Zarządzenie nr 5/2018
Dyrektora Galerii Sztuki WOZOWNIA w Toruniu
z dnia 24.05.2018 r. w sprawie procedury wdrożenia RODO

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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)

wprowadza się procedury postępowania dla Galerii Sztuki WOZOWNIA w Toruniu w przypadku zgłoszenia żądań przez osoby fizyczne dotyczące danych osobowych oraz postępowania w przypadku wycieku danych osobowych

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Galerii Sztuki WOZOWNIA
w TORUNIU
Anna Jackowska
29.05.2018

Sprawdzono pod względem
formalno - prawnym
data 24.05.2018r.
Podpis

PROCEDURA POSTĘPOWANIA dla Galerii Sztuki WOZOWNIA w Toruniu w PRZYPADKU ZGŁOSZENIA ŻĄDAŃ PRZEZ OSOBY FIZYCZNE DOTYCZĄCE DANYCH OSOBOWYCH ORAZ PROCEDURA POSTĘPOWANIA W PRZYPADKU WYCIEKU DANYCH OSOBOWYCH

na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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. z 2016 r. Nr 119), zwanego dalej: **"RODO"**

1. Prawa osób fizycznych

Osobom fizycznym, których dane osobowe przetwarzamy przysługują następujące prawa (określone w art. 15-22, 34 RODO):

a) Prawo dostępu do danych osobowych przysługujące osobie, której dane dotyczą;
b) Prawo do sprostowania danych osobowych;
c) Prawo do usunięcia danych osobowych ("prawo do bycia zapomnianym");
d) Prawo do ograniczenia przetwarzania;
e) Prawo do przenoszenia danych osobowych;
f) Prawo do sprzeciwu;
g) Prawo do niepodlegania zautomatyzowanej decyzji (w tym profilowania);
h) Prawo do uzyskania zawiadomienia o naruszeniu ochrony danych osobowych;

Działania administratora tj. Galerii Sztuki WOZOWNIA w Toruniu (określone przykładowo w art. 12 RODO), które musi podjąć w związku z żądaniem wykonania prawa osoby fizycznej:

Administrator ma obowiązek udzielać wszelkich informacji osobom, których dane przetwarza, w zwięzłej i zrozumiałej formie oraz prowadzić z nimi komunikację w związku z wykonywaniem i ich praw. Informacji osobom fizycznym udziela się głównie na piśmie (w tym elektronicznie). Administrator ułatwia wykonanie praw przysługujących osobom, których dane dotyczą.

W przypadku zwrócenia się z żądaniem dotyczącym praw osoby fizycznej administrator ma obowiązek niezwłocznie, nie później niż w terminie miesiąca, udzielić informacji o podjętych działaniach. W razie potrzeby termin ten można wydłużyć do dwóch miesięcy z uwagi na skomplikowany charakter żądania lub liczbę żądań.

Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, to niezwłocznie, jednak nie później niż w terminie jednego miesiąca od dnia otrzymania żądania, informuje osobę o powodach nie podjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Jeżeli żądania są ewidentnie nieuzasadnione lub nadmierne, administrator może odmówić podjęcia działań lub pobrać rozsądną opłatę.

Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości.

Opis prawa:

a) **Prawo dostępu do danych** (art. 15 RODO) – osoba fizyczna jest uprawniona do uzyskania od administratora potwierdzenia czy przetwarza jej dane osobowe, a jeśli tak:
   - jakie są cele przetwarzania,
   - jakie kategorie danych osobowych są przetwarzane,
   - komu zostały lub zostaną przekazane dane osobowe (wystarczą kategorie odbiorców),
   - okres przechowywania gdy jego ustalenie jest możliwe,
   - Informacje o prawie żądania sprostowania czy też usunięcia lub ograniczenia przetwarzania danych osobowych, prawie wniesienia sprzeciwu, sprawie wniesienia skargi do organu nadzorczego,
   - informacje o źródle pochodzenia danych osobowych,
   - informacje o profilowaniu.

Administrator ma obowiązek dostarczenia osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Można pobrać rozsądną opłatę od takiej kopii wynikającą z kosztów administracyjnych związanych z jej sporządzeniem.

b) **prawo do sprostowania danych** (art. 16 RODO) – osoba której dane dotyczą ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych. Osoba taka ma również prawo do uzupełnienia niekompletnych danych osobowych.

c) **Prawo do usunięcia danych osobowych** (art. 17 RODO) - osoba fizyczna ma prawo żądania usunięcia dotyczących i danych osobowych, natomiast administrator ma obowiązek niezwłocznie usunąć te dane osobowe, w przypadku, gdy:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie (zgodnie z art. 6 ust. 1 lit. a) RODO) i nie ma innej podstawy prawnej przetwarzania;
c) osoba, której dane dotyczą, wnosi sprzeciw na mocy wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania (tj. sprzeciw do przetwarzania danych do marketingu bezpośredniego);

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Przepis ten nie ma zastosowania w następujących sytuacjach, w jakich przetwarzanie danych jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;

b) 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;

c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;

d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że zrealizowanie prawa do usunięcia danych, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub

e) do ustalenia, dochodzenia lub obrony roszczeń.

