Łódź, dnia 25 maja 2018 roku

POLITYKA OCHRONY DANYCH OSOBOWYCH
W „FUNDACJA MEDIA KLASTER" z siedzibą w Łodzi

Na podstawie art. 24 (Obowiązki Administratora) 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.U.UE.L.2016.119.1), uznając, że jest to proporcjonalne w stosunku do czynności przetwarzania, wdraża się do stosowania niniejszą politykę ochrony danych osobowych.

Niniejsza Polityka dotyczy ochrony danych osobowych w Fundacji „FUNDACJA MEDIA KLASTER" z siedzibą w Łodzi, przy ul. Łąkowej 29, 90-554 Łódź, wpisanej do rejestru Stowarzyszeń, innych Organizacji Społecznych i Zawodowych, Fundacji oraz Samodzielnych Publicznych Zakładów Opieki Zdrowotnej prowadzonego przez Sąd Rejonowy dla Łodzi-Śródmieścia w Łodzi, XX Wydział Krajowego Rejestru Sądowego pod numerem 0000287861, numer NIP 727-27-10-297.

Treść polityki opracowana została z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

Definicje.

1) Dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (zwane dalej „d.o.");
2) przetwarzanie - 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;
3) ograniczenie przetwarzania - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
4) profilowanie - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
5) pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

6) zbiór danych - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
7) Administrator - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposób takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony Administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
8) podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora (zwany dalej: „Procesorem");
9) odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

§ 1
Postanowienia ogólne

1. W Fundacji przetwarzane są informacje stanowiące d.o. w rozumieniu art. 4 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

2. Niniejsza Polityka stanowi politykę bezpieczeństwa informacji Fundacji – jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu d.o. w zbiorach administrowanych przez Fundację.

3. Administrator, mając na względzie wagę zagrożeń prywatności, w tym zagrożeń dla bezpieczeństwa przetwarzanych d.o., obliguje się do podejmowania wszelkich możliwych działań koniecznych dla zapobieżenia m. in. takim zagrożeniom, jak:
    a. sytuacjom losowym lub nieprzewidzianym oddziaływaniom czynników zewnętrznych na zasoby systemów przetwarzających d.o., jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie;
    b. niewłaściwym parametrom środowiska, zakłócającym pracę urządzeń komputerowych (nadmierna wilgotność powietrza lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne);
    c. awariom sprzętu lub oprogramowania, które z wysokim prawdopodobieństwem wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie procedur serwisowych, w tym również przyzwolenie na naprawę sprzętu zawierającego d.o. poza siedzibą Administratora;
    d. naruszeniom bezpieczeństwa danych przez przetwarzanie ich bez zezwolenia;
    e. celowym lub przypadkowym rozproszeniu danych w Internecie z ominięciem zabezpieczeń systemu przetwarzającego d.o. lub z wykorzystaniem błędów tego systemu;
    f. atakom pochodzącym z sieci Internet;
    g. naruszeniom zasad przez osoby upoważnione do przetwarzania d.o., określonych w dokumentacji z zakresu ochrony d.o., związanych z nieprzestrzeganiem zasad ochrony danych, w tym w szczególności poprzez:
        - niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy;

- naruszenie bezpieczeństwa danych przez przetwarzanie ich bez stosowanego zezwolenia Administratora;
- ujawnienie zasad ochrony danych stosowanych u Administratora osobom nieupoważnionym;
- ujawnienie danych przetwarzanych przez Administratora osobom nieupoważnionym, w tym również nieumyślne ujawnienie danych osobom trzecim przebywającym bez nadzoru lub w niedostatecznie nadzorowanych pomieszczeniach, w których mogą być przetwarzane d.o.;
- brak tworzenia kopii zapasowych zgodnie z procedurami przyjętymi u Administratora;
- Przetwarzanie d.o. w sposób sprzeczny z celem określonym przez Administratora, w tym dla celów prywatnych;
- wprowadzanie zmian do systemu przetwarzającego d.o. u Administratora i instalowanie jakiegokolwiek oprogramowania bez zgody Administratora.

4. Fundacja przetwarza d.o. znajdujące się w administrowanych przez nią zbiorach w określonych celach i w określonym zakresie, w przypadku spełnienia jednej z przesłanek określonych w art. 6 ust. 1 lit. a-f Rozporządzenia, tj. w przypadku, gdy:
    a. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich d.o. w jednym lub większej liczbie określonych celów;
    b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
    c. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze;
    d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
    e. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
    f. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony d.o., w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

5. Fundacja nie przetwarza Szczególnych kategorii d.o., chyba że spełniony jest jeden z warunków określonych w art. 9 ust. 1 lit. a-j Rozporządzenia, tj. w przypadku, gdy:
    a. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych d.o. w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa powyżej;
    b. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
    c. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

d. przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez Fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że Przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że d.o. nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
e. przetwarzanie dotyczy d.o. w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
f. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
g. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
h. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania Systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem odpowiednich warunków i zabezpieczeń;
i. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi trans granicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
j. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 Rozporządzenia, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

6. Na dokumentację przetwarzania d.o. (dalej „Dokumentacja”) w Fundacji składają się Polityka ochrony d.o. oraz jej następujące załączniki w postaci:
   - Załącznik nr 1 – Rejestr czynności przetwarzania
   - Załącznik nr 2 – Lista zabezpieczeń fizycznych danych osobowych
   - Załącznik nr 3 – Raport naruszenia ochrony danych osobowych
   - Załącznik nr 3a – Zgłoszenie naruszenia do organu nadzorczego
   - Załącznik nr 3b – Zgłoszenie naruszenia do osoby, której dane dotyczą
   - Załącznik nr 4 – Wzór upoważnienia
   - Załącznik nr 5 – Wzór cofnięcia upoważnienia
   - Załącznik nr 6 – Ewidencja osób upoważnionych
   - Załącznik nr 7 – informacja o przetwarzaniu danych osobowych dla pracownika,
   - Załącznik nr 8 – Informacja o przetwarzaniu danych osobowych dla osoby wykonującej czynności na podstawie umowy cywilnoprawnej,
   - Załącznik nr 9 – Wzór umowy powierzenia danych osobowych.

§ 2
Administrator i jego obowiązki

1. Fundacja, będąca Administratorem d.o., ma obowiązek zastosować odpowiednie środki techniczne i organizacyjne zapewniające ochronę przetwarzanych d.o., a w szczególności ma obowiązek zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Rozporządzenia i zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator d.o. jest uprawniony do udostępnienia d.o. przetwarzanych we własnych zbiorach wyłącznie osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

3. Administrator ma obowiązek współpracować z Prezesem Urzędu Ochrony d.o. lub wyznaczonym przez niego innym Organem nadzorczym, stosownie do art. 51 Rozporządzenia, w ramach wykonywania przez niego swoich zadań, w szczególności na jego żądanie ma obowiązek udostępnić mu Rejestr czynności przetwarzania w celu monitorowania operacji przetwarzania, którego wzór stanowi Załącznik nr 1 do niniejszej Polityki.

