SmartMage Sp. z o.o.
ul. Światowida 2/52
45-325 Opole
NIP 7543167446
REGON: 369081082

POLITYKA BEZPIECZEŃSTWA INFORMACJI PRZETWARZANIA DANYCH OSOBOWYCH

I POSTANOWIENIA OGÓLNE

1. Niniejszy dokument został opracowany w oparciu o treść:

    a. przepisów 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;
    b. rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych;

    oraz określa zasady bezpieczeństwa przetwarzania danych osobowych osób fizycznych jakie powinny być przestrzegane i stosowane w SmartMage Sp. z o.o. (zwaną dalej Administratorem danych) przez pracowników i współpracowników, którzy przetwarzają dane osobowe.

2. Dane osobowe są przetwarzane przez firmę SmartMage Sp. z o.o. z poszanowaniem przepisów powyżej wskazanych aktów prawnych oraz wszelkich aktów wykonawczych związanych z powyżej wskazanymi źródłami prawa.

3. SmartMage Sp. z o.o. przetwarza dane osobowe w celu wykonania umów, której stroną jest osoba której dane dotyczą, lub podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.

4. Celem niniejszej Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie oraz zapewnienie optymalnego oraz zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w sklepie internetowym informacji zawierających dane osobowe, a nadto przyjęcie, wdrożenie i realizacja takich działań, które zapewniają maksymalny poziom bezpieczeństwa przetwarzania danych osobowych, chroniąc je przed nieautoryzowanym dostępem przez osoby nieuprawnione, utratą poufności, modyfikacją przez osoby nieuprawnione oraz służące zachowaniu ich integralności i rozliczalności.

5. Stosowanie zasad określonych w niniejszej Polityce Bezpieczeństwa ma na celu zapewnienie prawidłowej ochrony danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów Rozporządzenia, Ustawy oraz utratą, uszkodzeniem czy zniszczeniem.

6. Pracownicy firmy SmartMage Sp. z o.o. są odpowiedzialni za bezpieczeństwo danych, do których mają dostęp. W szczególności w systemie informatycznym odpowiadają oni za poprawne wprowadzenie informacji do systemu oraz użycie, zniszczenie lub uszkodzenie sprzętu raz z oprogramowaniem oraz znajdującymi się na nich danymi i oprogramowania.

7. Zarządzenie bezpieczeństwem zasobów danych osobowych stanowi proces ciągły, na który składają się taki elementy, jak:

    a) identyfikacja oraz analiza zagrożeń i ryzyka;

b) stosowanie odpowiednich zabezpieczeń;
c) monitorowanie wdrażania i eksploatacji zabezpieczeń;
d) wykrywanie i reagowanie na incydenty.

8. SmartMage Sp. z o.o. realizując politykę bezpieczeństwa w przedmiocie ochrony danych osobowych dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności, aby dane te były:
    a) przetwarzane zgodnie z prawem;
    b) merytorycznie poprawne i adekwatne w stosunku do celów, w jakim są przetwarzane;
    c) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnego z tymi celami;
    d) Przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej jednak niż jest to niezbędne do osiągnięcia celu przetwarzania.

II PODSTAWOWE POJĘCIA

Określenia użyte w niniejszej Polityce Bezpieczeństwa oznaczają:

1. **Administrator Danych Osobowych (ADO)** – osoba decydująca o celach i środkach przetwarzania danych osobowych;

2. **Administrator Bezpieczeństwa Informacji (ABI)** – osoba wyznaczona przez Administratora Danych Osobowych (ADO) do nadzoru przestrzegania zasad ochrony danych osobowych;

3. **Administrator Systemu Informatycznego (ASI)** – osoba wyznaczona przez Administratora Danych Osobowych (ADO) do nadzorowania i przestrzegania zasad ochrony danych osobowych w systemach informatycznych stosowanych do przetwarzania danych osobowych;

4. **Dane osobowe –** za dane osobowe zgodnie z treścią art. 4 pkt. 1) rozporządzenia 2016/679 uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba fizyczna, 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;

5. **Komórka organizacyjna –** zespół, dział, sekcja lub samodzielne stanowisko realizujące zadania określone w niniejszej Polityce Bezpieczeństwa;

6. **Identyfikator użytkownika –** nazwa, która w sposób jednoznaczny i transparentny identyfikuje użytkownika systemu informatycznego;

7. **Nośnik danych –** wszelkie nośniki, na których są zapisane informacje w postaci elektronicznej, w szczególności dyski twarde, dyskietki, dyski CD, DVD, karty magnetyczne lub pamięci przenośne;

8. **Odbiorca danych –** zgodnie z treścią art. 4 pkt. 9) rozporządzenia 2016/679 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 mającymi zastosowanie do celów przetwarzania;

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

10. **Ryzyko –** potencjalne straty, które można ponieść w zależności od prawdopodobieństwa wystąpienia straty. Straty mogą być zarówno materialne (tj. finansowe), jak i niematerialne (np. naruszenie dóbr osobistych).

