Załącznik nr 1
do Zarządzenia Nr 47/2018
Dyrektora Ośrodka Sportu i Rekreacji w Łukowie
z dn. 14.06.2018

POLITYKA OCHRONY DANYCH OSOBOWYCH W OŚRODKU SPORTU I REKREACJI W ŁUKOWIE

Załączniki:

1. *Załącznik Nr 1 – Klauzula informacyjna.*
2. *Załącznik Nr 2 – Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.*
3. *Załącznik Nr 3- Wykaz pomieszczeń gdzie dane są przetwarzane.*
4. *Załącznik Nr 4 – Formularz rejestracji incydentów.*
5. *Załącznik Nr 5 – Regulamin Ochrony Danych.*
6. *Załącznik Nr 6 – Oświadczenie o zapoznaniu się z Regulaminem Ochrony Danych Osobowych.*
7. *Załącznik Nr 7 – Wykaz zabezpieczeń.*
8. *Załącznik Nr 8 – Instrukcja Zarządzania Systemem Informatycznym.*
9. *Załącznik Nr 9 – Polityka Zrządzania Ryzykiem w procesie przetwarzania danych osobowych.*
10. *Załącznik Nr 10 – Upoważnienie do przetwarzania danych osobowych.*
11. *Załącznik Nr 11 – Cofnięcie upoważnienia do przetwarzania danych osobowych.*
12. *Załącznik Nr 12 – Ewidencja osób upoważnionych.*
13. *Załącznik Nr 13 – Rejestr czynności przetwarzania danych osobowych w OSiR w Łukowie.*
14. *Załącznik nr 14 – Wykaz zbiorów danych.*

Załącznik nr 1
do Zarządzenia Nr 47/2018
Dyrektora Ośrodka Sportu i Rekreacji w Łukowie
z dn. 14.06.2018

SPIS TREŚCI

Załącznik nr 1
do Zarządzenia Nr 47/2018
Dyrektora Ośrodka Sportu i Rekreacji w Łukowie
z dn. 14.06.2018

POLITYKA BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH

Rozdział 1

POSTANOWIENIA OGÓLNE

§ 1

Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych" zwany dalej Polityką ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Ośrodku Sportu i Rekreacji w Łukowie.

Dokument ten jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 27.04.2014 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1).

Skróty i definicje zawarte w Polityce ochrony danych osobowych:

1. **Polityka** – oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
2. **RODO** - oznacza rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 27.04.2014 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1).
3. **Dane** – oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.
4. **Dane dzieci** – oznaczają dane osób poniżej 16 roku życia.
5. **Dane szczególnych kategorii** – dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
6. **Osoba** – osoba, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
7. **IODO lub Inspektor** – Inspektor Ochrony Danych Osobowych.

8. **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
9. **Administrator Danych Osobowych** - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych.
10. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
11. **Stacja robocza** – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.
12. **Bezpieczeństwo systemu informatycznego** - wdrożenie przez administratora danych osobowych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
13. **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
14. **Osoba upoważniona** - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych (lub osobę uprawnioną przez niego) i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu (listę osób upoważnionych do przetwarzania danych osobowych posiada administrator bezpieczeństwa informacji w sytuacji kiedy zostanie powołany).
15. **Użytkownik systemu** - osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
16. **Osoba uprawniona** - osoba posiadająca upoważnienie wydane przez administratora danych osobowych do wykonywania w jego imieniu określonych czynności.

