Załącznik nr 6 do zapytania ofertowego
Znak sprawy: MAMMO/ZO/S/2024

UMOWA POWIERZENIA PRZETWARZANIA
DANYCH OSOBOWYCH

zawarta w……, w dniu …… r. (dalej jako „Umowa Powierzenia"), pomiędzy:
SALVE Spółka z ograniczoną odpowiedzialnością Spółka komandytowa
ul. Andrzeja Struga 3, 90-420 Łódź

reprezentowany przez:
Agnieszkę Sobkiewicz – Członka Zarządu Komplementariusza

zwanym dalej „**ADO"**

a

…… z siedzibą w ….., przy ul. …, KRS …. NIP … zwanym dalej „**Procesorem**"**,** reprezentowanym przez

1. ……,
2. …….

zwanymi dalej z osobna „**Stroną**" lub łącznie „**Stronami**"

o następującej treści:

W związku z zawarciem w dniu …… umowy nr …….. (Umowa Zasadnicza), której przedmiotem jest:

a) sprzedaż przez Wykonawcę Zamawiającemu 1 (jednego) cyfrowego aparatu mammograficznego (zwanego również dalej „sprzętem medycznym") dla wczesnego wykrywania nowotworów w ramach ***programu wieloletniego pn.: „Narodowa Strategia Onkologiczna";***
b) dostarczenie sprzętu medycznego do Zamawiającego oraz wniesienie do wskazanej przez Zamawiającego lokalizacji, instalacja sprzętu medycznego, uruchomienie całości systemu, przeprowadzenie procedury kalibracji, wykonanie kontroli jakości zestawu, testów akceptacyjnych i specjalistycznych, przeprowadzenie szkolenia i instruktażu stanowiskowego
w zakresie obsługi sprzętu medycznego personelu, wskazanego przez Zamawiającego;
c) demontażu i utylizacji posiadanego mammografu oraz dostarczenia dokumentów potwierdzających wykonanie utylizacji.

Strony postanawiają, co następuje:

Przedmiot Umowy Powierzenia
§ 1.

1. ADO zgodnie z art. 28 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), zwanego dalej „RODO", powierza Procesorowi przetwarzanie

danych osobowych, wyłącznie w zakresie i celu określonym Umową Zasadniczą i poleca Procesorowi ich przetwarzanie.

2. Procesor zobowiązuje się przetwarzać powierzone dane osobowe zgodnie z Umową Powierzenia, RODO oraz innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Strony postanawiają, że Procesor będzie przetwarzał powierzone dane osobowe wyłącznie na terytorium państw członkowskich Unii Europejskiej.

Zakres i cel przetwarzania

§ 2.

1. Powierzone dane osobowe dotyczą następujących kategorii osób: ……..……
2. ADO powierza Procesorowi przetwarzanie danych osobowych, w zakresie określonym w załączniku do Umowy Powierzenia - zał. nr 1 Rodzaj Danych.

Obowiązki Procesora

§ 3.

1. Procesor jest obowiązany wdrożyć odpowiednie środki techniczne i organizacyjne w celu zapewnienia odpowiedniego stopnia bezpieczeństwa powierzonych danych osobowych, odpowiadającego ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zgodnie z art. 32, w związku z art. 28 ust. 3 lit. c RODO.
2. W szczególności Procesor zobowiązany jest zagwarantować:
   1) prowadzenie dokumentacji w zakresie ochrony danych osobowych, o której mowa w art. 24 ust. 2 RODO, określającej, w szczególności środki techniczne i organizacyjne, służące zapewnieniu ochrony i bezpieczeństwa przetwarzanych danych osobowych, o których mowa w art. 32 RODO;
   2) posiadanie i przestrzeganie procedur w zakresie zgłaszania naruszeń ochrony danych osobowych, zapewniających prawidłową realizację obowiązków, o których mowa w ust. 6;
   3) przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo powierzonych danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, modyfikacją, zniszczeniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem;
   4) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, w szczególności poprzez wprowadzenia polityki haseł i loginów;
   5) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego (jak najszybsze przywrócenie możliwości dostępu do danych osobom upoważnionym, jak również przywrócenie im możliwości dokonywania operacji na danych);
   6) przetwarzanie w sposób zapewniający odporność systemów informatycznych służących do przetwarzania danych przed działalnością złośliwego oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych;
   7) wdrożenie mechanizmów wykrywania naruszeń bezpieczeństwa powierzonych danych osobowych;
   8) wprowadzenie środków ochrony fizycznej w miejscu przetwarzania danych osobowych - siedzibie Procesora, w postaci:
   a) ochrony budynku, gdzie przetwarzane będą dane osobowe;
   b) kontroli dostępu do budynku i pomieszczeń, gdzie przetwarzane będą dane osobowe;