11. **Rozporządzenie** - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

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

13. **Sieć lokalna** - połączenie systemów informatycznych ADO dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.

14. **System informatyczny** - jest to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

15. **Użytkownik**- osoba upoważniona do przetwarzania danych osobowych.

16. **Zbiór danych osobowych** - każdy posiadający strukturę logiczną zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

III BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1. Utrzymanie bezpieczeństwa przetwarzanych w SmartMage Sp. z o.o. informacji, a w szczególności danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności oraz rozliczalności na adekwatnym poziomie.

2. Przez poufność danych rozumie się właściwość zapewniającą, że dane nie są w żaden sposób udostępnianie nieupoważnionym i nieuprawnionym podmiotom.

3. Przez integralność danych rozumie się właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

4. Przez rozliczalność danych rozumie się właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

5. Zarządzanie bezpieczeństwem informacji jest związane z zapewnieniem:

    a. niezaprzeczalności odbioru rozumianej jako zdolności systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie;
    b. niezaprzeczalności nadania rozumianej jako zdolności systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie.

IV PODSTAWA PRAWNA

Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w:

1. Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 r. Nr 100 poz. 1024).
2. Rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych.
3. Rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 11maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.
4. Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

V ZAKRES ZASTOSOWANIA

Zasady określone przez niniejszy dokument mają zastosowanie do całego systemu przetwarzania danych, a w szczególności do:

1. Wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz będących w formie papierowej w których przetwarzane są lub będą dane osobowe.
2. Informacji będących własnością ADO lub jednostek obsługiwanych, o ile zostały przekazane na podstawie umów lub porozumień.
3. Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych oraz innych dokumentów zawierających dane osobowe.
4. Wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się dane osobowe podlegające ochronie.
5. Wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.
6. Wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

VI STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA

1. Dokumenty Polityki Bezpieczeństwa ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Zestaw dokumentów Polityki Bezpieczeństwa składa się z:
2.1. Niniejszego dokumentu Polityki Bezpieczeństwa.
2.2. Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych – Załącznik nr 1
2.3. Wykazu zbiorów danych osobowych wraz z ich strukturą, w których przetwarzane są dane osobowe - Załącznik nr 2
2.4. Wykazu miejsc tworzących obszar, w którym przetwarzane są dane osobowe - Załącznik nr 3
2.5. Wzorcowego oświadczenia pracownika do przetwarzania danych osobowych - Załącznik nr 4
2.6. Wzorcowego upoważnienia dla pracownika do przetwarzania danych osobowych Załącznik nr 5
2.7. Wzorcowej ewidencji osób upoważnionych do przetwarzania danych osobowych Załącznik nr 6
2.8. Procedury postępowania na wypadek zaistnienia incydentu związanego z przetwarzaniem danych osobowych - Załącznik nr 7
2.9. Wzorcowej umowy powierzenia danych osobowych podmiotowi zewnętrznemu – Załącznik nr 8.
2.10. Wzorcowej ewidencji udostępniania danych osobowych- Załącznik nr 9

VII ODPOWIEDZIALNOŚĆ I KOMPETENCJE W ZARZĄDZANIU BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

1. Za przetwarzanie danych osobowych niezgodnie z prawem, z powierzonymi celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą, grozi odpowiedzialność karna wynikająca z przepisów Ustawy lub pracownicza na zasadach określonych w Kodeksie pracy.

