POLITYKA BEZPIECZEŃSTWA

ZWIĄZEK OCHOTNICZYCH STRAŻY POŻARNYCH RP

UL. OBOŹNA 1, 00-340 WARSZAWA

Data i miejsce sporządzenia dokumentu:	22 maja 2018 / Warszawa
Ilość stron:	41

SPIS TREŚCI

1. WSTĘP

1.1. INFORMACJE OGÓLNE

1. Niniejsza Polityka Bezpieczeństwa wdrażana jest przez Zarząd Główny Związku Ochotniczych Straży Pożarnych Rzeczpospolitej Polskiej z siedzibą w Warszawie (00-340), Obożna 1, zwany dalej „Administratorem Danych Osobowych". Jej aktualizacja ma miejsce w związku z wejściem w życie 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, dalej zwane „RODO".

2. Administrator Danych Osobowych, będąc świadomym, iż jest zwolniony z obowiązku rejestracji zbiorów danych, a także posiadania samej Polityki Bezpieczeństwa postanawia wdrożyć niniejszy dokument przy zachowaniu wszelkich standardów wymaganych prawem dla przetwarzania danych osobowych. Opracowanie niniejszego dokumentu wynika ze zrozumienia znaczenia bezpieczeństwa danych we współczesnym świecie.

3. Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie bezpieczeństwa przetwarzanych danych w strukturze podległej Administratorowi Danych Osobowych oraz dostosowanie organizacji do standardów RODO, ustawy o ochronie danych osobowych z 2018 r. oraz aktów wykonawczych.

4. Polityki Bezpieczeństwa została opracowana w oparciu o wytyczne zawarte w następujących aktach prawnych:

    a) 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

    b) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

1.2. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i danych istotnych oraz zabezpieczenia ich przed nieuprawnionym dostępem.
2. Polityka Bezpieczeństwa składa się z następujących elementów:
    a) zadań i obowiązków ciążących na Administratorze Danych Osobowych oraz Inspektorze Danych Osobowych,
    b) wykazu zbiorów danych osobowych,
    c) określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,
    d) wzorów dokumentów stosowanych przez Administratora Danych Osobowych.

1.3. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

Sformułowania użyte w niniejszym dokumencie należy rozumieć w sposób następujący:

1. **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000), zwana dalej „Ustawą",
2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. **Dane istotne –** wszelkie dane, które zdaniem Administratora Danych Osobowych zasługują na szczególną ochronę oraz wobec których powinny być podjęte kroki w celu zapobieżenia ujawnieniu osobom trzecim. Są to dane takie jak umowy handlowe, dokumenty finansowe etc.
4. Dane **wrażliwe – dane szczególnie chronione przez przepisy prawa. Zgodnie z RODO są to:**
    a) dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych,
    b) dane genetyczne,
    c) dane biometryczne,
    d) dane dotyczące zdrowia, seksualności lub orientacji seksualnej,
    e) dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.
5. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych lub danych istotnych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
6. **Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
7. **Instrukcje zarządzania systemami informatycznymi** – zespół norm oraz zasad obowiązujących w systemach informatycznych Administratora Danych Osobowych, służące m.in. zapewnieniu bezpieczeństwa oraz poufności danych.

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1. INFORMACJE OGÓLNE

1. Osobami odpowiedzialnymi za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, RODO, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemami informatycznymi są:
   a) Administrator Danych Osobowych,
   b) Inspektor Ochrony Danych (zwany dawniej Administratorem Danych Osobowych),
   c) Osoby wykonujące pracę bądź świadczące usługi cywilnoprawne na rzecz Administratora Danych Osobowych.
2. Osoby wymienione w ust. 1 pkt. c uzyskują stosowne upoważnienie do przetwarzania danych osobowych.
3. Wzór upoważnienia, o którym mowa powyżej stanowi załącznik nr 4a oraz 4b do Polityki Bezpieczeństwa.