9) zabezpieczenia sprzętu, infrastruktury teleinformatycznej w zakresie integralności i poufności, poprzez:
   a) zapewnienie bezpieczeństwa sieci komputerowej – ochrona, nadzór, monitoring,
   b) monitorowanie i nadzór nad usługami teleinformatycznymi – monitorowanie zdarzeń, ochrona integralności, ocena logów systemu, prowadzenie i weryfikację dzienników zdarzeń,
   c) ochronę przed szkodliwym kodem, w tym ochrona antywirusowa,
   d) zarządzenie nośnikami danych i urządzeniami mobilnymi – ochrona danych, zapewnienie stosownego poziomu bezpieczeństwa,
   e) zabezpieczenia stacji roboczych, na których przetwarzane są dane osobowe tak, by eliminować ryzyko nieuprawnionego dostępu: bezpieczne hasła, zabezpieczenia kryptograficzne, polityka haseł, pełna rozliczalność użytkowników,
   f) okresową zmianę haseł.

3. Procesor oświadcza, że stosowane przez niego środki ochrony powierzonych danych osobowych są zgodne z przepisami RODO i zapewniają stopień bezpieczeństwa odpowiedni do ryzyka związanego z naruszeniem praw lub wolności osób, których dane dotyczą. Szczegółowy wykaz środków ochrony (technicznych i organizacyjnych), które zapewnia Procesor, stanowi załącznik nr 2 do Umowy Powierzenia. Ponadto Procesor niezwłocznie, nie później niż w terminie 7 dni od wystąpienia zmian, poinformuje ADO o wszelkich zmianach, które zaistnieją w obszarze zapewnionych środków ochrony.
4. Procesor zobowiązuje się nie wykorzystywać powierzonych danych osobowych w celach innych niż wyraźnie wskazane w Umowie Zasadniczej. Procesor zobowiązuje się ponadto, w tym również po ustaniu Umowy Powierzenia, nie ujawniać osobom nieupoważnionym informacji o powierzonych danych osobowych, zwłaszcza o środkach ochrony i zabezpieczeniach danych osobowych stosowanych przez niego lub ADO.
5. Procesor zobowiązuje się do udzielania ADO, na każde jego żądanie, wszelkich informacji na temat przetwarzania powierzonych danych osobowych, w szczególności informacji niezbędnych do wykazania spełnienia obowiązków spoczywających na Procesorze, w tym obowiązków określonych w art. 28 RODO.
6. Procesor, biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga ADO poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w Rozdziale III RODO.
7. Procesor pomaga ADO wywiązać się z obowiązków określonych w art. 32-36 RODO, uwzględniając charakter przetwarzania oraz dostępne mu informacje.
8. Procesor zobowiązuje się do niezwłocznego poinformowania ADO o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Procesora powierzonych danych osobowych, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych skierowanym do Procesora, a także o planowanych, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania powierzonych danych osobowych, w szczególności prowadzonych przez Urząd Ochrony Danych Osobowych.
9. Procesor bez zbędnej zwłoki zgłosi ADO, nie później jednak niż w ciągu 24 godzin od stwierdzenia naruszenia, każdy przypadek naruszenia ochrony danych osobowych, o którym mowa w art.4 pkt 12 RODO, które dotyczy powierzonych danych. Zgłoszenie powinno zostać dokonane w formie wiadomości e-mail wysłanej do Inspektora Ochrony Danych, którego powołał ADO na adres: iod@salvemedica.pl oraz osobie upoważnionej do współpracy w ramach wykonywanej umowy ze strony ADO tj.: ……tel:…….
10. W zgłoszeniu Procesor jest zobowiązany opisać co najmniej charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą, możliwe konsekwencje naruszenia ochrony danych oraz opisać środki

