WYBRANE ASPEKTY OCHRONY DANYCH OSOBOWYCH W ORGANIZACJI ZHIERARCHIZOWANEJ NA PRZYKŁADZIE JEDNOSTKI WOJSKOWEJ

mgr inż. Ewelina MACHURA
Akademia Obrony Narodowej

prof. dr hab. Józef JANCZAK
Akademia Obrony Narodowej

Streszczenie

W artykule przedstawiono, bazując na uregulowaniach prawnych obowiązujących w naszym kraju, specyfikę organizacji ochrony danych osobowych w organizacji zhierarchizowanej na przykładzie jednostki wojskowej. Szczególną uwagę zwrócono na rolę i zadania administratora danych osobowych, wymaganą dokumentację i zasady przetwarzania danych osobowych w jednostce wojskowej.

Słow kluczowe: dane osobowe, organizacja zhierarchizowna, jednostka wojskowa

Wprowadzenie

Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym[1]. Tym zapisem Konstytucja Rzeczpospolitej Polskiej gwarantuje ochronę prywatności oraz wszystkich danych osobowych każdego obywatela Polski. W Konstytucji znajdujemy również szczegółowszy zapis w art. 51:

1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.

4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Takie prawo daje nam ustawa zasadnicza, zaś aktem, który realizuje jej postanowienia, jest *Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych* (Dz.U. z 1997 r. nr 133, poz. 883 z późniejszymi zmianami). Normatyw ten określa zasady postępowania przy przetwarzaniu danych osobowych, prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych, a także obowiązki instytucji, organizacji gromadzących i wykorzystujących w swojej działalności dane osobowe. Błędne jest powszechnie jeszcze spotykane mniemanie, iż jednostki wojskowe jako element sił zbrojnych z racji swych zadań i przeznaczenia, tj. ochrony niepodległości państwa i niepodzielności jego terytorium oraz zapewnienia bezpieczeństwa i nienaruszalności jego granic, są zwolnione z obowiązków wynikających z ustawy o ochronie danych osobowych. Niewątpliwie w swoje działalności jednostki wojskowe, jako jednostki organizacyjne niebędące osobami prawnymi, mają obowiązek stosowania przepisów ustawy o ochronie danych osobowych. Nie jest to jednak takie proste, gdyż właśnie z racji swej specyfiki obowiązują je inne, równie istotne akty prawne, czyli *Ustawa o powszechnym obowiązku obrony* oraz *Ustawa z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych*. Sposób i zakres stosowania przepisów z każdej z tych ustaw są często niejasne i niezrozumiałe, a przez

[1] Ustawa z dnia 2 kwietnia 1997 roku, *Konstytucja Rzeczypospolitej Polskiej*, Dz. U. 1997 nr 78 poz. 483 z późn. zm., art. 47.

to niekiedy wymogi, jakie stawiają bywają niedostrzegane, a w konsekwencji nieuwzględniane w działalności jako nieobowiązujące. Jednostki wojskowe, mimo iż są organizacjami specyficznymi o zhierarchizowanych strukturach, to tak jak niemal wszystkie inne instytucje podlegają przepisom prawa ustawy o ochronie danych osobowych, ponieważ jej przepisy dotyczą organów państwowych, organów samorządu terytorialnego oraz państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, a także osób fizycznych i osób prawnych oraz jednostek organizacyjnych niebędących osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub realizacją celów statutowych.

W jednostkach wojskowych przepisy ustawy o ochronie danych osobowych są mało znane, co można wnioskować po fakcie, iż wielu żołnierzy, zarówno podoficerów – dowódców drużyn, jaki i oficerów – dowódców plutonów czy kompanii, nie wspominając o innych komórkach organizacyjnych, nie zdaje sobie sprawy z tego, iż gromadzenie podstawowych informacji o podległych żołnierzach, ewidencjonowanie wyników szkolenia, czy choćby tworzenie list obecności to w rozumieniu ustawy przetwarzanie danych osobowych. Ta sama sytuacja dotyczy prowadzenia wszelkiej korespondencji za pośrednictwem kancelarii jednostki, gdyż rejestr przychodzących i wychodzących pism jest zbiorem danych osobowych zawierających chronologicznie wpisywane dane w postaci: daty wpływu, daty wysyłki i danych określających nadawcę lub adresata korespondencji[2]. Skoro więc na poszczególnych poziomach dowodzenia, a także w innych komórkach organizacyjnych jednostki, nie są znane przepisy ustawy, sądzić można, iż polityka bezpieczeństwa danych osobowych prowadzona w tego typu organizacjach (instytucjach) nie zapewnia pełnej ochrony tychże danych, a tym samym jest niewystarczająca, wymaga dogłębnego przemyślenia, a w konsekwencji zmiany. Brak podstawowej znajomości zapisów ustawy owocuje brakiem wykonywania obowiązków, które ona nakłada, a w tym podstawowego obowiązku rejestracji danych i ich właściwej ochrony.

Celem niniejszego artykułu jest przybliżenie przepisów ochrony danych osobowych i obowiązków z nich wynikających w specyficznej organizacji zhierarchizowanej jaką jest jednostka wojskowa oraz konsekwencji jakie grożą za nieprzestrzeganie tych przepisów, a także zwrócenie uwagi na rolę, jaką pełni w tego typu organizacji prawidłowo prowadzona polityka bezpieczeństwa danych osobowych.

Ochrona danych osobowych – wybrane zagadnienia

W jednostkach wojskowych zwykle zdaje się panować przeświadczenie, iż wszelką ich działalność i funkcjonowanie normują trzy podstawowe akty prawne:

1. Ustawa z dnia 26 listopada 1967 r. o powszechnym obowiązku obrony (Dz.U. z 1967 r. nr 44, poz. 220 z późniejszymi zmianami),

2. Ustawa z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych (Dz.U. z 2010 r. nr 90, poz. 593 z późniejszymi zmianami);

3. Ustawa z dnia 05 sierpnia 2010r. o ochronie informacji niejawnych (Dz.U. z 2010 r. nr 182, poz. 1228).

Nic bardziej mylnego. Nie istnieje żaden zapis zwalniający tego typu organizację z przestrzegania przepisów dotyczących specyficznego rodzaju informacji, jakimi są dane osobowe, których ochrona i zabezpieczenie są równie ważne jak ochrona informacji niejawnych. Sama ustawa o ochronie danych osobowych[3] jest stosunkowo nowym aktem prawnym. Głównym motywem jej przygotowywania była potrzeba dostosowania naszego ustawodawstwa do systemu prawnego państw Unii Europejskiej[4].

Dlatego może wydawać się mniej istotna od wspomnianych wcześniej ustaw. Przepisy zawarte w ustawie nie stoją w sprzeczności z przepisami pozostałych ustaw i wymagają respektowania przez niemal wszystkie organizacje, z wyjątkiem

[2] http://www.giodo.gov.pl/1520049/id_art/2834/j/pl/.

[3] Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych dokonuje wdrożenia dyrektywy 95/46/WE Parlamentu Europejskiego i rady z dnia 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. WE L 281 z 23.11.1995, str. 31, z późn. zm.; Dz.Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, str. 355, z późn. zm.).

