Załącznik
do uchwały nr 87
Zarządu Okręgu Mazowieckiego Polskiego Związku Wędkarskiego w Warszawie
z 17 grudnia 2018 r
w sprawie przyjęcia polityki ochrony danych osobowych

POLITYKA
OCHRONY DANYCH OSOBOWYCH
Okręgu Mazowieckiego Polskiego Związku Wędkarskiego w Warszawie

PODSTAWY PRAWNE

§1

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 (ogólne rozporządzenie o ochronie danych).
2. Ustawa z 10 maja 2018 r. o ochronie danych osobowych.

PODSTAWOWE POJĘCIA

§2

1. Administrator – w tym dokumencie jest rozumiany, jako Okręg Mazowiecki Polskiego Związku Wędkarskiego w Warszawie.
2. RODO – w tym dokumencie rozumiane jako rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
3. Polityka – w tym dokumencie jest rozumiana jako „Polityka ochrony danych osobowych" obowiązująca u Administratora.
4. Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Administratora (Zarząd) do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez RODO. IOD powołany jest uchwałą Zarządu Administratora.
5. Użytkownik – osoba upoważniona do przetwarzania danych osobowych. Użytkownikiem może być osoba zatrudniona, wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, porozumienia wolontarystycznego, odbywająca staż.

Cele i zasady funkcjonowania polityki bezpieczeństwa

§3

Realizując Politykę bezpieczeństwa informacji zapewnia ich:

1) poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom;
2) integralność – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany;
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 skutki są spójne;
8) minimalizacji – zbierania jak najmniej danych osobowych i tylko takich jakie są wymagane do realizacji zadań Administratora.

§4

Polityka ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, to jest:

1) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone;

2) naruszeń przepisów prawa oraz innych regulacji;
3) utraty lub obniżenia reputacji;
4) strat finansowych ponoszonych w wyniku nałożonych kar.

§5

Realizując politykę w zakresie ochrony danych osobowych Administrator dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

1) przetwarzane zgodnie z prawem,
2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
3) merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów

§6

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem.
Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety, smartfony, telefony, karty pamięci, dyski zewnętrzne itp.
2. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
3. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych.
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
a) wylogować się z systemu informatycznego, a jeśli to wymagane - następnie wyłączyć sprzęt komputerowy
b) zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe.
7. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
8. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien trwale zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive młotkiem).
9. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez internet zobowiązani są do stosowania zasad bezpieczeństwa.

Zarządzanie uprawnieniami

§7

1. Każdy użytkownik z dostępem do danych osobowych (np. na swoim komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
2. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonych i przy realizacji informatyków-administratorów.
3. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień administratora.
4. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest zatem umożliwianie innym osobom praca na koncie innego użytkownika.

Polityka haseł

§8

1. Hasła powinny składać się z mi.n. 8 znaków.
2. Hasła powinny zawierać małe litery + cyfry
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy natychmiast go zmienić.
6. Hasła muszą być zmieniane co 30 dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.

Zabezpieczenie dokumentacji papierowej z danymi osobowymi

§9

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „Polityki czystego biurka". Polega ona na zabezpieczaniu (zamykaniu) dokumentów w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

Zasady wynoszenia nośników z danymi poza firmę/organizację

§10

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora.
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
4. Należy korzystać ze sprawdzonych firm kurierskich.

5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.

Zasady korzystania z internetu

§11

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

Zasady korzystania z poczty elektronicznej

§12

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 6 znaków: litery i cyfry a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu
5. Nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu” infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy.
6. Bez weryfikacji wiarygodności nadawcy, nie należy „klikać” na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając” na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych

osobowych lub zaszyfrowanie m przez kryptowirusy.
7. Należy zgłaszać administratorowi przypadki podejrzanych emaili.
8. Użytkownicy nie powinni rozsyłać „niezawodowych” emaili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 230 osób.
9. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”. Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”!
10. Użytkownicy powinni okresowo kasować niepotrzebne maile.
11. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
12. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
13. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
14. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
15. Użytkownik bez zgody Administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Administratora, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

Ochrona antywirusowa

§13

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy”, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Administratora.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

§14

1. Konserwacja baz danych i oprogramowania przeprowadzana jest przez Administratora Systemu.
2. Konserwacja sprzętu komputerowego przeprowadzana jest przez Administratora Systemu lub firmę zewnętrzną.
3. W przypadku awarii sprzętu, na którym znajdują się dane osobowe w zależności od uszkodzenia następuje:
a) naprawa na miejscu pod nadzorem Administratora Systemu,
b) demontowanie dysku i zabezpieczenie w ADMINISTRATOR na czas naprawy,
c) przegrywanie danych przez Administratora Systemu na inny nośniki usunięcia danych z przekazywanego do naprawy sprzętu.
4. W przypadku przekazania komputerów innemu użytkownikowi lub jednostce organizacyjnej, dane z dysków twardych są usuwane przez Administratora Systemu w sposób uniemożliwiający ich odtworzenie.
5. W przypadku złomowania sprzętu komputerowego, nośniki informacji (dyski twarde) są fizycznie niszczone przez Administratora Systemu.

