mgr Marcin Raczykiewicz
Menedżerska Akademia Nauk Stosowanych w Warszawie
ORCID: 0009-0009-0078-5884

https://doi.org/10.29316/9788368103243_14

OCHRONA DANYCH OSOBOWYCH SKŁADNIKIEM SYSTEMU *COMPLIANCE*

PERSONAL DATA PROTECTION AS A COMPONENT OF THE *COMPLIANCE* SYSTEM

Streszczenie

Biorąc za nadrzędne wartości związane z zapewnieniem bezpieczeństwa danych osobowych jako naturalnej, ludzkiej tajemnicy, na łamach rozdziału przybliżone zostaną elementy systemu *compliance* jako struktury, której wdrożenie powinno uniemożliwiać wystąpienie wszelkich nieprawidłowości, np. wycieku tajemnicy w przedsiębiorstwie. Celem rozważań jest określenie znaczenia ochrony danych osobowych dla funkcjonowania organizacji w ramach systemu *compliance.* Chcąc połączyć ochronę danych osobowych, będącą wiodącym tematem opracowania, na potrzeby ww. zagadnień skonstruowano szczegółowy problem badawczy, a mianowicie pytanie: kiedy informacje zawierające dane osobowe stają się tajemnicą przedsiębiorstwa i czy wtedy nadal są należycie chronione? Wyselekcjonowana literatura przedmiotu związana z danymi osobowymi oraz zagadnieniami z obszaru *compliance*, pozwoli również potwierdzić lub zaprzeczyć tezie, iż sprawny system *compliance* umożliwia efektywne zarządzenie informacją, jako strategicznym zasobem w niejednym przedsiębiorstwie.

Słowa kluczowe: tajemnica, bezpieczeństwo, zagrożenia, informacja, dane osobowe, system

Abstract

Taking as paramount values the assurance of personal data security as a natural human secret, this chapter presents the elements of the *compliance* system as a structure whose implementation should prevent any irregularities, such as the leakage of confidential

information within an enterprise. The purpose of the discussion is to determine the significance of personal data protection for the functioning of organizations within the *compliance* framework. To link personal data protection, which constitutes the leading theme of this study, with the above issues, a detailed research problem has been formulated, namely the following question: when do pieces of information containing personal data become a trade secret, and are they still adequately protected at that point? The selected literature on personal data as well as on *compliance* issues allows for either confirming or refuting the thesis that an efficient *compliance* system enables effective management of information as a strategic resource in many enterprises.

Keywords: secrecy, security, threats, information, personal data, system

Wstęp

Trudno wyobrazić sobie życie we współczesnym świecie bez obecności tajemnicy. Pomimo wszelkiej, możliwej transparentności, jaką uprawia się na łamach np. mediów społecznościowych w miejscach pracy, czy innych sferach życia społecznego, w których ludzie chcą być zauważeni. Jest ona szczególną wartością charakteryzującą człowieka mądrego, odpowiedzialnego i godnego zaufania – tajemnica. Towarzyszy człowiekowi od bardzo dawna, przez wielu pielęgnowana, trzymana w ukryciu, aż do śmierci, to przez drugich nie szanowana zmieniała właścicieli tracąc na swojej wartości. „Mądrość Sarycha", choć bardzo stara to raczej ponadczasowa, zawiera swoistą wskazówkę, „że tego kto dochowuje tajemnicy, trzeba kochać jak siebie samego. Bo ranę można obwiązać i po obeldze można się pojednać, ale kto zdradził tajemnicę, nadziei już mieć nie może"[1]. Informacja, tajemnica, dane osobowe, system *compliance* zdawałoby się wszystkie te słowa osobno stanowią odmienne obszary analiz, lecz gdy przyjrzeć się im bliżej to widać nierozerwalną, łączącą ich wzajemną wieź, która jednocześnie stanowi o ich indywidualnej sile i wartości. Biorąc za nadrzędne wartości związane z zapewnieniem bezpieczeństwa danych osobowych jako naturalnej, ludzkiej tajemnicy, na łamach rozdziału przybliżone zostaną elementy systemu *compliance* jako struktury, której wdrożenie powinno

[1] Ł. Roman, G. Winogrodzki, *Służby specjalne w systemie bezpieczeństwa państwa*, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide de Gasperi w Józefowie, Józefów 2016, s. 28.

uniemożliwiać wystąpienie wszelkich nieprawidłowości np. wycieku tajemnicy w przedsiębiorstwie. Chcąc połączyć ochronę danych osobowych, będącą wiodącym tematem opracowania, na potrzeby ww. zagadnień skonstruowano szczegółowy problem badawczy, a mianowicie pytanie: Kiedy informacje zawierające dane osobowe stają się tajemnicą przedsiębiorstwa i czy wtedy nadal są należycie chronione? Wyselekcjonowana literatura przedmiotu związana z danymi osobowymi oraz zagadnieniami z obszaru *compliance*, pozwoli również potwierdzić lub zaprzeczyć tezie**,** iż sprawny system *compliance* umożliwia efektywnie zarządzać informacją, jako strategicznym zasobem w niejednym przedsiębiorstwie.

Tajemnica informacji i *compliance*

Zasób informacyjny jest to element strategiczny. W chwili, gdy jest to wartość gospodarcza, tzn. przeliczalna, o charakterze poufnym, w stosunku do której przedsiębiorca podjął niezbędne działania, aby ją chronić, można mówić o niej jako o tajemnicy przedsiębiorstwa[2]. Tajemnica przedsiębiorstwa to poufny przepis, recepta sukcesu, stanowiąca o dystansie i przewadze przed konkurencją. Mówi o tym art. 11 Ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji, który brzmi: „przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności”[3].