§ 2

Filary ochrony danych osobowych:

1. **Poufność** – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
2. **Integralność** – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany,
3. **Dostępność** – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot,
4. **Rozliczalność** – możliwość jednoznacznego przypisania działań poszczególnym osobom,

5. **Autentyczność** – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
6. **Niezaprzeczalność** – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
7. **Niezawodność** – zamierzone zachowania i skutku są spójne,

Zasady ochrony danych OSiR

1. W oparciu o podstawę prawną i zgodnie z prawem (legalizm);
2. Rzetelnie i uczciwie (rzetelność);
3. W sposób przejrzysty dla osoby, której dane dotyczą (transparentność)
4. W konkretnych celach i nie „na zapas" (minimalizacja);
5. Nie więcej niż potrzeba (adekwatność);
6. Z dbałością o prawidłowość danych (prawidłowość);
7. Nie dłużej niż potrzeba (czasowość);
8. Zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

Za przestrzeganie zasad ochrony i bezpieczeństwa danych w komórkach organizacyjnych odpowiedzialna jest osoba wyznaczona przez Dyrektora OSiR.

§ 3

Realizację zamierzeń określonych w § 2 ust. 2 powinny zagwarantować następujące założenia:

1. wdrożenie procedur określających postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich odpowiedzialność za bezpieczeństwo tych danych,
2. przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,
3. przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory), zapewniających im dostęp do różnych poziomów baz danych osobowych – stosownie do indywidualnego zakresu upoważnienia,
4. podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,
5. okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
6. opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,
7. śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych:
   a. w miarę możliwości organizacyjnych i techniczno - finansowych
   b. wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania

systemami informatycznymi, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

§ 4

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:
   a. nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń , w których się one znajdują,
   b. wszelkie modyfikacje danych osobowych lub próby ich dokonania przez osoby nieuprawnione (np. zmian zawartości danych, utrata całości lub części danych),
   c. naruszenie lub próby naruszenia integralności systemu,
   d. zmianę lub utratę danych zapisanych na kopiach zapasowych,
   e. naruszenie lub próby naruszenia poufności danych lub ich części,
   f. nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
   g. udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
   h. zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w systemy informatyczne zmierzające do zakłócenia ich działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemach informatycznych lub kartotekach,
   i. inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy.
2. Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

Rozdział 2

KOMPETENCJE I ODPOWIEDZIALNOŚĆ

W ZARZĄDZANIU BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

§ 5

Za przetwarzanie danych osobowych niezgodne z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w kodeksie pracy.

Administrator Danych Osobowych (ADO):

1. Formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych.
3. Odpowiada za zgodne z prawem przetwarzanie danych osobowych.

Pracownik Przetwarzający Dane:

1. Chroni prawo do prywatności osób fizycznych powierzających swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w polityce bezpieczeństwa i ochrony przetwarzania danych osobowych i instrukcji zarządzania systemem informatycznym,
2. Zapoznaje się z zasadami określonymi w polityce bezpieczeństwa i ochrony przetwarzania danych osobowych i instrukcji zarządzania systemem informatycznym oraz składa oświadczenie o znajomości zawartych w nich przepisów,

Inspektor Ochrony Danych Osobowych

Status

1. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

2. Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

3. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

4. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.

5. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności

co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.

6. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

Zadania

1. **informowanie administratora,** podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2. **monitorowanie przestrzegania niniejszego rozporządzenia**, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3. **udzielanie na żądanie zaleceń co do oceny skutków** dla ochrony danych oraz monitorowanie jej wykonania;
4. **współpraca z organem nadzorczym;**
5. **pełnienie funkcji punktu kontaktowego** dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Rozdział 3

ZAGROŻENIA BEZPIECZEŃSTWA

§ 6

1. Charakterystyka możliwych zagrożeń:

   a. **Zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu,

   b. **Zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki przetwarzających dane, pozostawienie danych lub pomieszczeń bez nadzoru, błędy operatorów systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych lub naruszenia ich poufności,

c. **Zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenia, gdzie występują naruszenia poufności danych. Zagrożenia te możemy podzielić na: nieuprawniony dostęp z zewnątrz (włamanie), nieuprawniony dostęp do danych w wewnątrz (przez osoby nieuprawnione),

§ 7

2. Lista potencjalnych zagrożeń bezpieczeństwa danych:

Poniżej przedstawiono listy potencjalnych zagrożeń bezpieczeństwa danych z podziałem na zagrożenia miejsc przetwarzania oraz rodzajów danych, tj. zbiorów przetwarzanych tradycyjnie (papierowo) oraz z wykorzystaniem systemów informatycznych.

