

# Polityka ochrony danych

## Polityka Bezpieczeństwa Danych Osobowych w Stowarzyszeniu „Unia Nadwarciańska” z siedzibą w Słupcy ul. Poznańska 18

ROZDZIAŁ 1 – PRZEPISY OGÓLNE

ROZDZIAŁ 2 – PODSTAWA PRZETWARZANIA

ROZDZIAŁ 3 – OBOWIĄZKI INFORMACYJNEGO

ROZDZIAŁ 4 – INNE OBOWIĄZKI ADMINISTRATORA

ROZDZIAŁ 5 – REALIZACJA ZASADNOŚCI

ROZDZIAŁ 6 – ZARZĄDZANIE RYZYKIEM

ROZDZIAŁ 7 – WDRAŻANIE ZASAD OCHRONY DANYCH

ROZDZIAŁ 8 – POSTĘPOWANIE W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

ROZDZIAŁ 9 – OCENA SKUTKÓW DLA OCHRONY DANYCH

ROZDZIAŁ 10 – ŚRODKI TECHNICZNE I ORGANIZACYJNE

## Preambuła

Zarząd Stowarzyszenia „Unia Nadwarciańska”, uznając wagę ochrony prawa do prywatności osób, których dane dotyczą, realizując zasady zgodności z prawem, ograniczenia celu, minimalizacji danych, prawidłowości i aktualności, ograniczenia przechowywania, integralności i poufności oraz rozliczalności, wyrażonych w Rozporządzeniu 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), dalej jako RODO, a także spełniając wymogi Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przyjmuje niniejszą Politykę Bezpieczeństwa Danych Osobowych, zwaną dalej Polityką.

Zarząd zobowiązuje się do opracowywania, aktualizacji, przestrzegania i rozpowszechniania wśród współpracowników Stowarzyszenia „Unia Nadwarciańska” zasad ochrony danych osobowych, szczególnie danych wrażliwych. Zarząd Stowarzyszenia „Unia Nadwarciańska” jest świadom zagrożeń społecznych i technologicznych, na jakie narażone są te dane. Realizując zatem przepisy prawa i najwyższe standardy etyczne, podejmuje się za pomocą niniejszej polityki bezpieczeństwa i towarzyszących jej dokumentów chronić interesy osób, których dane mogłyby być zagrożone.

## Rozdział 1 Przepisy ogólne

§ 1. 1. Niniejsza Polityka Bezpieczeństwa Danych Osobowych w Stowarzyszeniu „Unia Nadwarciańska” (zwana dalej Polityką Bezpieczeństwa), powstała w celu realizacji obowiązków

wynikających z art. 36 ust. 2 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (dalej zwanej Ustawą) oraz Ogólnego rozporządzenia o ochronie danych.

1.2. Niniejsza polityka bezpieczeństwa określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w Stowarzyszeniu „Unia Nadwarciańska” w zakresie objętym postanowieniami aktów, o których mowa w § 1.1

1.3. Celem niniejszej polityki bezpieczeństwa jest zapewnienie przestrzegania obowiązującego prawa, zobowiązań Stowarzyszenia „Unia Nadwarciańska” oraz poszanowanie i ochrona interesów, w szczególności prawa do prywatności osób, których dane są przetwarzane.

**§ 2. 1 Administrator danych Stowarzyszenie „Unia Nadwarciańska” jest administratorem danych w rozumieniu art. 7 pkt 4 Ustawy oraz RODO, zwanym w dalszej części również ADO. 2.2.**

**W imieniu ADO działa Zarząd.**

**§ 3.1** Zasady przetwarzania Stowarzyszenie „Unia Nadwarciańska” dokłada wszelkich starań, aby zbierane dane osobowe były przetwarzane zgodnie z prawem oraz uwzględnia interesy i rozsądne oczekiwania osób, których dane są przetwarzane, zachowując przy tym wszystkie obowiązki informacyjne względem nich.

3.2. Dane zbierane są i przetwarzane jedynie w konkretnych, wyraźnie wskazanych i uzasadnionych celach. Dalsze przetwarzanie danych przez ADO, po ich zebraniu następuje po uzyskaniu odrębnej zgody. Przetwarzane są tylko takie dane osobowe, bez których nie da się osiągnąć zamierzonego celu przetwarzania.