[4] Dyrektywa Parlamentu Europejskiego i Rady 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dziennik Urzędowy Wspólnot Europejskich, Dz.U. L 281z 23.11.1995.

instytucji i osób zwolnionych przez ustawodawcę, do których jednostki wojskowe jednak nie należą. Dlatego też dowódcy jednostek chcąc wypełnić obowiązki na nich nałożone przez ustawę o ochronie danych osobowych powinni poddać wnikliwej i szczegółowej analizie przepisy oraz opracować i wdrożyć stosowne dokumenty regulujące tę dziedzinę działalności w zarządzanej instytucji, aby uniknąć grożących za ich zaniechanie konsekwencji karnych i zapewnić niezakłócone funkcjonowanie organizacji.

Czym są więc informacje, które stanowią dane osobowe? Dane osobowe, w myśl art. 6 ustawy, to wszelkie informacje dotyczące zidentyfikowanej, bądź też możliwej do zidentyfikowania osoby fizycznej. Zaś osobą fizyczną możliwą do zidentyfikowania jest osoba, której tożsamość można ustalić w sposób bezpośredni lub pośredni, głównie przez wykorzystanie numeru identyfikacyjnego, bądź specyficznych czynników i cech, które prezentują cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Jednak nie w sytuacji, gdy określenie tożsamości wymaga zbyt dużych nakładów czasowych czy finansowych. Jak widać ustawa nie określa jednoznacznie, czym są dane osobowe, definiuje je w sposób otwarty, dlatego też w każdym przypadku należy dokonywać oceny czy dane, które przetwarzamy stanowią dane osobowe i czy wymagają ochrony. Danymi osobowymi nie są przykładowo ogólne informacje typu wiek, wykształcenie, wyznanie, wielkość zarobków czy nazwy ulic – jeżeli występują pojedynczo i nie są w żaden sposób ze sobą powiązane, co uniemożliwia identyfikację konkretnej osoby. Ale już w sytuacji, gdy dane takie połączy się w grupy, a powstałe informacje pozwolą na identyfikację osoby fizycznej stanowią dane osobowe podlegające ochronie. Warto zwrócić również uwagę, że dane osobowe stanowią tylko te informacje, które dotyczą osoby fizycznej[5], czyli człowieka. Informacje dotyczące podmiotów i osób prawnych[6] jak kapitał, siedziba czy zakres działalności nie dotyczą konkretnej osoby, więc nie stanowią danych osobowych. Ustawa określa również szczególny rodzaj danych, których przetwarzanie jest zabronione, z wyjątkiem sytuacji określonych ustawą. Dane te zwyczajowo zwane są *danymi wrażliwymi* lub *sensytywnymi*[7], a zalicza się do nich informacje ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Na potrzeby właściwego zrozumienia istoty i znaczenia ochrony danych osobowych ważne jest wyjaśnienie terminu przetwarzania danych. Należy mieć świadomość, że aby przetwarzać dane nie trzeba wykonywać na nich żadnych operacji – wystarczy je posiadać, gdyż zgodnie z zapisem ustawy przetwarzanie danych to jakiekolwiek operacje wykonywane na nich, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te czynności, które wykonuje się w systemach teleinformatycznych. Przepisy ustawy stosuje się w sytuacji przetwarzanie danych osobowych w:

1. Kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.
2. Systemach informatycznych, także przetwarzanie danych poza zbiorem danych.

Obowiązek ochrony i zabezpieczenia wszelkich danych osobowych, ze szczególnym uwzględnieniem danych wrażliwych, spoczywa na administratorze danych osobowych.

Administrator danych osobowych – rola i zadania

Administratorem danych osobowych[8] jest organ, jednostka organizacyjna, podmiot lub osoba decydujące o celach i środkach przetwarzania tych danych. Jednostka wojskowa decyduje o celach i środkach przetwarzania danych osobowych, a więc jest w rozumieniu ustawy, administratorem danych osobowych. Z racji tego, iż pewnych czynności organizacja sama fizycznie nie może wykonywać, zadania te spoczywają na jej kierowniku, dyrektorze, bądź w przypadku jednostki wojskowej – dowódcy. W związku z tym na dowódcy,

[5] Określenie człowieka w prawie cywilnym, od chwili urodzenia do chwili śmierci (Dz.U. z 1964r., nr 16, poz. 93 z późn. zm. – Dział I, Rozdział I).

[6] Osobami prawnymi są Skarb Państwa i jednostki organizacyjne, którym przepisy szczególne przyznają osobowość prawną. (Ibidem, art. 33).

[7] http://pl.wikipedia.org/wiki/Dane_wrażliwe.

[8] Art. 7 pkt 4 *Ustawy*…

jako na administratorze danych, ciąży obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, która będzie stosowna do zagrożeń oraz kategorii przetwarzanych danych, ze szczególnym uwzględnieniem zabezpieczenia ich przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem w sposób naruszający przepisy ustawy, a także zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator danych sam pełni obowiązki, bądź wyznacza administratora bezpieczeństwa informacji, którego zadaniem jest nadzór nad przestrzeganiem zasad ochrony danych osobowych. Obowiązkiem administratora danych jest opracowanie i prowadzenie dokumentacji opisującej sposób przetwarzania danych.

Wymagana dokumentacja przetwarzania danych osobowych

W skład wymaganej przepisami dokumentacji dotyczącej przetwarzania danych osobowych wchodzą dwa dokumenty:

− polityka bezpieczeństwa,

− instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Ponadto instrukcję zarządzania systemem informatycznym uzupełniają odpowiednie dla każdego przypadku wzory upoważnień i oświadczeń stosowanych podczas eksploatacji systemu, w którym przetwarzane są dane osobowe.

Dokumentacja wymieniona powyżej powinna być prowadzona w formie pisemnej. Akt wykonawczy do ustawy *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz.U. z 2004 r., nr 100, poz. 1024) szczegółowo określa zakres informacji jakie powinny być ujęte we wspomnianych dokumentach.

Polityka bezpieczeństwa, w szczególności powinna zawierać następujące dane:

− wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

− wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

− opis struktur zbiorów danych wskazujący zawartość poszczególnych pól informatycznych i powiązania między nimi;

− sposób przepływu danych pomiędzy poszczególnymi systemami;

− określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych musi zawierać:

− procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie odpowiedzialnego za te czynności;

− stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

− procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

− procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

− sposób, miejsce i okres przechowywania;

− elektronicznych nośników informacji zawierających dane osobowe,

− kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

− sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do niego;

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

Administrator, prowadząc ewidencję wydanych upoważnień, powinien opracować dokument, w którym zawarte będzie:

− imię i nazwisko osoby upoważnionej,

− data nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,

− identyfikator (gdy dane przetwarzane są w systemie teleinformatycznym).

Z kolei osoby, które uzyskały upoważnienia są zobowiązane zachować w tajemnicy zarówno dane

osobowe, z którymi mają styczność, jak i sposoby oraz zasady ich zabezpieczenia.

Na administratorze danych spoczywa obowiązek zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone, a także komu są one przekazywane. Przetwarzanie danych można powierzyć innemu podmiotowi na zasadzie umowy pisemnej, który będzie je przetwarzał na potrzeby organizacji tylko w zakresie i celu określonym w umowie. Umowa taka nakłada na podmiot obowiązki administratora danych.