d) **prawo do ograniczenia przetwarzania (art. 18 RODO)** – w przypadku zgłoszenia żądania przez osobę fizyczną, administrator ma zakaz przetwarzania danych osobowych przez administratora (z wyjątkiem przechowywania danych) chyba że przetwarzanie w celu dochodzenia roszczeń lub ochrony praw innej osoby fizycznej lub prawnej, lub osoba której dane dotyczą wyraziła zgodę na inne rodzaje przetwarzania. Przypadki gdy niezbędne jest ograniczenie przetwarzania danych określa powyższy artykuł. Określa ono również czas na jaki ograniczenie przetwarzania jest konieczne. po uchyleniu ograniczenia przez administratora musi on poinformować o tym osobę, której dane dotyczą, a która żądała ograniczenia przetwarzania.

e) **Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO)** – istnieje obowiązek informowania przez administratora każdego odbiorcy danych osobowych o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania (dokonanego na podstawie któregoś z ww. praw) każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

f) **Prawo do przenoszenia danych (art. 20 RODO)** – w przypadku, gdy przetwarzanie danych odbywa się w sposób zautomatyzowany (np. w systemie informatycznym), osoba fizyczna ma

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Przepis ten nie ma zastosowania w następujących sytuacjach, w jakich przetwarzanie danych jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;

b) 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;

c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;

d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że zrealizowanie prawa do usunięcia danych, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub

e) do ustalenia, dochodzenia lub obrony roszczeń.

d) **prawo do ograniczenia przetwarzania (art. 18 RODO)** – w przypadku zgłoszenia żądania przez osobę fizyczną, administrator ma zakaz przetwarzania danych osobowych przez administratora (z wyjątkiem przechowywania danych) chyba że przetwarzanie w celu dochodzenia roszczeń lub ochrony praw innej osoby fizycznej lub prawnej, lub osoba której dane dotyczą wyraziła zgodę na inne rodzaje przetwarzania. Przypadki gdy niezbędne jest ograniczenie przetwarzania danych określa powyższy artykuł. Określa ono również czas na jaki ograniczenie przetwarzania jest konieczne. po uchyleniu ograniczenia przez administratora musi on poinformować o tym osobę, której dane dotyczą, a która żądała ograniczenia przetwarzania.

e) **Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO)** – istnieje obowiązek informowania przez administratora każdego odbiorcy danych osobowych o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania (dokonanego na podstawie któregoś z ww. praw) każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

f) **Prawo do przenoszenia danych (art. 20 RODO)** – w przypadku, gdy przetwarzanie danych odbywa się w sposób zautomatyzowany (np. w systemie informatycznym), osoba fizyczna ma

Naruszenie (tzw. wyciek) danych osobowych i prawo do uzyskania zawiadomienia o naruszeniu ochrony danych osobowych

Powyższe instytucje uregulowane zostały w art. 33 i 34 RODO.

Zgodnie z RODO "naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

W przypadku naruszenia danych osobowych należy poinformować o tym organ nadzorczy (Prezesa Urzędu Ochrony Danych Osobowych). Należy dokonać zgłoszenia **bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia**.

Nie **ma obowiązku zgłaszania naruszenia,** gdy jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu **po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia**.

Zgłoszenie musi:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Przykład zgłoszenia:

Naruszenie danych w postaci włamania się przez niewykrytego sprawcę do pomieszczenia, w którym znajdowały się dane osobowe pracowników spółki. Dotyczy to danych osobowych zawartych w umowach o pracę i aktach osobowych 10 pracowników. Brak jest pewności, czy sprawca lub sprawcy widzieli dokumenty, albowiem teczki nie były rozrzucone. Inspektorem danych osobowych jest ....., nr telefonu ..... Możliwymi konsekwencjami jest wyciek danych znajdujących się aktach pracowniczych. Administrator w

związku ze zdarzeniem postanowił zamontować drzwi antywłamaniowe oraz dodatkowo umieścić dane w sejfie.

Jeżeli przekazanie powyższych informacji jest niemożliwe, należy je przekazać, gdy tylko stanie się to możliwe.

Administrator **dokumentuje wszelkie naruszenia** ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja może być to w formie tabeli:

L.p.	Okoliczności naruszenia danych	Prawdopodobna data naruszenia	Data i godzina zgłoszenia PUODO naruszenia danych	Skutki naruszenia danych	Działania zaradcze	Wyznaczony inspektor ochrony danych (dane kontaktowe)	Kategoria i ilość osób, których dotyczy naruszenie, rodzaj danych osobowych
1.							

Zalecane jest jak najbardziej szczegółowe opisywanie naruszenia danych osobowych oraz jak najbardziej szczegółowe zgłaszanie naruszenia danych.

Zawiadomienie o naruszeniu osób, których dane dotyczą - prawo do uzyskania zawiadomienia o naruszeniu ochrony danych osobowych.

Jeżeli naruszenie ochrony danych osobowych może powodować **wysokie ryzyko naruszenia praw** lub wolności osób fizycznych, administrator **bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą**, o takim naruszeniu.

Zawiadomienie musi zostać napisane prostym i zrozumiałym językiem oraz musi:

a) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
b) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
c) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Nie ma konieczności zawiadamiania o naruszeniu danych w przypadkach, gdy:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.