2.2. ADMINISTRATOR DANYCH OSOBOWYCH

1. Administratorem Danych Osobowych jest **Związek Ochotniczych Straży Pożarnych Rzeczypospolitej Polskiej** z siedzibą w Warszawie, 00-340; ul. Obożna 1, REGON: 007024050, wpisany do Krajowego Rejestru Sądowego pod numerem: 0000116212.
2. Administrator Danych Osobowych ma świadomość, że przetwarza dane osobowe w związku z zatrudnieniem u niego (lub świadczeniem u niego usług na podstawie umów cywilnoprawnych) lub zrzeszeniem się, pełnieniem funkcji w organach zrzeszonych osób prawnych lub wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej.
3. Administrator Danych Osobowych przetwarza dane osobowe na podstawie zgody osób przetwarzanych, ale również w swoim prawnie uzasadnionym interesie jakim jest konieczność przetwarzania danych osobowych osób zrzeszonych w jednostkach Ochotniczej Straży Pożarnej, które są zrzeszone w strukturach Administratora Danych Osobowych.

2.3. INSPEKTOR OCHRONY DANYCH

1. Administrator Danych Osobowych może powołać Inspektora Ochrony Danych.
2. W przypadku powołania Inspektora Ochrony Danych do jego zadań będą należały poniższe czynności:

a) stały nadzór nad treścią Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym,
b) aktualizacja i modyfikacja ww. dokumentów,
c) informowanie Administratora Danych Osobowych, podmioty przetwarzające oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach związanych z przetwarzaniem danych osobowych spoczywających na nich na mocy przepisów prawa,
d) monitorowanie przestrzegania przepisów ochrony danych osobowych poprzez dokonywanie czynności sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania,
e) podejmowanie działań zwiększających świadomość ochrony danych osobowych personelu zatrudnionego u Administratora Danych Osobowych uczestniczącego w operacjach przetwarzania, w tym m.in. szkolenia i audyty,
f) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych,
g) prowadzenie rejestru czynności przetwarzania, jeżeli taki obowiązek zaistnieje na podstawie przepisów prawa lub Inspektor Danych Osobowych uzna to za sluszne,
h) prowadzenie ewidencji zbiorów danych osobowych,
i) pełnienie funkcji punktu kontaktowego dla osób przetwarzanych oraz Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych,
j) udział w kontrolach prowadzonych przez Prezesa Urzędu Ochrony Danych Osobowych,

3. Dotychczasowy Administrator Bezpieczeństwa Informacji z mocy prawa, z dniem 25 maja 2018 r. przyjmuje funkcje Inspektora Danych Osobowych.
4. Wzór rejestru czynności przetwarzania stanowi załącznik nr 12 do Polityki Bezpieczeństwa.

2.4. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Administrator Danych Osobowych może powołać Administratora Systemów Informatycznych.
2. W przypadku powołania Administratora Systemów Informatycznych do jego zadań będą należały poniższe czynności:
   a) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
   b) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
   c) zapewnienie ciągłości działania systemów informatycznych,
   d) sprawne realizowanie procedur tworzenia kopii zapasowych,
   e) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,

f) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych.

3. W przypadku niepowołania Administratora Systemów Informatycznych wszelkie ciążące na nim obowiązki spoczywają na Administratorze Danych Osobowych.

2.5. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, RODO, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.
3. Każda upoważniona osoba, wraz z wydaniem identyfikatora w systemie informatycznym, powinna zobowiązać się do zachowania poufności zgodnie ze wzorem stanowiącym załącznik nr 5 do niniejszej Polityki.

3. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważnienie do przetwarzania danych osobowych oraz innych istotnych danych wydaje w imieniu Administratora Danych Osobowych Inspektor Ochrony Danych.
2. Przyznawanie użytkownikowi identyfikatora w systemie informatycznym oraz nadawania lub modyfikację uprawnień użytkownika do zasobów systemu informatycznego spoczywa na Administratorze Systemów Informatycznych.
3. Wniosek o wydanie oraz cofnięcie upoważnienia kierowany jest przez Dział Kadr lub kierownika jednostki organizacyjnej bądź oddziałów ZOSP RP
4. Cofnięcie upoważnienia powinno następować wraz z ustaniem stosunku prawnego pomiędzy pracownikiem lub współpracownikiem, a Administratorem Danych Osobowych lub w przypadku stwierdzenia istotnego naruszenia przez osobę upoważnioną do stosowania zasad bezpieczeństwa informacji.
5. Upoważnienie wydawane jest w formie pisemnej, zgodnie ze wzorem stanowiącym załącznik nr 4a i 4b do niniejszej Polityki.
6. Każde upoważnienie zawiera zakres oraz cel przetwarzania danych.
7. Rejestr osób upoważnionych do przetwarzania danych opisanych w pkt. 1 prowadzi Inspektor Ochrony Danych, a w przypadku nie powołania go sam Administrator Danych Osobowych, w formie elektronicznej. Prowadzenie takiego rejestru nie jest obligatoryjne.
8. Rejestr osób upoważnionych do korzystania z systemów informatycznych oraz przetwarzania zawartych w nich danych osobowych jest prowadzony w bazach danych tych systemów informatycznych.

4. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. W przypadku, gdy Administrator Danych Osobowych zechce powierzyć przetwarzanie danych osobowych zewnętrznym podmiotom może się to obyć wyłącznie w drodze umowy powierzenia zawartej w formie pisemnej.

2. Umowa powierzenia przetwarzania powinna być przygotowana lub zatwierdzona przez Inspektora Ochrony Danych. Wzór umowy stanowi załącznik nr 11 do Polityki Bezpieczeństwa.

3. Inspektor Ochrony Danych prowadzi rejestr umów powierzenia przetwarzania danych osobowych.

4. W umowie powierzenia należy określić zbiór, który zostanie przekazany, cel tego przekazania oraz zakres planowanego przetwarzania danych przez inny podmiot, obowiązki przetwarzającego, prawo do kontroli dokonywanej przez przekazującego, zakres odpowiedzialności przetwarzającego oraz czas obowiązywania umowy. Umowa powinna zakazywać profilowania oraz przenoszenia danych osobowych poza terytorium Europejskiego Obszaru Gospodarczego.

5. W związku z ryzykiem związanym z powierzaniem przetwarzania danych osobowych zewnętrznym podmiotom należy robić to tylko gdy jest to zasadne pod względem realizacji zadań statutowych Administratora Danych Osobowych.

5. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. W trakcie przetwarzania danych osobowych w Związku Ochotniczych Straży Pożarnych RP stosowane będą następujące zasady:

    a. **Zasada przejrzystości** zgodnie z którą wszelkie komunikaty związane z przetwarzaniem danych osobowych były prezentowane w łatwo dostępny, zrozumiały sposób, a także jasnym i prostym językiem,

    b. **Zasada zgodności z prawem**, która wymaga aby przetwarzanie danych osobowych było wykonywane na podstawie przesłanek legalności, tj. najczęściej zgody osoby fizycznej lub prawnie uzasadnionego interesu Administratora Danych Osobowych,

    c. **Zasada ograniczenia celu** przetwarzania danych osobowych, która wymaga aby dane były zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,

    d. **Zasada minimalizacji danych**, która wymaga aby dane osobowe były adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum,

    e. **Zasada prawidłowości danych**, zgodnie z którą dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane,

    f. **Zasada ograniczenia przechowywania danych**, która wymaga, aby okres przetwarzania danych był ograniczony do czasu jaki jest niezbędny do tego, aby osiągnąć założony cel przetwarzania danych,

    g. **Zasada integralności i nienaruszalności** zgodnie z którą dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich.

2. Podstawową przesłanką legalności jest dobrowolna zgoda na przetwarzanie danych osobowych, która powinna mieć brzmienie zgodne z poniższym: „Wyrażam zgodę na przetwarzanie moich danych osobowych tj. ..... (np. imię, nazwisko, adres e-mail, adres zamieszkania, numer telefonu) przez Administratora Danych Osobowych, tj. Związek Ochotniczych Straży Pożarnych RP z siedzibą w Warszawie w celu ..... Moja zgoda może zostać cofnięta, może być wniesiony sprzeciw wobec przetwarzania Państwa danych osobowych lub mogą być one przeniesione w dowolnym momencie. Aby skontaktować się z Administratorem Danych Osobowych należy wysłać wiadomość e-

mail na adres abi@zosprp.org.pl spod adresu, którego zgoda dotyczy. Informujemy, że nie jesteście Państwo profilowani, a dane nie będą udostępniane innym podmiotom. Podanie danych jest dobrowolne. Państwa dane nie będą przekazywane poza EOG ani udostępniane organizacjom międzynarodowym."