zastosowane lub proponowane przez Procesora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków. W przypadku, gdy stwierdzone naruszenie może powodować wysokie ryzyko naruszania praw lub wolności osób fizycznych Procesor jest zobowiązany do uczestniczenia, w zakresie określonym przez ADO, w zawiadomieniu osób, których dane dotyczą, o takim naruszeniu.

11. Procesor zobowiązany jest niezwłocznie zastosować się do zaleceń ADO, dotyczących przetwarzania powierzonych danych osobowych, zwłaszcza dotyczących ich zabezpieczenia.
12. Procesor prowadzi rejestr kategorii czynności przetwarzania dokonywanych w imieniu ADO, zawierający informacje określone w art. 30 ust. 2 RODO oraz zobowiązuje się udostępnić rejestr na każde żądanie ADO.
13. Procesor niezwłocznie przekaże ADO kontakt do wyznaczonego przez siebie inspektora ochrony danych, a w przypadku gdy inspektor ochrony danych nie został wyznaczony, Procesor jest zobowiązany do przekazania danych kontaktowych do innej osoby koordynującej u Procesora zadania z zakresu ochrony danych osobowych.

§ 4.

1. Procesor ograniczy dostęp do powierzonych do przetwarzania danych osobowych wyłącznie do osób, które posiadają imienne upoważnienie do przetwarzania powierzonych do przetwarzania danych osobowych.
2. ADO umocowuje Procesora do wydawania i odwoływania osobom, o których mowa w ust. 1, upoważnień do przetwarzania danych osobowych, powierzonych na podstawie § 1 ust. 1, w zakresie i celu niezbędnym do wykonania przedmiotu Umowy Zasadniczej.
3. Procesor zapewni prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.
4. Procesor oświadcza, że osoby upoważnione do przetwarzania danych osobowych, zgodnie z ust. 1, przed przystąpieniem do przetwarzania danych osobowych powierzonych przez ADO zostaną przeszkolone z zakresu ochrony danych osobowych oraz zostaną zobowiązane do stosowania przepisów prawa z zakresu ochrony danych osobowych, w szczególności RODO, oraz procedur ochrony danych obowiązujących u Procesora.
5. Procesor zobowiąże osoby, upoważnione do przetwarzania powierzonych do przetwarzania danych osobowych, do dochowania należytej staranności w zakresie odnoszącym się do ochrony danych osobowych oraz przestrzegania następujących zasad postępowania z powierzonymi danymi osobowymi:

1) świadczenia pracy jedynie przy użyciu danych osobowych, niezbędnych do wykonania obowiązków wynikających z Umowy Zasadniczej;
2) przechowywania danych osobowych w czasie nie dłuższym niż czas niezbędny do zrealizowania zadań, do których wykonania dane są przeznaczone;
3) nietworzenia kopii danych osobowych innych niż niezbędne do realizacji Umowy Zasadniczej;
4) zachowania w tajemnicy, o której mowa w art. 28 ust. 3 lit. b RODO, powierzonych do przetwarzania danych osobowych zarówno w trakcie trwania stosunku prawnego łączącego pracownika z Procesorem, jak i po jego ustaniu;
5) zabezpieczenia i ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem, o których mowa w art.4 pkt.12 RODO

6. Procesor będzie stale nadzorował pracowników upoważnionych do przetwarzania powierzonych do przetwarzania danych osobowych - w zakresie zabezpieczenia przetwarzania danych osobowych.