W każdym przypadku, w sytuacji stwierdzenia wystąpienia któregokolwiek z zagrożeń należy niezwłocznie powiadomić Administratora danych.

a. Zagrożenia miejsc przetwarzania danych:
   - Włamania od strony okien – wybite szyby, niedomknięte skrzydła.
   - Włamania od strony drzwi – zerwane plomby, uszkodzone klamki, źle działające zamki, niedomknięte drzwi, ślady po narzędziach.
   - Oddziaływanie czynników zewnętrznych – wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana.
   - Pozostawienie niezamkniętych drzwi lub okien – jeżeli w pomieszczeniu nie pozostają osoby uprawnione do przetwarzania danych.
   - Pozostawienie bez nadzoru osób nieuprawnionych do przebywania w pomieszczeniach.

b. Zagrożenia związane z tradycyjnym przetwarzaniem danych:
   - Pozostawienie danych na biurkach, półkach, regałach, itp. po zakończeniu pracy.
   - Pozostawienie dokumentów zawierających dane osobowe w kserokopiarce lub skanerze.
   - Pozostawienie po zakończeniu pracy otwartych szaf, w których gromadzone są dane osobowe.
   - Przechowywanie dokumentów w miejscach do tego nieprzeznaczonych.
   - Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.
   - Przetwarzanie danych przez osoby nieuprawione.
   - Nieuzasadnione sporządzanie kserokopii danych.

c. Zagrożenia związane z przetwarzaniem danych za pomocą systemów informatycznych:

- Dopuszczenie zapisywania na nośniki zewnętrzne wynoszone poza obszar przetwarzania lub przesyłanie poprzez Internet danych niezaszyfrowanych.
- Dopuszczanie do nieuzasadnionego kopiowania dokumentów i utraty kontroli nad kopią.
- Sporządzanie kopii danych w sytuacjach nie przewidzianych procedurą.
- Utrata kontroli nad kopią danych osobowych.
- Podmiana lub zniszczenie nośników z danymi osobowymi.
- Pozostawienie zapisanego hasła dostępu do bazy danych.
- Samodzielne instalowanie jakiegokolwiek oprogramowania.
- Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.
- Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.
- Odczytywanie dysków przenośnych i innych nośników przed sprawdzeniem ich programem antywirusowym.
- Niezabezpieczenie komputera zasilaczem awaryjnym podtrzymującym napięcie na wypadek braku zasilania.
- Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania osób nieuprawnionych.
- Ujawnianie sposobu działania aplikacji oraz jej zabezpieczeń osobom niepowołanym.
- Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.
- Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.
- Pojawianie się komunikatów alarmowych.
- Awarie sprzętu i oprogramowania, które mogą wskazywać na działanie osób trzecich.
- Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.
- Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.
- Dopuszczanie, aby osoby nieuprawnione, podłączały jakikolwiek urządzenia,

demontowały elementy sieci lub dokonywały innych manipulacji.

- Ślady manipulacji przy układach sieci komputerowej lub komputerach.
- Obecność nowych urządzeń i kabli o nieznanym przeznaczeniu i pochodzeniu.
- Naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji.

§ 8

3. Przedsięwzięcia zabezpieczające przed naruszeniem ochrony danych osobowych:
Na podstawie przeprowadzonej charakterystyki możliwych zagrożeń podjęto zabezpieczenia, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, Administrator danych wprowadza określone poniżej środki organizacyjne:

- Przetwarzanie danych osobowych w OSiR w Łukowie może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
- Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie. Wzór upoważnienia stanowi do niniejszej dokumentacji.
- Odwołanie upoważnienia następuje na piśmie,(załącznik nr 11)
- Każdy pracownik OSiR w Łukowie musi odbyć szkolenie z zakresu ochrony danych osobowych. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.
- Ponadto każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa.
- Nie należy gromadzić w podręcznej dokumentacji danych osobowych. Wszystkie dane niezbędne do prawidłowej pracy powinny znajdować się w zbiorach. Jeżeli posiadane druki lub zestawienia są niezbędne należy je zanonimizować (usunąć dane osobowe, np. adres, pesel, pozostawiając tylko nazwiska, imiona itd.).
- Dokumenty zawierające dane osobowe należy niszczyć w specjalistycznych niszczarkach.
- Każdorazowe zbieranie danych zgodnie z art. 24 oraz 25 ustawy o ochronie danych osobowych rodzi obowiązek informacyjny. Obowiązek należy realizować umieszczając odpowiednią treść informacyjną pod formularzem z danymi.
- Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

- Dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza biuro OSiR lub przesyłane pocztą elektroniczną, należy zabezpieczyć poprzez nadanie im haseł odczytu.
- Zbiory osobowe przetwarzane elektronicznie należy zabezpieczać poprzez wykonywanie kopii bezpieczeństwa, zapisywanych na zewnętrznych nośnikach i przechowywanych pod zamknięciem.
- Pliki edytorów tekstu lub arkuszy kalkulacyjnych należy traktować jak kopie zbiorów, z których pochodzą przetwarzane w nich dane i odpowiednio zabezpieczać stosując wytyczne zawarte w Instrukcji zarządzania systemem informatycznym będącej częścią niniejszej dokumentacji.

§ 9

Wykaz potencjalnych środków technicznych stosowanych w celu ochrony danych osobowych

1. **Ogólna ochrona budynku** – alarm antywłamaniowy, całodobowy dozór służb ochrony, gaśnice lub systemy p-poż.
2. **Zabezpieczenia okien** – pomieszczenia można dodatkowo zabezpieczyć poprzez montaż krat, rolet lub szyb antywłamaniowych, zwłaszcza, jeśli istnieje do nich dostęp przez tarasy, dachy niższych budynków, drabiny p-poż, itp.
3. **Zabezpieczenie drzwi** – w zależności od kategorii danych i zagrożeń zastosowane są drzwi tradycyjne zamykane na klucz lub p-pożarowe, zaś w miejscach szczególnie narażonych na zagrożenia - drzwi antywłamaniowe.
4. **Zabezpieczenia zbiorów tradycyjnych (papierowych)** – w zależności od kategorii danych i zagrożeń do przechowywania danych można stosować szafy tradycyjne zamykane na klucz, szafy metalowe lub sejfy (dla danych szczególnie ważnych). Dane przeznaczone do zniszczenia niszczone są w niszczarkach.
5. **Zabezpieczenia zbiorów elektronicznych** – dane elektroniczne zabezpieczone są poprzez wyposażenie komputerów w zasilacze awaryjne podtrzymujące napięcie na wypadek braku zasilania oraz w programy antywirusowe. Kopie danych gromadzone są w szafach metalowych lub sejfach.

Rozdział 4

POSTĘPOWANIE W WYPADKU KLĘSKI ŻYWIOŁOWEJ

§ 10

Klęską żywiołową jest katastrofa, spowodowana działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.

§ 11

W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

§ 12

1. O zagrożeniu, jego skali i podjętych krokach zaradczych pracownik upoważniony zobowiązany jest niezwłocznie powiadomić dyrektora, a jeżeli jest to niemożliwe w następnej kolejności jego zastępcę jeśli jest to również niemożliwe z kierownikami działów.
2. Numery telefonów Dyrektora/Administratora Danych Osobowych, Zastępcy Dyrektora oraz Kierowników Działów z którymi należy się kontaktować na wypadek klęski żywiołowej powinny być znane pracownikom.

§ 13

Osoby biorące udział w akcji ratunkowej, mają prawo wejść do pomieszczeń w których przetwarzane są dane osobowe bez dopełniania obowiązku podpisania niezbędnych upoważnień.

§ 14

W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy, przebywający w pomieszczeniach, w których przetwarzane są dane osobowe, obowiązani są do przerwania pracy, a w miarę możliwości przed opuszczeniem tych pomieszczeń do:

1. Zamknięcia systemu informatycznego.
2. Zabezpieczenia danych osobowych gromadzonych w kartotekach.

§ 15

W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Danych Osobowych oraz obecni użytkownicy powinni, w miarę możliwości, zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem.
Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych Osobowych, obecnych przy akcji ratunkowej.

Rozdział 5

INWENTARYZACJA DANYCH

§ 16

Dane osobowe wymagające ochrony przedstawione są w postaci zbiorów. Administrator opracował je w postaci papierowej. (Załącznik Nr 2). W OSiR została opracowana również Polityka Zarządzania Ryzykiem w przetwarzaniu danych osobowych, określająca zasady szacowania skali ryzyka i prawdopodobieństwa jego wystąpienia (Załącznik Nr 9).

Opis zbiorów obejmuje takie informacje, jak:

1. Nazwę zbioru;
2. Charakter, zakres dokumentowanych danych osobowych;
3. Dostępność do zbiorów;
4. Zastosowany poziom bezpieczeństwa;
5. Aktywa służące do przetwarzania (programy).

Rozdział 6

PRZETWARZANIE DANYCH OSOBOWYCH

§ 17

1. Administrator zapewnia, że:
   a. dane osobowe są przetwarzane legalnie na podstawie art. 6 i 9 RODO;
   b. zakres danych osobowych jest adekwatny do celów przetwarzania, z zachowaniem zasady minimalizacji danych;
   c. Administrator przechowuje dane osobowe przez konkretnie określony czas, z uwzględnieniem zasad określonych w Jednolitym Rzeczowym Wykazie Akt.
   d. wobec osób, których dane są przetwarzane wykonano obowiązek informacyjny (art. 12, 13, 14 RODO) wraz ze wskazaniem: prawa dostępu do danych osobowych, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, „bycia zapomnianym";
   e. osoby, których dane osobowe są przetwarzane zostały poinformowane o funkcji IODO i przekazano dane kontaktowe;
   f. potwierdzenie danych osobowych zgodnie z prawem znajduje się w (załączniku Nr 2) Wykaz Zbiorów Danych Osobowych.
   g. wzory klauzul informacyjnych znajdują się w (załączniku nr 1).
2. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego oraz kartotek odbywa się wyłącznie na obszarze wyznaczonym przez Administratora Danych Osobowych.
3. Przetwarzanie danych osobowych za pomocą urządzeń przenośnych może odbywać się

poza obszarem przetwarzania danych wyłącznie za zgodą Administratora Danych Osobowych czy też Inspektora Ochrony Danych Osobowych w przypadku, gdy został powołany.

4. Szczegółowy wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe określa (załącznik nr 3) do Polityki Ochrony Danych Osobowych.

§ 18

Upoważnienia

1. Administrator odpowiada za nadawanie/anulowanie upoważnień do przetwarzania danych w zbiorach papierowych i systemach informatycznych.
2. Każda osoba upoważniona może przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisów prawa.
3. Upoważnienia nadawane są na wniosek przełożonych/kierowników działów. Upoważnienia określają zakres operacji na danych.
4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, wykonania czynności służbowych.

Administrator prowadzi ewidencję upoważnień w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych (Załącznik Nr 12)

§ 19

W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano

przetwarzanie danych osobowych, należy zapewnić, aby:

1. Wydawanie kluczy do pomieszczeń podlegało kontroli sekretariatu i kierownika działu.
2. Pracownicy Administratora Danych Osobowych są zobowiązani do przestrzegania zasad określających dopuszczalne sposoby przemieszczania się osób trzecich w obrębie pomieszczeń, w których przetwarzane są dane osobowe.
3. Przebywanie osób trzecich w pomieszczeniach może odbywać się wyłącznie w obecności użytkowników lub za zgodą Administratora Danych Osobowych.

§ 20

1. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko upoważnieni użytkownicy oraz Informatyk.
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, osób innych, niż wymienione w ust. 1, jest możliwy wyłącznie w obecności, co najmniej jednego użytkownika lub za zgodą Administratora Danych Osobowych.
3. Przebywanie użytkownika po godzinach pracy w pomieszczeniach, w których

przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą kierownika komórki organizacyjnej.

§ 21

W trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych jest zabronione.

§ 22

1. Administrator Danych Osobowych jest odpowiedzialny za całość zagadnień dotyczących ochrony i bezpieczeństwa danych osobowych.
2. Kierownicy komórek organizacyjnych zobowiązani są do przestrzegania przepisów o ochronie danych osobowych na terenie podległych komórek organizacyjnych, a także do ścisłej współpracy z Administratorem Danych Osobowych.

§ 23

Szczegółowy wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania określa (załącznik Nr 2).

Niszczenie danych osobowych

§ 24

Ustawa o ochronie danych osobowych nakłada na podmioty zobowiązane do jej stosowania obowiązek należytego przetwarzania takich danych, tak, aby spełniony został podstawowy cel ustawy w postaci zapewnienia każdemu ochrony dotyczących go danych osobowych. Jednym z obowiązków administratora danych osobowych w zakresie ich przetwarzania jest ich usuwanie, w momencie kiedy ustanie celowość ich przetwarzania zgodnie z wytycznymi wynikającymi z odrębnych ustaw.

Usuwanie danych osobowych, polega na:

a) trwałym, fizycznym ich zniszczeniu wraz z ich nośnikami w stopniu uniemożliwiającym ich odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod,
b) anonimizacji danych osobowych, zbiorów polegającej na pozbawieniu danych osobowych, ich zbiorów – cech umożliwiających identyfikację osób fizycznych, których dane dotyczą.

W zależności od nośnika, na którym przechowywane są dane osobowe, ich usuwanie polega na:

1. Dokumentacja tradycyjna (wydruki, notatki, dokumenty) – należy dokumentację zniszczyć bądź zanonimizować w sposób uniemożliwiający odczyt. Zgodnie z obowiązującą normą DIN 66399 opracowaną przez *Standards Committee for*

Information Technology and Applications (*Komitet Normalizacyjny ds. Technik Informacyjnych i ich Zastosowań*) niszczarki stosowane do niszczenia danych osobowych powinny spełniać poniższe wymagania:

a. Klasa B: Ochrona przeznaczona dla danych poufnych, przeznaczonych dla wąskiego grona odbiorców.
b. Stopień 3: Nośniki z danymi chronionymi i poufnymi, a także danymi osobowymi, które wymagają większej ochrony - kategoria P-3 dla papieru,
c. Stopień 4: Nośniki z danymi szczególnie chronionymi i poufnymi, a także z danymi osobowymi, które podlegają większej ochronie, takie jak dane wrażliwe - kategoria P-4 dla papieru

2. Nośniki elektroniczne (pendrive/karty pamięci/dyski twarde SSD) – obecnie istniejące sposoby niszczenia danych można podzielić na dwie główne grupy metod:

a. Niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych. Istnieje specjalne oprogramowanie dostępne na rynku służące do nadpisywania (definitywnego usuwania) danych. Wadą tej metody jest możliwość częściowego odzyskania danych za pomocą specjalistycznego oprogramowania, zaletą natomiast możliwość ponownego wykorzystania nośnika,
b. Niszczenie sprzętowe – polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń. Wadą tej metody jest brak możliwości ponownego wykorzystania nośnika, zaletą natomiast całkowity brak możliwości nawet częściowego odzyskania danych,

3. Nośniki magnetyczne (dyski twarde HDD) – oprócz sposobów niszczenia danych dostępnych dla nośników elektronicznych, istnieje również możliwość demagnetyzacji nośników, jako jednego z rodzajów niszczenia sprzętowego.

Niezależnie od nośnika, na którym są przechowywane dane osobowe przeznaczone do zniszczenia, samo ich zniszczenie powinno odbyć się komisyjnie, a z samej operacji powinien zostać sporządzony protokół.

Rozdział 7

ZARZĄDZANIE RYZYKIEM

§ 25

Ryzyka to niepewne zdarzenie lub zbiór zdarzeń, które w przypadku ich wystąpienia będą mieć wpływ na bezpieczeństwo informacji. Zarządzanie ryzykiem odnosi się do systematycznego stosowania procedur dotyczących zadań identyfikowania i oceniania ryzyk, a następnie planowania i wdrażania reakcji na nie.

1. Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.

2. Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru danych osobowych lub grupy zbiorów charakteryzujących się podobieństwem celów i sposobów przetwarzania, odrębnie dla każdego zbioru.

§ 26

Procedury zarządzania ryzykiem

W OSiR w Łukowie procedura zarządzania ryzykiem obejmuje pięć następujących kroków:

1. Identyfikuj

2. Oceniaj

3. Planuj

4. Wdrażaj

5. Komunikuj

1. **Identyfikowanie ryzyk** polega na możliwym rozpoznaniu zagrożeń, które mogą wpływać na bezpieczeństwo informacji. W tym celu przyjęto jako podstawową technikę mieszaną, będącą połączeniem technik „przeglądu doświadczeń" oraz „burzy mózgów". Przegląd doświadczeń opiera się na wiedzy eksperckiej oraz analizie wcześniejszych incydentów związanych z naruszeniem bezpieczeństwa informacji. Burza mózgów opiera się na myśleniu grupowym, które może być bardziej produktywne niż indywidualne oraz umożliwia zrozumienie poglądów innych na temat zidentyfikowanych ryzyk.
2. **Ocenianie** polega na oszacowaniu zagrożeń oraz możliwości ich zmaterializowania w przypadku nie podjęcia odpowiednich działań. Do tego celu wykorzystano „macierz prawdopodobieństwo/wpływ". Zawiera ona wartości niezbędne do sklasyfikowania zagrożeń w ujęciu jakościowym. Skale prawdopodobieństwa są miarami pochodzącymi z wartości procentowych, natomiast skale wpływu są wybrane w celu określenia miary oddziaływania na OSiR.
3. **Planowanie** polega na przygotowaniu określonych reakcji zarządczych w celu usunięcia lub zmniejszenia zagrożeń wynikających ze zmaterializowania się określonego ryzyka. Wprowadza się następujące możliwe reakcje na ryzyko:
    a. Unikanie (prewencja) - jeżeli to możliwe podjęcie stosownych reakcji zarządczych tak aby zagrożenie (przypisane do danego ryzyka) nie mogło wpłynąć na bezpieczeństwo informacji lub nie mogło zaistnieć.
    b. Redukowanie - działania podjęte w celu zmniejszenia prawdopodobieństwa wystąpienia zdarzenia lub ograniczenia jego wpływu (redukcja jednego lub dwóch parametrów z macierzy prawdopodobieństwo/wpływ).
    c. Plan rezerwowy - opracowanie działań, które zostaną podjęte w celu zredukowania skutków zagrożenia dla ryzyka, które się zmaterializowało.

4. **Wdrażanie** polega na zapewnieniu, aby planowane reakcje na ryzyko zostały zrealizowane oraz aby podjęte zostały działania korygujące w przypadku gdyby reakcje te nie spełniły związanych z nimi oczekiwań. Istotnym elementem ról i obowiązków w zarządzaniu ryzykiem. Wprowadza się następujące role:
   a. Właściciela ryzyka - wskazane stanowisko lub osoba odpowiedzialna zarządzanie, monitorowanie i kontrolowanie wszystkich aspektów przypisanego jej ryzyka łącznie z wdrożeniem wybranych reakcji na zagrożenie.
   b. Wykonawca reakcji na ryzyko - stanowisko lub osoba wyznaczona do wykonywania działań związanych z reakcją na konkretne ryzyko. Wykonawca reakcji wspiera właściciela ryzyka i otrzymuje od niego polecenia.
5. **Komunikacja** polega na zapewnieniu, aby wszystkie informacje o zagrożeniach docierały do wszystkich zainteresowanych.