Administrator danych zobowiązany jest dołożyć szczególnych starań, aby zapewnić ochronę interesów osób, których dane dotyczą, co oznacza, iż musi zapewnić, aby dane te były:

− przetwarzane zgodnie z prawem,

− zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami (z wyjątkiem sytuacji, gdy nie narusza praw i wolności osoby, której dane dotyczą oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych z ograniczeniami ustawy),

− merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

− przetwarzane w postaci, która umożliwia identyfikację osób, których dotyczą, jednak nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Zasady przetwarzania danych osobowych

Samo przetwarzanie danych osobowych odbywać się może tylko w sytuacji przestrzegania zasad, które narzuca ustawodawca. Przede wszystkim osoba, której dane dotyczą, musi wyrazić zgodę na przetwarzanie danych, z wyjątkiem sytuacji, gdy chodzi o usunięcie danych jej dotyczących. Przez zgodę osoby, której dane dotyczą rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda taka nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści, może być w każdej chwili odwołana, a także może obejmować przetwarzanie danych w przyszłości, w sytuacji kiedy niezmienni się cel przetwarzania. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a nie ma możliwości uzyskania zgody w danym momencie, można je przetwarzać bez takiej zgody do chwili, kiedy będzie można ją uzyskać. Przetwarzanie danych jest także dopuszczalne, gdy jest niezbędne dla zrealizowania uprawnienia, bądź spełnienia obowiązku wynikającego z przepisu prawa, kiedy jest konieczne do realizacji umowy, a osoba, której dane dotyczą, jest jej stroną lub jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, gdy jest wymagane do wykonania określonych prawem zadań realizowanych dla dobra publicznego, a także w sytuacji, kiedy jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów (marketing bezpośredni własnych produktów lub usług, dochodzenie roszczeń z racji prowadzonej działalności gospodarczej) realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw osoby, której dane dotyczą.

W przypadku zbierania i gromadzenia danych od osoby, której dotyczą, administrator danych ma obowiązek informowania tej osoby o:

− adresie swojej siedziby oraz pełnej nazwie (gdy administratorem jest osoba fizyczna – o miejscu zamieszkania oraz imieniu i nazwisku),

− celu zbierania danych (przede wszystkim o przewidywanych odbiorcach),

− prawie dostępu do treści danych oraz możliwości ich poprawienia,

− dobrowolności lub obowiązku podania danych (wraz z podstawą prawną).

Jeżeli administrator zbiera dane nie bezpośrednio od osoby, której dotyczą musi udzielić informacji w zakresie określonym powyżej, bezpośrednio po utrwaleniu zebranych danych.

Nieco odmiennie sprawa wygląda, gdy zachodzi konieczność przetwarzania danych osobowych „wrażliwych". Generalnie, przetwarzanie tego typu informacji jest zabronione przez ustawodawcę, który dopuszcza tylko kilka możliwości, w których administrator może przeprowadzić na nich określone operacje, a zalicza się do nich sytuacje gdy:

− osoba, której dotyczą, wyrazi na to pisemną zgodę (z wyjątkiem usunięcia danych),

− przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby z jednoczesnym zapewnieniem gwarancji ich ochrony,

− przetwarzanie tych danych jest niezbędne do ochrony żywotnych interesów osoby, której dotyczą, lub innej osoby (gdy osoba, której dotyczą

fizycznie bądź prawnie, nie jest zdolna do wyrażenia zgody – do czasu ustanowienia kuratora lub opiekuna prawnego),

− jest to niezbędne do wykonania statusowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji czy instytucji o celach politycznych, naukowych, religijnych, filozoficznych, ale tylko gdy dane te dotyczą ich członków lub osób utrzymujących z nimi stałe kontakty,

− przetwarzanie obejmuje dane niezbędne do dochodzenia praw przed sądem,

− przetwarzanie jest konieczne do wykonania zadań administratora danych odnoszących się do zatrudnienie pracowników w zakresie określonym ustawą,

− przetwarzanie jest prowadzone w celu ochrony zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez uprawnione osoby przy pełnej gwarancji ochrony danych osobowych,

− przetwarzanie dotyczy danych podanych do wiadomości publicznej przez osobę, której dotyczą,

− jest to niezbędne do prowadzenia badań naukowych, ale publikowanie wyników badań nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone,

− przetwarzanie jest prowadzone w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Obowiązek pozyskania zgody i informacyjny w jednostkach wojskowych dotyczy jedynie pracowników wojska, sytuacja ma się inaczej, jeśli chodzi o żołnierzy. Zgodnie z zapisami *Ustawy z dnia 11 września 2003r. o służbie wojskowej żołnierzy zawodowych* (Dz.U. z 2010r. nr 90, poz. 593 z późniejszymi zmianami) wszyscy żołnierze objęci są ewidencją wojskową, którą prowadzą przez dyrektora departamentu Ministerstwa Obrony Narodowej właściwego do spraw kadr, organ właściwy do wyznaczania na stanowisko służbowe i dowódcę jednostki wojskowej, w której żołnierz pełni zawodową służbę wojskową oraz wojskowego komendanta uzupełnień (art. 48). Dane ujmowane w ewidencji wojskowej to:

− dane osobowe żołnierza zawodowego (nazwisko i imiona, nazwisko rodowe, nazwisko i imiona poprzednie, imiona rodziców, nazwiska rodowe rodziców, imię i nazwisko małżonka oraz jego nazwisko rodowe, imiona dzieci, płeć, datę i miejsce urodzenia, obywatelstwo, numer PESEL, stopień wojskowy, adres zameldowania, adres zamieszkania oraz rodzaj, serię i numer dokumentu tożsamości),

− dane dotyczące przebiegu czynnej służby wojskowej,

− stan zdrowia,

− wykształcenie,

− kwalifikacje,

− stan cywilny i rodzinny,

− wyróżnienia,

− orzeczenia wydane w stosunku do żołnierza w postępowaniu sądowym, administracyjnym lub dyscyplinarnym,

− odpowiedzialność zawodowa.

Ustawodawca zastrzegł, iż przetwarzanie danych osobowych zgromadzonych w ewidencji wojskowej może odbywać się bez wiedzy i zgody osoby (żołnierza), której dotyczą te dane. Oznacza to, że w przypadku ewidencji wojskowej – przetwarzania danych osobowych do celów związanych z przebiegiem zawodowej służby wojskowej nie stosuje się przepisów rozdziału 3. (*Zasady przetwarzania danych osobowych)* ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[9]. A więc administrator danych osobowych, którym jest dowódca jednostki wojskowej ma obowiązek stosowania w swojej działalności przepisów ustawy z pominięciem zapisów dotyczących informowania żołnierzy o przetwarzaniu danych ich dotyczących, jeżeli są jego podwładnymi, a dane przetwarzane są w celach związanych z przebiegiem służby.

W sytuacji, gdy osoba, której dane osobowe dotyczą, wykaże ich niekompletność, nieaktualność, nieprawdziwość, bądź fakt zbierania ich z naruszeniem przepisów prawa, albo że są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych ma obowiązek uzupełnić je, uaktualnić, sprostować błędy, a także czasowo lub stale wstrzymać ich przetwarzanie, a nawet usunąć ze zbioru, chyba że dotyczy to danych, których tryb zmiany określają odrębne ustawy. Administrator musi również bezzwłocznie powiadomić innych administratorów, którym udostępnił zbiór danych o dokonanych zmianach.