3. W przypadku przetwarzania danych osobowych osoby niepełnoletniej wymagane jest otrzymanie zgody od ich prawnego opiekuna.

4. Administrator Danych Osobowych nie przetwarza w swoich działań danych wrażliwych.

5. Osoba, której dane są przetwarzane ma prawo do: uzyskania informacji, dostępu do danych osobowych, sprostowania danych osobowych, usunięcia danych osobowych, ograniczenia przetwarzania danych osobowych, przenoszenia danych osobowych, sprzeciwu wobec przetwarzania danych osobowych, wniesienia skargi do organu nadzorczego, do zapomnienia.

6. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH ORAZ DANYCH ISTOTNYCH

1. Wprowadzenie, odpowiednich ze względu na charakter organizacji pracy Administratora Danych Osobowych, ogólnych zasad bezpieczeństwa przetwarzania danych - zgodnie z wymaganiami przepisów prawnych z zakresu ochrony danych osobowych – pozwoli na prawidłowe przetwarzanie danych.
2. Za bezpieczeństwo przetwarzania danych osobowych i danych istotnych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
3. Pracownicy mający dostęp do danych osobowych i danych istotnych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. W miejscu przetwarzania danych osobowych i danych istotnych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka". Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe i dane istotne w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
5. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe i dane istotne musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
6. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe i dane istotne poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe i dane istotne odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
7. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe lub dane istotne jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
8. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe i dane istotne w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

7. INSTRUKCJA POSTĘPOWNIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH I DANYCH ISTOTNYCH

1. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe lub dane istotne bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi Systemów Informatycznych.
2. Do czasu przybycia na miejsce naruszenia ochrony danych Administratora Systemów Informatycznych lub upoważnionej przez niego osoby, osoba powiadamiająca powinna:
    a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
    b) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
    c) udokumentować wstępnie zaistniałe naruszenie,
    d) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Systemów Informatycznych lub osoby upoważnionej.
3. Po przybyciu na miejsce naruszenia ochrony danych osobowych lub danych istotnych, Administrator Systemów Informatycznych lub osoba go zastępująca:
    a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania,
    b) wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.
4. Administrator Systemów Informatycznych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport w ciągu 48 godzin od incydentu, według wzoru stanowiącego Załącznik nr 10 do niniejszej Polityki. Raport, o którym mowa powyżej Administrator Systemów Informatycznych niezwłocznie przekazuje Inspektorowi Ochrony Danych, a w przypadku jego nieobecności osobie wyznaczonej.
5. W ciągu 72 godzin od incydentu Inspektor Ochrony Danych ma obowiązek zgłoszenia tego faktu Prezesowi Urzędu Ochrony Danych Osobowych.
6. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator Systemów Informatycznych zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych.

8. KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Związku Ochotniczych Straży Pożarnych RP sprawuje Inspektor Ochrony Danych oraz Administrator Systemów Informatycznych - w odniesieniu do danych osobowych i danych istotnych przetwarzanych w systemach informatycznych służących do przetwarzania tych danych.
2. Czynności kontrolne przeprowadzane są nie rzadziej niż raz na kwartał.
3. Z czynności kontrolnych sporządzany jest protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i przeprowadzonych czynności.
4. Protokół podpisywany jest przez osoby wykonujące czynności kontrolne. Dołącza się go do dokumentacji przechowywanej u Inspektora Ochrony Danych.
5. Wzór protokołu z kontroli lub czynności sprawdzających, o których mowa w niniejszym Rozdziale stanowi Załącznik nr 8 do niniejszej Polityki.

9. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

1. Wzór zestawienia zastosowanych środków technicznych i organizacyjnych przedstawiono w załączniku nr 7 do Polityki Bezpieczeństwa.