2. Do zadań ADO należy:

a. Zapewnienie środków technicznych i organizacyjnych do ochrony przetwarzanych danych osobowych, odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, w szczególności zabezpieczeniem danych przed:

- Udostępnieniem osobom nieupoważnionym.
- Zabraniem przez osobę nieuprawnioną.
- Zmianą, utratą, uszkodzeniem lub zniszczeniem.

b. Zapewnienie legalności przetwarzania danych osobowych, a w szczególności zadbanie, by:

- Została pozyskana zgoda osoby, której dane dotyczą lub została spełniona inna przesłanka dopuszczająca przetwarzanie danych osobowych.
- Został spełniony obowiązek informacyjny wobec osoby, której dane dotyczą.
- Dane były przetwarzane zgodnie z obowiązującymi przepisami prawa oraz normami i dobrymi praktykami oraz normami społecznymi.
- Dane zbierane były w oznaczonym zgodnym z prawem celem.
- Dane były merytorycznie poprawne oraz zakres danych był adekwatny do celu zbierania.
- Były przetwarzane z ograniczeniem czasowym

c. Wyznaczenie Administratora Bezpieczeństwa Informacji,

d. Dopuszczanie do przetwarzania danych wyłącznie osoby zaznajomionej z przepisami z zakresu ochrony danych osobowych i posiadającej imienne upoważnienie, oraz wydawanie i zarządzanie upoważnieniami.

e. Nadzorowanie i dbanie o zgodne z prawem przekazywanie danych osobowych (udostępnianie i powierzanie).

f. Respektowanie prawa osób, których dane dotyczą, a w szczególności prawa do uzyskania informacji o:

- ADO.
- Celu, zakresie i sposobie przetwarzania danych.
- Terminu od kiedy i jakie dane są przetwarzane.
- Źródle, z którego dane pochodzą.

- Sposobie udostępniania danych oraz ich odbiorcach.

3. Do zadań ASI należy:

a. Przestrzeganie zasad ochrony danych osobowych określonych w "Polityce bezpieczeństwa danych osobowych" oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych i dokumentach z nimi związanych.

b. Zapewnienie prawidłowej eksploatacji systemu informatycznego, zgodnej z celami przetwarzania danych osobowych.

c. Nadzorowanie wykonywania kopii zapasowych, odpowiedniego ich przechowywania oraz okresowego sprawdzania pod kątem ich dalszej przydatności do odtwarzania danych osobowych w przypadku awarii systemu.

d. Zapewnienie ochrony nośników zawierających kopie zbiorów danych osobowych.

e. Realizację wytycznych ADO w zakresie ochrony danych osobowych przetwarzanych z wykorzystaniem środków informatycznych.

f. Wyjaśnianie wszystkich zgłoszonych nieprawidłowości i incydentów.

4. Do zadań każdego Pracownika i/lub współpracownika należy:

a. Zapoznanie się z zasadami określonymi w niniejszej Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym. Pracownik potwierdza swoją znajomość Polityki przez podpisanie oświadczenia o zapoznaniu się z Polityką.

b. Przestrzeganie zasad określonych w niniejszej Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.

c. Ochrona prawa do prywatności osób fizycznych powierzających swoje dane osobowe, poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w polityce bezpieczeństwa i Instrukcji Zarządzania Systemem informatycznym

VIII OBOWIĄZEK INFORMACYJNY

1. W przypadku zbierania danych osobowych na formularzach, umowach, drukach (zarówno papierowych jak i elektronicznych) należy umieszczać na nich odpowiednie klauzule informacyjnej. Klauzula taka powinna informować osobę, której dane zbieramy o:

1.1. Adresie siedziby i pełnej nazwie ADO.

1.2. Celu zbierania danych.

1.3. Prawie dostępu do treści swoich danych oraz ich poprawiania.

1.4. Dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej oraz zgodnie z regulacjami określonymi w RODO:

1.5. Informacji o profilowaniu (bądź nie) przetwarzanych danych osobowych.

1.6. Prawie do przenoszenia przetwarzanych przez ADO danych osobowych.

1.7. Prawie do sprzeciwu, ograniczeniu przetwarzanych danych osobowych.

1.8. Prawie do bycia zapomnianym.

2. Postanowienia wskazanego w pkt. 1 niniejszego działu nie stosuje się, jeżeli:

2.1. Przepis prawa powszechnie obowiązującego zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania.

2.2. Osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1

3. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, ADO jest zobowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

3.1. Adresie siedziby i pełnej nazwie ADO.

3.2. Celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych.

3.3. Źródle danych.