Każdy, którego dane osobowe są przetwarzane, ma prawo do ich kontroli, a w szczególności do:

− uzyskania wyczerpujących informacji, czy istnieje zbiór zawierający takie dane, kto jest ich

[9] http://www.giodo.gov.pl/1520012/id_art/2928/j/pl/.

administratorem, jaki ma adres siedziby i nazwę (w przypadku administratora, którym jest osoba fizyczna – jej miejsca zamieszkania, imienia i nazwiska),

− pozyskania informacji o celu, zakresie i sposobie przetwarzania danych,

− uzyskanie informacji o źródle, z jakiego dane pozyskano, chyba że administrator ma obowiązek zachować to w tajemnicy na mocy prawa,

− żądania uzupełnienia, uaktualnienia, sprostowania danych, wstrzymania ich przetwarzania bądź ich usunięcia, jeżeli są niekompletne, nieaktualne czy zbędne,

− wniesienia pisemnego, uzasadnionego żądania zaprzestania przetwarzania danych w sytuacjach szczególnych,

− wniesienia sprzeciwu wobec przetwarzania jej danych, gdy administrator zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych innemu administratorowi danych.

Zgłoszenie zbiorów danych osobowych

Kolejnym obowiązkiem administratora danych jest zgłoszenie zbiorów danych osobowych Generalnemu Inspektorowi Ochrony Danych Osobowych[10] (GIODO), jeżeli zgodnie z ustawą podlegają one rejestracji. Zgłoszeniu danych podlegają wszystkie zbiory danych z wyjątkiem:

− zbiorów zawierających informacje niejawne, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez uprawnionych funkcjonariuszy,

− przetwarzanych przez właściwe organy na potrzeby postępowania sądowego oraz w oparciu o przepisy (przetwarzane przez Generalnego Inspektora Informacji Finansowej, w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, a także przetwarzane na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej),

− gdy dotyczą osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tej grupy wyznaniowej,

− związanych z zatrudnieniem, świadczeniem usług na podstawie umów cywilno prawnych, a także osób u nich zrzeszonych bądź uczących się,

− dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta,

− tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, powiatów itd.,

− dotyczących osób pobawionych wolności, w zakresie niezbędnym do wykonania tymczasowego aresztowania bądź kary pozbawienia wolności,

− przetwarzanych wyłącznie na potrzeby wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,

− powszechnie dostępnych,

− przetwarzanych w celu przygotowania rozprawy niezbędnej do ukończenia szkoły wyższej bądź uzyskania stopnia naukowego,

− dotyczących drobnych bieżących spraw życia codziennego.

Zgłoszenia dokonuje się zgodnie z ustalaną zasadą na specjalnych formularzach, zgodnie z zasadami określonymi w *Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych* (Dz.U. z 2008r. nr 229, poz. 1536). Jeżeli w zarejestrowanym zbiorze danych zaistniała zmiana administrator danych jest zobowiązany zgłosić ją Generalnemu Inspektorowi w terminie do 30 dni od dnia dokonania zmiany w zbiorze danych. Natomiast jeżeli zmiana należy do kategorii danych wrażliwych należy ją zgłosić przed dokonaniem zmiany w zbiorze. Niezgłoszenie zbioru danych, który podlega rejestracji grozi karą grzywny, ograniczenia wolności lub jej pozbawienia do roku.

Niewypełnienie pozostałych obowiązków wynikających z ustawy obłożone jest także sankcjami karnymi. Samo przetwarzanie danych, których przetwarzanie nie jest dopuszczalne, bądź do przetwarzania których nie jest się dopuszczonym, zagrożone jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli czynności te dotyczą tzw. danych wrażliwych karą może być grzywna, ograniczenie wolności albo pozbawienie wolności do lat 3. Karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2 zagrożona jest również osoba, która ad-

[10] Zgodnie z Ustawą Art. 8. 1. Organem do spraw ochrony danych osobowych jest Generalny Inspektor Ochrony Danych Osobowych.

ministruje zbiorem danych lub będąc zobowiązana do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieuprawnionym. Jeżeli działanie takie jest nieumyślnie osobie takiej grozi grzywna, ograniczenia wolności albo pozbawienia wolności do roku. Tą samą karą zagrożone jest również administrowanie danymi, w trakcie którego choćby nieumyślnie naruszany jest obowiązek zabezpieczenia danych przed ich zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, a także niedopełnienie obowiązku informacyjnego w stosunku do osób, których dane dotyczą. Karane jest również udaremnianie i utrudnianie wykonywania czynności kontrolnych grzywną, ograniczeniem wolności lub jej pozbawieniem do lat 2.

Chcąc wyegzekwować przestrzeganie przepisów normujących ochronę danych osobowych, ustawodawca powołał organ kontrolny, którym jest Generalny Inspektor Ochrony Danych Osobowych, powoływany i odwoływany przez Sejm Rzeczypospolitej Polskiej za zgodą Senatu. Generalnym Inspektorem może być obywatel polski, który na stałe zamieszkuje terytorium Rzeczypospolitej Polskiej, posiada wysoki autorytet moralny, posiada wyższe wykształcenie prawnicze i doświadczenie zawodowe oraz nie był karany za przestępstwo. Kompetencje oraz zakres uprawnień i obowiązków Generalnego Inspektora oraz pracowników jego biura określono w ustawie, nadając im uprawnienia do szeroko rozumianej kontroli w zakresie przestrzegania przepisów ochrony danych osobowych. Po zakończeniu czynności kontrolnych w organizacji zespół kontrolujący sporządza protokół, który zawiera opis zastanego stanu faktycznego stanowiący podstawę oceny zgodności przetwarzania danych osobowych oraz ich zbiorów z przepisami o ochronie danych osobowych. Jeżeli zostaną stwierdzone naruszenia w zakresie danych osobowych, generalny inspektor ma prawo wydania decyzji administracyjnej nakazującej:

− usunięcie stwierdzonych usterek,

− uzupełnieni, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych,

− zastosowanie dodatkowych środków zabezpieczających zbiory danych,

− wstrzymanie przekazywania danych osobowych do państwa trzeciego[11],

− zabezpieczenie danych lub przekazanie ich innym podmiotom,

− usunięcie danych osobowych.

Gdy naruszenia są jednak zbyt poważne, a działanie administrującego danymi lub jego brak wyczerpuje znamiona przestępstwa, które określa ustawa, generalny inspektor dostarcza dowody i zgłasza do prokuratury zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

Co więc zrobić i jak postępować, aby, będąc kierującym jednostką organizacyjną, również jednostką wojskową, uniknąć sankcji karnych, jakie grożą za niedopełnienie obowiązków wynikających z ustawy oraz prowadzić racjonalną politykę bezpieczeństwa ochrony danych osobowych?

Specyfika organizacji ochrony danych osobowych w jednostce wojskowej

Dowódca jednostki, aby zapewnić w swojej organizacji właściwą i zgodną z przepisami prawa ochronę danych osobowych powinien swoje działania zapoczątkować wyznaczeniem administratora danych osobowych, który w jego imieniu poprzez opracowanie i wdrożenie polityki bezpieczeństwa, instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz prowadzenie ewidencji wydanych upoważnień będzie nadzorował przestrzeganie zasad ochrony danych osobowych. Ponadto w sytuacji, gdy jednostka ma rozbudowane struktury (duża liczba żołnierzy i pracowników) lub rozmieszczona jest na kilku kompleksach (miejscowościach) wskazane jest wyznaczenie nawet kilku administratorów lokalnych, którzy odpowiadać będą za nadzór nad ochroną danych osobowych w swoich obiektach, bądź nawet w każdym batalionie. Takie rozwiązanie może w dużym stopniu ułatwić zapewnienie integralności, poufności i rozliczalność danych osobowych, które są przetwarzane niemal na wszystkich szczeblach hierarchii organizacyjnej jednostki wojskowej.