2. Wzór o którym mowa w ust. 1 powinien zawierać wykaz środków technicznych i organizacyjnych, które zostały zastosowane przez Administratora Danych Osobowych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych, a także dla zagwarantowania poufności, integralności i rozliczalności przetwarzanych danych osobowych.

10. ZAŁĄCZNIKI

Załącznik nr 1 – Ustanowienie Inspektora Ochrony Danych.

Załącznik nr 2 – Upoważnienie Administratora Systemów Informatycznych do nadawania upoważnień.

Załącznik nr 3 – Ustanowienie Administratora Systemów Informatycznych.

Załącznik nr 4a – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę.

Załącznik nr 4b – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy innej niż umowa o pracę.

Załącznik nr 5 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności.

Załącznik nr 6 – Wykaz podmiotów, którym Administrator Danych Osobowych powierzył przetwarzanie danych osobowych.

Załącznik nr 7 – Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Załącznik nr 8 – Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzających.

Załącznik nr 9 – Raport dokumentujący naruszenie bezpieczeństwa danych.

Załącznik nr 10 – Instrukcja zarządzania systemami informatycznymi.

Załącznik nr 11- Wzór umowy o powierzeniu przetwarzania danych osobowych.

Załącznik nr 12 – Wzór rejestru czynności przetwarzania.

Dokument sporządzono: Data: 22./05./2018. (dd/mm/rrrr) Miejsce: WARSZAWA	**Pełen podpis Administratora Danych Osobowych:**	**Pieczęć**
	Wiesław Golański Krzysztof Szelągowski Marian Zalewski	Dyrektor Zarządu Wykonawczego ZOSP RP mgr Wiesław Golański Zastępca Dyrektora Zarządu Wykonawczego ZOSP RP mgr inż. Krzysztof Szelągowski Zastępca Dyrektora Zarządu Wykonawczego ZOSP RP dr Marian Zalewski

Załącznik nr 1 – Ustanowienie Inspektora Ochrony Danych

Niniejszym, zgodnie z dyspozycją Rozdziału 2 Polityki Bezpieczeństwa oraz reprezentując Administratora Danych Osobowych – Związek Ochotniczych Straży Pożarnych RP,

wyznaczam

Panią/Pana .....

na stanowisko **Inspektora Ochrony Danych (IOD)** Związku Ochotniczych Straży Pożarnych RP.

Zakres obowiązków oraz warunki pełnienia funkcji Inspektora Ochrony Danych określone są ustawą o ochronie danych osobowych z dnia 10 maja 2018 r. oraz dokumentacją z zakresu ochrony danych osobowych tj. Polityką Bezpieczeństwa wdrożoną dnia .../ ... / ..... (dd/mm/rrrr) w Związku Ochotniczych Straży Pożarnych RP.

DATA I PODPIS OSOBY WYZNACZONEJ NA STANOWISKO IDO

DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH OSOBOWYCH

Załącznik nr 2 – Upoważnienie Inspektora Ochrony Danych do nadawania upoważnień

Niniejszym, zgodnie z dyspozycją Rozdziału 3 Polityki Bezpieczeństwa oraz reprezentując Administratora Danych Osobowych – Związek Ochotniczych Straży Pożarnych RP,

upoważniam

Panią/Pana .....

Inspektora Ochrony Danych w Związku Ochotniczych Straży Pożarnych RP do nadawania w imieniu Administratora Danych Osobowych upoważnień do przetwarzania danych osobowych.

DATA I PODPIS OSOBY WYZNACZONEJ
NA STANOWISKO ADO

DATA I PODPIS OSOBY REPREZENTUJĄCEJ
ADMINISTRATORA DANYCH OSOBOWYCH

Załącznik nr 3 – Ustanowienie Administratora Systemów Informatycznych

Niniejszym, zgodnie z dyspozycją Rozdziału 2 Polityki Bezpieczeństwa oraz reprezentując Administratora Danych Osobowych – Związku Ochotniczych Straży Pożarnych RP,

wyznaczam

Panią/Pana .....

na stanowisko **Administratora Systemów Informatycznych (ASI)** w Związku Ochotniczych Straży Pożarnych RP.