3.3. Administrator dokłada szczególnej staranności w celu zbierania danych merytorycznie poprawnych, odpowiadających rzeczywistości stanowi rzeczy oraz nie pozyskuje danych ze źródeł niewiadomego pochodzenia. Nieaktualne lub nieprawdziwe dane są niezwłocznie usuwane lub prostowane, w przypadku zaistnienia takich okoliczności.

3.4. Niezanonimizowane dane usuwane są po upływie okresu, w którym ich przetwarzanie było niezbędne do osiągnięcia celu przetwarzania.

3.5. ADO podejmuje wszelkie środki techniczne i organizacyjne, adekwatne do ryzyka naruszenia bezpieczeństwa danych, w tym ochronę przed niezgodnym z prawem przetwarzaniem, utratą, zniszczeniem i uszkodzeniem.

## **Rozdział 2**

### **Podstawa przetwarzania**

**§ 4. 1.** Kiedy ADO może przetwarzać dane – Przetwarzanie zebranych danych osobowych jest zgodne z prawem, gdy: otrzymano zgodę na ich przetwarzanie od osoby, której dane dotyczą,

a) jest to niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą,

b) jest to niezbędne do wykonania obowiązku prawnego, ciążącego na ADO

c) jest to niezbędne do ochrony żywotnych interesów osoby fizycznej,

d) ADO realizuje zadanie w interesie publicznym lub w ramach powierzonej mu władzy publicznej,

e) przetwarzanie wynika z prawnie uzasadnionych interesów ADO lub osoby trzeciej chyba, że jako nadrzędne należy uznać prawa i wolności osoby, której dane dotyczą, w szczególności w przypadku danych dziecka.

**§5.1.** Zgoda – Zgoda na przetwarzanie danych osobowych jest zbierana, o ile to możliwe, pisemnie (w wersji papierowej, elektronicznej). Zgoda może zostać udzielona ustnie. Zgodę udziela się odrębnie dla każdego celu przetwarzania.

5.2. Zgodę na przetwarzanie, wyrażoną w formie pisemnej, ADO wyróżnia spośród pozostałej części tekstu, o ile jest ona częścią innego dokumentu. Zgoda formułowana jest w sposób maksymalnie przystępny, jasnym i zrozumiałym językiem.

5.3. ADO informuje o możliwości wycofania zgody w każdym momencie. Wycofanie zgody powinno być tak samo łatwe jak jej udzielenie.

5.4. W przypadku zbierania dodatkowych danych, ADO wyróżnia, które dane są niezbędne do realizacji umowy, a które mogą być podane dobrowolnie w innych celach przetwarzania.

5.5. W przypadku, w którym ADO będzie zbierał dane osobowe, w celu świadczenia usług drogą elektroniczną, odpłatnie (tzw. usługi społeczeństwa informacyjnego), oferowanych bezpośrednio dziecku, ADO dokłada wszelkich starań, aby za pomocą dostępnej technologii zweryfikować, czy osoba sprawująca opiekę nad dzieckiem poniżej 13 roku życia wyraziła zgodę na przetwarzanie danych osobowych.

5.6. Zgodę na przetwarzanie danych wrażliwych takich jak: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, ADO uzyskuje tylko w formie pisemnej, z jednoczesnym, wyraźnym wskazaniem celu przetwarzania. Wymóg ten nie dotyczy realizacji obowiązków wynikających z przepisów prawa pracy, ubezpieczeń społecznych i podatkowego i zabezpieczenia socjalnego.

## **Rozdział 3**

### **Obowiązki informacyjne**

§6.1. Klauzule informacyjne – ADO, zbierając dane osobowe, w maksymalnie zwięzły, zrozumiały i transparentny sposób, starając się, aby forma była łatwo dostępna, przekazuje informacje: nazwa i dane kontaktowe Stowarzyszenia „Unia Nadwarciańska”.

- a) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych lub osoby, odpowiedzialnej za procesy przetwarzania danych, z zaznaczeniem, że nie jest ona inspektorem ochrony danych,
- b) cele przetwarzania danych osobowych oraz podstawę prawną,
- c) opis prawnie uzasadnionych interesów ADO lub osoby trzeciej, dla których celów przetwarzanie jest niezbędne
- d) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
- e) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej wraz ze wzmianką o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
- f) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
- g) o prawie do żądania od Stowarzyszenia „Unia Nadwarciańska” dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu, w sytuacji, gdy zachodzą sytuacje o których mowa w §10 Polityki, w szczególności wobec przetwarzania w celach marketingu bezpośredniego, a także o prawie do przenoszenia danych,

- h) informacje o prawie do cofnięcia zgody w dowolnym momencie z zaznaczeniem, że wycofanie zgody nie powoduje, że dotychczasowe przetwarzanie było bezprawne,
- i) o prawie wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych, z podaniem adresu,
- j) czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
- k) gdy ma to zastosowanie – informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
- l) jeżeli Stowarzyszenie „Unia Nadwarciańska” planuje przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym celu.