4. Za współpracę z Prezesem Urzędu Ochrony d.o. lub wyznaczonym przez niego innym Organem nadzorczym odpowiedzialna jest osoba wyznaczona przez Administratora do zapewnienia zgodności przetwarzania d.o. z przepisami prawa.

5. Administrator bieżąco monitoruje wytyczne, zalecenia oraz najlepsze praktyki określone przez Europejską Radę Ochrony danych na podstawie art. 70 ust. 1 lit. d-j i m Rozporządzenia i uwzględnia je w swoich działaniach związanych z przetwarzaniem d.o.

6. Administrator wykonuje swoje obowiązki przestrzegając zasady podejścia opartego na ryzyku. W szczególności zobowiązuje się do przeprowadzenia analizy procesów przetwarzania i dokonania ogólnej oceny ryzyka, jakie wiąże się z przetwarzaniem danych w konkretnym przypadku, ze szczególnym uwzględnieniem ryzyka dla praw lub wolności osób, których dane dotyczą.

7. Po weryfikacji wszystkich okoliczności związanych z przetwarzaniem d.o. w Fundacji, w szczególności dotyczących procesów, w ramach których dane są przetwarzane, celów przetwarzania, zaangażowania podmiotów wewnętrznych i zewnętrznych w proces przetwarzania d.o., zakresu i podstaw przetwarzania, a także wykorzystywanych narzędzi i stosowanych zabezpieczeń, Administrator przygotowuje ocenę ryzyka.

8. Mając na względzie charakter, zakres, okoliczności związane z przetwarzaniem d.o. i cele ich przetwarzania w strukturach Administratora oraz stopień ryzyka naruszenia praw lub wolności osób fizycznych o zróżnicowanym prawdopodobieństwie i randze zagrożenia, Administrator ma obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z Rozporządzeniem oraz w celu wykazania tej okoliczności. Środki te, w zależności od potrzeb, są poddawane okresowym przeglądom i uaktualniane, w razie zaistnienia zmiany okoliczności uzasadniających aktualizację.

9. Realizując swoje obowiązki Administrator współpracuje z Procesorami, współadministratorami i osobami, których dane dotyczą, a także Prezesem Urzędu Ochrony d.o. lub wyznaczonym przez niego Organem nadzorczym.

§ 3
Zadania Administratora

1. Zadania Administratora w zakresie ochrony d.o., zmierzające do zapewnienia przestrzegania przepisów Rozporządzenia, to w szczególności:
    a. nadzór opracowania i aktualizacji dokumentacji dotyczącej ochrony d.o.;
    b. nadzór nad przestrzeganiem zasad określonych w dokumentacji dotyczącej ochrony d.o.;
    c. zapewnienie adekwatnych środków technicznych i organizacyjnych zapewniających ochronę d.o. w stosunku do zagrożeń i kategorii przetwarzanych d.o.,
    d. zabezpieczenie d.o. przed:
        - ujawnieniem osobom nieupoważnionym;
        - zabraniem przez osobę nieuprawnioną;
        - zmianą, utratą, uszkodzeniem lub zniszczeniem;
    e. zapewnienie legalności przetwarzania d.o., a w szczególności dbałość o:
        - przetwarzanie d.o. na podstawie jednej z przesłanek legalizujących przetwarzanie, które to przesłanki wymienione są w art. 6 ust. 1 lit. a-f albo w art. 9 ust. 2 lit. a-j Rozporządzenia;
        - spełnienie wobec osoby, której dane dotyczą obowiązku informacyjnego, o którym mowa w art. 13 i 14 Rozporządzenia;
        - przetwarzanie d.o. zgodnie z obowiązującymi przepisami prawa, dobrymi praktykami i zwyczajami oraz normami i zasadami współżycia społecznego;
        - przetwarzanie d.o. w sposób spójny z postanowieniami niniejszej Polityki.
    f. powołanie, w razie konieczności, inspektora ochrony danych, odpowiedzialnego za nadzór nad Przetwarzaniem d.o. zgodnie z przepisami o ochronie d.o.;
    g. powołanie, w razie konieczności, Administratora jako osoby odpowiedzialnej za bezpieczeństwo systemów służących do przetwarzania d.o. oraz określenie zakresu jego obowiązków;
    h. zapewnienie zapoznania osób, którym mają być nadane upoważnienia do przetwarzania d.o., z przepisami o ochronie d.o. oraz zasadami ochrony d.o. poprzez zorganizowanie dla nich szkolenia, prowadzonego przez osobę posiadającą odpowiednią wiedzę i kompetencje z zakresu ochrony d.o.;
    i. upoważnianie użytkowników do przetwarzania d.o. w niezbędnym zakresie;
    j. nadzorowanie i dbałość o zgodne z prawem przekazywanie d.o. (Udostępnianie i Powierzanie);
    k. zapewnianie użytkownikom odpowiednie stanowiska pracy, w tym sprzęt informatyczny, umożliwiające bezpieczne i zgodne z prawem Przetwarzanie d.o.;
    l. podejmowanie odpowiednich środków w przypadku naruszenia lub podejrzenia naruszenia zasad bezpiecznego przetwarzania d.o.;
    m. w sytuacji przekazywania d.o. do państwa trzeciego, dbałość o stosowanie przepisów rozdziału V Rozporządzenia.
2. Administrator dokłada wszelkich starań dla zapewnienia poszanowania praw osób, których dane dotyczą, a w szczególności przekazuje informacje o:
    - Administratorze;
    - celu, zakresie i sposobie przetwarzania d.o.;
    - terminie od kiedy i jakie d.o. są przetwarzane;
    - źródle, z którego d.o. pochodzą;
    - sposobie ujawniania d.o. oraz ich Odbiorcach.
3. Administrator zapewnia przestrzeganie praw osób, których dane dotyczą, w szczególności:
    - Prawa do żądania sprostowania lub uaktualnienia d.o.;
    - Prawa do żądania ograniczenia przetwarzania d.o.;
    - Uprawnienie do wniesienia sprzeciwu wobec przetwarzania d.o.;
    - Prawa do żądania usunięcia d.o.;

- Uprawnienia do żądania potwierdzenia przetwarzania, dostępu do d.o. i uzyskania ich kopii;
- Uprawnienia do żądania przeniesienia d.o.;
- Prawa do odwołania zgody na Przetwarzanie d.o.;
- Uprawnienia do żądania zaniechania zautomatyzowanego podejmowania decyzji.

