Załącznik Nr 8 do Polityki Ochrony Danych Osobowych

REJESTR NARUSZEŃ DOTYCZĄCY PRZYJĘTYCH SPOSOBÓW OCHRONY DANYCH OSOBOWYCH ORAZ INCYDENTÓW BEZPIECZEŃSTWA DANYCH

L. P.	Opis / okoliczności naruszenia/ incydentu	Skutki naruszenia/ incydentu	Liczba osób których dotyczy naruszenie /incydent	Przewidziane działania zaradcze	Data rozpoczęcia wdrożenia działań	Data zakończenia wdrażania działań	Osoba odpowiedzialna za wdrożenie działań	Analiza czy konieczne jest zawiadomienie organu nadzorczego lub osób których dane dotyczą
1.								
2.								
3.								
4.								

Przykładowy opis naruszeń i incydentów, które powinny zostać zarejestrowane i wymagające dokonania analizy ryzyka naruszenia praw i wolności osób fizycznych:

1) zgubienie, kradzież utrata nośników danych zawierających dane osobowe (w tym nośników elektronicznych),
2) nieuprawniony dostęp osób trzecich do danych osobowych,
3) niepoprawnie zaadresowana korespondencja (w tym e-mail),
4) korespondencja e-mail seryjna z ujawnieniem adresów mailowych adresatów w przypadku np. wysyłki e-maili do uczestników wyjazdów,
5) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
6) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników),
7) nieodpowiednie usunięcie danych (np. wyrzucenie na śmietnik dokumentacji która nie została zniszczona w niszczarkach, wyrzucenie niezniszczonych nośników elektronicznych).

Opis postępowania w przypadku wykrycia incydentu i naruszenia.

W przypadku stwierdzenia naruszenia lub incydentu w ochronie danych osobowych Administrator Danych Osobowych/upoważniony kierownik działu przy udziale Inspektora Ochrony Danych, przeprowadza postępowanie wyjaśniające, w toku którego:

1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
2) zabezpiecza ewentualne dowody,
3) ustala osoby odpowiedzialne za naruszenie,
4) podejmuje działania naprawcze (usunięcie skutków incydentu i ograniczenie szkody),
5) inicjuje ewentualne działania dyscyplinarne,
6) wyciąga wnioski i rekomenduje działania korygujące, które będą zmierzać do wyeliminowania prawdopodobieństwa, że w przyszłości wystąpi podobny incydent lub naruszenie w ochronie danych osobowych,
7) dokumentuje prowadzone postępowanie.

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu.

1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia -zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W każdym więc przypadku należy wykonać procedurę oceny czy naruszenie będzie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, wykorzystując przy tym procedurę analizy ryzyka zawartą w Polityce Ochrony Danych Osobowych przyjętej przez Administratora.
2. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
3. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi.
4. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
   1) 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;

2) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
4) 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.

5. Jeżeli - i w zakresie, w jakim - informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
6. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.

1. 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.
2. Zawiadomienie, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d).
3. Zawiadomienie, nie jest wymagane, w następujących przypadkach:
   1) 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;
   2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
   3) 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.
4. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy - biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko - może zażądać od Administratora takiego działania lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust.3.

Opis postępowania w przypadku wykrycia incydentu i naruszenia – jako Podmiot przetwarzający.

1. Po stwierdzeniu naruszenia ochrony danych osobowych Biebrzański Park Narodowy bez zbędnej zwłoki, zgłasza ten fakt Powierzającemu (Administratorowi), wskazując w zgłoszeniu:
   1) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie oraz przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
   2) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
   3) opis możliwych konsekwencji naruszenia ochrony danych osobowych,
   4) opis środków zastosowanych lub proponowanych przez Procesora w celu zapobieżeniu naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.
2. Zgłoszenie naruszenia ochrony danych osobowych następuje drogą elektroniczną.

3. Jeśli informacji, o których mowa w ust. 1 pkt. 3 i pkt. 4 powyżej, nie da się udzielić w tym samym czasie co pozostałych, Procesor ma obowiązek udzielić ich Powierzającemu w terminie 24 godzin od przekazania informacji o naruszeniu.
4. Do czasu przekazania Procesorowi instrukcji postępowania w związku z naruszeniem ochrony danych, Procesor podejmuje bez zbędnej zwłoki wszelkie działania mające na celu ograniczenie i naprawnienie negatywnych skutków naruszenia.
5. Bez wyraźnej instrukcji Powierzającego, Procesor nie jest zobowiązany do informowania o naruszeniu ochrony danych osobowych organu nadzorczego ani osób, których dane dotyczą.
6. Procesor dokumentuje wszelkie naruszenia ochrony powierzonych mu przez Powierzającego danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze, jak również udostępnia tę dokumentację Powierzającemu na jego żądanie.