**§7.1.** Prawo dostępu – Osoba, której dane dotyczą, może zwrócić się do ADO o potwierdzenie, czy dane są przetwarzane oraz na jakich zasadach.

7.2. ADO na żądanie dostarcza kopię danych osobowych. Za każdą kolejną kopię mogą być naliczone opłaty, odpowiadające kosztom administracyjnym ich wydania.

**§8.1.** Prawo do “bycia zapomnianym” Na żądanie osoby, której dane dotyczą ADO usuwa je bez zbędnej zwłoki.

8.2. Obowiązek usunięcia aktualizuje się w przypadku, gdy:

- cofnięto zgodę na przetwarzanie,
- osiągnięto cel przetwarzania i nie są one już niezbędne,
- obowiązek usunięcia wynika z wniesienia sprzeciwu w zakresie przetwarzania w celu marketingu bezpośredniego lub w przypadku przetwarzania wynikającego z zadania realizowanego przez ADO w interesie publicznym lub w ramach sprawowania władzy (np. zadania zlecone przez JST) lub z uwagi na niezbędność przetwarzania z powodu prawnie uzasadnionych interesów.
- usunięcie wynika z obowiązku prawnego, któremu podlega ADO, gdy zgoda na przetwarzanie danych osobowych dziecka poniżej 13 roku życia, dotyczących usług społeczeństwa informacyjnego zostały zebrane bez zgody rodzica/opiekuna prawnego.

8.3. Prawo do przenoszenia danych – Na żądanie osoby, której dane dotyczą ADO przekazuje jej kopię przetwarzanych danych w formacie możliwym do odczytu maszynowego, które może przesłać innemu administratorowi. ADO, o ile jest to technicznie możliwe, na żądanie osoby fizycznej umożliwia przesłanie jej danych bezpośrednio innemu administratorowi. Obowiązek ten aktualizuje się w przypadku zautomatyzowanego przetwarzania danych, przekazanych na podstawie umowy lub zgody na przetwarzanie danych.

**§9.1.** Prawo do ograniczenia danych – Ograniczenie przetwarzania danych oznacza, że ADO zobowiązany jest do przechowywania dotychczas zebranych danych, przy czym brak jest możliwości dokonywania na nich innych operacji niż przechowywanie, chyba że:

- osoba wyrazi zgodę na inny rodzaj przetwarzania lub
- przetwarzanie jest konieczne w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego

9.2. ADO ma obowiązek zrealizować żądanie ograniczenia przetwarzania danych, gdy:

- kwestionowana jest prawidłowość danych, do czasu sprawdzenia ich poprawności,

- ADO przetwarza dane niezgodnie z prawem, ale osoba uprawniona żąda w zamian ograniczenia,
- dane nie są potrzebne ADO do przetwarzania, ale są potrzebne uprawnionemu do ustalenia roszczeń, dochodzenia roszczeń, obrony roszczeń
- osoba uprawniona wniosła sprzeciw (do czasu ustalenia uprawnienia do przetwarzania).

9.3. Zautomatyzowane podejmowanie decyzji – Stowarzyszenie „Unia Nadwarciańska” nie podejmuje decyzji w zakresie danych osobowych w sposób zautomatyzowany oraz nie dokonuje czynności profilowania. W przypadku zmiany sytuacji Stowarzyszenie „Unia Nadwarciańska” zawsze informuje o takim celu przetwarzania, dbając, aby przetwarzanie odbyło się na podstawie świadomej zgody osoby, której dane dotyczą.

**§10.1.** Prawo sprzeciwu – Prawo do wniesienia sprzeciwu przeciwko przetwarzaniu danych, przysługuje w dowolnym momencie osobie, której dane dotyczą, gdy przetwarzane są one na potrzeby marketingu bezpośredniego, w tym profilowania.