Wszelkie dane osobowe przetwarza się w zbiorach, przez które ustawodawca rozumie każdy posiadający strukturę zestaw o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Administrator danych osobowych musi zidenty-

[11] Państwo nienależące do Europejskiego Obszaru Gospodarczego.

fikować te zbiory, opisać ich struktury oraz zakres informacji gromadzonych w danym zbiorze. W jednostce wojskowej o strukturze batalionowej czy choćby kompanijnej, a więc hierarchicznej występują dane osobowe w zbiorach rozproszonych oraz podzielonych funkcjonalnie, ponieważ różne dane osobowe przetwarzane są na poszczególnych szczeblach dowodzenia wybiórczo, zaś całość zbiorów danych gromadzi się na szczeblu sztabu jednostki. Sytuację taką rozumieć należy w ten sposób, że dowódca drużyny przetwarza dane osobowe żołnierzy swojej drużyny, dowódca plutonu dane osobowe żołnierzy plutonu (w tym wspomnianej drużyny), dowódca kompanii dane żołnierzy wszystkich drużyn i plutonów wchodzących w skład jego kompanii i tak, aż do szczebla najwyższego, czyli sztabu jednostki, gdzie przetwarza się dane osobowe wszystkich żołnierzy i pracowników wojska danej jednostki wojskowej. Rozpoznanie zbiorów danych, ich struktur oraz powiązań i relacji między nimi w organizacji zhierarchizowanej nie jest więc łatwe, ale wykonanie tych czynności prawidłowo jest niezbędną podstawą do opracowania komplementarnej polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, gdyż obecnie systemy takie istnieją zapewne w każdej jednostce wojskowej. Ważne jest wskazanie nazw zborów danych oraz nazw systemów informatycznych, w których dane takie są przetwarzane. Dane osobowe zawarte w zbiorach przetwarza się bądź w sposób tradycyjny, czyli w kartotekach, skorowidzach, księgach i wykazach, bądź z wykorzystaniem systemów teleinformatycznych. Opisując zbiory danych podać trzeba sposób ich przetwarzania. Określając zbiory danych można dowolnie konstruować wykaz korzystając z tabele i schematów, gdyż ustawodawca nie narzucił sformalizowanego układu, pamiętając jednak o dokładnym wskazaniu wszystkich elementów zbioru oraz miejsca ich przetwarzania i wykorzystywanego do tego programu komputerowego. Wykaz zbiorów danych może przyjąć postać tabeli przedstawionej poniżej, z uwzględnieniem wszystkich zbiorów danych występujących w jednostce organizacyjnej.

Tabela 1

Wykaz zbioru danych – wariant I (opracowanie własne)

Lp.	Komórka organizacyjna	Nazwa zbioru danych	Forma przetwarzania	System informatyczny/ nazwa programu komputerowego	Zakres danych wchodzących w zbiór	Lokalizacja zbioru
1	POIN[a)] / Pełnomocnik ds. Ochrony IN	Wykaz osób zatrudnionych lub pełniących służbę w jednostce	FP/ FE*	Stacja MIL-WAN/ MS Office Excel	klauzula tajności stanowiska, nazwa stanowiska /Rodzaj pracy zleconej/, NIS, imię, stopień wojskowy, nazwisko, imię ojca, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, okres pełnienia służby /pracy/ na stanowisku, numer poświadczenia	Sztab JW. Budynek nr 6, piętro II /kancelarie nr 207, 208/
2		Wykaz uczestników szkolenia z zakresu ochrony informacji niejawnych	FP	brak	stopień wojskowy, imiona, nazwisko, data szkolenia, podpis	
3		Wykaz osób, wobec których przeprowadzono postępowania sprawdzające do klauzuli „POUFNE”	FP	brak	stopień wojskowy, imiona, nazwisko, imię ojca, data i miejsce urodzenia, miejsce zamieszkania, miejsce pracy/ służby, stanowisko, data i numer wydanego poświadczenia bezpieczeństwa itd.	

Lp.	Komórka organizacyjna	Nazwa zbioru danych	Forma przetwarzania	System informatyczny/ nazwa programu komputerowego	Zakres danych wchodzących w zbiór	Lokalizacja zbioru
4		Rejestr wydanych zaświadczeń stwierdzających odbycie szkolenia z OIN	FP	brak	stopień imię i nazwisko, PESEL, jednostka (komórka) organizacyjna, numer zaświadczenia, data szkolenia, rodzaj szkolenia	
5	POIN/ Kancelaria tajna	Rejestr wydanych dokumentów /RTD/	FP	brak	Oznaczenie klauzuli tajności, stopień, imię i nazwisko wykonawcy, data wydania dokumentu, stopień, imię i nazwisko oraz podpis osoby pobierającej	Budynek nr 6, piętro I /pomieszczenie nr 12/
6		Wykaz osób upoważnionych do dostępu do informacji niejawnych	FP/ FE	Stacja MIL-WAN/ MS Office	stopień, imię i nazwisko, nazwa komórki organizacyjnej, data wydania i numer poświadczenia bezpieczeństwa, klauzula, data ważności	Budynek nr 6, piętro I /pomieszczenie nr 12/
7		Dziennik ewidencyjny /DE/	FP/ FE	Stacja MIL-WAN/ ARCUS	Klauzula tajności dokumentu, numer, data rejestracji, nazwa nadawcy, adres, liczba stron, nazwa dokumentu, czego dotyczy	Budynek nr 6, piętro I /pomieszczenie nr 12/
8	POIN/ Kancelaria jawna	Rejestr dokumentów wchodzących	FP/ FE	Stacja MIL-WAN/ ARCUS	numer, data rejestracji, nazwa nadawcy, adres, liczba stron, nazwa dokumentu, czego dotyczy	Budynek nr 6, piętro I /pomieszczenie nr 18/
8		Rejestr dokumentów wychodzących	FP/ FE	Stacja MIL-WAN/ ARCUS	numer, data rejestracji, nazwa adresata, adres, liczba stron, nazwa dokumentu, czego dotyczy	Budynek nr 6, piętro I /pomieszczenie nr 18/
9	Sztab JW./ Sekcja personalna	Dane kadrowe – pracownicy wojska	FP/ FE	Stacja MIL-WAN/ SEW on-line	imiona, nazwisko, imię ojca, data i miejsce urodzenia, PESEL, adres zamieszkania, miejsce /stanowisko/ pracy, rodzaj zatrudnienia, czas itd.	Budynek nr 6, piętro I /pomieszczenia nr 21, 22/
10	Sztab JW./ Sekcja personalna	Dane kadrowe – żołnierze zawodowi	FP/ FE	Stacja MIL-WAN/ SEW on-line	Stopień, imiona, nazwisko, imię ojca, data i miejsce urodzenia, PESEL, adres zamieszkania, miejsce /stanowisko/ służby, kontrakt, stan zdrowia, ukończone kursy, szkolenia, itd.	Budynek nr 6, piętro I /pomieszczenia nr 21, 22/
11	5 batalion zmechanizowany/ Sztab	Dane żołnierzy batalionu	FP/ FE	Stacja MIL-WAN/ MS Office	Stopień, imiona, nazwisko, imię ojca, data i miejsce urodzenia, PESEL, adres zamieszkania, miejsce /stanowisko/ służby, kontrakt, stan zdrowia, ukończone kursy, szkolenia, itd.	Budynek 7, parter, Pomieszczenia nr 1 i 2
12		Ewidencja szkolenia	FP	brak	Stopień, imię i nazwisko, komórka organizacyjna, oceny ze szkolenia	Budynek 7, parter, Pom. nr 10 i 11
13	5 batalion zmechanizowany/ 1 kompania	Dane żołnierzy kompanii	FP/ FE	Stacja MIL-WAN/ MS Office	Stopień, imiona, nazwisko, imię ojca, data i miejsce urodzenia, PESEL, adres zamieszkania, miejsce /stanowisko/ służby, kontrakt, stan zdrowia, ukończone kursy, szkolenia, itd.	Budynek 10, piętro I, Pomieszczenie nr 111