4. Administrator wdraża odpowiednie środki techniczne i organizacyjne, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, inne okoliczności związane z przetwarzaniem d.o., jak również cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i randze zagrożenia, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym w szczególności:
    a. poprzez pseudonimizację i szyfrowanie d.o.;
    b. w celu zapewnienia zdolności do ciągłego zapewnienia poufności, Integralności, dostępności i odporności Systemów i usług przetwarzania;
    c. w celu zapewnienia zdolności do szybkiego przywrócenia dostępności d.o. i dostępu do nich w razie incydentu fizycznego lub technicznego;
    d. poprzez regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
5. Szczegółowy wykaz stosowanych przez Administratora zabezpieczeń sprzętowych infrastruktury informatycznej i telekomunikacyjnej dla fizycznych elementów systemu przetwarzającego d.o., ich połączeń oraz systemów operacyjnych zostały wskazane w Załączniku nr 2 do niniejszej Polityki.

§ 4
Rejestr czynności przetwarzania d.o.

1. Obowiązkiem Administratora jest prowadzenie rejestru czynności przetwarzania. W rejestrze tym odnotowuje się procesy, podczas których przetwarzane się d.o. Rejestr czynności przetwarzania jest prowadzony w formie elektronicznej. Wzór rejestru stanowi załącznik nr 1 do niniejszej Polityki.
2. Rejestr czynności przetwarzania jest wykorzystywany przy realizacji obowiązków Administratora, szczegółowo opisanych w niniejszej Polityce.
3. Osobą odpowiedzialną za prowadzenie rejestru czynności przetwarzania jest Agata Wielgus.
4. Rejestr czynności przetwarzania jest aktualizowany regularnie, nie rzadziej niż co 6 miesięcy.
5. Na żądanie Prezesa Urzędu Ochrony d.o. lub upoważnionego przez niego organu nadzorczego Administrator ma obowiązek udostępnienia mu prowadzonego rejestru czynności przetwarzania.

§ 5
Realizacja zasad Privacy by Design i Privacy by Default (Art. 25 Rozporządzenia)

1. Administrator na etapie planowania czynności związanych z przetwarzaniem d.o., jak i w trakcie samego procesu przetwarzania, ma obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne, w celu zapewnienia zgodności z wymogami Rozporządzenia i efektywnej ochrony praw osób, których dane dotyczą, mając jednocześnie na uwadze charakter, zakres, inne okoliczności związane z przetwarzaniem d.o., w tym również cele ich przetwarzania oraz wynikającego z nich zagrożenia dla praw i wolności osób fizycznych (zasada prywatności w fazie projektowania).

2. Administrator ma obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były tylko te d.o., które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych d.o., zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności powinien

dołożyć wszelkich starań, by d.o. nie były udostępniane bez interwencji konkretnej osoby nieokreślonej liczbie osób fizycznych (zasada prywatności w ustawieniach domyślnych).

§ 6
Zadania Administratora w zakresie oceny skutków przetwarzania d.o.

1. Jeżeli na podstawie analizy ryzyka wynika, że dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony d.o.. W celu określenia, czy dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator weryfikuje:
    a. charakter,
    b. zakres,
    c. kontekst i
    d. cele przetwarzania.

2. Ocena skutków dla ochrony danych jest wymagana przede wszystkim w przypadku, gdy Przetwarzanie spełnia co najmniej dwie z poniższych przesłanek:
    a. przetwarzanie jest powiązane z oceną, w tym również z profilowaniem i prognozowaniem, w szczególności na podstawie aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą;
    b. dochodzi do automatycznego podejmowania decyzji wywołującej wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób istotnie na nią wpływającej;
    c. przetwarzanie obejmuje szczególne kategorie d.o. lub dane o charakterze szczególnie osobistym;
    d. dochodzi do przetwarzania d.o. na dużą skalę;
    e. przetwarzanie jest wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych, które są gromadzone poprzez sieć lub ramach systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie;
    f. dochodzi do dopasowywania lub łączenia zbiorów Danych, w szczególności pochodzących z co najmniej dwóch różnych operacji przetwarzania danych, przeprowadzonych w różnych celach lub przez różnych Administratorów Danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą;
    g. Przetwarzanie obejmuje d.o. osób wymagających szczególnej opieki, w tym np. dzieci lub pracowników;
    h. następuje innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych;
    i. samo przetwarzanie uniemożliwia osobom, których dane dotyczą, wykonywanie własnych praw lub korzystanie z usługi lub umowy.

3. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem Administrator przeprowadza indywidualną ocenę, zgodnie z powyższymi wytycznymi.

4. Administrator uwzględnia wykazy rodzajów operacji przetwarzania podlegających lub niepodlegających wymogowi dokonania oceny skutków dla ochrony danych, ustanowione przez organ nadzorczy zgodnie z art. 35 ust. 4 i 5 Rozporządzenia.

5. W przypadkach, w których nie jest jasne, czy wymagane jest przeprowadzenie oceny skutków dla ochrony danych, Administrator powinien przeprowadzić taką ocenę.

6. Ocena skutków dla ochrony danych powinna rozpocząć się jak najwcześniej, najlepiej w fazie projektowania operacji przetwarzania. Jeśli zachodzi taka konieczność, w szczególności ze względu na zastosowane w fazie projektowania środki techniczne lub organizacyjne, w miarę postępu procesu rozwoju lub w związku z istotną modyfikacją procesu, poszczególne etapy oceny należy powtórzyć.

7. Jeżeli dana operacja przetwarzania jest całkowicie lub częściowo realizowana przez Procesora, Administrator konsultuje się z Procesorem (Przetwarzającym).

8. Administrator, w razie wątpliwości może zasięgnąć opinii osób, których dane dotyczą, lub ich przedstawicieli. Jeżeli ostateczna opinia Administratora różni się od opinii osób, których dane dotyczą, Administrator dokumentuje powody podjęcia bądź niepodjęcia decyzji. Administrator uzasadnia także niezasięgnięcie opinii osób, których dane dotyczą, jeśli nie uzna tej procedury za konieczną.

9. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, Administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

10. Ocena skutków dla ochrony d.o. powinna zawierać co najmniej:
    a. krótki opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez Administratora;
    b. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
    c. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
    d. środki planowane w celu wykluczenia ryzyka, w tym wskazanie zabezpieczeń oraz środków i mechanizmów bezpieczeństwa mających zapewnić ochronę d.o..

11. Administrator powinien prowadzić wskazaną wyżej dokumentację w taki sposób, by móc wykazać przestrzeganie dotyczących jej przepisów, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

12. Jeżeli ocena skutków dla ochrony danych wykaże, że przy braku lub niedostatecznym poziomie planowanych zabezpieczeń i stosowanych środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko Przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a Administrator uznaje, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia, to przed rozpoczęciem przetwarzania Administrator powinien zasięgnąć opinii organu nadzorczego.