§ 5.

Powierzenie danych osobowych podmiotom trzecim

1. Wyłącznie w celu określonym w Umowie Zasadniczej, Procesor może w zakresie przetwarzania powierzonych do przetwarzania danych osobowych korzystać z usług innego podmiotu przetwarzającego, pod warunkiem, że Procesor zawrze na piśmie z tym podmiotem umowę powierzenia przetwarzania danych osobowych, zobowiązującą do stosowania tych samych obowiązków ochrony danych osobowych, które zostały nałożone na Procesora niniejszą umową Powierzenia
2. Procesor informuje ADO o zamiarze korzystania z usług innego podmiotu przetwarzającego dane osobowe, w celu realizacji Umowy zasadniczej. Procesor przedstawia projekt umowy w zakresie przetwarzania danych osobowych z innym podmiotem. ADO może w ciągu 7 dni roboczych od otrzymania danej informacji zgłosić sprzeciw, który skutkuje brakiem możliwości zawarcia umowy powierzenia przetwarzania danych z innym podmiotem. Procesor zobowiązuje się do przekazania ADO w terminie 5 dni roboczych kopii zawartej z podmiotem trzecim umowy.
3. Procesor ponosi pełną odpowiedzialność wobec ADO za niewywiązywanie się ze spoczywających na innym podmiocie przetwarzającym obowiązków ochrony danych.

§ 6.

Prawo kontroli

1. Procesor umożliwi ADO lub podmiotowi przez niego upoważnionemu, przeprowadzenie kontroli w zakresie niezbędnym dla sprawdzenia, czy środki zastosowane przez Procesora przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych, spełniają postanowienia Umowy Powierzenia.
2. ADO może realizować prawo kontroli w miejscu przetwarzania powierzonych danych osobowych – siedzibie Procesora, w godzinach pracy Procesora z minimum 5-dniowym jego uprzedzeniem, z zastrzeżeniem ust. 3.
3. W przypadku powzięcia przez ADO wiadomości o naruszeniu ochrony danych powierzonych, o których mowa w art.4 pkt.12 RODO, Procesor umożliwi ADO lub podmiotowi przez niego upoważnionemu dokonanie niezapowiedzianej kontroli, w celu sprawdzenia prawidłowości przetwarzania oraz zabezpieczenia powierzonych do przetwarzania danych osobowych.
4. W ramach kontroli ADO lub podmiot przez niego upoważniony mają w szczególności prawo wglądu do wszelkich dokumentów, dotyczących ochrony danych osobowych, mających bezpośredni związek z przedmiotem kontroli, przeprowadzenia oględzin urządzeń, nośników oraz systemu informatycznego, służącego do przetwarzania powierzonych do przetwarzania danych osobowych, a także prawo do żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego.
5. Procesor jest zobowiązany do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez ADO.
6. ADO zastrzega sobie prawo do dokonania kontroli przetwarzania danych osobowych powierzonych do dalszego przetwarzania na podstawie § 5.
7. Procesor zobowiąże podmioty, o których mowa w § 5 ust. 1, do zastosowania się do zaleceń sporządzonych w wyniku kontroli - w celu zapewnienia zgodności przetwarzania powierzonych do przetwarzania danych osobowych z RODO lub Umową Powierzenia, a tym samym poprawy jakości ich zabezpieczenia i sposobu przetwarzania.
8.

§ 7.

