŁĄCZNIK A – WZÓR PROTOKOŁU O KTÓRYM MOWA W PKT. 4 LIT. F) TIRET DRUGI PROCEDURY NA WYPADEK NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH.

Niniejszy protokół sporządza się w celu udokumentowania naruszenia ochrony danych osobowych, zgodnie z art. 33 ust. 5 RODO.

1) **Administrator danych osobowych**:

   Powszechna Spółdzielnia Mieszkaniowa „PRZYMORZE" z siedzibą w Gdańsku (80-365), przy ul. Czarny Dwór 12, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Gdańsk-Północ w Gdańsku, VII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000059746, e-mail: biuro.zao@przymorze.gda.pl, tel. 58 34612 57

2) **Data powstania naruszenia ochrony danych osobowych**:

   ……

3) **Data stwierdzenia naruszenia ochrony danych osobowych**:

   ……

4) **Naruszenie ochrony danych osobowych stwierdził(a)**:

   ……

5) **Charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą oraz kategorię i przybliżoną liczbę wpisów danych osobowych, których naruszenie dotyczy**:

   ……..

6) **Możliwe konsekwencje naruszenia ochrony danych osobowych:**

   ……..

7) **Środki zastosowane lub proponowane przez administratora danych osobowych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków:**

   ……..

8) **Ocena prawdopodobieństwa czy naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, których dane dotyczą:**

   ……..

Miejsce i data sporządzenia protokołu: Gdańsk, dnia……..

Podpisy i stanowiska osób biorących udział w powyższych czynnościach:

1) ……..
2) ……..
3) ……..
4) ……..

ZAŁĄCZNIK B – WZÓR ZGŁOSZENIA DO ORGANU NADZORU O KTÓRYM MOWA W PKT. 4 LIT. F) TIRET TRZECI PROCEDURY NA WYPADEK NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH.

Gdańsk, dnia……

Powszechna Spółdzielnia Mieszkaniowa „PRZYMORZE
ul. Czarny Dwór 12
80-365 Gdańsk
KRS: 0000059746
e-mail: biuro.zao@przymorze.gda.pl
tel. 58 34612 57

Prezes Urzędu Ochrony Danych Osobowych
Urząd Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

Zgłoszenie naruszenia ochrony danych osobowych w trybie art. 33 ust. 1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO)

Niniejszym na mocy art. 33 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), informujemy, że w dniu……miało miejsce zdarzenie stanowiące naruszenie ochrony danych osobowych, którego charakterystyka zostaje podana niżej.

1) Opis charakteru naruszenia danych osobowych, w tym kategoria i przybliżona liczba osób, których dane dotyczą oraz kategoria i przybliżona liczba wpisów danych osobowych, których naruszenie dotyczy:
   ……
2) Opis możliwych konsekwencji naruszenia ochrony danych osobowych:
   ……
3) Opis środków zastosowanych lub proponowanych przez administratora danych osobowych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków:
   ……

Informujemy, że u administratora danych został powołany inspektor ochrony danych osobowych,
tel. (58) 346-12-57 ; e-mail:iod.zao@przymorze.gda.pl

Gdańsk, dnia…… Podpis:

ZAŁĄCZNIK C – WZÓR ZAWIADOMIENIA OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH, O KTÓRYM MOWA W PKT. 4 LIT. F) TIRET CZWARTY PROCEDURY NA WYPADEK NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH.

Gdańsk, dnia……

Powszechna Spółdzielnia Mieszkaniowa „PRZYMORZE
ul. Czarny Dwór 12
80-365 Gdańsk
KRS: 0000059746
e-mail: biuro.zao@przymorze.gda.pl
tel. 58 34612 57

……
……
……
……

Zawiadomienie o naruszeniu ochrony danych osobowych w trybie art. 34 ust. 1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO)

Szanowny Panie / Pani,

Wykonując obowiązek prawny na mocy art. 34 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchyleniu dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych), niniejszym zawiadamiamy, że w dniu ……doszło do naruszenia ochrony danych osobowych polegającego na……

Mając na uwadze, że powyższe może skutkować……

administrator wdrożył następujące środki ochronne w celu zaradzenia naruszeniu oraz minimalizacji ewentualnych negatywnych skutków……

Osobą do kontaktu w sprawie jest:……tel……e-mail:……

Z poważaniem,