13. Konsultując się z organem nadzorczym zgodnie z ust. powyżej, Administrator przekazuje mu następujące informacje:
    a. cele i sposoby zamierzonego przetwarzania;
    b. środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą;
    c. dane kontaktowe inspektora ochrony danych;
    d. ocenę skutków dla ochrony danych.

14. Administrator ma obowiązek współpracować z organem nadzorczym, w szczególności na jego żądanie udostępniać mu wszystkie informacje w zakresie opiniowanej kwestii.

15. Projektując operacje przetwarzania, wymagające uprzednich konsultacji, Administrator uwzględnia określone w art. 36 ust. 2 Rozporządzenia terminy na udzielenie przez organ nadzorczy zaleceń lub podjęcie środków naprawczych.

16. Administrator uwzględnia zalecenia organu nadzorczego wydane na skutek uprzednich konsultacji i stosuje się do innych środków podjętych przez organ.

§ 7
Sposób przetwarzania d.o.

1. Dostęp do zbioru d.o. oraz ich przetwarzania mają tylko osoby wpisane do ewidencji prowadzonej przez Administratora (użytkownicy).

2. Osoby zatrudnione w Fundacji przy przetwarzaniu d.o. są zobowiązane do przechowywania d.o. we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.

§ 8
Obowiązki informacyjne użytkowników

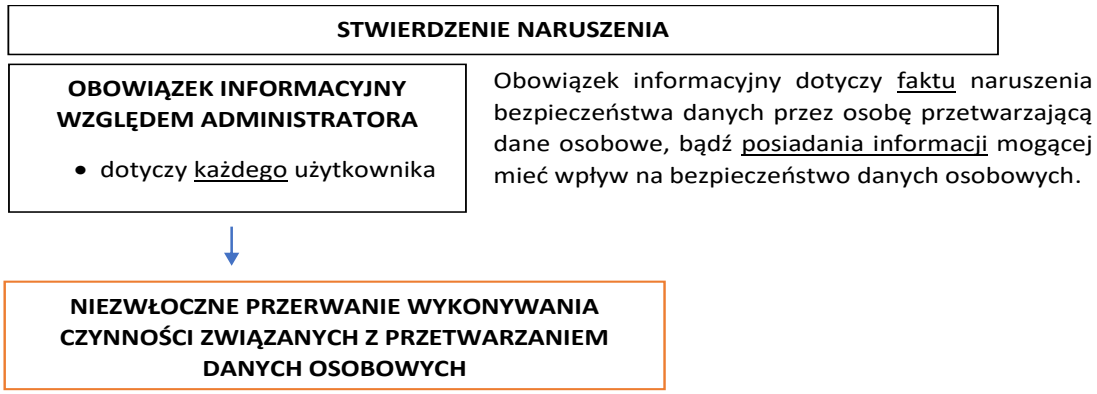
1. Osoby zatrudnione przy przetwarzaniu danych są zobowiązane powiadomić Administratora o ewentualnych naruszeniach bezpieczeństwa systemu ochrony d.o. w każdym zbiorze danych lub systemie informatycznym zawierającym d.o..

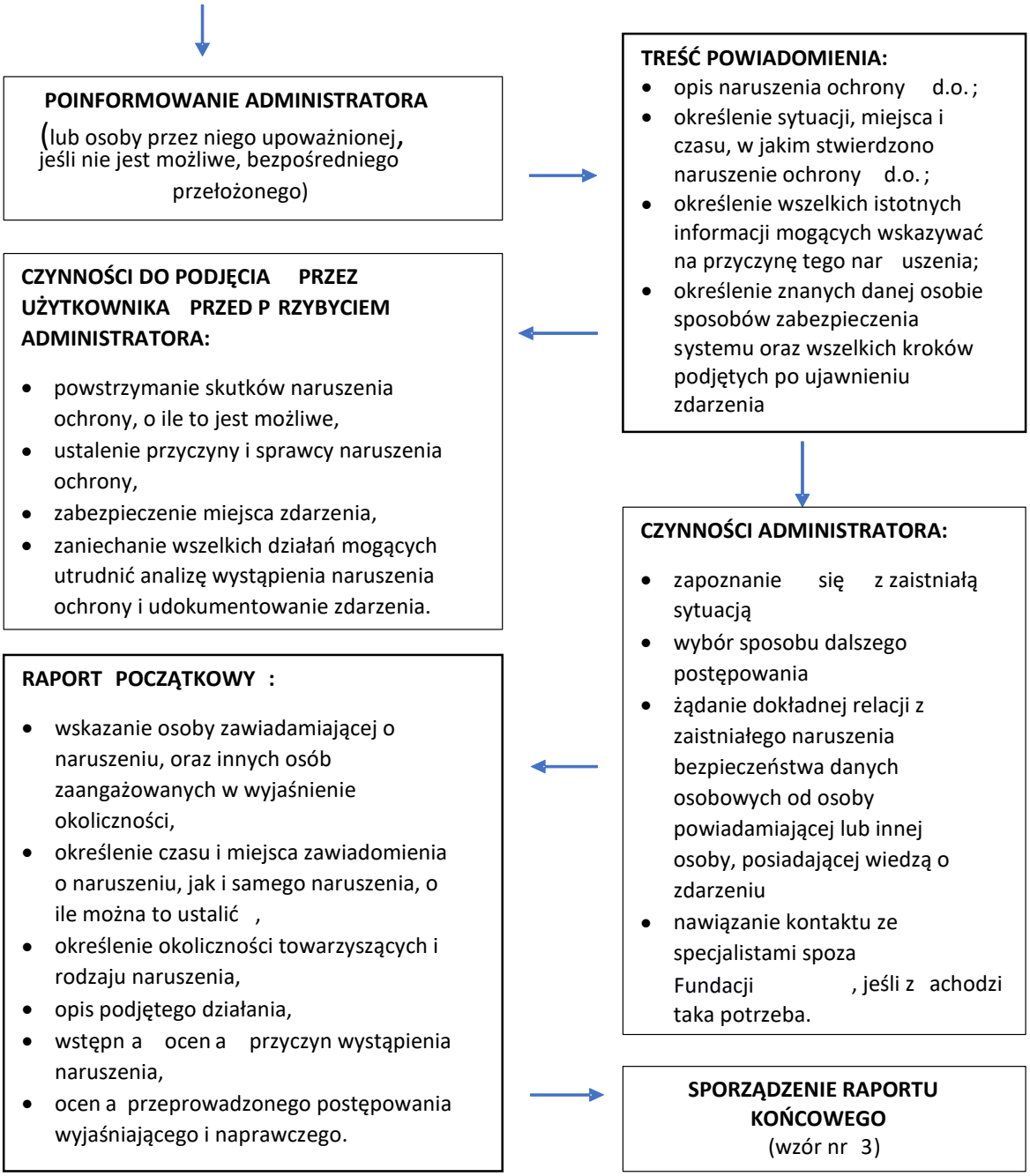
2. Rejestracji podlegają wszystkie przypadki awarii systemu, działania konserwacyjne w systemie oraz naprawy.