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemów Informatycznych określone są Ustawą o ochronie danych osobowych z dnia 10 maja 2018 roku oraz dokumentacją z zakresu ochrony danych osobowych – Polityką Bezpieczeństwa wdrożoną dnia .../ ... / ..... (dd/mm/rrrr) w Związku Ochotniczych Straży Pożarnych RP

DATA I PODPIS OSOBY WYZNACZONEJ
NA STANOWISKO ADO

DATA I PODPIS OSOBY REPREZENTUJĄCEJ
ADMINISTRATORA DANYCH OSOBOWYCH

Załącznik nr 4a – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Inspektor Ochrony Danych w Związku Ochotniczych Straży Pożarnych RP (dalej ZOSP RP), na podstawie ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. **upoważniam:**

Imię i nazwisko upoważnionego pracownika	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych Osobowych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. oraz RODO wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w ZOSP RP wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.

Upoważnienie jest ważne do odwołania.

.....
Data i podpis upoważniającego

.....
Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w ZOSP RP (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

.....
Data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

Załącznik nr 4b – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie innej umowy niż umowa o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Inspektor Danych Osobowych w Związku Ochotniczych Straży Pożarnych RP (dalej ZOSP RP), na podstawie ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. **upoważniam:**

Imię i nazwisko upoważnionego	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych Osobowych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ustawy z dnia 10 maja 2018 r. oraz RODO wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w ZOSP RP wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz odpowiedzialności cywilnej.

Upoważnienie jest ważne do odwołania.

....

Data i podpis upoważniającego Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w ZOSP RP (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych w związku z pełnioną przeze mnie funkcją i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu stosunku prawnego łączącego mnie z Administratorem Danych Osobowych.

.....

Data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

Załącznik nr 5 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności

....., dnia .....

Oświadczenie o zobowiązaniu się do zachowania poufności

Ja niżej podpisana/y ..... zamieszkała/y w .....
..... zatrudniona/y na stanowisku .....
zobowiązuję się zachować w tajemnicy informacje uzyskane w związku z .....
Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

.....

Podpis

Załącznik nr 6 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych (fakultatywnej)

Nr	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Indywidualny identyfikator w systemie informatycznym	Nazwy zbiorów objętych zakresem upoważnienia
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					

Załącznik nr 7 – Wykaz podmiotów, którym Administrator Danych Osobowych powierzył przetwarzanie danych osobowych

	Adres / lokalizacja	Uwagi
Podmioty, którym Administrator Danych Osobowych powierzył przetwarzanie danych osobowych		

	Administrator Danych Osobowych	Uwagi
Dane osobowe przetwarzane jako Administrator Danych Osobowych		

Załącznik nr 8 – Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych i danych istotnych

ŚRODKI TECHNICZNE

Środek ochrony technicznej i fizycznej	Zastosowano (TAK / NIE)	Uwagi
1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym **drzwiami zwykłymi** (niewzmacnianymi, nie przeciwpożarowymi).		
2. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za **pomocą krat, rolet lub folii antywłamaniowej.**		
3. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w **system alarmowy przeciwwłamaniowy.**		
4. Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są **systemem kontroli dostępu.**		
5. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez **system monitoringu z zastosowaniem kamer przemysłowych.**		
6. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie **nieobecności zatrudnionych** tam pracowników **nadzorowany przez służbę ochrony.**		
7. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej **niemetalowej szafie.**		
8. Zbiór danych osobowych w formie papierowej przechowywany jest w **zamkniętej metalowej szafie.**		
9. Zbiór danych osobowych w formie papierowej przechowywany jest **w zamkniętym sejfie lub kasie pancernej.**		

10. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są w **zamkniętej niemetalowej szafie.**		
11. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są **w zamkniętej metalowej szafie**.		
17. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych 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 ORGANIZACYJNE

Środek organizacyjny	Zastosowano (TAK / NIE)	Uwagi
Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych		
Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych		
Wyznaczono Inspektora Ochrony Danych		
Opracowano i wdrożono Politykę Bezpieczeństwa o której mowa w ustawie o ochronie danych osobowych		
Opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych		
Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych		
Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy		
Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym		
Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco		

