Ład czy nieład

Bardzo wzruszyła mnie sprawa kierownika basenu miejskiego w Kutnie. Otóż Prezes UODO nałożył na niego karę w wysokości 20 tys. złotych przede wszystkim za to, że nie prowadził nadzoru na żadnym etapie procesu wdrażania nowego programu kadrowo-płacowego. Decyzja zapadła po 3 latach i 8 miesiącach od daty zgłoszenia naruszenia wynikającego z zagubienia pendrive'a z danymi osobowymi pracowników basenu przez pracownika podmiotu przetwarzającego.

Po raz pierwszy spotkałam się z tak dobitnym podkreśleniem znaczenia nadzoru nad informatyką, czyli **governance of IT**, w organizacji.

Nadzór zyskuje na znaczeniu

Przy dzisiejszym stopniu cyfryzacji firm i instytucji nadzór nad informatyką staje się szczególnie istotny. Jego brak może oznaczać poważne kłopoty we wdrażaniu i utrzymaniu systemów informatycznych oraz zapewnieniu efektywności i ciągłości działania organizacji, o czym boleśnie przekonali się w Kutnie.

Tak się składa, że uczestniczyłam w pracach nad metodyką COBIT **nadzoru nad informacjami i technologią w firmie** (*a framework for enterprise governance of information and technology*) – opublikowaną przez międzynarodowe stowarzyszenie ISACA (www.isaca.org/resources/cobit). Metodyka może być stosowana w sektorze prywatnym, biznesowym i w sektorze publicznym. Wszędzie tam, gdzie od informatyki zależy funkcjonowanie danego podmiotu, czyli praktycznie w całym naszym otoczeniu.

Może ład, może rządzenie

W polskich opracowaniach pojęcie *governance* jest różnie tłumaczone. Oprócz słowa „nadzór" najczęściej pojawia słowo „ład", szczególnie w kontekście „ładu korporacyjnego" (*corporate governance*).

Dla przykładu w sektorze finansowym mamy rekomendację Z dotyczącą zasad **ładu wewnętrznego** (*internal governance*) w bankach, wydaną przez Komisję Nadzoru Finansowego na podstawie ustawy – Prawo bankowe. Jak zaznaczono w dokumencie: „Na ład wewnętrzny składają się w szczególności: system zarządzania bankiem, organizacja banku, zasady działania, uprawnienia, obowiązki i odpowiedzialność oraz wzajemne relacje rady nadzorczej, zarządu i osób pełniących kluczowe funkcje w banku".

W uzupełnieniu warto zacytować definicję **ładu korporacyjnego w bankowości** (*corporate governance in banking*) podanej w „Kompendium terminów z zakresu bankowości" dostępnym na stronach Ministerstwa Finansów (str. 28):

Zgodnie z metodyką COBIT sprawny nadzór nad informatyką ma na celu:

- **uzyskiwanie korzyści przez dany podmiot dzięki cyfryzacji;**
- **optymalizację ryzyka wynikającego ze stosowania technologii informatycznych;**
- **optymalizację zasobów – kadry, sprzętu, oprogramowania.**

Nadzór jest sprawowany poprzez:

- **szacowanie potrzeb i oczekiwań interesariuszy i wyznaczanie wynikających z nich celów;**
- **określanie kierunku stosownych działań wraz z wyznaczeniem priorytetów;**
- **monitorowanie sprawności i zgodności z wyznaczonymi celami.**

System nadzoru obejmuje procesy, struktury organizacyjne, polityki i procedury, przepływy informacji, postawy i zachowania, wiedzę i umiejętności oraz infrastrukturę.

Ład korporacyjny odnosi się do roli zarządu w nadzorowaniu kierowników wyższego szczebla spółek notowanych na giełdzie. Skuteczny nadzór jest konieczny nawet w odniesieniu do najlepszych kierowników. [...] Bez względu jednak na kwalifikacje, trzeba uważnie kontrolować ich działania, nie ingerując w bieżący proces zarządzania. [...] Osoba niewywierająca wpływu na codzienne zarządzanie, ale znająca sprawy przedsiębiorstwa, powinna trzymać rękę na pulsie i upominać się o interesy udziałowców.