Lp.	Komórka organizacyjna	Nazwa zbioru danych	Forma przetwarzania	System informatyczny/ nazwa programu komputerowego	Zakres danych wchodzących w zbiór	Lokalizacja zbioru
14		Ewidencja szkolenia	FP	brak	Stopień, imię i nazwisko, pododdział, oceny ze szkolenia	Budynek 10, piętro I, Pomieszczenie nr 111
15	5 batalion zmechanizowany/ 1 kompania/ 1 pluton	Dane żołnierzy plutonu	FP/ FE	Stacja MIL-WAN/ MS Office	Stopień, imiona, nazwisko, imię ojca, data i miejsce urodzenia, PESEL, adres zamieszkania, miejsce /stanowisko/ służby, kontrakt, stan zdrowia, ukończone kursy, szkolenia, itd.	Budynek 10, piętro I, Pomieszczenie nr 119
16		Ewidencja szkolenia	FP	brak	Stopień, imię i nazwisko, oceny ze szkolenia	Budynek 10, piętro I, Pomieszczenie nr 119 (dziennik lekcyjny zabierany na zajęcia)

[a)] Pion Ochrony Informacji Niejawnych.

* FP – forma papierowa, FE – forma elektroniczna

Oczywiście opis zbiorów danych, ujęty w ten sposób, może być bardzo rozbudowany, jednak szczegółowe ich określenie znacznie ułatwi rozliczalność przetwarzanych danych osobowych oraz pozwoli szczegółowo określić żołnierzy i pracowników wojska, odpowiedzialnych za ich właściwą ochronę. Ułatwi to także prowadzenie szkoleń dla osób, którym wydane zostaną upoważnienia do przetwarzania danych osobowych wraz ze szczegółowym określeniem kompetencji. Tworzenie tego typu opisu zbiorów danych jest jednak bardzo pracochłonne, a w przypadku jednostek wojskowych wiąże się również z koniecznością rozstrzygnięcia kwestii nadania stosownej klauzuli tajności dokumentu. Oczywiście opis struktur zbiorów danych można sporządzić nieco prościej określając obszary zawartość poszczególnych pól informacyjnych i sposób przetwarzania (tabela 2).

Przyjmując powyższą formę wykazu zbiorów danych konieczne jest uzupełnienie wykazu o informacje dotyczące miejsca przetwarzania (tabela 3), z uwzględnieniem adresu – jeżeli jednostka zlokalizowana jest w kilku miejscach pod różnymi adresami oraz numerami budynków i pomieszczeń.

Tabela 2

Wykaz zbioru danych – wariant II (opracowanie własne)

Lp.	Nazwa zbioru głównego i podzbiorów	Sposób przetwarzania	Opis zawartości zbioru
1	OCHRONA INFORMACJI NIEJAWNYCH **A** Rejestr wydanych zaświadczeń stwierdzających odbycie szkolenia z zakresu ochrony informacji niejawnych.	FP/ FE	Klauzula tajności stanowiska, nazwa stanowiska /Rodzaj pracy zleconej/, NIS, imię, stopień wojskowy, nazwisko, imię ojca, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, numer telefonu, okres pełnienia służby /pracy/ na stanowisku, numer poświadczenia, data szkolenia
	B Wykaz osób, wobec których przeprowadzono postępowania sprawdzające do klauzuli „POUFNE”.	FP	
	C Wykaz uczestników szkolenia z zakresu ochrony informacji niejawnych.	FP	
	D Wykazu osób zatrudnionych lub pełniących służbę w jednostce	FP	

Lp.	Nazwa zbioru głównego i podzbiorów	Sposób przetwarzania	Opis zawartości zbioru
2	**DZIAŁALNOŚĆ KADROWA** **A** Rozkaz dzienny	FP/ FE	Stopień wojskowy, nazwisko, imiona, imiona rodziców, nazwisko rodowe, data urodzenia, wykształcenie, adres zamieszkania lub pobytu, numer PESEL, seria i numer dowodu osobistego, NIP, data zatrudnienia, jednostka organizacyjna, stanowisko, nr telefonu, dane osobowe członka rodziny, obywatelstwo, numer specjalności wojskowej, wykształcenie wojskowe, przynależność do WKU, nr książeczki wojskowej, przydział mobilizacyjny do sił zbrojnych RP
	B Dane pracowników wojska	FP/ FE	
	C Dane żołnierzy zawodowych – oficerów	FP/ FE	
	D Dane żołnierzy zawodowych – podoficerów	FP/ FE	
	E Dane żołnierzy zawodowych – szeregowych	FP/ FE	
	F Dane żołnierzy rezerwy przeznaczonych na uzupełnienie jednostki	FP/ FE	
	G Skargi i wnioski.	FP	
3	**OBSŁUGA KANCELARYJNA** **A** Rejestr wydanych dokumentów /RTD/.	FP	Oznaczenie klauzuli tajności, stopień, imię i nazwisko wykonawcy, data wydania dokumentu, stopień, imię i nazwisko oraz podpis osoby pobierającej, nazwa komórki organizacyjnej, data wydania i numer poświadczenia bezpieczeństwa, data ważności, data rejestracji, nazwa nadawcy, adres, liczba stron, nazwa dokumentu, czego dotyczy
	B Wykaz osób upoważnionych do dostępu do informacji niejawnych.	FP/ FE	
	C Dziennik ewidencyjny /DE/.	FP	
	D Rejestr dokumentów wchodzących	FP/ FE	
	E Rejestr dokumentów wychodzących	FP/ FE	
4	SZKOLENIE	FP/ FE	Stopień, imię nazwisko, pododdział, ocena

Tabela 3

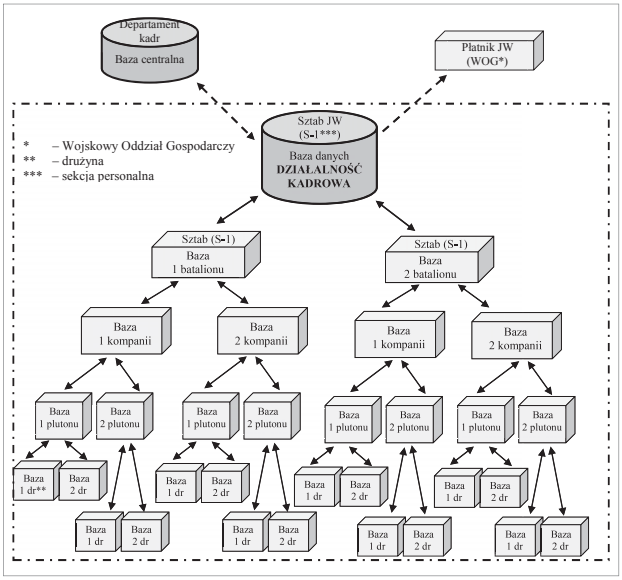
Wykaz miejsc przetwarzania danych osobowych – wariant (opracowanie własne)