10.2. W innych przypadkach prawo do wniesienia sprzeciwu powstaje z przyczyn związanych ze szczególną sytuacją osoby, gdy ADO przetwarza dane osobowe, w tym dokonuje profilowania w związku z następującymi podstawami:

- z uwagi na niezbędność do zrealizowania zadania w interesie publicznym,
- w ramach sprawowania władzy publicznej powierzonej ADO,
- gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią.

**§11.1.** Realizacja żądań co do przetwarzania – W przypadku zgłoszenia przez osobę, której dane dotyczą, żądań określonych w §6.1. lit. h- §10, ADO podejmuje niezwłoczne działania w celu ustalenia zasadności żądania oraz jego zrealizowania. O swojej decyzji lub podjętych działaniach informuje niezwłocznie w sposób jasny i zrozumiały.

11.2. Żądanie może być wyrażone w każdej formie. Na stronie internetowej ADO zamieszcza się krótką informację o danych kontaktowych osoby odpowiedzialnej za przetwarzanie danych osobowych (o ile zostanie wyznaczona) albo ogólne dane kontaktowe, dzięki którym mogą być realizowane powyższe uprawnienia osób, których dane dotyczą.

## **Rozdział 4**

### **Inne obowiązki Administratora**

**§12.1.** Ogólne – ADO uwzględnia charakter, zakres, kontekst i cele przetwarzania oraz bierze pod uwagę ryzyko naruszenia praw i wolności osób fizycznych. W tym celu wdraża odpowiednie środki techniczne i organizacyjne.

12.2. Powierzenie przetwarzania – W przypadku powierzenia przetwarzania innym podmiotom, w szczególności w zakresie usług IT, chmury obliczeniowej, działalności statutowej ADO, w internecie, przesyłania danych osobowych, ADO korzysta z usług podmiotów, które gwarantują poziom zabezpieczeń zgodny z wymogami UE i prawa krajowego.

12.3. Aktualizacja – ADO w miarę możliwości, szczególnie w przypadku zwiększania zakresu i kategorii przetwarzania danych oraz wprowadzania nowych narzędzi technologicznych, dokonuje przeglądu istniejących procedur ochrony danych oraz zastosowanych środków technicznych i organizacyjnych, nie rzadziej niż raz na rok.

12.4. Ocenę ryzyka i aktualizację dokumentacji bezpieczeństwa informacji przeprowadza się także w przypadku pojawienia się nowego urządzenia technicznego, nowego sposobu przetwarzania informacji, nowej kategorii przetwarzanych danych lub nowego procesu przetwarzania.

## **Rozdział 5**

### **Realizacja zasad**

**§13.1.** Zasada ochrony danych w fazie projektowania – Wprowadzając nowe narzędzia, związane z prowadzonymi działaniami statutowymi, albo planując kolejne działania, w tym projektując i wprowadzając nowe rozwiązania technologiczne, ADO przeprowadza analizę obejmującą odpowiedzi na następujące pytania:

- czy projektowane rozwiązanie będzie wymagało przetwarzania danych osobowych lub jest wprowadzane w celu ich przetwarzania?
- jakie środki techniczne i organizacyjne są konieczne do zapewnienia bezpieczeństwa?
- czy możliwa jest pseudonimizacja danych, szyfrowanie?
- w jaki sposób ograniczyć prawdopodobieństwo udostępnienia danych osobom nieupoważnionym?

13.2. Analiza, o której mowa w niniejszym paragrafie, powinna zostać przeprowadzona przed rozpoczęciem przetwarzania danych osobowych. Wnioski z analizy powinny zostać utrwalone.

13.3. Po dokonaniu identyfikacji czy istnieje ryzyko naruszenia praw osób, których dane dotyczą, ADO podejmuje działanie w celu jego minimalizacji, co może obejmować:

- 1) uniknięcie ryzyka poprzez powstrzymanie się od wykonywania określonej czynności obciążonej ryzykiem,
- 2) usunięcie źródeł ryzyka,
- 3) podjęcie działań pozwalających zmniejszyć prawdopodobieństwo wystąpienia ryzyka,
- 4) podjęcie działań umożliwiających uniknięcie następstw wystąpienia ryzyka.

13.4. Domyślna ochrona danych – W przypadku stosowania rozwiązań technologicznych, ADO zapewnia, aby domyślne przetwarzanie danych dotyczyło jedynie danych niezbędnych do realizacji zadania. Żadne dodatkowe informacje nie powinny być udostępniane bez interwencji osoby, której dane zebrano nieokreślonej liczbie osób fizycznych.

13.5. ADO uwzględnia stan wiedzy technicznej dotyczącej możliwych do zastosowania środków oraz koszt wdrożenia tych środków.

## **Rozdział 6**

### **Zarządzanie ryzykiem**

**§14.1.** Stowarzyszenie „Unia Nadwarciańska” przeprowadza szczegółową analizę prowadzonych procesów przetwarzania danych i dokonuje samodzielnej oceny ryzyka naruszenia ochrony przetwarzanych danych w konkretnym przypadku.

14.2. Oceny ryzyka bezpieczeństwa informacji dokonuje w imieniu i na rzecz Stowarzyszenia „Unia Nadwarciańska” – Zarząd, członek Zarządu, któremu delegowano realizację obowiązków z zakresu ochrony danych osobowych, Iwona Suszka, Inspektor Ochrony Danych, o ile zostanie powołany lub inna powołana do tego osoba.

14.3. Istnieje możliwość zlecenia dokonania oceny ryzyka podmiotowi zewnętrznemu lub osobie odpowiedzialnej za określony proces przetwarzania danych.

14.4. Ryzyko jest szacowane na podstawie obiektywnej i rzeczowej analizy, której celem jest określenie stopnia ryzyka, wiążącego się z operacjami przetwarzania danych (wysokie lub niskie).

14.5. Ocenę ryzyka przeprowadza się przed przystąpieniem do przetwarzania danych, uwzględniając zasadę ochrony danych osobowych w fazie projektowania rozwiązań, nie rzadziej niż raz na rok.

14.6. Ocenę ryzyka o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wynikające z przetwarzania danych, przeprowadza się uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych.

14.7. Ocena ryzyka dokonywana jest w miarę możliwości w sposób ilościowy i jakościowy.

W przypadku niemożliwości lub zbytnej trudności dokonania oceny ilościowej dopuszczalne jest ograniczenie się do jakościowej oceny ryzyka.

14.8. Ocenę ryzyka i aktualizację dokumentacji bezpieczeństwa informacji można przeprowadzić w każdym innym czasie, o ile jest to celowe, zwłaszcza po wystąpieniu naruszenia lub jego realnej możliwości.

## **Rozdział 7**

### **Wdrażanie zasad ochrony danych osobowych**

**§15.1** Upoważnienia – Zarząd instruuje pracowników i wolontariuszy oraz osoby, które współpracują z Stowarzyszeniem „Unia Nadwarciańska” na podstawie umów cywilnoprawnych o obowiązkach, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych oraz niniejszej polityki i innych dokumentów wewnętrznych.

15.2. Podmioty wymienione w ustępie poprzednim, współpracujące z Stowarzyszeniem „Unia Nadwarciańska” potwierdzają na piśmie zapoznanie się z dokumentacją dotyczącą ochrony danych osobowych.

15.3. Zarząd nadaje upoważnienia osobom dopuszczonym do przetwarzania danych osobowych. Upoważnienia mogą być nadawane w formie pisemnej lub elektronicznie. W razie konieczności ADO prowadzi rejestr upoważnień w formie elektronicznej.

**§16.1.** Klauzule w umowach – Umowy, zawierane przez Stowarzyszenie „Unia Nadwarciańska” zawierają klauzulę zobowiązującą podmioty wymienione w poprzednim paragrafie do zachowania w tajemnicy danych osobowych przetwarzanych przez Stowarzyszenie „Unia Nadwarciańska” i przestrzegania ww. obowiązków, o ile tylko przewiduje się, że podmiot będzie mieć dostęp do tych danych.

16.2. Umowy wskazane w poprzednim ustępie, będą przewidywać odpowiedzialność ww. podmiotów w przypadku naruszenia przez nie obowiązków w zakresie ochrony danych osobowych.

17.1. ADO wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający określonemu ryzyku, w tym w zależności od potrzeb i celów przetwarzania:

- a. pseudonimizację i szyfrowanie danych osobowych,
- b. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

- c. zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- d. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

## **Rozdział 8**

### **Postępowanie w przypadku naruszenia bezpieczeństwa danych osobowych**

**§ 18. 1.** Zgłoszenie – Podejrzenie naruszenia bezpieczeństwa danych lub jego realną możliwość zgłasza się niezwłocznie Zarządowi. Zgłoszenia dokonuje podmiot, który ww. naruszenie lub jego realną możliwość odkrył lub podejrzewa.

18.2. Zarząd sprawdza czy nastąpiło naruszenie lub jego realna możliwość, a jeśli tak – w jakiej skali i jakich danych dotyczy.

18.3. W przypadku naruszenia bezpieczeństwa informacji lub realnej możliwości jego wystąpienia, Zarząd podejmuje wszelkie niezbędne kroki dla powstrzymania naruszenia lub jego możliwości, a także zminimalizowania ich skutków.

18.4. Zarząd bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Generalnemu Inspektorowi Ochrony Danych, dalej jako GIODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego GIODO po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

18.5. Zarząd dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Jego treść zawiera szczegółowe dane o naruszeniu lub możliwości jego wystąpienia, takie jak metoda naruszenia, zaangażowane podmioty, zagrożone dane. Zarząd opisuje także podjęte środki techniczne i instytucjonalne, służące powstrzymaniu naruszenia i zabezpieczające przed wystąpieniem naruszenia w przyszłości. Sprawozdanie może także sugerować dalsze kroki do podjęcia przez Stowarzyszenie „Unia Nadwarciańska” w tym zwłaszcza ponowną ocenę ryzyka.

**§ 19.1.** Zawiadomienie osoby, której dane dotyczą o naruszeniu – Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Zarząd bez zbędnej zwłoki powiadamia osoby, których dane dotyczą, o takim naruszeniu.

19.2. Zawiadomienie sporządza się jasnym i prostym językiem. Zawiadomienie opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej następujące informacje i środki:

- a. imię i nazwisko oraz dane kontaktowe osoby, której dotyczy naruszenie;
- b. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- c. opisywać środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

19.3. Zawiadomienie, o którym mowa w ust. 1 i 2, nie jest wymagane, gdy:

- a. wdrożono 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. zastosowano 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.

**§20.1.** Naruszenia dokonane przez współpracowników – W przypadku naruszenia bezpieczeństwa danych przez pracowników, wolontariuszy lub osoby pozostające ze Stowarzyszeniem „Unia Nadwarciańska” w stosunku cywilnoprawnym, Stowarzyszenie „Unia Nadwarciańska” może wyciągnąć wobec nich konsekwencje przewidziane odpowiednimi umowami.

20.2. Jeśli jest to celowe, Zarząd po wystąpieniu naruszenia lub jego realnej możliwości, instruuje odpowiednich współpracowników o wprowadzonych zmianach i sposobach przetwarzania danych i ich ochrony.

20.3. W przypadku naruszeń dokonanych przez pracowników, Stowarzyszenie „Unia Nadwarciańska” stosuje środki przewidziane kodeksem cywilnym.

## **Rozdział 9**

### **Ocena skutków dla ochrony danych**

**§ 21.1.** Przesłanki – W przypadku przetwarzania danych osobowych na dużą skalę lub w sposób zautomatyzowany, w tym profilowania dokonywanych za pomocą chmury obliczeniowej Stowarzyszenie „Unia Nadwarciańska” dokonuje oceny skutków dla ochrony danych w związku z ww. sposobem przetwarzania.

21.2. Elementy oceny – Ocena skutków zawiera, co najmniej:

- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania,
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1;
- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

## **Rozdział 10**

### **Środki techniczne i organizacyjne**

**§ 22.1.** Lokal – Stowarzyszenie „Unia Nadwarciańska” przetwarza dane osobowe w lokalu przy ul. Plac Szkolny 16a, 62-400 Słupca. Lokal znajduje się na pierwszym piętrze. Lokal zabezpieczony jest drzwiami wejściowymi z podwójnym zamkiem.

22.2. Lokal składa się z 6 pomieszczeń zamykanych na zamki, kluczem.

22.3. Dostęp do lokali jest ograniczony. Klucze do lokali dysponują pracownicy wg sporządzonego rejestru .

22.4. Dane w formie tradycyjnej – Dane przetwarzane w sposób tradycyjny znajdują się w ww. lokalu w pomieszczeniach, z których korzystają, zarząd i pracownicy. Dane znajdują się w szafach zamkniętych na klucz, do których dostęp mają tylko upoważnione osoby. Po zakończonej pracy klucze

do szaf chowane są do zamykanej szuflady, a następnie klucz do pomieszczenia odnoszony do pokoju kierownika.

22.5. Dane przetwarzane elektronicznie są przetwarzane za pomocą programów:

- usługi Office 365 – dysk w chmurze oraz aplikacje biurowe
- pakiet biurowy Office

22.6. Ww. dane są przetwarzane na komputerach przenośnych i stacjonarnych, należących do Zarządu Stowarzyszenia „Unia Nadwarciańska”.

22.7. Hasło – Dostęp do jednostek roboczych należących do Stowarzyszenia „Unia Nadwarciańska” zabezpieczony jest bezpiecznym hasłem. Hasło składa się z minimum 8 znaków, w tym wielkiej litery, cyfry i znaku specjalnego.

22.8. Stowarzyszenie „Unia Nadwarciańska” zobowiązuje swoich współpracowników, by zabezpieczali jednostki robocze, na których dokonują przetwarzania informacji, za pomocą hasła spełniającego te kryteria.

22.9. Każdy współpracownik ma własny login/identyfikator, który umożliwia powiązanie dokonywanych przez niego czynności na danych osobowych w systemie teleinformatycznym (e-mail).

22.10. Niektóre dane przetwarzane w sposób tradycyjny, są również przetwarzane elektronicznie. Stowarzyszenie „Unia Nadwarciańska” ogranicza do minimum przetwarzanie danych osobowych w formie elektronicznej.

22.11. Stowarzyszenie „Unia Nadwarciańska” zawarło stosowne aneksy z dostawcami usług, zapewniające odpowiedni do wymogów UE poziom ochrony danych stosowany przez dostawcę usługi.

**§ 23.1.** Środki techniczne – Po wyczerpaniu celów przetwarzania dane osobowe w formie tradycyjnej są niszczone za pomocą niszczarki znajdującej się w biurze. Nośniki elektroniczne danych są czyszczone z zawartości, a jeśli nie jest to możliwe – uszkodzane w sposób uniemożliwiający odczyt. Nośniki elektroniczne danych nie są przekazywane innym podmiotom ani nie służą innym celom niż przetwarzanie danych.

23.2. Środki sprzętowe, elektroniczne i logistyczne – Dostęp do komputera zabezpieczony jest nazwą użytkownika i hasłem 8-znakowym, w którym występują litery wielkie i małe i cyfry lub znaki specjalne. Komputer jest zabezpieczony przed nieuprawnionym dostępem z zewnątrz za pomocą oprogramowania antywirusowego i systemowej „zapory ogniowej” (firewall) o parametrach ustalonych przez producenta systemu.

23.3. Oprogramowanie jest aktualizowane na bieżąco za pomocą wbudowanego mechanizmu aktualizacji. System operacyjny jest aktualizowany na bieżąco za pomocą wbudowanego mechanizmu aktualizacji.

23.4. Stowarzyszenie „Unia Nadwarciańska” zobowiązuje osoby współpracujące i pracowników do stosowania zasad bezpieczeństwa, w szczególności zmiany haseł, a także nie przetwarzania danych osobowych na prywatnych komputerach.

23.5. Przetwarzanie przez współpracowników danych osobowych na prywatnym komputerze powinno odbywać się za wyraźną zgodą Zarządu po upewnieniu się, że pracownik stosuje wszystkie konieczne zasady bezpieczeństwa.

23.6. Zabronione jest przetwarzanie danych osobowych na prywatnych smartfonach oraz przesyłanie danych osobowych, przetwarzanych przez Stowarzyszenie „Unia Nadwarciańska” poprzez prywatne konta pocztowe takie jak @gmail.com, publiczne, darmowe chmury obliczeniowe takie jak google drive, na portalach społecznościowych takich jak Facebook, czy whatsapp, messenger.

23.7. Strona <https://unianadwarcianska.pl/> posiada certyfikat SSL oraz protokół https/.

**§24.1.** Środki organizacyjne – Pracownicy, wolontariusze i współpracownicy, z którymi podpisano umowy cywilnoprawne, którzy mają do czynienia z danymi osobowymi, zostali poinstruowani o sposobach postępowania przy ich przetwarzaniu. Wyżej wymienione osoby zostały zobowiązane do utrzymywania przetwarzania danych osobowych w ścisłej tajemnicy.

24.2. Instalowane jest tylko oprogramowanie z zaufanych źródeł. ADO przeprowadza wewnętrzne szkolenia z zakresu ochrony danych osobowych.