Załącznik nr 9 - Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/ czynności sprawdzających

.....

miejscowość, data

PROTOKÓŁ

Z KONTROLI / CZYNNOŚCI SPRAWDZAJĄCYCH*

w zakresie ochrony danych osobowych

1. Nazwa kontrolowanej jednostki organizacyjnej:.....
2. Zbiory danych osobowych, których przetwarzanie podlega kontroli: .....
3. Data wykonania czynności kontrolnych:.....
4. Imię i nazwisko oraz stanowisko osoby wykonującej czynności kontrolne: .....
5. Imiona i nazwiska osób udzielających informacji dotyczących ochrony danych osobowych w kontrolowanej komórce organizacyjnej:.....
6. Ustalenia dokonane w trakcie czynności kontrolnych:.....
7. Wnioski i zalecenia pokontrolne:

.....

(data i podpis osoby wykonującej czynności kontrolne)

.....

(data i podpis kierownika kontrolowanej kom. organizacyjnej)

Otrzymują:
1 x Kierownik kontrolowanej jednostki organizacyjnej
1 x Inspektor Ochrony Danych

* niepotrzebne skreślić

.....

miejscowość, data

RAPORT DOKUMENTUJĄCY PRZYPADEK NARUSZENIA BEZPIECZEŃSTWA DANYCH

w zakresie ochrony danych osobowych i danych istotnych

1. Osoba powiadamiająca o zaistniałym zdarzeniu:.....
2. Lokalizacja zdarzenia: .....
3. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące.....
   .....
   .....
   .....
4. Opis przebiegu naruszenia: .....
   .....
   .....
   .....
5. Przyczyny wystąpienia zdarzenia .....
   .....
   .....
   .....
6. Podjęte działania.....
   .....
   .....
   .....
7. Wnioski wynikające ze zdarzenia:.....
   .....
   .....
   .....
8. Postępowanie wyjaśniające:.....
   .....
   .....
   .....
9. Działania które należy podjąć:.....
   .....
   .....

.....

(data i podpis osoby wykonującej czynności kontrolne)

.....

(data i podpis Administratora Systemów Infomatycznych)

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Opracowana zgodnie z §3 ust.1 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 (Dz. U. Nr 100 poz. 1024).

§ 1
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu.
2. Każdy identyfikator użytkownika zabezpieczony jest hasłem.
3. Administrator Danych Osobowych stosuje następujące zasady tworzenia hasła:
   a) hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów,
   b) hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
   c) hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury,
   d) hasło nie może być jednakowe z identyfikatorem użytkownika,
   e) hasło musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.
4. Hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.
5. Zaleca się zmienianie hasła nie rzadziej niż co 30 dni. Jeżeli zmiana hasła nie jest możliwa w wymaganym czasie, należy jej dokonać w najbliższym możliwym terminie.
6. W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie Administratora Danych.

7. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.

§ 2
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych

1. Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić Administratora Systemów Informatycznych.
2. Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.
3. W przypadku opuszczenia stanowiska pracy trwającego dłużej niż 1 h, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych lub danych istotnych.
4. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następują poprzez wylogowanie się z tego systemu. Za wykonanie kopii danych odpowiedzialny jest Administrator Systemów Informatycznych. Użytkownik może wykonywać kopie tylko pod nadzorem Administratora Systemów Informatycznych.

§ 3
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Za sporządzanie kopii zapasowych zbiorów danych odpowiedzialny jest Administrator Systemów Informatycznych systemu informatycznego służącego do przetwarzania danych osobowych.
2. Kopie zapasowe powinny być kontrolowane przez Administratora Systemów Informatycznych, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.

3. Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych lub danych istotnych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.
4. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

§ 4
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.
2. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe nie mogą być wynoszone poza pomieszczenia stanowiące obszar przetwarzania danych osobowych, określony w Polityce Bezpieczeństwa.
3. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w Polityce Bezpieczeństwa, w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.
4. W przypadku uszkodzenia lub zużycia nośnika informacji zwierających dane osobowe lub dane istotne należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych.