Lp.	Zbiór/ podzbiór	Nazwa	Miejsce przetwarzana	
			Adres	Budynek/ pomieszczenie
1.	1 A	Rejestr wydanych zaświadczeń stwierdzających odbycie szkolenia z zakresu ochrony informacji niejawnych.	ul. Zielona 43	Budynek nr 5 – pomieszczenia 7, 10, 15
				Budynek nr 8 – pomieszczenia 22, 23
2.	1 B	Wykaz osób, wobec których przeprowadzono postępowania sprawdzające do klauzuli „POUFNE”.	ul. Kwiatowa 12	Budynek nr 3 – pomieszczenia 4 ,5
3.	2 A	Rozkaz dzienny	ul. Zielona 43	Budynek nr 4 – pomieszczenia 18,19
			ul. Kwiatowa 12	Budynek nr 1 – pomieszczenia 14, 15
				Budynek nr 5 – pomieszczenia 3, 17, 25
4.	2 B	Dane pracowników wojska	ul. Zielona 43	Budynek nr 5 – pomieszczenia 8,10,12
5.	2 C	Dane żołnierzy zawodowych – oficerów	ul. Zielona 43	Budynek nr 5 – pomieszczenia 7, 10, 15
				Budynek nr 6 – pomieszczenia 12, 10, 15
				Budynek nr 7 – pomieszczenia 2, 18, 24
			ul. Kwiatowa 12	Budynek nr 8 – pomieszczenia 22, 23

Po zakończeniu procesu określania zbiorów danych występujące w jednostce organizacyjnej oraz ich struktury i miejsca przetwarzania, należy wskazać powiązania pomiędzy poszczególnymi polami informacyjnymi, a także przepływ danych pomiędzy poszczególnymi systemami – jeżeli takowy istnieje. W jednostkach wojskowych przepływ danych z reguły jest dwukierunkowy – odczyt i zapis. Dostęp do baz danych może odbywać się bądź z autonomicznego stanowiska komputerowego (nie będącego elementem sieci) lub też w resortowej sieci teleinformatycznej przeznaczonej do użytku wyłącznie w resorcie obrony narodowej, czyli sieci MIL-WAN, która nie ma połączenia z sieciami publicznymi. Na niższych szczeblach strukturalnych jednostek tj. plutonu czy drużyny, przetwarzanie danych osobowych odbywa się przeważnie w sposób tradycyjny, bez wykorzystania systemów informatycznych. Przepływ danych można zobrazować w postaci schematu, w którym ujmuje się bazy danych oraz relacje zachodzące między nimi (schemat 1).

Schemat 1

Uproszczony schemat przepływu danych osobowych w zbiorze Działalność kadrowa – wariant



Opracowanie własne.

Prawidłowe określenie wszystkich zbiorów danych osobowych w organizacji pozwala administratorowi bez większych trudności wytypować te, które podlegają obowiązkowej rejestracji, czyli zgłoszeniu Generalnemu Inspektorowi Danych Osobowych i te, które z tego obowiązku są zwolnione.

Rolą administratora jest także określenie i zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii przetwarzanych danych osobowych. W jednostkach wojskowych nie stanowi to większego problemu z uwagi na szczególne wymagania ochrony i zabezpieczeń, jakie stawiane są tego typu instytucjom przez odrębne akty normatywne, a co wynika z roli i zadań jakie wykonują. Jak wspomniano powyżej dane osobowe w tego typu organizacjach przetwarza się bądź na stacjach roboczych MIL-WAN, bądź na autonomicznych stacjach roboczych, które zawsze posiadają stosowne klauzule tajności, a tym samym podlegają szczególnej ochronie. Większość zasobów przetwarzana jest na podstawowym poziomie bezpieczeństwa (nieprzetwarzane są dane wrażliwe, system informatyczny nie jest połączony z siecią publiczną) oraz podwyższonym (przetwarzane są dane wrażliwe, ale system informatyczny nie jest połączony z siecią publiczną)[12]. Uzyskanie samego dostępu do sieci MIL-WAN wymaga przejścia procedur dopuszczających, posiadania stosownego poświadczenia bezpieczeństwa, przeszkolenia, akceptacji wniosku przez pełnomocnika ds. ochrony informacji niejawnych oraz zgody dowódcy jednostki. Każdy użytkownik, który uzyskał dostęp do sieci MIL-WAN posiada indywidualny identyfikator (login) oraz hasło, które zobowiązany jest nikomu nie udostępniać oraz zmieniać w cyklicznie. Prócz tego same systemy służące do prowadzenia ewidencji wojskowej oraz przetwarzania danych osobowych posiadają nadane klauzule tajności, a dostęp do nich również wiąże się z posiadaniem indywidualnych loginu i hasła. W jednostka wojskowych najczęściej wykorzystuje się system informatyczny SI ETAT, który po wprowadzeniu danych uzyskuje klauzule POUFNE oraz centralny moduł ewidencyjny SEW on-line o klauzuli ZASTREŻONE. Ustawa o ochronie danych osobowych mówi, że jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, stosuje się

[12] *Rozporządzenie MSWiA z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz.U. z 1004r., nr 100, poz. 1024).

przepisy tych ustaw. W instytucjach wojskowych takie zastosowanie ma właśnie *Ustawa o ochronie informacji niejawnych.*

Istotna jest także ochrona urządzeń służących do przetwarzania danych, materiałów zawierających dane osobowe, nośników oraz pomieszczeń, w których się je przetwarza. Ponieważ w jednostka wojskowych istnieje wiele dokumentów z nadanymi klauzulami tajności, a wymogi ochrony informacji niejawnych są restrykcyjnie przestrzegane, niemal każda kancelaria czy miejsce pracy biurowej wyposażone jest w sejfy, bądź stalowe szafy i kartoteki, które w zupełności spełnią wymagania, jakie stawiane są przed urządzeniami przeznaczonymi do przechowywania nośników zawierających dane osobowe (dyski, płyty CD, dyskietki itp.), a także kartotek, ksiąg, wykazów itd. Ponadto budynki i pomieszczenia zabezpieczone są zwykle technicznymi systemami wspierającymi fizyczną ochronę, do których zaliczyć można systemy alarmowe, drzwi antywłamaniowe, kraty w oknach, system telewizji przemysłowej. Dodatkowo tern jednostek wojskowych monitorowany jest przez system całodobowych służb dyżurnych oraz ochraniany, zwykle przez formacje SUFO[13].

Pod dokonaniu wszystkich powyższych czynności i analiz administrator sporządza politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, którą drukuje i zatwierdza, a następnie wprowadza do użytku rozkazem dowódcy jednostki. Kolejnym krokiem w kierunku właściwej ochrony danych osobowych w organizacji jest wdrożenie polityki bezpieczeństwa, czyli zastosowanie w działalności organizacji procedur i środków bezpieczeństwa określanych przez nią, a także przeprowadzić szkolenia, które dadzą pewność, że wszyscy upoważnieni do przetwarzania danych osobowych pracownicy jednostki zapoznali się z dokumentem oraz mają świadomość konsekwencji z niego wynikających. Prowadzona przez administratora ewidencja upoważnień zawierająca imię, nazwisko, datę nadania i ustania oraz zakres uprawnień do przetwarzania danych, pozwala dokładnie określić, jakie osoby powinny być systematycznie szkolone z zakresu ochrony danych osobowych.