§ 27

Analiza ryzyka

1. Ważnym elementem zarządzania bezpieczeństwem informacji jest przeprowadzanie okresowej analizy ryzyka i opracowania planów postępowania z ryzykiem (wyznaczania celów bezpieczeństwa informacji).
2. Analiza jej wyników stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów OSiR. Poziom ryzyka określa się na podstawie matrycy analizy ryzyka.
3. Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem. Przyjmuje się, że w danym okresie wyznacza się plan zarządzana ryzykiem dla ryzyk, których wartość jest najwyższa. Za okres przyjmuje się rok kalendarzowy.
4. Ryzyka są przeglądane i aktualizowane co najmniej raz w roku oraz po zmianach mających wpływ na system bezpieczeństwa informacji.

Rozdział 8

INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

§ 28

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego lub Inspektora Ochrony Danych.

2. Do typowych podatności bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. W przypadku stwierdzenia wystąpienia incydentu, Administrator lub IODO prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
    b. proponuje ewentualne działania dyscyplinarne;
    c. proponuje działania na rzecz przywrócenia działań organizacji po wystąpieniu incydentu;
    d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze (Załącznik Nr 4). Formularz rejestracji incydentu.
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

Przed przystąpieniem do pracy użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, w tym zwrócić

szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora Danych Osobowych lub IODO

§ 29

1. Do czasu przybycia Administratora Danych Osobowych czy też Inspektora Ochrony Danych Osobowych (w sytuacji gdy został powołany), zgłaszający:
a. Powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
b. Zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych,
c. Podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
2. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia, jak i w przypadku podejrzenia naruszenia ochrony danych.

§ 30

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, Administrator lub Inspektor w przypadku, gdy został powołany, po przybyciu na miejsce:

a. Ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu,
b. Wysłuchuje relacji osoby, która dokonała powiadomienia,
c. Podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

§ 31

1. Administrator Danych Osobowych lub Inspektor Ochrony Danych Osobowych w przypadku gdy został wyznaczony sporządza z przebiegu zdarzenia raport, w którym powinny się znaleźć w szczególności informacje o:
    a. Dacie i godzinie powiadomienia;
    b. Godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane;
    c. Sytuacji, jaką zastał;

d. Podjętych działaniach i ich uzasadnieniu.
2. Kopia raportu przekazywana jest również Administratorowi Danych Osobowych.

Rozdział 9

REGULAMIN OCHRONY DANYCH

Regulamin Ochrony Danych ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania (Załącznik Nr 5). Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania (Załącznik Nr 6).

Wykaz zabezpieczeń

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych (Załącznik Nr 7) - Wykaz zabezpieczeń.
2. Wykaz jest aktualizowany po każdej analizie ryzyka.

Szkolenia

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO.
2. Za przeprowadzenie szkolenia odpowiada Administrator Danych Osobowych.
3. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

Rozdział 10

POSTANOWIENIA KOŃCOWE

§ 32

Polityka Ochrony Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.

§ 33

1. Każda osoba przetwarzająca dane osobowe zobowiązana jest do zapoznania się z treścią Polityki oraz Instrukcji Zarządzania Systemem Informatycznym,

2. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, że został zapoznany z przepisami ustawy o ochronie danych osobowych, obowiązującą Polityką Ochrony Danych Osobowych oraz Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.
3. Oświadczenia przechowywane są w aktach personalnych pracownika.

§ 34

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce Ochrony Danych Osobowych.