3.4. Prawie dostępu do treści swoich danych oraz ich poprawiania.

3.5. Prawie do sprzeciwu, ograniczeniu przetwarzanych danych osobowych.

3.6. Prawie do bycia zapomnianym.

IX DOSTĘP DO INFORMACJI

1. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w zasad ochrony danych osobowych określonych niniejszym dokumentem.
2. Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.
3. Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, powinno odbywać się wg określonych odrębnymi przepisami procedur postępowania.
4. Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z przepisami powszechnie obowiązującego prawa w zakresie ochrony danych osobowych oraz zasadami zawartymi w obowiązującej w Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.

X POWIERZANIE DANYCH OSOBOWYCH

1. ADO może powierzyć przetwarzanie danych osobowych innemu podmiotowi na podstawie umowy powierzenia zawartej na piśmie, z zastrzeżeniem wyjątków wynikających z przepisów powszechnie obowiązującego prawa.
2. Przekazanie zbiorów podmiotowi zewnętrznemu w celu ich przetwarzania nie powoduje zmiany właściwego ADO.
3. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych zobowiązany jest wykorzystywać powierzone mu dane wyłącznie w celach i w zakresie, które zostały wskazane w zawartej z nim umowie.
4. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych obowiązany jest w szczególności do:
   4.1. Stosowania odpowiednich środków ochrony danych osobowych, w tym do zapewnienia fizycznej ochrony pomieszczeń w których przetwarzane są dane oraz tworzenia kopii bezpieczeństwa systemów informatycznych, w których przetwarzane są powierzone dane osobowe.
   4.2. Opracowania dokumentacji dotyczącej przetwarzania danych osobowych.
   4.3. Niezwłocznego powiadomienia SmartMage Sp. z o.o. o przypadkach naruszenia przetwarzania powierzonych danych osobowych oraz do dokumentowania wszelkich informacji, które mogą pomóc w ustaleniu okoliczności tego naruszenia.
   4.4. Zapewnienia, aby każda osoba stanowiąca personel podmiotu zewnętrznego przetwarzająca powierzone dane osobowe posiadała upoważnienie do przetwarzania tych danych osobowych.
   4.5. Zniszczenia lub zwrotu przekazanych danych stosownie do zapisów umowy powierzenia przetwarzania danych.
5. Wzór umowy powierzenia danych osobowych do przetwarzania podmiotowi zewnętrznemu stanowi Załącznik nr 8.

XI UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Udostępnianie danych osobowych odbiorcom danych może nastąpić, podobnie jak przetwarzanie danych, w przypadku spełnienia jednej z poniżej wskazanych przesłanek:
   1.1. Osoba, której dane dotyczą, wyrazi na to zgodę.

   1.2. Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
   1.3. Jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.
   1.4. Jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.
   1.5. Jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych

   przez odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.
2. Osoby upoważnione do przetwarzania danych, którzy w ramach swych obowiązków służbowych udostępniają dane osobowe mają obowiązek prowadzić ewidencję danych, które są udostępniane (określającą odbiorcę danych, przyczynę udostępnienia, zakres danych oraz datę udostępnienia).
3. Wzór ewidencji określonej w pkt. 2 niniejszego działu stanowi Załącznik nr 9.

XII ANALIZA RYZYKA ZWIĄZANEGO Z PRZETWARZANIEM DANYCH OSOBOWYCH

Identyfikacja zagrożeń:

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA
Dane przetwarzane w sposób tradycyjny (papierowe)	• Oszustwo. • Kradzież. • Sabotaż. • Zdarzenia losowe (powódź, pożar, zawalenie budynku itd). • Zaniedbania pracowników (niedyskrecja, przypadkowe/celowe udostępnienie danych osobie nieupoważnionej). • Niekontrolowana obecność osób nieupoważnionych w obszarze przetwarzania danych; pokonanie zabezpieczeń fizycznych. • Podsłuchy, podglądy; atak terrorystyczny. • Brak rejestrowania udostępniania danych. • Niewłaściwe miejsce i sposób przechowywania dokumentacji.

Dane przetwarzane w systemach informatycznych	• Wadliwe zarządzanie systemem identyfikatorów. • Niewłaściwa administracja systemem. • Niewłaściwa konfiguracja systemu. • Zniszczenie (sfałszowanie) kont użytkowników. • Kradzież danych kont. • Pokonanie zabezpieczeń programowych. • Zaniedbanie pracowników (niedyskrecja, udostępnianie danych osobom nieupoważnionym). • Niekontrolowana obecność nieuprawnionych osób. • Zdarzenia losowe (powódź, pożar). • Niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania za pomocą nośników informacji i komputerów przenośnych. • Naprawy i konserwacja systemu lub sieci teleinformatycznej wykonane przez osoby nieuprawnione; przypadkowe lub celowe uszkodzenie systemów i aplikacji informatycznych lub sieci. ! Przypadkowe lub celowe wprowadzanie zmian do chronionych danych osobowych; brak rejestrowania zdarzeń, tworzenia lub modyfikowania danych.

Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych stosuje się wysoki poziom bezpieczeństwa. Okresowo należy przeprowadzić analizę ryzyka dla poszczególnych systemów i na tej podstawie określa środki techniczne i organizacyjne, celem zapewnienia właściwej ochrony przetwarzanym danym.

XIII ZABEZPIECZENIE PRZETWARZANYCH DANYCH OSOBOWYCH

W SmartMage Sp. z o.o. należy stosować następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:

1.1. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane na klucz i kategorycznie nie mogą pozostawać otwarte bez opieki właściwego personelu.

1.2. Pomieszczenia, w których przetwarzane są dane osobowe zlokalizowane w miejscach zabezpieczonych przed ingerencją osób nieupoważnionych.

2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:

2.1. Przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach.

2.2. Przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby, osoby nieupoważnione nie mogą mieć bezpośredniego dostępu do tych pomieszczeń.

3. Zabezpieczenia organizacyjne:

3.1. Osoby bezpośrednio odpowiedzialne za bezpieczeństwo danych na bieżąco kontrolują z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami, pracę pracowników odpowiedzialnych za przetwarzanie danych osobowych oraz systemu informatycznego.

3.2. Winny być regularnie prowadzone przez ADO kontrole stanu bezpieczeństwa systemów informatycznych i przestrzegania zasad ochrony informacji.

4. Zabezpieczenia informatyczne.

4.1. Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w Instrukcji Zarządzania Systemem Informatycznym, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego.

4.2. Ochronę danych osobowych należy realizować z wykorzystaniem następujących minimalnych zabezpieczeń:

4.2.1. Przyznawania indywidualnych identyfikatorów.

4.2.2. Zapewnienie stopniowania uprawnień.

4.2.3. Zapewnienia wymuszania zmiany haseł.

4.2.4. Odnotowania daty pierwszego wprowadzenia danych w systemie.

4.2.5. Odnotowania identyfikatora użytkownika wprowadzającego dane.

4.2.6. Odnotowania źródła danych, w przypadku zbierania danych nie od osoby, której dane dotyczą.

4.2.7. Odnotowania informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia.

4.2.8. Zapewnienie możliwości sporządzenia i wydrukowania raportu zawierającego dane osobowe wraz z informacjami o historii przetwarzania danych.

5. W ramach zabezpieczenia danych osobowych ochronie podlegają:

5.1. Sprzęt komputerowy- serwer, komputery osobiste, drukarki i inne urządzenia zewnętrzne.

5.2. Oprogramowanie - kody źródłowe, programy użytkowe, systemy operacyjne, narzędzia wspomagające i programy komunikacyjne.

5.3. Dane zapisane na dyskach oraz dane podlegające przetwarzaniu w systemie.

5.4. Hasła użytkowników.

5.5. Pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa.

5.6. Dokumentacja - zawierająca dane systemu, opisująca jego zastosowanie, przetwarzane informacje.

5.7. Związana z przetwarzaniem danych osobowych dokumentacja papierowa, z której dane są wprowadzane do systemu informatycznego lub też funkcjonująca niezależnie od niego.

XIII ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

1. Archiwizację dokumentów zawierających dane osobowe prowadzi się w odpowiednio zabezpieczonych pomieszczeniach i na właściwie zabezpieczonych nośnikach informatycznych lub tradycyjnych.
2. Dane zbędne dla prowadzonych spraw są natychmiast niszczone poprzez działania fizyczne i informatyczne uniemożliwiające ich odczytanie.

XIV POSTANOWIENIA KOŃCOWE

1. Wszyscy pracownicy i współpracownicy przetwarzający dane osobowe zobowiązani są do zapoznania się z treścią niniejszej polityki.
2. Polityka bezpieczeństwa wchodzi w życie z dniem podpisania.
3. Jakiekolwiek zmiany wprowadzane w załącznikach do niniejszej polityki nie wymagają zmiany polityki.