Utrzymanie właściwego poziomu ochrony danych osobowych wymaga opracowania systemu szkoleń, dla osób mających upoważnienie do przetwarzania danych osobowych, co zapewni znajomość przepisów ustawy, jej wymogów oraz sankcji karnych grożących za niedopełnienie obowiązków z niej wynikających. Szkolenie nie może być jednorazowe – poprzedzające wydanie upoważnieni do przetwarzania danych osobowych, ale powinno mieć formę cykliczną, aby podkreślić wagę problemu ochrony danych osobowych oraz uświadamiać pracownikom zakres odpowiedzialności, a jednocześnie móc przekazać wszelkie istotne zmiany, rozwiązać pojawiające się problemy czy usprawnić system przetwarzania danych z zapewnieniem pełnej ich ochrony. W jednostkach wojskowych również szkolenia nie powinny stanowić większego problemu, gdyż można je prowadzić w ramach Szkolenia Uzupełniającego zarówno dla pracowników wojska jak i żołnierzy, które odbywa się regularnie. Najbardziej optymalne byłoby prowadzenie szkoleń co najmniej raz na kwartał, gdyż pozwoliłoby to administratorowi danych na stałą kontrolę zarówno wiedzy i świadomości osób przetwarzających dane osobowe, jak również szybką diagnozę przyczyn utrudnień w sytuacji pojawiających się zagrożeń oraz ich zażegnanie.

Zadanie administratora nie kończy się z chwilą wydania, zatwierdzenia i wdrożenia polityki bezpieczeństwa, gdyż nie jest to czynność jednorazowa. Jest to dokument, który może ulegać modyfikacjom, a nawet powinien być stopniowo zmieniany i udoskonalany, co dobrze zostało ukazane w zasadzie zwanej cyklem Deminga inaczej PDCA, pierwotnie zastosowanym w stosunku do procesu biznesowego organizacji. Cykl ten określa ciągłą ewolucję, proces doskonalenia i ulepszania systemu opierający się na czterech elementach:

1. zaplanowanie *(plan)* – przyjęcie polityki dotyczącej ciągłości działalności, wskazanie celów, procesów, procedur i kontroli niezbędnych dla zarządzania ryzykiem i poprawy działania, tak aby ich wynik był zgodny z celami organizacji

2. wykonanie *(do)* – wdrożenie i realizacja polityki w organizacji

3. sprawdzanie *(check)* – stałe monitorowanie i kontrola w odniesieniu do celu polityki, przekazywanie wyników kierownictwu, a także określenie i zatwierdzenie czynności zmierzających do naprawy i usprawnienia procesu

[13] Specjalistyczne Uzbrojone Formacje Ochronne – wewnętrzne służby ochrony najczęściej ochraniające jednostki wojskowe.

4. poprawa *(act)* – usprawnienie procesu poprzez działania prewencyjne i naprawcze oparte na wynikach kontroli. Na tym poziomie dokonuje się aktualizacji i modyfikacji polityki, dostosowania do nowych uwarunkowań zewnętrznych i wewnętrznych.

Częstotliwość zachodzenia takiego cyklu w organizacji zależne jest od stopnia jej złożoności oraz dynamiki procesów w niej zachodzących. Wskazane jest przetwarzanie takiego cyklu nie rzadziej niż raz w roku[14]. Dobrze jest wdrożyć taki cykl w jednostce wojskowej w celu zachowania najwyższej jakości polityki bezpieczeństwa danych osobowych w organizacji.

Podsumowanie

Prowadzenie racjonalnej i zrównoważonej polityki bezpieczeństwa danych osobowych w jednostkach wojskowych to w obecnych czasach nie tylko wymóg przepisów prawa, ale niezbędne działanie, które ma zapewnić właściwą ochronę informacji stanowiących jeden z cenniejszych zasobów tego typu organizacji. Polityka bezpieczeństwa, jako aspekt działalności, będąca spójnym zbiorem reguł, zasad i procedur, zgodnie z którymi organizacja gromadzi, zarządza i udostępnia dane osobowe, powinna określać cel i sposób działania zapewniający maksymalną ich ochronę, a także wskazać osoby, które będą ponosić odpowiedzialność za ich bezpieczeństwo. Gwarantuje to wzrost świadomości i poczucia odpowiedzialności wśród pracowników i żołnierzy, a tym samym prowadzenie działalności służbowej zapewniającej przestrzegania przepisów prawa.

Jednak, aby cały ten proces miał sens i szansę powodzenia, szczególnie w jednostce wojskowej, niezbędne jest zrozumienie i akceptacja konieczności prowadzenia takiej polityki przez dowódcę, co ma priorytetowe znaczenie w czasie jej wdrażania i adaptacji. Wciąż jeszcze obowiązek prowadzenia polityki bezpieczeństwa danych osobowych bywa lekceważony i pomijany, traktowany jako mniej ważny w stosunku do innych aspektów działalności, pomimo że powinien być uważany za jeden z podstawowych warunków dostosowania działań do wymogów prawa. Proces adaptacji zapisów ustawy o ochronie danych osobowych jest działaniem złożonym i skomplikowanym, wymagającym współpracy nie tylko dowódcy i osób obarczonych odpowiedzialnością za nadzór nad ich ochroną, ale wszystkich żołnierzy i pracowników wojska przetwarzających dane osobowe. Mimo piętrzących się trudności, prowadząc właściwą politykę bezpieczeństwa danych osobowych dowódca nie tylko spełnia obowiązek ustawowy, ale zapewnia sobie i podległej jednostce bezpieczeństwo prawne, co daje gwarancję niezakłóconego funkcjonowania i bytu.

[14] R. W. Kaszubski, D. Romańczuk (red.), *Księga dobrych praktyk w zakresie zarządzania ciągłością działania (Business Continuity Management)*, Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa 2011, s. 60.

Bibliografia

Aleksandrowicz T. R., *Komentarz do ustawy o dostępie do informacji publicznej*, Wyd. IV, Wyd. LexisNexis 2008.

Barta J., *Ochrona danych osobowych*, Wyd. Wolters Kluwer Polska Sp. z o , Kraków 2007.

Drozd A., *Ustawa o ochronie danych osobowych (komentarz, wzory pism, przepisy)*, Wyd. LexisNexis, Warszawa 2008.

Litwiński P., *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*. Oficyna a Wolters Kluwer Polska Sp. z o.o., Warszawa 2009.

Kaszubski R. W., D. Romańczuk (red.), Księga dobrych praktyk w zakresie zarządzania ciągłością działania (Business Continuity Management), Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa 2011.

Drozd A., Zabezpieczenie danych osobowych. Wyd. Presscom 2008.

ABC ochrony danych osobowych, Biuro Generalnego Inspektora Ochrony Danych Osobowych, Wydawnictwo Sejmowe, Warszawa 2007.

Dyrektywa Parlamentu Europejskiego i Rady 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dziennik Urzędowy Wspólnot Europejskich, Dz.U. L 281z 23.11.1995.

Ustawa z dnia 11 września 2003r. o służbie wojskowej żołnierzy zawodowych (Dz.U. z 2010 r. nr 90, poz. 593 z późniejszymi zmianami).

Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. z 1997 r. nr 133, poz. 883 z późniejszymi zmianami).

Ustawa z dnia 05 sierpnia 2010r. o ochronie informacji niejawnych (Dz.U. 2010 r., nr 182, poz. 1228).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r., nr 100, poz. 1024).

Kodeks Cywilny (Dz.U. 1974 nr 24, poz. 141 z późniejszymi zmianami).

Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. z 2008 r. nr 229, poz. 1536).

Strony internetowe

http://www.giodo.gov.pl/1520012/id_art/2928/j/pl/
http://pl.wikipedia.org/wiki/Dane_wrażliwe