Usunięcie danych osobowych

1. Procesor po zakończeniu świadczenia usług związanych z przetwarzaniem, zobowiązuje się do zwrotu lub trwałego i nieodwracalnego usunięcia powierzonych do przetwarzania danych osobowych oraz usunięcia wszelkich kopii tych danych ze wszystkich nośników będących w posiadaniu Procesora i podmiotów, o których mowa w § 5, chyba że dalsze przetwarzanie danych osobowych przez Procesora będzie miało swoje podstawy w przepisach prawa. ADO informuje Procesora o podjętej decyzji dotyczącej

usunięcia lub zwrócenia danych w formie pisemnej, przed planowanym terminem zakończenia świadczenia usług związanych z przetwarzaniem.
2. W przypadku zaistnienia okoliczności stanowiących podstawę do wypowiedzenia przez ADO Umowy zasadniczej, ADO informuje Procesora o podjętej decyzji dotyczącej usunięcia lub zwrócenia danych wraz z dokonaniem wypowiedzenia.
3. Zwrot bądź usuniecie powierzonych do przetwarzania danych osobowych zostanie potwierdzone, na żądanie ADO, stosownym protokołem.

§ 8.
Czas trwania Umowy Powierzenia

1. Umowa Powierzenia wchodzi w życie w dniu jej zawarcia.
2. Umowa Powierzenia zostaje zawarta na czas obowiązywania zawartej przez Strony Umowy Zasadniczej.

§ 9.
Postanowienia końcowe

1. Procesor ponosi odpowiedzialność wobec ADO lub osób trzecich za szkody powstałe w związku z nieprzestrzeganiem przepisów RODO, jak również za przetwarzanie powierzonych do przetwarzania danych osobowych niezgodnie z Umową Powierzenia, na zasadach określonych w art. 82 RODO i w ustawie z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2020 r. poz. 1740).
2. Zmiana Umowy Powierzenia wymaga zachowania formy pisemnej pod rygorem nieważności.
3. W sprawach nieuregulowanych Umową Powierzenia zastosowanie będą miały przepisy Kodeksu cywilnego oraz RODO.
4. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach – jeden egzemplarz dla ADO oraz jeden egzemplarz dla Procesora.
5. Integralną część Umowy Powierzenia stanowią:
   1) załącznik nr 1: Rodzaj Danych osobowych;
   2) załącznik nr 2: Szczegółowy wykaz środków ochrony (technicznych i organizacyjnych), umożliwiających należyte zabezpieczenie danych osobowych.

ADO Procesor

Załącznik nr 1
do Umowy Powierzenia Przetwarzania Danych Osobowych

Szczegółowy wykaz rodzajów przetwarzanych danych osobowych

Kategorie danych osobowych	Kategorie osób

Załącznik nr 2
do Umowy Powierzenia Przetwarzania Danych Osobowych

Szczegółowy wykaz środków ochrony (technicznych i organizacyjnych)

(właściwe ☐ zaznaczyć znakiem „X")

☐ został wyznaczony inspektor ochrony danych osobowych lub inna osoba nadzorująca przestrzeganie zasad ochrony przetwarzanych danych osobowych, należy podać dane kontaktowe (imię i nazwisko, numer telefonu oraz adres poczty elektronicznej):
……
……

☐ do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie w przedmiotowym zakresie,
☐ prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,
☐ została opracowana i wdrożona dokumentacja w zakresie ochrony danych osobowych, spełniająca wymagania określone dla środków organizacyjnych, o których mowa w art. 24 ust. 2 RODO; należy ją wyszczególnić poniżej:
……
……

Środki ochrony fizycznej danych		
W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do fizycznego zabezpieczenia przetwarzanych danych osobowych.		
1	☐	Dane osobowe przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
2	☐	Dane osobowe przechowywane są w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min.
3	☐	Dane osobowe przechowywane są w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.
4	☐	Dane osobowe przechowywane są w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
5	☐	Pomieszczenia, w których przetwarzane są dane osobowe, wyposażone są w system alarmowy przeciwwłamaniowy.
6	☐	Dostęp do pomieszczeń, w których przetwarzany są dane osobowe, objęte są systemem kontroli dostępu.
7	☐	Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
8	☐	Dostęp do pomieszczeń, w których przetwarzany są dane osobowe jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.
9	☐	Dostęp do pomieszczeń, w których przetwarzany są dane osobowe, przez całą dobę jest nadzorowany przez służbę ochrony.