3. Naprawy i konserwacje sprzętu składającego się na system informatyczny odbywają się w miarę możliwości w siedzibie Fundacji.

4. W przypadku, gdy uszkodzenie sprzętu zawierającego nośnik danych, na którym zapisane są d.o. wymusza konieczność przekazania go poza siedzibę Fundacji, nośnik ten powinien zostać wymontowany.

§ 9
Procedura postępowania w razie naruszenia d.o.




POINFORMOWANIE ADMINISTRATORA
(lub osoby przez niego upoważnionej, jeśli nie jest możliwe, bezpośredniego przełożonego)
TREŚĆ POWIADOMIENIA:
opis naruszenia ochrony d.o.;
określenie sytuacji, miejsca i czasu, w jakim stwierdzono naruszenie ochrony d.o.;
określenie wszelkich istotnych informacji mogących wskazywać na przyczynę tego nar uszenia;
określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia
CZYNNOŚCI DO PODJĘCIA PRZEZ UŻYTKOWNIKA PRZED P RZYBYCIEM ADMINISTRATORA:
powstrzymanie skutków naruszenia ochrony, o ile to jest możliwe,
ustalenie przyczyny i sprawcy naruszenia ochrony,
zabezpieczenie miejsca zdarzenia,
zaniechanie wszelkich działań mogących utrudnić analizę wystąpienia naruszenia ochrony i udokumentowanie zdarzenia.
CZYNNOŚCI ADMINISTRATORA:
zapoznanie się z zaistniałą sytuacją
wybór sposobu dalszego postępowania
żądanie dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej lub innej osoby, posiadającej wiedzą o zdarzeniu
nawiązanie kontaktu ze specjalistami spoza Fundacji , jeśli z achodzi taka potrzeba.
RAPORT POCZĄTKOWY :
wskazanie osoby zawiadamiającej o naruszeniu, oraz innych osób zaangażowanych w wyjaśnienie okoliczności,
określenie czasu i miejsca zawiadomienia o naruszeniu, jak i samego naruszenia, o ile można to ustalić ,
określenie okoliczności towarzyszących i rodzaju naruszenia,
opis podjętego działania,
wstępn a ocen a przyczyn wystąpienia naruszenia,
ocen a przeprowadzonego postępowania wyjaśniającego i naprawczego.
SPORZĄDZENIE RAPORTU KOŃCOWEGO
(wzór nr 3)

DALSZE CZYNNOŚCI ADMINISTRATORA

↓

ZGŁOSZENIE NARUSZENIA ORGANOWI NADZORCZEMU (DO 72 GODZIN)
(wzór nr 3a)

→

NIE JEST KONIECZNE, GDY:

- jeśli jest mało prawdopodobne, aby naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

POINFORMOWANIE OSOBY KTÓREJ D.O. DOTYCZĄ O WYSTĄPIENIU NARUSZENIA
(wzór nr 3b)

→

NIE JEST KONIECZNE, GDY:

- zostały wdrożone odpowiednie techniczne i organizacyjne środki ochrony, które zostały zastosowane do d.o., których dotyczy naruszenie (np. szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym do dostępu do d.o.);
- następnie zostały zastosowane środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
- wymagałoby to niewspółmiernie dużego wysiłku (w takim wypadku należy wydać publiczny komunikat lub zastosować podobny środek, za pomocą którego osoby, zostają poinformowane w równie skuteczny sposób).

OCENA ZDARZENIA

- dokonuje wyznaczony przez Administratora zespół. W skład zespołu wchodzą:
  a. przewodniczący,
  b. koordynator zespołu,
  c. właściciele poszczególnych procesów oraz aktywów,
  d. eksperci.

1. Naruszenie ochrony d.o. oznacza każde naruszenie bez względu na jego przyczynę prowadzące do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do d.o. przesyłanych, przechowywanych lub w inny sposób przetwarzanych, a w szczególności:
   a. nieautoryzowany dostęp do d.o.;
   b. utratę nośników zawierających d.o.;
   c. nieautoryzowaną modyfikację lub zniszczenie d.o.;
   d. bezpodstawne udostępnienie d.o.;
   e. pozyskiwanie d.o. z nielegalnych źródeł.

§ 10
Gromadzenie d.o.

D.o. przetwarzane w Fundacji mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą, w szczególności od klientów albo od osób przez nich upoważnionych do działania w ich imieniu albo z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 11
Środki ochrony przetwarzania d.o.

1. Dostęp do pomieszczeń, w których przetwarzane są d.o. Fundacji podlega kontroli

2. Zabezpieczenia dotyczące pracowników i organizacji pracy:
   a) pracownicy mający dostęp do zbiorów zostali zaznajomieni z obowiązującymi przepisami dotyczącymi przetwarzania d.o. i procedurami wewnętrznymi określonymi w dokumentacji wewnętrznej,
   b) pracownicy są zobowiązani do utrzymywania w tajemnicy informacji uzyskanych w ramach pracy, w szczególności w zakresie stosowanych zabezpieczeń systemu informatycznego,
   c) osoby przetwarzające d.o. powinny posiadać upoważnienie do przetwarzania d.o.,
   d) prowadzona jest ewidencja osób upoważnionych do przetwarzania d.o.,
   e) pracownicy nie mogą udostępniać osobom trzecim haseł i kodów dostępu bez zgody Administratora.

3. Do zabezpieczeń programowych i zabezpieczeń transmisji należą:
   a) identyfikator i hasło dostępu do danych na poziomie aplikacji dla każdego użytkownika wyznaczony jest odrębny identyfikator, użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych d.o., do których mają uprawnienia,
   b) komputer, z którego możliwy jest dostęp do d.o. zabezpieczony jest hasłem uruchomieniowym, stosowane jest wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika, stosowana jest blokada hasłem podczas dłuższej nieaktywności użytkownika,
   c) ochrona sprzętu komputerowego, serwerów, komputerów osobistych, innych urządzeń, danych zapisanych na dyskach i podlegających przetwarzaniu w systemie, oprogramowania, haseł, baz danych i kopii zapasowych, wydruków i ochrona związana z przetwarzaniem danych dokumentacji papierowej,
   e) system informatyczny służący do przetwarzania d.o. chroni się przed zagrożeniami pochodzącymi z sieci publicznej przez wdrożenia fizycznych lub technicznych zabezpieczeń przed nieuprawnionym dostępem.