Procedura tworzenia kopii zapasowych

§15

1. Kopie całościowe sporządzane są raz w miesiącu.
2. Kopie sporządzane są na płytach dyskach zewnętrznych lub płycie DVD/CD.
3. Każda nośnik jest opisany datą jej sporządzenia.
4. Kopie zapasowe przechowywane są tak długo jak wymagają tego przepisy prawa.
5. Dostęp do kopii mają osoby upoważnione przez administratora.
6. Kopie przechowywane są miejscu zabezpieczonym na terenie siedziby Administratora.

Procedura napraw w serwisach zewnętrznych

§16

1. Komputery przeznaczone do naprawy należy wysyłać bez dysków a urządzenia mobilne bez kart pamięci.
2. W przypadku naprawy sprzętu z danymi osobowymi na nośniku należy je wpierw trwale usunąć z użyciem specjalistycznego oprogramowania
3. W przypadku naprawy sprzętu z danymi osobowymi na nośniku trzeba zawrzeć umowę powierzenia przetwarzania danych osobowych.
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła.
5. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta.

Regulamin użytkowania komputerów przenośnych

§17

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.
2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Administratora, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).
3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny,
o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Administratora.
4. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych (IOD), zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
a) zaleca się przenoszenie go w specjalnym futerale. Dobrym sposobem na zmylenie potencjalnego złodzieja jest przenoszenie komputera przenośnego w zwykłej teczce-aktówce. Sugeruje to przenoszenie dokumentów
a ukrywa fakt transportu komputera przenośnego.
b) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru. W chwili obecnej złodzieje dysponują aparaturą umożliwiającą wykrywanie nawet ukrytych komputerów przenośnych.
c) podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod tylnym siedzeniem kierowcy. Zabrania się przewożenia go np. na siedzeniach, co może skutkować kradzieżą na skrzyżowaniach, przejściach dla pieszych lub w korkach.

6. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp
7. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach
8. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
9. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

§18

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Administratora w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych
2. Do sytuacji wymagających powiadomienia, 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, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do incydentów wymagających powiadomienia, 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. Typowe przykłady incydentów wymagające reakcji:
a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania
b) dokumentacja jest niszczona bez użycia niszczarki
c) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie
d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe
e) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe
f) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Administratora
g) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej
h) telefoniczne próby wyłudzenia danych osobowych
i) kradzież, zagubienie komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi
j) maile zachęcające do ujawnienia identyfikatora i/lub hasła,
k) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów
l) hasła do systemów przyklejone są w pobliżu komputera

5. W przypadku naruszenia ochrony danych osobowych w ciągu 24 godzin należy o tym zawiadomić Administratora o naruszeniu.

Obowiązek zachowania poufności i ochrony danych osobowych

§19

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
a) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach,
b) zachowania w tajemnicy danych osobowych do których mam lub będzie miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora,
c) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora,
d) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
e) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem
2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.
3. Osoby zapoznane z treścią Polityki lub przeszkolone zobowiązane są podpisać oświadczenie o poufności.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.

Postępowanie dyscyplinarne

§20

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Administratora za naruszenie przepisów karnych zawartych RODO i ustawie.

Polityka kluczy

§21

1. Polityka kluczy obejmuje pomieszczenia Administratora.
2. Klucze do pomieszczeń posiadają jedynie osoby upoważnione przez Administratora i mogą je zabierać po zakończeniu pracy. Trzeba jednak dochować wszelkiej staranności, tak by nie zostały one skradzione lub zgubione.
3. Klucze zapasowe przechowywane są u administratora budynku. Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą Administratora. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić.
4. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane oraz schowane w miejscu zabezpieczonym.

5. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność.
6. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
7. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
8. Po zakończeniu pracy, pracownicy są zobowiązani do zabezpieczenia pomieszczeń, a w szczególności wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych, wyłączenia oświetlenia, zabezpieczenia i zamknięcia okien i drzwi.
9. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 kodeksu pracy oraz z art. 363 § 1. kodeksu cywilnego.

.

Udostępnianie i powierzanie danych osobowych

§22

1. Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.
2. Administrator odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.
3. Powierzenie danych może nastąpić wyłącznie w drodze pisemnej umowy, w której podmiot przyjmujący dane zobowiązuje się do przestrzegania obowiązujących przepisów RODO. Umowa powinna zawierać informacje o podstawia prawnej powierzenia danych, celu i sposobie ich przetwarzania.

Obowiązek informacyjny i wyrażenie zgody

§23

1. Każdy pracownik który zbiera dane osobowe w imieniu administratora, jest zobowiązany do przekazania zainteresowanemu obowiązku informacyjnego.
2. Dedykowany obowiązek informacyjny powinien być zamieszczony w każdym miejscu, gdzie są zbierane dane osobowe (np. na stronie internetowej, w postępowaniu przetargowym, w formularzach zgłoszeniowych).
3. Zaleca się, by obowiązek informacyjny oraz zgoda na przetwarzanie danych osobowych była, o ile to możliwe, zawsze podpisana przez osobę, której dane dotyczą.

Monitoring wizyjny

§24

1. W kołach, w których znajduje się monitoring, Administrator musi na swoim terenie poinformować o monitoringu, poprzez zmieszczenie wyraźniej informacji na drzwiach, korytarzach, płotach itp. Tablice informujące o zainstalowanym monitoringu powinny być widoczne, syntetyczne, umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc, zaś wymiary tablic muszą być proporcjonalne do miejsca, gdzie zostały umieszczone. Stosowane mogą być dodatkowo piktogramy informujące o objęciu dozorem kamer. Nie jest wystarczające oznaczenie obszaru objętego monitoringiem jedynie piktogramami
2. Należy zastosować obowiązek informacyjny, o którym mowa w §23, ale nie trzeba wywieszać go w każdym miejscu monitorowania. Obowiązek ten musi znajdować się miejscu widocznym przy

portierni.
3. Prawa osób objętych monitoringiem obejmują m.in.:
- prawo do informacji o istnieniu monitoringu w określonym miejscu, jego zasięgu, celu, nazwie podmiotu odpowiedzialnego za instalację, jego adresie i danych do kontaktu;
- prawo dostępu do nagrań w uzasadnionych przypadkach;
- prawo żądania usunięcia danych jej dotyczących;
- prawo do anonimizacji wizerunku na zarejestrowanych obrazach i/lub usunięcia dotyczących jej danych osobowych;
- prawo do przetwarzania danych przez ograniczony czas.
4. Okres przechowywania danych po dokonaniu nagrania nie może być dłuższy niż 30 dni.
5. Do ekranu, na którym odtwarzany jest monitoring mają dostęp tylko osoby upoważnione przez Administratora.
6. Rejestrator monitoringu jest obowiązkowo przechowywany w miejscu zamkniętym dla osób trzecich, a dostęp do niego mają tylko osoby upoważnione przez administratora.

Identyfikacja obszarów wymagających szczególnych zabezpieczeń

§25

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka, stosuje się wysoki poziom bezpieczeństwa. Poziom ryzyka wyniósł 23,48, co stanowi niskie ryzyko. IOD przeprowadza okresową (nie rzadziej niż raz na pół roku) analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawiają Administratorowi propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

Załączniki

Załącznik nr 1 – Rejestr osób upoważnionych do przetwarzania danych osobowych.
Załącznik nr 2 – Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych.
Załącznik nr 3 – Raportu z naruszenia bezpieczeństwa danych osobowych.

Załącznik nr 1

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data odebrania uprawnień	Uwagi

Załącznik nr 2

……
(imię i nazwisko)

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany/a oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze zobowiązań wobec Okręgu Mazowieckiego Polskiego Związku Wędkarskiego w Warszawie, zarówno w czasie trwania relacji (m.in. umowy, porozumienia), jak i po jej ustaniu.

Oświadczam, że zostałem/am poinformowany/a o obowiązujących w Okręgu Mazowieckim Polskiego Związku Wędkarskiego w Warszawie zasadach dotyczących przetwarzania danych osobowych, określonych w Polityce ochrony danych osobowych i zobowiązuję się ich przestrzegać.

Zostałem/am zapoznany/a z przepisami o ochronie danych osobowych Poinformowano mnie również o grożącej, stosownie do przepisów odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, ze złamanie zasad ochrony danych osobowych, obowiązujących w Okręgu Mazowieckim Polskiego Związku Wędkarskiego w Warszawie może zostać uznane za ciężkie naruszenie podstawowych obowiązków i skutkować odpowiedzialnością dyscyplinarną.

……
(podpis osoby upoważnionej)

Załącznik nr 3

……, dnia …… r.

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Data: ..... r. Godzina: .....
2. Osoba powiadamiająca o zaistniałym zdarzeniu: .....
   .....
   (imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)
3. Lokalizacja zdarzenia: .....
   .....
   (np. nr pokoju, nazwa pomieszczenia)
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
   .....
   .....
   .....
5. Przyczyny wystąpienia zdarzenia:
   .....
   .....
6. Podjęte działania:
   .....
   .....

.....
(podpis zgłaszającego)