10	☐	Dane osobowe w formie papierowej przechowywane są w zamkniętej niemetalowej szafie.
11	☐	Dane osobowe w formie papierowej przechowywane są w zamkniętej metalowej szafie.
12	☐	Dane osobowe w formie papierowej przechowywane są w zamkniętym sejfie lub kasie pancernej.
13	☐	Kopie zapasowe / archiwalne danych osobowych przechowywane są w zamkniętej niemetalowej szafie.
14	☐	Kopie zapasowe / archiwalne danych osobowych przechowywane są w zamkniętej metalowej szafie.
15	☐	Kopie zapasowe / archiwalne danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej.
16	☐	Dane osobowe przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach.
17	☐	Pomieszczenie, w którym przetwarzany jest są dane osobowe, zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i / lub wolnostojącej gaśnicy.
18	☐	Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej		
W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do: ✓ technicznych środków zabezpieczenia komputerów przed skutkami awarii zasilania, ✓ opisu infrastruktury sieci informatycznej, w której użytkowane są komputery wykorzystywane do przetwarzania danych osobowych, ✓ sprzętowych i programowych środków ochrony przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji, ✓ sprzętowych i programowych środków ochrony poufności danych przesyłanych drogą elektroniczną (środków ochrony transmisji), ✓ sprzętowych i programowych środków ochrony przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych.		
1	☐	Dane osobowe przetwarzane są przy użyciu komputera przenośnego.
2	☐	Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.
3	☐	Zastosowano urządzenia typu UPS, generator prądu i / lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
4	☐	Dostęp do danych osobowych, które przetwarzane są na wydzielonej stacji komputerowej / komputerze przenośnym, zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.
5	☐	Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

6	☐	Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena.
7	☐	Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej.
8	☐	Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
9	☐	Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
10	☐	Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
11	☐	Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
12	☐	Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
13	☐	Zastosowano procedurę oddzwonienia (callback) przy transmisji realizowanej za pośrednictwem modemu.
14	☐	Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
15	☐	Zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity.
16	☐	Użyto system Firewall do ochrony dostępu do sieci komputerowej.
17	☐	Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.
Środki ochrony w ramach narzędzi programowych i baz danych		
W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do technicznych i programowych środków bezpieczeństwa zastosowanych w procedurach, aplikacjach i programach oraz innych narzędziach programowych wykorzystywanych do przetwarzania danych osobowych.		
1	☐	Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych danych osobowych.
2	☐	Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych
3	☐	Dostęp do danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4	☐	Dostęp do danych osobowych wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN lub tokena.
5	☐	Dostęp do danych osobowych wymaga uwierzytelnienia z wykorzystaniem technologii biometrycznej.
6	☐	Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym danych osobowych dla poszczególnych użytkowników systemu informatycznego.
7	☐	Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do danych osobowych.
8	☐	Zastosowano kryptograficzne środki ochrony danych osobowych.
9	☐	Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

10	☐	Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.
Środki organizacyjne		
W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do innych środków organizacyjnych zastosowanych przez administratora w celu ochrony danych, takich jak: instrukcje, szkolenia, zobowiązania.		
1	☐	Osoby zatrudnione przy przetwarzaniu danych zostały przeszkolone z zakresu ochrony danych osobowych.
2	☐	Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
3	☐	Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
4	☐	Kopie zapasowe danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

Jeżeli zastosowane zostały dodatkowo inne środki nie wymienione w udostępnionych listach, należy je wyszczególnić poniżej: ……
……
……