Każda firma czy przedsiębiorstwo może mieć swoje własne tajemnice, lecz nie każda je ma. Wszelkie informacje takie jak: dane i projekty technologiczne, stanowiące o efektywnej polityce rynkowej przedsiębiorstwa, systemy i programy usprawniające linie produkcyjne, a także w wielu przypadkach te

[2] *Tajemnica przedsiębiorstwa. Definicja ustawowa i praktyczne znaczenie – Tajemnica Przedsiębiorstwa*, portal tajemnica-przedsiebiorstwa.pl, https://tajemnica-przedsiebiorstwa.pl/tajemnica-przedsiebiorstwa, [dostęp: 16.05.2025].

[3] *Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji*, portal https://sip.lex.pl Dz.U.2004.90.864/2, [dostęp: 25.02.2024].

informacje, które w swojej treści zawierają, np. dane osobowe – mogące zidentyfikować rzeszę inżynierów, projektantów czy programistów jako „ojców" niejednego sukcesu i tym samym zysku w przedsiębiorstwie, mogą stanowić same w sobie tajemnice. Jest jeszcze jeden, kluczowy element, aby treść informacji stanowiła o ich tajemnicy. Mianowicie wartość gospodarcza. Nie jest możliwe objęcie tajemnicą przedsiębiorstwa danych i informacji, które nie mają żadnej wartości gospodarczej, nawet w sytuacji, gdy są poufne, a przedsiębiorca działa w celu zachowania ich poufności. Poniżej kilka przykładów, kiedy informacja posiada wartość gospodarczą[4]:

- kiedy jej wykorzystanie przez innego przedsiębiorcę może zaoszczędzić mu wydatków lub zwiększy zysk oraz pozwoli pozyskać nowych klientów,
- w sytuacji, kiedy jej bezprawne pozyskanie, wykorzystanie lub ujawnienie może spowodować szkody dla interesów osoby, która zgodnie z prawem sprawuje nad nimi kontrolę, szkodząc jej naukowemu lub technicznemu potencjałowi, interesom gospodarczym lub finansowym, pozycji strategicznej lub zdolności do konkurowania.

Zatem warunkiem uznania za tajemnicę przedsiębiorca jest to, aby sam przedsiębiorca podjął wobec tych informacji działania mające na celu utrzymanie ich w poufności przy zachowaniu należytej staranności[5]. Te informacje, stanowiące tajemnice w przedsiębiorstwie uznawane są za równie wartościowe jak patenty i inne rodzaje praw własności intelektualnej. Wykorzystywana poufność informacji stała się narzędziem zarządzania konkurencyjnością przedsiębiorstw i planowanie innowacji w działalności badawczej w przedsiębiorstwach. Stały się wyznacznikiem wykraczającym poza wiedzę techniczną i dane handlowe[6]. Jednym słowem przedsiębiorca musi działać na różnych

[4] *Tajemnica przedsiębiorstwa. Definicja ustawowa i praktyczne znaczenie – Tajemnica Przedsiębiorstwa, portal tajemnica-przedsiebiorstwa.pl*, https://tajemnica-przedsiebiorstwa.pl/tajemnica-przedsiebiorstwa, [dostęp: 16.05.2025].

[5] *Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji* (Dz. U. z 1993 r. Nr 47, poz. 211).

[6] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem*, portal eur-lex.europa.eu, https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX:32016L0943, [dostęp: 16.05.2023].

kierunkach. Musi on działać rozsądnie w danych okolicznościach, zmierzając do eliminacji pośredniego lub bezpośredniego dotarcia do informacji przez osoby z zewnątrz przedsiębiorstwa, bez podjęcia przez nich szczególnych czynności. Uwzględnić tu należy elementy takie jak: rodzaj informacji, wielkość przedsiębiorstwa, liczba osób, sposób rejestrowania informacji, itp. Tu prawo do końca nie precyzuje i nie wskazuje o jaki katalog działań chodzi. Wybór i strategia działania, dotyczące klasyfikacji użytych środków bezpieczeństwa należą tylko do przedsiębiorcy. Jest wiele rozwiązań czysto praktycznych, których użycie przez przedsiębiorcę pozwoli na ochronę zarządzanego przez niego koncernu. Jednym z nich, które na łamach rozdziału zasadnym jest wskazać jest system „comoplayans", jako nowoczesny model organizacji przedsiębiorstwa.

Pojęcie *compliance* wywodzi się z medycyny i w rozumieniu tej definicji oznacza „stosowania się pacjenta w procesie terapii do zaleceń lekarza"[7]. Dla wyobrażenia sobie czym jest *compliance* na potrzeby zdefiniowania owego zagadnienia posłużyć się należy opisem, które na łamach „Compliance w przedsiębiorstwie" zawarł B. Makowicz, a mianowicie: „jest on całokształtem środków zmierzających do zapewnienia przestrzegania prawnych nakazów i niewykraczania poza ustawowe zakazy przez przedsiębiorstwa, członków organów oraz pracowników"[8]. To taka organizacja przedsiębiorstwa wymagająca stworzenie struktur i stosowania środków, które zredukują do minimum ryzyko wystąpienia w przedsiębiorstwie wszelkich nieprawidłowości, które mogłyby powstać wskutek działania osób lub partnerów handlowych, wiążących się ze złamaniem regulacji prawnych, zasad prawa lub tych innych, istotnych, wewnętrznych, przyjętych przez przedsiębiorstwo reguł. To również działanie sprzeczne z przyjętymi ogólnie zasadami i standardami etycznymi[9]. Wyznacznikiem efektywnego *compliance*, będzie zatem wyznaczony przez przedsiębiorcę cel. W ramach próby usystematyzowania celów jest ich podział na nadrzędne i podrzędne. Warto jest zaznaczyć, że realizacja drobnych celów podrzędnych w efekcie zbliża przedsiębiorstwo do realizacji celu nadrzędnego. Cel nadrzędny systemu *compliance* jest generalnie prosty, a mianowicie

[7] W. Chomiczewski, *Systemy zarządzania zgodnością: compliance w praktyce*, Wolters Kluwer, Warszawa 2020, s. 25.

[8] B. Makowicz, *Compliance w przedsiębiorstwie*, Wolters Kluwer Polska, Warszawa 2011, s. 16.

[9] Tamże, s. 17.

zapobiegać niepowodzeniom. To jest realne wtedy, kiedy realizuje się podstawowe trzy podrzędne cele, a więc[10]:

- zapobieganie prawnemu ryzyku, które może zrealizować się w postaci sankcji i szkody dla reputacji przedsiębiorstwa,
- stworzenie transparentnych struktur w przedsiębiorstwie poprzez zapewnienie efektywnej komunikacji organów zarządzających, udziałowców i kadry pracowniczej,
- okresowa, efektywna kontrola i obserwacja przedsiębiorstwa w obszarach w sferach bezpiecznych z powiązanym dokumentowaniem tych procesów.

Dla lepszego zrozumienia celów *compliance* oraz pojęcia materii tego systemu posłuży poniższa ilustracja (rysunek 1), jako zestawienie scenariuszy dobrego i złego przedsiębiorstwa oraz zmian, jakie może wprowadzić w systemowym ujęciu *compliance*.



Rysunek 1. Dobre i złe przedsiębiorstwo w systemie *compliance*

Źródło: B. Makowicz, *Compliance w przedsiębiorstwie*, Wolters Kluwer Polska, Warszawa 2011, s. 19.

[10] Tamże, s. 19.

Cel realizują ludzie, czyli w przypadku tego systemu zakres personalny. Powinien on obejmować wszystkich przynależnych do danego przedsiębiorstwa, głównie pracowników, ale także sztab kierowniczy każdego szczebla, dyrekcję, członków zarządu – słowem wszystkich mogących wpływać swoim działaniem na kondycję przedsiębiorstwa. Działanie tych osób kojarzone jest z przedsiębiorstwem i musi zostać objęte systemem *compliance*[11]. Równie daleko jak zakres personalny sięga zakres materialny definicji *compliance* – słowem wszelkie nieprawidłowości. To zatem wszystkie działania, które swoim zakresem mogą rozpocząć działanie maszyny przyczynowo skutkowej np.: naruszenie wszelkich, obowiązujących regulacji prawnych (lokalne, państwowe, międzynarodowe), przyjęcie innych regulacji prawnych – wewnętrznych, wiążących dla osób tylko w danym przedsiębiorstwie oraz naruszenie zasad ogólnie przyjętych jako standardów etycznych. Te ostatnie choć nie zawsze sankcjonowane prawnie, mogą doprowadzić do identycznych konsekwencji, jak popełnianie przestępstw w obszarze np. bezpieczeństwa informacji przez poszczególnych pracowników[12]. Efektywne zarządzanie informacją za pośrednictwem sprawnie wdrożonego systemu *compliance* ma jeszcze kilka zalet. Są nimi funkcje jakie proponuje sam system, jest ich wiele, ale kluczowe dla utrzymania należytych standardów w przedsiębiorstwie to: funkcja prewencyjna sprawia, że system ten jest swoistym strażnikiem bezpieczeństwa, gdzie większość zagrożeń jest identyfikowana i rozpoznawana w zarodku. Funkcja ochronna to taka, która w postaci powłoki ochronnej uniemożliwi próby podjęcia działań negatywnych wewnątrz przedsiębiorstwa, lecz również udaremni te ofensywne działania skierowane w bezpieczeństwo przedsiębiorstwa z zewnątrz. Według wielu ekspertów najważniejsza funkcja obserwacyjna, bo tylko stała obserwacja i monitoring nie tylko miejsc i procesów newralgicznych w przedsiębiorstwie, lecz także tych bezpiecznych, które uchodzą za podwaliny stabilności systemu. W wielu przypadkach to właśnie te miejsca są rzadko kontrolowane i tam właśnie pojawia się idealne środowisko wewnątrz przedsiębiorstwa, w którym pojawiają się konkretne nieprawidłowości[13].

Nie od dziś wiadomo, iż potrzeba zmian jest obowiązkiem, z rygorem jego kontroli, który wprowadzony i uprawomocniony będzie efektywny. Biorąc pod

[11] Tamże, s. 17.

[12] Tamże, s. 18.

[13] Tamże, s. 26.

uwagę członkostwo Polski w Unii Europejskiej, tajemnica przedsiębiorstwa jest różnie postrzegana. Różnice między państwami członkowskimi pod względem ochrony prawnej tajemnic przedsiębiorstwa oznaczają, że tajemnice te nie są objęte należytą ochroną w całej Unii Europejskiej. Prowadzi to do rozłamu rynku wewnętrznego w dziedzinie tego typu obostrzeń, a co za tym idzie nie odstrasza należycie jak powinno. Stwarza to duże ryzyko dla przedsiębiorstw w państwach członkowskich charakteryzujących się niższym poziomem ochrony, ze względu na możliwości łatwiejszej kradzieży tajemnic przedsiębiorstw, danych osobowych kadry pracowników i informacji technologicznych lub ich pozyskania w sposób nielegalny[14].

Dobrze zaprojektowany i wdrożony system *compliance* będzie bardzo dobrą inwestycją dla każdego przedsiębiorstwa. To przyszłe budowanie dobrego wizerunku firmy, na fundamentach bezpiecznej informacji i kanałów komunikacji. Budowany rozsądnie i rzetelnie na gruncie prawnym i etycznym, powodując zazdrość i podziw u konkurencji z jednoczesnym poczuciem niedostępności każdego ze swoich elementów.

Bezpieczeństwo danych osobowych jako obszar informacji niejawnych

Przedstawione na wielu płaszczyznach zagadnienia, dotyczące zapewnienia bezpieczeństwa informacji, tych związanych z zachowaniem prywatności np. danych osobowych oraz tych, bezpośrednio związanych z bezpieczeństwem państwa, można zaklasyfikować i rozpatrywać w wielu obszarach. Ochrona aktywów informacyjnych w systemie bezpieczeństwa państwa nie jest niczym nowym. Zasadnicze działania w kwestii prawnych i technicznych aspektów tej ochrony podejmowane były i są na szczeblu najwyższych władz państwa. Informacja stanowi niewyczerpalny zasób o zróżnicowanym charakterze i postaci. Powielana i przenoszona z miejsca na miejsce, w czasie i przestrzeni, przetwarzana zaś nie nosi oznak zniszczenia lub zużycia. Przy rozpatrywaniu większej ilości informacji osiąga się lepszy efekt, aniżeli analiza pojedynczych treści. Naturalnym jest w takim razie gromadzenie informacji w zbiory, bazy

[14] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem*, portal eur-lex.europa.eu, https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX:32016L0943, [dostęp: 16.05.2023].

i katalogowanie jej oraz archiwizacja[15]. Wiadomym jest, że dla wielu ta sama informacja posiada wielorakie znaczenie. Uzależniona jest od wielu kontekstów, czyli słów, które ja poprzedzają czy następują po niej. Posiada ona również jak każdy zasób pewne cechy, które pozwalają na jej ewentualne wykorzystanie. Tu warto przytoczyć min. aktualność, powiazanie z czasem przyszłym bez jednoczesnej utraty aktualności, to czy jest zrozumiała dla odbiorcy, operatywna, jej dokładność czy co w wielu przypadkach najważniejsze jej wiarygodność[16]. Jet ona ogromną bronią i dlatego rola informacji w funkcjonowaniu człowieka i zbiorowości sprawiają, że wszelkie procesy informacyjne z jej udziałem winny być szczególnie nadzorowane i chronione. Wiąże się to nie tylko z samą „jakością" informacji, lecz w większej tego części na zorganizowaniu całego zaplecza, środowiska, w którym będzie ona przechowywana, przetwarzana i za pośrednictwem, którego przekazywana jako np. niejawny element procesu decyzyjnego.

Jednym z wielu obszarów aktywności państwa w dziedzinie szerokorozumianego bezpieczeństwa zewnętrznego i wewnętrznego oraz jego obywateli jest wszelka regulacja spraw związanych z ochroną informacji niejawnych[17]. W związku z tym, dziś, kiedy rozwój nowoczesnych technologii i techniki przekazu powoduje, że pojawiają się coraz to nowsze zagrożenia, zagadnienia związane z ochroną i bezpieczeństwem danych w tym informacji niejawnych są szczególnie ważne[18]. Prawidłowa i skuteczna ich ochrona wytyczona jest za pośrednictwem przepisów prawnych rangi krajowej i międzynarodowej, np. Ustawy z dnia 14 grudnia 2018 roku o ochronie danych osobowych oraz Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 27 kwietnia 2016 roku. Rodzi się pytanie, co w przypadku, gdy dane osobowe, biorąc za kluczowe ich klasyfikację, staną się jednym z zasobów systemu niejawnego – informacją niejawną? Bazując na Ustawie z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych ustawodawca uwypukla jednoznacznie powyższą kwestię w art. 1 pkt. 4 i 5, a mianowicie: „do danych osobowych stanowiących

[15] D. Krzewiak, *Nadzór i kontrola Internetu jako instrument polityki bezpieczeństwa informacyjnego współczesnych państw*, De Securitate Et Defensione. O Bezpieczeństwie i Obronności, t. 7, nr 1, 2021, s. 192.

[16] Tamże, s. 193.

[17] J. Depo, S. Mazur, *Administracja bezpieczeństwa, informacji niejawnych i danych osobowych: vademecum*, Oficyna Wydawnicza AFM, Kraków 2015, s. 13.

[18] Tamże, s. 13.

informacje niejawne nie stosuje się przepisów o ochronie danych osobowych", jak również dalej „do danych osobowych stanowiących informacje niejawne stosuje się przepisy niniejszej ustawy"[19]. Zatem jednym z najważniejszych procesów, który umożliwia zastosowanie tych regulacji jest klasyfikacja informacji i w wyniku tego nadanie jej charakteru niejawnego. Proces klasyfikacji, to bardzo odpowiedzialna rzecz, uprawniona osoba, która z tytułu właściwości jest upoważniona do podpisania dokumentu, nadaje mu odpowiednią klauzulę. Informacje są chronione jako zasoby niejawne w momencie ich zaklasyfikowania przez uprawniona osobę. Dokonuje ona oceny klasyfikowanej informacji, biorąc za podstawę szkody, jakie po ujawnieniu ww. informacji wyrządziłyby interesowi Rzeczypospolitej Polskiej lub jednostce organizacyjnej w jakiej została wytworzona. Pozostaje jeszcze ocena ryzyka wyrządzenia szkód po ujawnieniu informacji. Samo zdefiniowanie zasobów i interesów wymagających ochrony z jednoczesną ich oceną, wiąże się z przyjętym przez państwo systemem aksjonormatywnym. Ochrona informacji niejawnych jest swoistą pochodną interesów państwa w sferze jego bezpieczeństwa i wiąże się z przyjętą strategią, zawartymi umowami międzynarodowymi, które wzmacniają zewnętrzne relacje w wyniku pojawienia się zagrożeń min. informacyjnych[20]. Dane osobowe zgodnie z obowiązującymi, przytoczonymi powyżej przepisami nie mogą pozostawać do względu ogólnego. Nie jest to jednoznaczne z tym, że obligatoryjnie stają się informacjami niejawnymi. Jest jednak kilka odstępstw od powyższego i w przypadku, kiedy chodzi o dane mogące zidentyfikować kluczowe i strategiczne osoby w państwie w takiej sytuacji informacje te mogą otrzymać klauzule tajności i wtedy stać się informacją niejawną. Informacje niejawne i dane osobowe podlegają szczególnej ochronie, lecz w takim przypadku właściwość ochrony danych osobowych będących zasobem niejawnym pozostaje we właściwości Ustawy o Ochronie Informacji Niejawnych.

Sprawnie wdrożony i efektywnie działający, w dużym stopniu przyczyni się do zapewnienia ochrony zasobów niejawnych w niejednej jednostce organizacyjnej. Jest on już późniejszym etapem tej ochrony, gdyż ochrona sama w sobie zaczyna się w momencie jej planowania. To świadomość, że wiele czynników oraz elementów, będą miały kluczowy wpływ na zapewnienie ochrony

[19] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz. U. z 2023 r. poz. 756).

[20] R. Zapart, *Teoria i praktyka ochrony informacji niejawnych – wybrane zagadnienia dotyczące bezpieczeństwa informacji*, Polityka i Społeczeństwo, t. 18, nr 3, 2020, s. 113.

ww. informacji w przyszłości. Rozpoczęcie planowania działań i procedur należałoby zacząć od poszczególnych elementów systemu ochrony informacji niejawnych, które obejmują: bezpieczeństwo osobowe, bezpieczeństwo przemysłowe, bezpieczeństwo fizyczne bezpieczeństwo teleinformatyczne. Podkreślić należy, iż najważniejszym elementem systemu ochrony informacji niejawnych jest bezpieczeństwo osobowe, dlatego, że dotyczy ono osób odpowiadających za cały proces ochrony informacji oraz dotyczy osób posiadających dostęp do klauzulowanych zasobów[21]. Zgodnie z ustawą z dnia 5 sierpnia 2010 roku za ochronę informacji niejawnych oraz za stworzenie pionu ochrony odpowiada Kierownik jednostki organizacyjnej, a powołany przez niego Pełnomocnik ds. Ochrony Informacji Niejawnych odpowiedzialny jest za przestrzeganie przepisów o ochronie informacji niejawnych. Bezpieczeństwo osobowe samo w sobie nie jest do końca zdefiniowane, bazując na literaturze przedmiotu przyjmuje się, że jest to szereg przedsięwzięć organizacyjnych, ustaleniowo-sprawdzeniowych, które zmierzają do dopuszczenia do zasobów niejawnych tylko osoby dające gwarancję rękojmi zachowania tajemnicy[22].

Posiadane informacje i dane, kiedy już się stają niejawne mogą być przetwarzane tylko za pośrednictwem systemów teleinformatycznych. Chcąc odpowiednio zabezpieczyć niejawne systemy teleinformatyczne, zasadnym i koniecznym jest wprowadzenie i przestrzeganie procedur związanych z uzyskaniem świadectw akredytacji, wydawanych przez ABW i SKW jako odpowiedzialnych w tej materii służb specjalnych. To szereg wymogów, zawierających szczegółowe wytyczne, po zrealizowaniu których będą one zatwierdzone, a systemy dopuszczone do eksploatacji. Tu wartym uwagi jest art. 8 cytowanej ustawy a mianowicie[23]:

- mogą być udostępniane wyłącznie osobom uprawnionym, że zgoda z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności,
- przetwarzanie możliwe w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych,

[21] A. Lasota-Jądrzak, *Planowanie ochrony informacji niejawnych w jednostce organizacyjnej*, Związek Przedsiębiorców i Pracodawców Wielkopolska, Poznań 2018, s. 1.

[22] Tamże.

[23] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz. U. z 2023 r. poz. 756, art. 8).

obiegu materiałów i środków bezpieczeństwa fizycznego odpowiednich do danych klauzul,
– muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w nn. Ustawie i innych przepisach wykonawczych, które wydane zostały na jej podstawie.

Zachowanie tajemnicy przez kierownictwo jak i przez szeregowy personel jest możliwe dzięki prawidłowo zaplanowanemu, zaprojektowanemu i zarządzającemu systemowi bezpieczeństwa. Powyższe zagadnienia wskazują bezpieczną drogę ku bezpieczeństwu informacji. Informacja, jej klasyfikacja, decyzje oraz cały, sprawnie działający pion ochrony nie stanowią jednak o tym, że czynnik ludzki zostaje całkowicie wyeliminowany. Nie jest do końca istotnym jakie informacje są chronione, istotny zaś jest jeden, najważniejszy szczegół. Ludzie wytwarzają, rozpowszechniają i zarazem chronią zasoby informacyjne z jednoczesnym wydobywaniem najważniejszych tajemnic na światło dzienne. Potrzeba ciągłego budowania świadomości ludzkiej, powielania zagadnień związanych z pojmowaniem danych osobowych i informacji niejawnych jako strategicznych zasobów spowoduje, że będą one pieczołowicie i należycie zabezpieczone.

Kodeks etyki wyznacznikiem bezpieczeństwa informacji

Japońscy samurajowie i ich kodeks należą już do historii i często kojarzą się tylko z filmami Kurosawy czy serialem Shogun, niemniej jednak warto poświecić im kilka wersów. Kodeks Bushido jako unikat nigdy nie został spisany, stając się w epoce Edo podstawą etyki i osądu moralnego, a nawet w pewnym sensie swoistym prawem[24]. Kodeks sam w sobie był tworem określonego miejsca, ludzi i czasu. Jego idee odnoszące się do konkretnej klasy społecznej – wojowników, okazały się na tyle uniwersalne, że wykroczyły poza te warstwę, jak również epokę Edo. Można powiedzieć, że przekroczył realne granice Japonii, stając się nie tylko ciekawostką naukową, ale również podręcznikiem etyki, którego studiowanie mogło przybliżyć w pewnym stopniu do innego spojrzenia na moralność, skłaniając wielu do poznania własnej etyki i moralności[25]. Jego domeną było zdobywanie doświadczenia, rozwijał siłę, samokontrolę czy

[24] D. Barańska, *Kodeks samurajski Bushido a normy moralne i etyka społeczna*, Krakowskie Studia Miedzynarodowe, t. 3, nr 1, 2006, s. 9.

[25] Tamże, s. 9.

inne cnoty. Podstawą treści kodeksu było: podejmowanie własnych decyzji, bazując na zasadach religijnych i moralnych, dzielność oraz heroizm, współczucie i życzliwość wobec wszystkich ludzi, uprzejmość i właściwe zachowanie, prawdomówność i szczerość, honor i chwała czy w wielu przypadkach najważniejsze poświęcenie, czy lojalność. Na próżno dziś wypatrywać w kuluarach obiektów administracji publicznej, spółkach skarbu państwa czy przedsiębiorstwach uzbrojonych w miecze, postępujących zgodnie z kodeksem japońskich wojowników. Choć pewnie byliby znakomitymi stróżami wszystkich procesów, związanych z szerokorozumianym bezpieczeństwem informacji, jednak nie są to ich czasy.

Wszechobecne zmiany w otoczeniu międzynarodowym mają bezpośredni wpływ na kształtowanie się polityki dotyczącej bezpieczeństwa informacji. Prawdziwy sens zarządzania takim bezpieczeństwem wiąże się z ustaleniem pewnej hierarchii wartości oraz jej wdrożeniem w codzienne działanie. To odpowiedzialność społeczna, zawodowa rodzi w sercach i umysłach ludzi pewną wrażliwość na porządek ludzi, którzy zdają sobie sprawę z faktycznych potrzeb tych społecznych, czy tych, które winni byli wykonywać dla np. organizacji. To wzmacnia ich zaangażowanie w plan, projekt i cel przedsięwzięcia[26]. Zatem wprowadzenie kodeksu etyki w przedsiębiorstwie może w dużym stopniu usprawnić jego działanie. Zasadnicza kwestia, to dawanie przykładu „idącego góry". Przede wszystkim członkowie zarządu oraz osoby na stanowiskach kierowniczych powinni swoim zachowaniem utożsamiać się z przyjętymi zasadami etycznymi oraz odpowiednimi standardami w tym zakresie. Jeśli próba wprowadzenia kodeksu i reguł etyki na tym poziomie okaże się nie skuteczna, to trudno ją będzie kontynuować na niższych poziomach[27]. Wprowadzone reguły etyczne i odpowiednie standardy moralne powinny uwzględniać katalog zachowań w danym środowisku zawodowym. Pracownik administracji publicznej, czy referent w przedsiębiorstwie powinien być świadomy, kiedy i komu może udostępnić informację, w jakich okolicznościach ma obowiązek odmówić przekazania np. zasobu informacyjnego oraz, że spoczywająca na nim odpowiedzialność zgłaszania incydentów, co pozwala w przyszłości na zwiększenie poziomu bezpieczeństwa informacji. Podobnie jak z przedstawia-

[26] E. Jedrych, M. Sidor-Rządkowska, *Kodeksy etyczne instrumentem good government w organizacjach*, Zeszyty Naukowe Uczelni Vistula, t. 4, nr 55, 2017, s. 73.

[27] B. Makowicz, *Compliance w przedsiębiorstwie*, dz. cyt., s. 145.

nym powyżej systemem *compliance*, kiedy jego budowa opiera się o konkretne wartości społeczne, zostaje dostrzeżona i wdrożona na każdym poziomie bezpieczeństwa[28]. Zapewnienie bezpieczeństwa informacji to nie tylko obowiązek pracowników w przedsiębiorstwach sektora cywilnego, lecz także jest to priorytet w strukturach administracji publicznej. Ciągły transfer informacyjny w urzędach administracji publicznej, powinien wymuszać na zatrudnionej kadrze stosowanie się do etyki zawodowej. Etyka w administracji publicznej ma za zadanie wzmocnienie gwarancji wykonywanych przez pracowników urzędów zadań w sposób poprawny. Jakość pracy administracji zależy w dużej mierze od jej sprawności, pragmatyki, wyposażenia, planowania i od stanu przestrzegania prawa. Kluczowa jest jakość kadry służby publicznej, czyli: kultury pracy, kompetencji, umiejętności, walorów moralnych i odpowiedzialności za decyzje[29]. W przypadku tej profesji urzędniczej podstawa etyki to zasady, odnoszące się do podmiotowo-osobowościowych atrybutów przedstawicieli tego zawodu, a mianowicie[30]:

- zasada odpowiedzialności – gotowość poniesienia odpowiedzialności za swoje decyzje i działanie,
- zasada profesjonalizmu – zwana również zasada kompetencji, wyraża się poprzez pogłębianie wiedzy i chęci wysiłku intelektualnego,
- zasada poufności – zachowanie tajemnicy państwowej, czyli urzędowej, służbowej, wojskowej jako słuszność zachowania konfidencji niektórych informacji,
- zasada służby publicznej (interesu publicznego) – lojalność, polegająca na przekładaniu dobra publicznego czy interesu społecznego na własne profity,
- unikanie konfliktu interesu – urzędnik wycofuje się ze sprawy w momencie wystąpienia dla niego jakiś sprzyjających okoliczności,
- zasada bezstronności i jawności – zakaz podejmowania prac kolidujących z pracą urzędnika.

[28] Tamże, s. 146.

[29] L. Kowalczyk, F. Mroczko, *Kreatywność i innowacyjność w zarządzaniu i pedagogice w erze cyfrowej, Zarządzanie operacyjne w teorii i praktyce organizacji biznesowych, publicznych i pozarządowych*, Wydawnictwo Wyższej Szkoły Zarządzania i Przedsiębiorczości z siedzibą w Wałbrzychu, t. 48, nr 2, 2019, s. 264.

[30] Tamże, s. 266.

To zatem odpowiedzialność wielopoziomowa, a kodeks jest drogowskazem w sytuacjach trudnych. Chęć stworzenia struktur uczciwej działalności, a nie na granicy prawa lub wyboru między dobrem czy złem, powinna być naturalną tego przyczyną.

Przekładając powyższe na obszar bezpieczeństwa informacji, podkreślić wypada, iż większość problemów związanych z administrowaniem informacją daje się rozstrzygnąć od strony moralnej. Zadbać należy, aby wszyscy zatrudnieni, zaangażowani w proces przetwarzania informacji poznali te rozwiązania, zamiast nieustannie rozważali „za" czy „przeciw"[31].

Kodeksy etyki wzbudzają wiele kontrowersji, mając swoich zwolenników i przeciwników. Czasami ciężko sobie wyobrazić funkcjonariusza publicznego, któremu jest potrzeba zaimplementowania kodeksu etyki. W wielu przypadkach zatrudnienia sam status powinien spowodować podejście godne wszelkim normom i zasadom. Kodeks jest narzędziem wprowadzenia i sformalizowania określonych zasad etycznych, które powinny przyświecać każdemu pracownikowi i kierować jego postepowaniem. Szefowie czy pracownicy codziennie stają przed szeregiem dylematów, a kodeksy powinny pomagać rozwiązać niektóre z nich, dać podpowiedź jak postąpić w konkretnej sytuacji i dokonać najbardziej etycznych wyborów[32].

Podsumowanie

Wprowadzenie systemu *compliance* wiąże się jednoznacznie ze stosowaniem określonych rozwiązań. Główny obszar, w których system ten z zasady działa najsprawniej to przeciwdziałanie zagrożeniom skierowanym w politykę bezpieczeństwa informacji również tych poufnych, ochrona wszelkich danych w tym danym osobowych, oraz nadzór nad wszelką zgodnością. W dzisiejszych czasach pojawienie się ryzyka wymaga sprawnego zarzadzania nim, dlatego *compliance* dostawać należy do osobowości i konkretnego modelu przedsiębiorstwa czy instytucji. Rozpatrując plany wdrożenia efektywnego systemu *compliance* zasadnym jest poświęcić czas i skupić się już na etapie procentowania tej polityki bezpieczeństwa, na bardzo ważnej roli zarządu czy kierownictwa np. przedsiębiorstwa. Budowa takiego autorytetu jakim jest rzetelne podejście do polityki *compliance* przez zespół nadzorcujący, będzie procentować

[31] E. Jedrych, M. Sidor-Rządkowska, *Kodeksy etyczne instrumentem...*, dz. cyt.., s. 79.

[32] Tamże.

w przyszłości i stanowić o sile tej, co by nie mówić, jeszcze nowej inicjatywy i idei. To szczególnie ważne, bo wiadomym jest, że postawa pracownika firmy czy instytucji, który nie stosuje się do zasad kodeksu etycznego, czy obce mu są obowiązujące wartości w dużej mierze uzależniona jest z tym jak jego przełożony postrzega te same wartości i jak egzekwuje wprowadzone w firmie przepisy od podległej jemu kadry.

Dokonując powyższych rozważań, tych związanych bezpośrednio z bezpieczeństwem informacji i tych poruszających obszar danych poufnych oraz tajemnic w przedsiębiorstwie, jak i tych z dziedziny systemu *compliance* jednoznacznie można odpowiedzieć, iż wszelkie informacje, które noszą znamiona danych osobowych, kiedy stają się tajemnicą przedsiębiorstwa podlegają bardziej poważnym jurysdykcjom. Możliwe jest to z prostego powodu, a mianowicie z mocy definicji zachowania tajemnicy, jak również co naturalne jako skuteczna metoda przeciwdziałania zagrożeniom, skierowanym w bezpieczeństwo informacyjne przedsiębiorstwa, jego kondycję gospodarczą czy potencjał osobowy. Jak przedstawiono w prowadzonych rozważaniach, wdrożony system *compliance* jest skuteczną możliwością zapanowania nad poprawnym stosowaniem przepisów i efektywnym „korzystaniu" przez kadrę z informacji w przedsiębiorstwie, czy innej placówce publicznej, potwierdzając tym samym powyższą tezę, iż sprawny system *compliance* umożliwi efektywnie zarządzać informacją.

Pomimo ogromnej mocy sprawczej zagadnień przytoczonych powyżej, brakuje jeszcze jednej rzeczy, aby można mówić o swoistej recepcie na bezpieczeństwo. Jest jeszcze jeden, bardzo ważny i kluczowy składnik, a mianowicie kadra zarządzająca, kierownictwo, pracownicy, po prostu ludzie, jako czynnik nad wyraz istotny i podstawowy, który może, ale nie musi skutecznie angażować się w politykę firmy czy przedsiębiorstwa. Czasy teraźniejsze, nowoczesne nie wymuszają przecież na społeczeństwie wprowadzania czy stosowania coraz tu większej ilości przepisów prawnych, czy wewnętrznych regulacji. Choć skala zagrożeń wynikająca z globalizacji i cyfryzacji jest nie porównywalnie inna niż za czasów, kiedy elektryczność i cyfrowa łączność międzyludzka była tylko marzeniem. To postrzegania realiów powinno wywrzeć na człowieku zmiany, jego chęć transformacji skupiająca się na tym co jest dziś i na tym co może być jutro. Decyzje, które podejmowane są dziś, będą miały niekiedy przełożenie na kreowanie życia jutrzejszego, zaletą jest to po prostu pojąć. Nie można tego rozważać tylko jako stwierdzenia, że człowiek jest znowu najsłabszym

ogniwem. Stało się to utartym i rzecz jasna swoistym stereotypem klasyfikującym człowieka, jako istotę nad wyraz chwiejną i kruchą w swoim działaniu. Nie jest możliwe stworzenie czegoś wielkiego, bezpiecznego, czy sprawnie działającego bez udziału poszczególnych osób jako podstaw planu, projektu i realizacji. Wiara w wartość jednostki jest nagminnie niedoceniona, a przecież jej moc sprawcza jest tak ogromna, iż będzie procentować na podłożu różnych dziadzin i środowisk bezpieczeństwa, wpływając i kreując np. politykę bezpieczeństwa informacji.

Literatura

1. Barańska D., *Kodeks samurajski Bushido a normy moralne i etyka społeczna*, Krakowskie Studia Miedzynarodowe, t. 3, nr 1, 2006.
2. Chomiczewski W., *Systemy zarządzania zgodnością: compliance w praktyce*, Wolters Kluwer, Warszawa 2020.
3. Depo J., Mazur S., *Administracja bezpieczeństwa, informacji niejawnych i danych osobowych: vademecum*, Oficyna Wydawnicza AFM, Kraków 2015.
4. Jedrych E., Sidor-Rządkowska M., *Kodeksy etyczne instrumentem good government w organizacjach*, Zeszyty Naukowe Uczelni Vistula, t. 4, nr 55, 2017.
5. Kowalczyk L, Mroczko F., *Kreatywność i innowacyjność w zarządzaniu i pedagogice w erze cyfrowej, Zarządzanie operacyjne w teorii i praktyce organizacji biznesowych, publicznych i pozarządowych*, Wydawnictwo Wyższej Szkoły Zarządzania i Przedsiębiorczości z siedzibą w Wałbrzychu, t. 48, nr 2, 2019.
6. Krzewiak D., *Nadzór i kontrola Internetu jako instrument polityki bezpieczeństwa informacyjnego współczesnych państw*, De Securitate Et Defensione. O Bezpieczeństwie i Obronności, t. 7, nr 1, 2021.
7. Lasota-Jądrzak A., *Planowanie ochrony informacji niejawnych w jednostce organizacyjnej,* Związek Przedsiębiorców i Pracodawców Wielkopolska, Poznań 2018.
8. Makowicz B., *Compliance w przedsiębiorstwie*, Wolters Kluwer Polska, Warszawa 2011.
9. Roman Ł., Winogrodzki G., *Służby specjalne w systemie bezpieczeństwa państwa*, Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide de Gasperi w Józefowie, Józefów 2016.

10. Zapart R., *Teoria i praktyka ochrony informacji niejawnych – wybrane zagadnienia dotyczące bezpieczeństwa informacji*, Polityka i Społeczeństwo, t. 18, nr 3, 2020.

Akty prawne

1. *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem*, portal eur-lex.europa.eu, https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX:32016L0943, [dostęp: 16.05.2023].
2. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz. U. z 2023 r. poz. 756).
3. *Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji* (Dz. U. z 1993 r. Nr 47, poz. 211).

Netografia

1. *Tajemnica przedsiębiorstwa. Definicja ustawowa i praktyczne znaczenie – Tajemnica Przedsiębiorstwa*, portal tajemnica-przedsiebiorstwa.pl, https://tajemnica-przedsiebiorstwa.pl/tajemnica-przedsiebiorstwa, [dostęp: 16.05.2025].