Z kolei w dokumentach dawnego Ministerstwa Rozwoju Regionalnego użyto słowa „rządzenie" w kontekście ciekawej koncepcji **dobrego rządzenia** (*Good Governance*), wprowadzonej przez Bank Światowy na początku lat 90. Jak wynika z podanej definicji:

„Dobre rządzenie to sprawowanie władzy publicznej w ramach wzajemnych relacji rządu, administracji i społeczeństwa, cechujące się otwartością, partnerstwem, rozliczalnością, skutecznością, efektywnością i spójnością".

Rządzenie nie zarządzanie

Wrócę do pytania, które zadałam w mojej analizie opublikowanej w numerze 2/2024 „Domeny": czy ministrowie zasiadają w rządzie (government) czy w zarządzie (management) Rzeczpospolitej Polskiej? Zdecydowanie w rządzie, bowiem sprawują władzę publiczną. Zatem *governance* nie jest zarządzaniem.

Metodyka COBIT również wyraźnie rozróżnia nadzór/ład/rządzenie (*governance*) od zarządzania (*management*) w stosunku do cyfryzacji: „Zarządzanie informatyką polega na planowaniu, ustalaniu, wykonywaniu i monitorowaniu czynności, dzięki którym wyznaczone cele są osiągane – zgodnie z kierunkiem ustanowionym przez rządzących".

> *Stąd moje oburzenie i mój sprzeciw na zrównanie pojęć „governance" i „management" za pomocą jednego polskiego odpowiednika „zarządzanie" w polskiej wersji Rozporządzenia o sztucznej inteligencji (AI Act).*

Ponieważ Ministerstwo Cyfryzacji nie dostrzega i chyba nie rozumie problemu – chociaż powinno jako koordynator wdrożenia Rozporządzenia w Polsce – 12 sierpnia br. przesłałam swoje zastrzeżenia bezpośrednio do sprawców zamieszania, czyli do Rady Unii Europejskiej. Czekam na odpowiedź. Sprawdziłam także tłumaczenie obu pojęć we wszystkich oficjalnych wersjach językowych Rozporządzenia. Okazało się, że tylko w polskiej wersji użyto jednego polskiego słowa dla dwóch różnych pojęć występujących w oryginale. Dodam, że w Rozporządzeniu występuje też pojęcie *supervision* słusznie przetłumaczone jako „nadzorowanie" lub „nadzór" w zależności od treści danego artykułu. Zatem jako odpowiedniki *governance* zostają „ład" lub moje ulubione „rządzenie".

Brak rządzenia

Wyniki kolejnych kontroli przeprowadzonych przez Najwyższą Izbę Kontroli dotyczących cyfryzacji, cyberbezpieczeństwa, bezpieczeństwa teleinformatycznego i ochrony danych osobowych wykazują jedno: w jednostkach sektora finansów publicznych brak rządzenia informatyką. Jest tylko lepsze lub gorsze zarządzanie informatyką przez samych informatyków, którzy wykazują się różnym poziomem szeroko pojętej wiedzy zawodowej.

Kontrola NIK „Zapewnienie ochrony i prawidłowego przetwarzania danych, w tym danych osobowych gromadzonych w formie elektronicznej przez jednostki samorządu terytorialnego oraz podległe jednostki organizacyjne na stronach internetowych, poczcie elektronicznej oraz w związku z odbywającymi się sesjami organów uchwałodawczych w województwie podlaskim" z 2023 r. stwierdziła wieloletnie zaniedbania dotyczące ochrony danych osobowych, nieświadomość zagrożeń, brak jednoznacznych wytycznych, używanie domen publicznych bez stosownych umów gwarantujących bezpieczeństwo. Oznacza to, że podstawowe elementy systemu ochrony danych osobowych w jednostkach samorządowych są nieskuteczne.

W wyniku kontroli NIK „Zapewnienie bezpieczeństwa teleinformatycznego przez jednostki samorządu terytorialnego województwa zachodniopomorskiego" z 2024 r. ujawniono wieloletnie zaniedbania dotyczące cyberbezpieczeństwa, nieświadomość i brak skutecznych procedur reagowania na zagrożenia, a także wykorzystywanie oprogramowania, które miało krytyczne luki.

> *Ewidentnie kierownicy jednostek sektora publicznego nie wiedzą, jak rządzić informatyką.*

Cedują zadania i obowiązki dotyczące cyfryzacji na informatyków zatrudnionych na etacie lub na umowę zlecenie bądź na wynajęte firmy informatyczne. Nie wiedzą też, jak rozliczać informatyków i inne osoby odpowiedzialne za cyberbezpieczeństwo, bezpieczeństwo informacji i ochronę danych osobowych. Obecnie trwa kontrola NIK „Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego". Czy wykaże poprawę? Przekonamy się w przyszłym roku, gdy zgodnie z planem poznamy wyniki.

W raportach z kontroli NIK „Ochrona danych pacjentów przed cyberatakami w podmiotach leczniczych na terenie województwa warmińsko-mazurskiego" z 2024 r. możemy przeczytać:

- **W latach 2021–2022 nie zrealizowano niektórych obowiązków określonych w SZBI. Dyrektor wyjaśnił, że pełnił obowiązki kierownika jednostki od 1 lipca 2023 r. i nie posiadał wiedzy, dlaczego w okresie objętym kontrolą nie zrealizowano powyższych obowiązków (według stanu kontroli na 16 lutego 2024 r.).**

- **Jak wyjaśnił dyrektor, faktycznie w regulaminie organizacyjnym szpitala niewłaściwie opisano strukturę organizacyjną komórki zajmującej się IT, w szczególności pominięto uwidocznienie stanowiska Kierownika IT, podległego bezpośrednio Dyrektorowi i nadzorującego pracę pozostałych informatyków. Problem został zauważony i omawiany w trakcie prac nad aktualizacją regulaminu organizacyjnego na przełomie 2022 i 2023 r. Dodał jednak, że przez niedopatrzenie pracowników administracji SP ZOZ, opis komórki IT nie został zaktualizowany.**

- **Dyrektor wyjaśnił, że upoważnienia powinny być przygotowane przez IOD. Nie miał wiedzy o ich braku. Inspektor Ochrony Danych zapewniał go o prawidłowym prowadzeniu spraw związanych m.in. z nadawaniem upoważnień do przetwarzania danych osobowych dla pracowników szpitala.**

- **Prezes szpitala w wyjaśnieniach potwierdziła, że tylko niektóre elementy funkcjonującego do 11 lipca 2022 r. SZBI zostały opracowane na podstawie Polskiej Normy PN-ISO/IEC 27001.**

- **Do 1 lutego 2024 r. nie opracowano systemu SZBI na podstawie Polskiej Normy PN-ISO/IEC 27001. Prezes zarządu mi.in. z uwagi na upływ czasu nie potrafiła podać przyczyn powyższej nieprawidłowości. Wskazała, że osobą odpowiedzialną za opracowanie SZBI był IODO. Również IODO nie potrafił wskazać przyczyn ww. nieprawidłowości.**

- **W okresie od 1 stycznia 2020 r. do 31 grudnia 2023 r. w szpitalu 26 byłym pracownikom odbierano dostęp do systemów informatycznych zawierających dane osobowe pacjentów w terminie od 2 do 653 dni, licząc od dnia rozwiązania z nimi stosunku pracy bądź umowy cywilnoprawnej. Ani prezes zarządu, ani informatyk zajmujący się tymi sprawami nie potrafili podać przyczyn powyższej nieprawidłowości.**

- **Opowiedzi Prezesa Zarządu na pytania kontrolera NIK o przyczyny nieopracowania, nieustanowienia i niewdrożenia SZBI w zakresie, o jakim mowa w § 20 rozporządzenia KRI oraz przyczyny nieopracowania obowiązującej w szpitalu polityki ochrony danych na podstawie Polskiej Normy PN-ISO/IEC 27 0001 nie obejmowały wyjaśnień w tym zakresie.**

- **W okresie objętym kontrolą w SGZOZ nie wyznaczono IOD, co było niezgodne z art. 37 ust. 1 RODO. Dyrektor przychodni wyjaśniła, że została zapewniona przez informatyka zatrudnionego na podstawie umowy serwisowej, że skoro on posiada wyznaczonego IOD w ramach swojej działalności, to jednocześnie SGZOZ też posiada wyznaczonego IOD.**

- **Dyrektor podała, że informatycy SGZOZ poinformowali ją, że nie ma konieczności zawierania z (…).com umów powierzenia przetwarzania danych i nie weryfikowała tych informacji.**

Jak rządzić?

Gdzie w Polsce rządzący znajdą wytyczne, wskazówki, podpowiedzi, jak rządzić informatyką w jednostkach sektora publicznego? **NIGDZIE** (pomijam metodykę COBIT, której najnowsza wersja nie jest dostępna w języku polskim).

W 2023 r. NASK opublikował dwa poradniki: „Cyberbezpieczny Samorząd" – skierowany do jednostek samorządu terytorialnego zainteresowanych podniesieniem poziomu cyberbezpieczeństwa i „Firma Bezpieczna Cyfrowo" – przygotowany, by pomagać w poprawie cyberbezpieczeństwa i jakości usług cyfrowych w firmach niezależnie od ich wielkości. Niestety, publikacje dotyczą tylko cyberbezpieczeństwa i tylko zarządzania nim.

Zajrzałam do Bazy Dobrych Praktyk, która gromadzi opisy dobrych i sprawdzonych rozwiązań z zakresu doskonalenia zarządzania usługami publicznymi i rozwojem jednostek samorządu terytorialnego, w tym rozwojem instytucjonalnym.

Od kwietnia 2019 r. Baza Dobrych Praktyk jest wspierana w ramach projektu System Monitorowania Usług Publicznych (SMUP), zaś od 2020 r. prace nad rozwojem bazy koordynuje Związek Miast Polskich. SMUP jest nowym wymiarem prezentacji i przetwarzania danych statystycznych przez Główny Urząd Statystyczny. Niestety, znalezienie projektów informatycznych wymaga przejrzenia całej bazy, bowiem proponowane listy usług i wskaźników nie uwzględniają cyfryzacji.

Znalazłam ciekawą praktykę pt. *Scentralizowane usługi informatyczne na poziomie gminy Margonin podstawą efektywnego zarządzania zasobami ludzkimi i technicznymi* (https://www.dobrepraktyki.pl/praktyka/368,scentralizowane-uslugi-informatyczne-na-poziomie-gminy-podstawa-efektywnego-zarzadzania-zasobami-ludzkimi-i-technicznymi.html). W jej ramach realizowane są cele:

- **zarządcze – ujednolicone zostały procedury obsługi informatycznej podległych jednostek oświatowych (trzy szkoły podstawowe oraz przedszkole z trzema filiami) i samego Centrum Usług Wspólnych;**
- **efektywnościowe – zoptymalizowano zatrudnienie pionu IT w stosunku do potrzeb, obniżono poziom ryzyka realizowanych procesów dzięki specjalizacji kadrowej, uchwycono rzeczywiste koszty usług informatycznych, co prowadzić będzie do obniżenia ich jednostkowych kosztów;**
- **innowacyjności – pion IT na bieżąco monitoruje wymogi stawiane przed szkolnymi systemami informatycznymi i wspiera szkoły w ich wdrażaniu, np. metody i techniki zdalnej edukacji.**

Włodarze gminy mają więc własny pomysł na rządzenie informatyką w swoich placówkach oświatowych.

Może strategicznie?

Pod koniec października br. ministerstwo przekazało do konsultacji społecznych projekt Strategii Cyfryzacji Państwa do 2035 r. Głównym celem Strategii ma być poprawa jakości życia obywateli dzięki cyfryzacji. W dokumencie zaznaczono również, że „sfera technologii cyfrowych jest kluczowym polem nasilającej się rywalizacji geopolitycznej, a inwestycje w tej dziedzinie pośrednio (za sprawą technologii podwójnego zastosowania) lub bezpośrednio przekładają się na poziom bezpieczeństwa państwa". W związku z tym spodziewałam się szczególnego nacisku na rządzenie cyfryzacją dla skutecznego osiągania wyznaczonych celów przy optymalizacji występującego ryzyka i dostępnych zasobów.

Słowa *governance* użyto tylko dwa razy w kontekście *data governance*. Natomiast słowo „zarządzanie" pojawia się w wielu odmianach, które mogą odnosić się do *governance*: zarządzanie strategiczne, zintegrowane zarządzanie usługami publicznymi, zarządzanie cyfryzacją, zarządzanie sztuczną inteligencją, zarządzania informatyzacją państwa, zarządzeni danymi. Sprawdziłam też słowo „nadzór". Pojawia się w kontekście nadzoru i monitoringu wdrażania Architektury Informacyjnej Państwa, nadzoru człowieka nad rozwojem AI i nadzoru nad bezpieczeństwem zastosowań AI oraz nadzorowania i integrowania działań różnych podmiotów zajmujących się przeciwdziałaniem dezinformacji.

Kto ma rządzić cyfryzacją państwa? Zgodnie ze Strategią zajmie się tym Komitet do Spraw Cyfryzacji, który zastąpi obecnie działający Komitet Rady Ministrów do Spraw Cyfryzacji. Do pomocy będą pełnomocnicy ds. informatyzacji, którzy zostaną powołani obligatoryjnie w urzędach obsługujących ministrów kierujących działami administracji rządowej oraz w Kancelarii Prezesa Rady Ministrów (fakultatywnie natomiast w pozostałych urzędach). Jak wynika z informacji na stronie https://www.gov.pl/web/krmc, dotychczasowy Komitet zajmował się przede wszystkim zapewnieniem koordynacji realizacji projektów informatycznych administracji rządowej. Ostatnie opublikowane sprawozdanie z jego działalności dotyczy 2020 r. Ku mojemu zaskoczeniu nie znalazłam projektu Strategii wśród projektów dokumentów rządowych opiniowanych przez członków Komitetu w 2024 r. Oby nowy Komitet wiedział, na czym polega dobre rządzenie cyfryzacją Rzeczpospolitej Polskiej.

7 listopada 2024 r. projekt Strategii został zaprezentowany na posiedzeniu Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Sejmu RP (https://www.sejm.gov.pl/Sejm10.nsf/PosKomZrealizowane.xsp?komisja=CNT#36). Dyskusja trwała tylko godzinę. Szczególnie polecam wypowiedź profesor Marty Grabowskiej z Centrum Europejskiego UW. Ostro skrytykowała zaproponowane wskaźniki efektywności. Ja też miałam do nich uwagi po porównaniu ich z przykładowymi miernikami procesu AP002 Zarządzana Strategia zawartymi w metodyce COBIT.

Jak nie rządzić?

Na koniec kilka słów o niepokojącym zwyczaju, który ostatnio zaobserwowałam. Przywołane dobre rządzenie polega m.in. na partnerstwie z trzecim sektorem. Toteż nie zdziwiła mnie współpraca urzędów państwowych w kwestii ochrony dzieci w internecie z fundacjami, które od lat zajmują się tym problemem. W jednym przypadku urząd opublikował poradniki otrzymane od fundacji bez jakichkolwiek zmian. W drugim – ministerstwo bezrefleksyjnie przepisało do swoich wytycznych zaproponowane przez fundację zasady dotyczące bezpiecznego korzystania z internetu i mediów. W obu przypadkach wysłałam swoje zastrzeżenia, bowiem poradniki i wytyczne zawierały zapisy sprzeczne z obowiązującymi przepisami, standardami i dobrymi praktykami dotyczącymi zapewnienia cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych osobowych. Zdziwił mnie brak właściwej reakcji. Zatem przypomnę, że za stosowanie udostępnionych porad i wytycznych wprowadzających w błąd rozliczani będą rządzący firmami i jednostkami, a nie ich autorzy.

Joanna Karczewska

Wszystkie informacje zawarte w artykule są podane według stanu na 15 listopada 2024 r.