4. Dodatkowe środki ochrony fizycznej i zabezpieczenia przetwarzanych papierowych d.o. stosowane w Fundacji są następujące:
   a) urządzenia służące do przetwarzania d.o. znajdują się wyłącznie w szafkach zabezpieczonych zamkami lub kodami dostępu,
   b) dokumenty i inne nośniki zawierające d.o. i informacje poufne są składowane w zamykanych szafkach lub szyfrowane,
   c) dokumenty papierowe zawierające d.o. przechowywane są wyłącznie w zamykanych szafach,
   d) zabezpieczenie systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu,

§ 12
Upoważnienia do przetwarzania d.o.

1. Upoważnienie może zostać wydane na czas określony lub do odwołania. Cofnięcie upoważnienia jest konieczne wyłącznie w przypadku uprzedniego wydania upoważnienia na czas do odwołania.

2. Administrator zobowiązany jest do wydawania, ewidencjonowania i przechowywania imiennych upoważnień do przetwarzania d.o., cofniętych upoważnień i prowadzenia ewidencji osób upoważnionych do przetwarzania d.o.. Wzór ewidencji osób upoważnionych stanowi załącznik do Polityki.

3. Formularze dotyczące udzielenia upoważnienia, cofnięcia upoważnienia oraz wzór ewidencji osób upoważnionych do przetwarzania d.o. stanowią załącznik nr 4, nr 5 i nr 6 do niniejszej Polityki.

4. Brak ważnego imiennego upoważnienia do przetwarzania d.o. uniemożliwia powierzenie użytkownikowi wykonywania zadań i obowiązków związanych z przetwarzaniem d.o..

5. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te d.o. oraz sposoby ich zabezpieczenia również w przypadku ustania stosunku pracy.

6. Do przetwarzania d.o. mogą zostać dopuszczone wyłącznie osoby przeszkolone, którym Administrator nadał na piśmie lub w formie dokumentowej odpowiednie upoważnienie do przetwarzania d.o. – wzór upoważnienia do przetwarzania d.o. stanowi załącznik nr 4 do Polityki.

7. Z zastrzeżeniem ust. 3 niniejszego paragrafu, każdy dopuszczony do przetwarzania d.o. pracownik po odbyciu szkolenia oraz po otrzymaniu upoważnienia do przetwarzania d.o. składa na piśmie oświadczenie o poufności, którego treść uzależniona jest od zakresu obowiązków danego pracownika– wzory oświadczeń o poufności stanowią załączniki do Polityki.

8. W przypadku, gdy do przetwarzania d.o. dopuszczona jest osoba świadcząca usługi w ramach cywilnoprawnej formy zatrudnienia lub osoba prowadząca indywidualną działalność gospodarczą, stale współpracująca z Administratorem, z osobą taką, po nadaniu jej na piśmie lub w formie dokumentowej odpowiedniego upoważnienia do przetwarzania d.o., zawierana jest umowa o poufności – wzór umowy o poufności stanowi załącznik nr 8 do Polityki.

9. Administrator dołoży wszelkich starań, by każda osoba fizyczna działająca z jego upoważnienia, posiadająca dostęp do d.o., przetwarzała je wyłącznie na polecenie Administratora, chyba że wymaga tego od niej prawo Unii Europejskiej lub prawo państwa członkowskiego.

10. W przypadku przedłużającej się nieobecności osoby upoważnionej lub zaprzestania wykonywania przez nią części lub wszystkich obowiązków, uzasadniających potrzebę upoważnienia jej do przetwarzania d.o., upoważnienie musi zostać w odpowiednim zakresie odwołane – wzór odwołania upoważnienia stanowi załącznik nr 5 do Polityki.

11. Utrata uprawnień do przetwarzania d.o. objętych upoważnieniem może nastąpić w szczególności w przypadku:
    a. cofnięcia upoważnienia przez Administratora bez podania przyczyny;
    b. rozwiązania stosunku pracy bądź innego stosunku prawnego łączącego osobę upoważnioną z Administratorem;
    c. zmiany stanowiska pracy osoby upoważnionej u Administratora na stanowisko nieuzasadniające konieczności posiadania dostępu do zbiorów d.o., jeżeli nowy zakres czynności nie wykazuje obowiązków służbowych związanych z Przetwarzaniem d.o.;
    d. umyślnego naruszenia przez osobę upoważnioną zasad ochrony d.o. określonych w Rozporządzeniu, ustawie, Polityce

12. W przypadku utraty uprawnień do przetwarzania d.o., Administrator niezwłocznie odwołuje upoważnienie do przetwarzania d.o. oraz dokonuje zmian w ewidencji osób upoważnionych do przetwarzania d.o..

13. Dla wszystkich użytkowników uprawnienia nadawane są zgodnie z zasadą niezbędnego minimum (zasada minimalizacji danych) potrzebnego do wykonywania obowiązków pracowniczych lub służbowych.

14. Administrator Systemu Informatycznego – jeśli został powołany - w porozumieniu z Administratorem, a jeśli nie został powołany, to sam Administrator nadaje określone uprawnienia dostępu do systemów informatycznych służących do przetwarzania d.o..

15. Administrator Systemu Informatycznego – jeśli został powołany, na żądanie Administratora, nadaje, zmienia lub odwołuje uprawnienia w Systemie informatycznym służącym do przetwarzania d.o..

16. Do obsługi systemu informatycznego służącego do przetwarzania d.o. oraz urządzeń wchodzących w jego skład, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania d.o. nadane przez Administratora.

17. Użytkownicy powinni pracować na kontach zwykłych użytkowników. Praca na kontach Administracyjnych jest dopuszczalna tylko przez Administratora Systemu Informatycznego (jeśli został powołany) oraz upoważnionych przez niego osób.

18. W przypadku wycofania uprawnień użytkownika do Systemu informatycznego, w którym przetwarzane są d.o., Administrator Systemu Informatycznego – jeśli został powołany - niezwłocznie blokuje konto użytkownika i informuje o tym fakcie Administratora i inspektora ochrony danych.

19. Identyfikator nowego konta w Systemie informatycznym nadany zgodnie z wnioskiem przez Administratora Systemu Informatycznego – jeśli został powołany - musi być unikalny w obrębie Systemu.

20. W przypadku zmian przepisów dotyczących ochrony d.o. lub zasad przetwarzania i ochrony d.o. u Administratora osoba wyznaczona przez Administratora przeszkoli członków personelu.

21. Nieprzestrzeganie zasad określonych w Polityce stanowi w przypadku pracowników naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności pracowniczej określonej w Kodeksie pracy.

22. Jeżeli skutkiem działania określonego w ustępie powyżej jest szkoda, użytkownik:
    a. będący pracownikiem ponosi odpowiedzialność materialną na zasadach określonych w Kodeksie pracy,
    b. niebędący pracownikiem ponosi odpowiedzialność za zasadach ogólnych Kodeksu cywilnego.

§ 13
Powierzenie przetwarzania osobom trzecim – Procesor (Przetwarzający)

1. Powierzenie d.o. podmiotom mającym siedzibę w jednym z państw EOG podlega ogólnym zasadom powierzenia d.o. wynikającym z Rozporządzenia. Powierzenie d.o. podmiotom mającym

siedzibę w państwie trzecim lub organizacji międzynarodowej wymaga dodatkowo wypełnienia przesłanek i obowiązków nałożonych przepisami rozdziału V Rozporządzenia.

2. Dokonując wyboru Procesora Administrator korzysta z usług tylko takich Procesorów, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby Przetwarzanie danych spełniało wymogi przepisów i chroniło prawa osób, których dane dotyczą. Administrator bierze pod uwagę w szczególności fachową wiedzę, wiarygodność i zasoby Procesora.
3. Wystarczające gwarancje, o których mowa w ust. 1, Procesor może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 Rozporządzenia, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 Rozporządzenia.
4. Wzór umowy powierzenia przetwarzania d.o. oraz wzór postanowień regulujących Powierzenie przetwarzania d.o., niestanowiących odrębnej umowy, ale sformułowanych w celu uzupełnienia innych zawieranych umów, stanowią załączniki do Polityki.
5. Administrator odnotowuje w rejestrze czynności przetwarzania umowy powierzenia przetwarzania.
6. Administrator w miarę potrzeby przeprowadzi audyt Procesora w zakresie zgodności wykonywania przez niego czynności przetwarzania d.o. z postanowieniami umowy, o której mowa w § 29 Polityki, oraz obowiązującymi przepisami o ochronie Danych, w szczególności w celu sprawdzenia wykonywania przez Procesora ciążących na nim obowiązków.

§ 14
Zasady ujawniania danych odbiorcom innym niż Procesorowi

1. Ujawnianie d.o. odbiorcom innym niż Procesorowi dopuszczalne jest tylko w przypadku spełnienia jednej z przesłanek przetwarzania d.o. określonych w § 3 Polityki.
2. Ujawnianie d.o. może nastąpić tylko po uprzednim przedstawieniu wniosku o ich ujawnienie. Wzór wniosku stanowi załącznik do Polityki.
3. Ujawnienie d.o. innemu odbiorcy na podstawie ustnego wniosku może nastąpić wyłącznie w sytuacji, gdy nastąpi konieczność niezwłocznego udostępnienia tych danych. Osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.

§ 15
Prawa podmiotu danych

1. Administrator nie udostępnia d.o. osobom trzecim. Prawo wglądu do d.o. mają tylko osoby, których one dotyczą lub ich przedstawiciele ustawowi.

2. W celu realizacji swoich praw, podmiot danych kontaktuje się z inspektorem ochrony danych, jeżeli został on powołany. W innym wypadku podmiot Danych powinien kontaktować się z Agatą Wielgus, tel. 883699 959, e-mail: info@filmteractive.eu

3. Przetwarzanie d.o. przez Administratora powinno być zgodne z prawem i rzetelne. Dla osób, których dane dotyczą, powinno być przejrzyste, że dotyczące ich d.o. są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te d.o. są lub będą przetwarzane. Wszelkie informacje i wszelkie komunikaty związane z Przetwarzaniem tych d.o. powinny być łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem.

4. Osobom, których dane dotyczą, należy uświadamiać ryzyka, zasady, zabezpieczenia i prawa związane z Przetwarzaniem d.o. oraz sposoby wykonywania praw przysługujących im w związku z

takim Przetwarzaniem. W szczególności konkretne cele przetwarzania d.o. przez Administratora powinny być wyraźne, uzasadnione i określone w momencie ich zbierania.

5. Zgoda powinna być dobrowolnym, konkretnym, świadomym i jednoznacznym okazaniem woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na Przetwarzanie dotyczących jej d.o. w konkretnym celu. Na różne cele przetwarzania powinna być odbierana osobna Zgoda.

6. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

7. Wyrażenie zgody na Przetwarzanie danych nie może stanowić warunku zawarcia umowy lub świadczenia usługi.

8. Żądanie usunięcia danych lub sprzeciw osoba, której dane dotyczą, może złożyć w formie pisemnej, elektronicznej, w tym za pośrednictwem strony internetowej Administratora, telefonicznie lub ustnie do protokołu w siedzibie Administratora.

OBOWIĄZKI ADMINISTRATORA WZGLĘDEM OSÓB, KTÓRYCH DANE OSOBOWE DOTYCZĄ

OBLIGATORYJNE:

- Przy pozyskiwaniu danych: pouczenie o treści w § 13 ust. 1, 2 i 3 Rozporządzenia, chyba że:
  - danych nie pozyskano od osoby, której dane dotyczą,
  - ta osoba dysponuje już tymi informacjami;
  - udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
  - pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega Administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą.
- Obowiązek informacyjny (w rozsądnym terminie po pozyskaniu d.o. - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania d.o.; jeżeli d.o. mają być stosowane do komunikacji z osobą, której Dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub jeżeli planuje się ujawnić d.o. innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu). Wzory klauzul informacyjnych stanowią załączniki do Polityki.
- Zachowanie poufności danych zgodnie z obowiązkiem zachowania tajemnicy zawodowej
- wykazanie, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich D.o., jeśli zgoda ta jest wymagana,
- W przypadku planu zmiany celu przetwarzania danych, Administrator ponowne zwrócenie się do osoby, której dane dotyczą, o zgodę na przetwarzanie jej danych co do innego celu, dla którego dane były zbierane i przetwarzane
- Weryfikacja merytorycznej poprawności d.o. wskazanych w żądaniu sprostowania lub uzupełnienia danych i wyrażenie odmowy sprostowania, jeśli byłoby niezgodne z prawem,
- usunięcie danych, w przypadku, gdy:
  - d.o. nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
  - osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie, i nie ma innej podstawy prawnej przetwarzania;
  - osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 Rozporządzenia wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 Rozporządzenia wobec przetwarzania;
  - d.o. były przetwarzane niezgodnie z prawem;
  - d.o. muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator;

Wyjątek, gdy przetwarzanie jest konieczne:

- do korzystania z prawa do wolności wypowiedzi i informacji;
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 Rozporządzenia;
- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 Rozporządzenia, o ile prawdopodobne jest, że usunięcie danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
- do ustalenia, dochodzenia lub obrony roszczeń.

- w przypadku upublicznienia danych, które powinny być usunięte, podjęcie rozsądnych działań, w tym środków technicznych, by poinformować Administratorów przetwarzających te d.o., że osoba, której dane dotyczą, żąda, by Administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych d.o. lub ich replikacje.

NA WNIOSEK:

- ograniczenie przetwarzania d.o. w następujących przypadkach:
  - osoba kwestionuje prawidłowość d.o. - na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych;
  - Przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu d.o., żądając w zamian ograniczenia ich wykorzystywania;
  - dane nie są potrzebne do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
  - osoba wniosła sprzeciw na mocy art. 21 ust. 1 Rozporządzenia wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne,
- umożliwienie osobie, której dane dotyczą, wycofanie zgody w dowolnym momencie w taki sam sposób, w jaki nastąpiło jej wyrażenie,
- umożliwienie osobie uzyskania potwierdzenia, czy przetwarzane są d.o. jej dotyczące, a jeżeli ma to miejsce, również uzyskanie dostępu do nich,
- niezwłoczne sprostowanie nieprawidłowych danych,
- zaniechanie przetwarzania d.o. do celów marketingu bezpośredniego niezwłocznie po otrzymaniu sprzeciwu osoby, której dane dotyczą, wobec przetwarzania do takich celów,
- przekazanie d.o. bezpośrednio innemu Administratorowi, chyba że mogłoby ono niekorzystnie wpływać na prawa i wolności innych,
- poinformowanie osoby wnoszącej o zaprzestanie przetwarzania d.o. o dotychczasowych odbiorcach danych osobowych, osoba, której dane dotyczą, tego zażąda, mając na względzie dostępną technologię i zasoby.

§ 16
Zautomatyzowane przetwarzanie d.o.

1. Administrator dopuszcza podejmowanie decyzji, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołują skutki prawne wobec osoby, której dane dotyczą, lub w podobny sposób istotnie na nią wpływają, wyłącznie jeżeli taka decyzja:
   a. jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a Administratorem;
   b. jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega Administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
   c. opiera się na wyraźnej zgodzie osoby, której dane dotyczą.
2. W przypadkach, o których mowa w ust. 1 lit. a i c, na żądanie osoby, której dane dotyczą, Administrator zapewni weryfikację. Administrator umożliwi osobie, której dane dotyczą, wyrażenie własnego stanowiska i zakwestionowanie decyzji podjętej w sposób określony w ust. 1.
3. Decyzje, o których mowa w ust. 2, nie mogą opierać się na Szczególnych kategoriach d.o., chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) Rozporządzenia i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

§ 17
Przekazywanie danych osobowych poza Europejski Obszar Gospodarczy

1. Ujawnianie Danych osobowych podmiotom mającym siedzibę w jednym z państw Europejskiego Obszaru Gospodarczego podlega ogólnym zasadom przetwarzania Danych osobowych wynikającym z Rozporządzenia. Administrator danych z EOG, tak samo jak Administrator przetwarzający Dane na terytorium Polski, jest zobowiązany m.in. do wypełnienia jednego z warunków legalności przetwarzania Danych osobowych, przestrzegania zasad przetwarzania Danych określonych w § 4 oraz do wdrożenia odpowiednich środków technicznych i organizacyjnych, zapewniających odpowiedni stopień bezpieczeństwa danych.
2. Administrator przekazuje Dane do państwa trzeciego lub organizacji międzynarodowej wyłącznie pod warunkiem spełnienia kryteriów określonych poniżej, dbając o to, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w Rozporządzeniu.
3. Przekazanie Danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, jeżeli Komisja Europejska stwierdziła, że to Państwo trzecie, terytorium lub określone sektory w tym państwie trzecim lub dana Organizacja międzynarodowa zapewniają odpowiedni stopień ochrony; w braku decyzji Komisji Europejskiej, przekazanie Danych do państwa trzeciego może nastąpić, jeżeli:
    a. zostały zapewnione odpowiednie zabezpieczenia ochrony Danych osobowych niewymagające uzyskania specjalnego zezwolenia ze strony organu nadzorczego, za pomocą jednego z następujących instrumentów:
        - prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi;
        - wiążących reguł korporacyjnych, szczegółowo uregulowane w art. 47 Rozporządzenia;
        - standardowych klauzul ochrony Danych przyjętych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2 Rozporządzenia;
        - standardowych klauzul ochrony Danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2 Rozporządzenia;
        - zatwierdzonego kodeksu postępowania zgodnie z art. 40 Rozporządzenia wraz z wiążącymi i egzekwowalnymi zobowiązaniami Administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich gwarancji, w tym w odniesieniu do praw osób, których Dane dotyczą; lub
        - zatwierdzonego mechanizmu certyfikacji zgodnie z art. 42 Rozporządzenia wraz z wiążącymi i egzekwowalnymi zobowiązaniami Administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich gwarancji, w tym w odniesieniu do praw osób, których Dane dotyczą;
    b. zostały zapewnione odpowiednie zabezpieczenia ochrony Danych osobowych za pomocą jednego z następujących instrumentów:
        - klauzul umownych między Administratorem lub Procesorem a Administratorem, Procesorem lub odbiorcą danych w państwie trzecim lub organizacji międzynarodowej; lub
        - postanowień porozumień administracyjnych między organami lub podmiotami publicznymi, w których przewidziano egzekwowalne i skuteczne prawa osób, których Dane dotyczą - pod warunkiem uzyskania zezwolenia właściwego organu nadzorczego.
4. W braku decyzji Komisji Europejskiej lub w braku odpowiednich zabezpieczeń, o których mowa powyżej, jednorazowe lub wielokrotne przekazanie Danych osobowych do państwa trzeciego może nastąpić, wyłącznie pod warunkiem, że:
    a. osoba, której Dane dotyczą, została poinformowana o ewentualnym ryzyku, z którym – z uwagi na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz brak odpowiednich zabezpieczeń - może się dla niej wiązać proponowane przekazanie, i w sposób wyraźny wyraziła na nie zgodę;

b. przekazanie jest niezbędne do wykonania umowy między osobą, której Dane dotyczą, a Administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której Dane dotyczą;
c. przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której Dane dotyczą, między Administratorem a inną osobą fizyczną lub prawną;
d. przekazanie jest niezbędne ze względu na ważne względy interesu publicznego;
e. przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń;
f. przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której Dane dotyczą, lub innych osób, jeżeli osoba, której Dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; lub
g. przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem polskim ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes - ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie polskim.

§ 18
Postanowienia końcowe

1. Polityka wchodzi w życie z dniem 25 maja 2018 roku.
2. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w jakiejkolwiek formie.
3. Każdy użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zapoznany z przepisami Rozporządzenia i ustawy oraz postanowieniami Polityki, a także o zobowiązaniu się do ich przestrzegania.
4. Oświadczenie, o którym mowa w ustępie powyżej, złożone przez użytkownika będącego pracownikiem przechowywane jest jego w aktach osobowych.
5. W sprawach nieuregulowanych w Polityce zastosowanie mają przepisy Rozporządzenia i ustawy.