§ 5
Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych

1. Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych stosowane jest oprogramowanie antywirusowe.
2. Każdy zbiór wczytywany do komputera, w tym także wiadomość e-mail, musi być przetestowany programem antywirusowym.
3. Na każdym stanowisku wyposażonym w dostęp do sieci Internet musi być zainstalowanie oprogramowanie antywirusowe. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.
4. Aktualizacje oprogramowania antywirusowego powinno odbywać się nie rzadziej niż raz w miesiącu.

§ 6
Sposób zapewnienia odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia

1. W systemie informatycznym służącym do przetwarzania danych osobowych odnotowywane są informacje o odbiorcach danych, a w szczególności imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia.
2. W przypadku, gdy w systemie informatycznym służącym do przetwarzania danych osobowych nie jest możliwe odnotowywanie takich informacji, Administrator Danych Osobowych odnotowuje je w rejestrze odbiorców danych osobowych.
3. W rejestrze odnotowywane są imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia. Rejestr prowadzony w formie elektronicznej będzie przekazywany w formie wydruku z systemu informatycznego na każdorazowe żądanie Inspektora Ochrony Danych.

§ 7
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w Polityce Bezpieczeństwa przez firmy zewnętrzne na

podstawie zawartych umów. W umowie musi znajdować się zapis o powierzeniu danych osobowych.

2. W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności Administratora Danych Osobowych.
3. Przeglądy techniczne wykonywane muszą być nie rzadziej niż raz w roku.
4. Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych, systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych pełni Administrator Systemów Informatycznych.
5. Zabronione jest wykonywanie przeglądów i konserwacji systemów informatycznych służących do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych samodzielnie przez pracownika lub współpracownika Administratora Danych Osobowych.

§ 8
Pozostałe zasady ochrony systemu informatycznego służącego do przetwarzania danych osobowych

1. Administrator Danych Osobowych ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.
2. Należy instalować zalecane przez producentów oprogramowania poprawki i uaktualnienia systemu informatycznego służącego do przetwarzania danych osobowych celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.

Umowa powierzenia przetwarzania danych osobowych
zawarta dnia _____ pomiędzy:
(zwana dalej „Umową")

_____ (*dane podmiotu który umowę zawiera)

zwany w dalszej części umowy „Podmiotem przetwarzającym"
reprezentowana przez:

_____

oraz

_____ (*dane podmiotu który umowę zawiera)

zwany w dalszej części umowy „Administratorem danych" lub „Administratorem"
reprezentowana przez:

_____

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane (*należy podać rodzaj danych) ..... np. dane zwykłe oraz dane szczególnych kategorii ..... (*należy podać kategorię osób, których dane dotyczą) np. pracowników administratora, klientów administratora itd. w postaci ..... np. imion i nazwisk, adresu zamieszkania, nr PESEL itd.
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu ..... (*należy podać cel przetwarzania danych przez podmiot przetwarzający) np. realizacji umowy z dnia ..... nr ..... w zakresie prowadzenia kadr.

§3
Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.

5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe (należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu 24 godzin od zdarzenia.

§4
Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum …….. (*należy wpisać z ilu dniowym wyprzedzeniem Administrator informuje o kontroli) jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni (*administrator termin może określić dowolnie).
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5
Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.

2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §3 ust. 2 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6
Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7
Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas nieokreślony/określony* od ….. do ….. .

2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem ..... * okresu wypowiedzenia.

§8
Rozwiązanie umowy

Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
b) przetwarza dane osobowe w sposób niezgodny z umową;
c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

§9
Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10
Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.

3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych (*lub Podmiotu przetwarzającego w zależności od postanowień stron).

Administrator danych	Podmiot przetwarzający

REJESTR CZYNNOŚCI PRZETWARZANIA

(podstawa prawna art. 30 ogólnego rozporządzenia o ochronie danych)

Lp.	Nazwa oraz dane kontaktowe administratora oraz wszelkich współadministratorów	Cele przetwarzania	Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	Informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowych	Planowane terminy usunięcia poszczególnych kategorii danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (art. 32 ust.1)
1.							
2.							
3.							

Rozporządzenie Parlamentu Europejskiego i Rady Europy 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych).