K A M I L A K L E P A S – K R A S Z K A
a d w o k a t

KANCELARIA ADWOKACKA
60-275 POZNAŃ, UL. TĘCZOWA 8
T. 604 7777 95
e-mail: adwokat@klepas.pl

Poznań, dnia 01.03.2021 roku

AUDYT WEWNĘTRZNY

***na zlecenie*: Zarządu Spółdzielni Mieszkaniowej „Dębina" w Poznaniu**

***w przedmiocie*: ogólnego badania w zakresie przestrzegania procedur RODO obowiązujących w Spółdzielni Mieszkaniowej „Dębina" z siedzibą w Poznaniu**

I. Wstęp

Przedmiotem badania objęta została działalność organów Spółdzielni Mieszkaniowej „Dębina" z siedzibą w Poznaniu - Rady Nadzorczej i Zarządu oraz pracowników administracyjnych i innych podmiotów współpracujących ze Spółdzielnią na podstawie umów cywilnoprawnych, którym zostały powierzone tzw. *dane wrażliwe* w celach świadczenia pracy (w ramach stosunku pracy) oraz realizacji przedmiotu umów zawartych z podmiotami zewnętrznymi. Badaniu podlegały treści umów oraz weryfikacja treści upoważnień administratora danych i stosownych oświadczeń podmiotów w zakresie powierzenia im w/w danych.

Niniejsze badanie obejmuje weryfikację obowiązujących w Spółdzielni procedur określonych w poniżej wymienionych aktach wewnętrznych tj. *w Polityce Bezpieczeństwa Spółdzielni Mieszkaniowej „Dębina" w Poznaniu, w*

dokumencie - Bezpieczeństwo informatyczne - Instrukcji zarządzania Systemem Informatycznym oraz w Polityce tzw. czystego biurka, a także ich ocenę w kontekście poprawności wdrożenia procedur, ich stosowania i przestrzegania oraz wprowadzenia ewentualnych zmian w zakresie zgodności z obowiązującymi przepisami prawa.
Dodatkowo, w trakcie czynności kontrolnych Zarząd Spółdzielni przedstawił dodatkowe dokumenty w postaci:

a. 5 losowo wybranych umów najmu lokali mieszkalnych,
b. 10 losowo wybranych akt lokatorskich,
c. 10 losowo wybranych umów o współpracy z podmiotami zewnętrznymi, w tym w szczególności umów na obsługę informatyczną,
d. akta osobowe pracowników Spółdzielni,

w celu weryfikacji poprawności gromadzenia danych osobowych oraz kompletności dokumentacji z zakresu danych osobowych (stosownych oświadczeń, upoważnień, dodatkowych umów, itp.).

Po przeprowadzeniu analizy dokumentów źródłowych, należy stwierdzić że Spółdzielnia przetwarza następujące dane osobowe:

1. członków Spółdzielni,
2. innych osób (nie będących członkami), którym przysługują prawa do lokali mieszkalnych i o innym niż mieszkalne przeznaczeniu znajdujących się w zasobach Spółdzielni,
3. pracowników,
4. osób współpracujących na podstawie umów cywilnoprawnych,
5. inne dane osobowe bez kategorii.

Przetwarzanie w/w danych związane jest z realizacją celów spółdzielni mieszkaniowej określonych w ustawie z 15 grudnia 2000 r. *o spółdzielniach mieszkaniowych* i w Statucie. Wiodącym celem Spółdzielni jest zaspokajanie potrzeb mieszkaniowych i innych potrzeb członków oraz ich rodzin, przez dostarczanie im lokali mieszkalnych, oraz lokali o innym niż mieszkalne przeznaczeniu. Przetwarzanie danych osobowych wiąże się również z przedmiotem działalności Spółdzielni, o którym jest mowa w Statucie, a

prowadzona działalność warunkuje zakres przetwarzania danych osobowych. Spółdzielnia ma obowiązek zarządzania nieruchomościami stanowiącymi jej mienie lub nabyte mienie jej członków.

W Spółdzielni prowadzone są następujące zbiory danych osobowych:

1. rejestr członków,
2. zbiór osób, którym przysługuje i przysługiwało prawo do lokalu,
3. dane związane z zatrudnieniem,
4. dziennik korespondencyjny,
5. rejestry skarg i wniosków,
6. osoby współpracujące ze Spółdzielnią na podstawie umów cywilnoprawnych,
7. rejestr dłużników.

Zakres przetwarzanych danych osobowych w/w zbiorach powinien odpowiadać zasadom ogólnym określonym w ustawie z 10 maja 2018 r. o ochronie danych osobowych oraz Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych* (Dz. Urz. UE.L Nr 119, s. 1). Zgodnie z art. 5 ust. 1 rozporządzenia **dane osobowe** muszą być:
a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość");
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami ("ograniczenie celu").

Natomiast, zgodnie z art. 6 ust. 1 rozporządzenia **przetwarzanie jest zgodne z prawem** *wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:*

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Katalog przesłanek jest zamknięty, a zatem spełnienie jednej z nich stanowi o zgodnym z prawem przetwarzaniu danych osobowych. W praktyce oznacza to, że nie można przy braku zgody osoby, której dane dotyczą, uznać, że administrator danych przetwarza jej dane osobowe bez podstawy prawnej, naruszając obowiązujące przepisy w zakresie danych osobowych, w szczególności przepisy rozporządzenia, ponieważ ustawodawca dopuścił możliwość przetwarzania danych także na mocy innych przesłanek. Zważyć należy, że ocena dopuszczalności przetwarzania danych musi być dokonywana każdorazowo w sposób zindywidualizowany z uwzględnieniem konkretnych okoliczności i celów przetwarzania danych.

Mając powyższe na uwadze, stwierdzić należy, że ustawa *o ochronie danych osobowych* zawiera jedynie ogólne zasady postępowania obowiązujące w związku z przetwarzaniem danych osobowych oraz określa prawa osób fizycznych, których dane są lub mogą być przetwarzane w

zbiorach danych. Natomiast, w/w ustawa nie znajduje zastosowania ilekroć kwestie w niej zawarte dotyczące dostępu do danych osobowych są szczegółowo uregulowane w innych aktach prawnych dotyczących szeroko rozumianego prawa spółdzielczego, w myśl ogólnej zasady *lex specialis derogat legi generali* (*przepis szczególnych uchyla moc prawną przepisu ogólnego*). A zatem, pomocne będą w razie wątpliwości rozważania także na gruncie przepisów ustawy z dnia 16.09.1982 roku *Prawo spółdzielcze*, w szczególności: art. 18 §2 pkt 3 i §3 ustawy *Prawo spółdzielcze*, które stanowią wprost do jakich dokumentów członek spółdzielni ma dostęp oraz w odniesieniu do jakich dokumentów dostęp ten może być ograniczony (przepis art. 18 §3 ustawy nakłada na spółdzielnię obowiązek dokonania oceny czy udostępnienie umów zawieranych z podmiotami trzecimi nie naruszy praw tych osób lub czy istnieje obawa, że członek wykorzysta uzyskane informacje w celach np. sprzecznych z interesem Spółdzielni) oraz art. 8^1 ustawy *o spółdzielniach mieszkaniowych*.

II. **Badanie poszczególnych kategorii dokumentów źródłowych wraz z ich wstępną oceną**:

W przedmiocie badania akt osobowych stwierdzam, że akta zawierają wyłącznie dokumenty niezbędne do ich prowadzenia zgodnego z przepisami prawa pracy i przepisami o ochronie danych osobowych. W aktach Głównego Księgowego oraz dwóch pracowników brak wpiętych oświadczeń w zakresie RODO - zgodnie z opracowanym i obowiązującym wzorcem upoważnienia do przetwarzania danych osobowych oraz zobowiązania do zachowania w tajemnicy danych stanowiących tajemnicę Spółdzielni i innych danych przekazywanych w związku z zatrudnieniem i stosownego oświadczenia pracownika w przedmiocie zobowiązania się do *przestrzegania* obowiązujących procedur i standardów, na podstawie Polityki Bezpieczeństwa. Rekomenduję, włączenie upoważnień i oświadczeń do akt osobowych w/w pracowników w celu ujednolicenia dokumentów pracowniczych oraz zachowania ich kompletności.

W pozostałym zakresie nie mam uwag i nie wnoszę zastrzeżeń. Niezależnie od przedmiotu badania przypominam o numerowaniu akt osobowych.

Natomiast, w aktach osobowych członków Zarządu znajdują oświadczenia o zachowaniu w tajemnicy wszelkich informacji z zakresu ochrony danych osobowych i danych objętych tajemnicą służbową.

W zakresie badania umów najmu lokali mieszkalnych, stwierdzam, że akta są w sposób prawidłowo prowadzone, zawarte w nich dane wrażliwe dotyczą wyłącznie danych koniecznych do realizacji przedmiotu umowy najmu – tj. imion i nazwisk najemców.

Jeżeli chodzi o dane osób wspólnie z najemcami zamieszkującymi, to z przepisów ustawy o spółdzielniach mieszkaniowych ani Prawa spółdzielczego, nie wynika aby Spółdzielnia mogła gromadzić w/w informacje, nie dotyczy to jednak informacji o liczbie osób zamieszkujących w danym lokalu, chyba że każda z tych osób, której dane dotyczą wyrazi na to zgodę (art. 23 ust 1 pkt 1 ustawy *o ochronie danych osobowych*). Względem tych osób należy zastosować się do obowiązku wynikającego z art. 24 ust. 1 ustawy *o ochronie danych osobowych* (**obowiązek informacyjny**).

Dodatkowo, w treści umów najmu zawarte są klauzule informacyjne dotyczące ochrony danych osobowych w Spółdzielni Mieszkaniowej „Dębina" w Poznaniu. Powyższa klauzula, jest zgodna z obowiązującymi przepisami prawa, spełnia obowiązki informacyjne Spółdzielni jako Administratora danych i zawiera następujące dane: Administratora danych, informację o prawie do wniesienia sprzeciwu, o okresie przechowywania danych wraz z informacją o możliwości przekazania danych osobowych pracownikom Spółdzielni, którzy posiadają stosowne upoważnienia. A nadto, innych uprawnieniach związanych z przetwarzaniem danych osobowych osób, których te dane bezpośrednio dotyczą, a mianowicie: dostępu do swoich danych oraz otrzymania ich kopii, sprostowania (poprawiania) swoich danych, żądania usunięcia, ograniczenia lub wniesienia sprzeciwu wobec ich przetwarzania, przenoszenia danych oraz wniesienia skargi do organu nadzorczego. Powyższe, jest zgodnie z art. 13 ust. 1-2 Rozporządzenia

Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych) (dalej „**RODO**") informuję, że: **dane osobowe mogą zostać przekazywane wyłącznie pracownikom Spółdzielni, którym powierzono pisemnie przetwarzanie danych osobowych i którzy ponoszą odpowiedzialność za naruszenie zasad przetwarzania.**
Z treści informacji wynika, że **podanie danych przez osobę, której dane bezpośrednio dotyczą jest dobrowolne oraz że w każdej chwili przysługuje tej osobie prawo do wycofania zgody na przetwarzanie danych osobowych, której udzieliła składając podpis na dokumencie Informacji.**

Odnośnie prowadzenia akt lokatorskich, co do zasady nie stwierdzono nieprawidłowości, dane w nich zawarte gromadzone są w określonym celu i ograniczone wyłącznie do danych niezbędnych dla realizacji celów ustawowych i statutowych Spółdzielni. Akta windykacyjne dotyczące dłużników Spółdzielni w tym: osób posiadających status członków Spółdzielni jak również właścicieli lokali bez statusu członkowskiego oraz najemców i osób nieposiadających tytułu prawnego do lokalu wskutek jego utraty lub wygaśnięcia są prowadzone według tych samych zasad, spełniają wymogi ustawowe. Ponadto, w aktach windykacyjnych znajdują się kopie nakazów zapłaty (wyroków) wydanych w sprawach sądowych i kopie dokumentów egzekucyjnych oraz w niektórych ugody pozasądowe – wszystkie dokumenty gromadzone w celach rozliczenia zaległości i ich egzekucji.

W toku badania dokumentów zawierających udzielone przez mieszkańców (tj. członków Spółdzielni i właścicieli lokali niebędących członkami oraz najemców) pisemne zgody na przetwarzanie i gromadzenie danych osobowych w/w osób wymagają aktualizacji danych. Wszelkie czynności z tym związane należy podejmować na bieżąco, ewentualnie cyklicznie, by podstawa prawna gromadzenia i przetwarzania danych nie

odpadła, z tym tylko zastrzeżeniem, że dane wrażliwe przechowywać należy przez okres niezbędny dla prawidłowej realizacji umowy, nie dłużej jednak niż do przedawnienia dochodzenia ewentualnych roszczeń.

Dokumentacja w przedmiocie w/w zgód oraz oświadczeń o wyrażeniu zgody na przesyłanie mieszkańcom korespondencji drogą elektroniczną (garaże i lokale mieszkalne) przechowywana jest w odrębnym zbiorze dokumentów nazwanym „*OŚWIADCZENIA*", podczas gdy rekomendacja audytora jest taka, aby oświadczenia przyporządkować do poszczególnych akt lokalowych, celem ujednolicenia dokumentacji administracyjnej (członkowskiej) i przeciwdziałania tworzeniu dodatkowych zbiorów dokumentów zawierających dane wrażliwe.

Natomiast, w wybranych do badania umowach o współpracy z podmiotami zewnętrznymi, które w większości dotyczyły umów podpisanych z dostawcami mediów, umowy z zakresu świadczenia usług rynku nieruchomości stwierdzam, że zawarto w nich standardowe postanowienia w zakresie uregulowań dotyczących ochrony danych osobowych, a dodatkowo w tej ostatniej zawarto umowę o powierzeniu przetwarzania danych osobowych – praktyka oceniona jako prawidłowa.
Zastrzeżenie zgłaszam do umowy rozliczeniowo – abonamentowej na wykonanie usługi rozliczenia kosztów c.o. i wody przy wykorzystaniu podzielników kosztów i modułów radiowych, wodomierzy, a mianowicie w zakresie upoważnienia *Spółki ista* w ramach realizacji w/w umowy, przedstawiciele Spółki nie złożyli podpisów po oświadczeniem dotyczącym zabezpieczenia serwerów. Rekomenduję więc uzupełnienie brakujących podpisów, z uwagi na późniejsze złożenie podpisu niż wskazuje na to data zawarcia umowy, Spółka winna złożyć dodatkowe oświadczenie w przedmiocie przyjęcia praw i obowiązków zarówno z datą złożenia podpisu jak i przed tą datą (tj. od dnia realizacji umowy na rzecz Spółdzielni).

Odnośnie umów zawartych o wykonanie prac porządkowych nie przyporządkowano do żadnej z nich oświadczeń osób zatrudnionych na podstawie w/w umów cywilnoprawnych z zakresu RODO. Natomiast, stosowna dokumentacja znajduje się w odrębnym segregatorze pod nazwą

„*DOZORCY*”. Audytor konsekwentnie rekomenduje także w ramach tej grupy przyporządkowanie w/w oświadczeń do poszczególnych umów, celem ujednolicenia dokumentacji i przeciwdziałania tworzeniu dodatkowych zbiorów dokumentów zawierających dane wrażliwe.
Do badania została przedłożona również umowa w przedmiocie organizacji przetargu sprzedaży mieszkań na podstawie obowiązującego w Spółdzielni *Regulaminu Przetargów* w sposób prawidłowy wykonano obowiązek informacyjny jak również zabezpieczono dane potencjalnych nabywców nieruchomości (oferentów) poprzez wprowadzenie dodatkowych klauzul i zgód na przetwarzanie danych osobowych w celach związanych z organizacją przetargu.

Jeżeli chodzi o umowę o przeprowadzenie sprawozdania finansowego zawartą w czerwcu 2020 roku, w sposób prawidłowy zostały zabezpieczone informacje zawierające dane wrażliwe, umowa zawierała standardowe przepisy o ochronie danych osobowych zgodne z aktualnie obowiązującymi przepisami prawa.

Z niektórymi podmiotami współpracującymi ze Spółdzielnią jeszcze przed datą wejścia w życie przepisów RODO - zostały dodatkowo zawarte umowy powierzenia przetwarzania danych osobowych, w celu dostosowania obowiązków związanych z ochroną danych.

Natomiast, jeżeli chodzi o umowy z grupy szeroko rozumianej obsługi informatycznej stwierdzono, że niezbędne klauzule z zakresu ochrony danych osobowych zostały do umów wprowadzone, udzielono stosownych upoważnień – usługi są świadczone, zgodnie z polityką Bezpieczeństwa Informatycznego - Instrukcją zarządzania Systemem Informatycznym, stanowiącą załącznik do Polityki Bezpieczeństwa aktualnie obowiązującej w Spółdzielni. W Systemie informatycznym stosuje się uwierzytelnianie na poziomie dostępu do systemu operacyjnego. System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej.

Zabezpieczenie obejmuje:

a. zabezpieczenie sieci – Firewall DRAYTEK
b. system antywirusowy i antyspamowy - ESET
c. szyfrowanie nośników danych – BIT LOCKER
d. poczta e-mail – (domena) smdebina.poznan.pl
e. użytkowany system jest automatycznie skanowany
f. aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy,

Z uzyskanych od Zarządu wyjaśnień dotyczących wprowadzenia przez rząd obostrzeń i ograniczeń związanych z pandemią, Spółdzielnia zleciła służbom informatycznym wprowadzenie dodatkowych zabezpieczeń w związku ze świadczeniem przez pracowników Spółdzielni pracy w trybie hybrydowym (częściowo zdalnie). Aktualna sytuacja w kraju jest wyjątkowa, ale długotrwała – wobec powyższego, zasadnym wydaje się więc stworzenie dodatkowych pisemnych procedur i zasad postępowania, tak aby były przejrzyste i mogły podlegać ocenie zgodności z obowiązującymi przepisami prawa. W konsekwencji, by odpowiedzialność podmiotów, którym dane powierzono była realna.

Przedmiot badania obejmuje również procedury wdrożenia zasad bezpieczeństwa i ich przestrzegania podczas wykonywania obowiązków służbowych przez organy Spółdzielni i pracowników zatrudnionych na podstawie umów o pracę, na kanwie przeprowadzonej w/w analizy oraz dodatkowych wyjaśnień.

Członkowie organów zarządczych, pracownicy oraz członkowie organu nadzoru są upoważnieni do przetwarzania danych osobowych w zakresie niezbędnym do wykonywania czynności związanych z pełnionymi przez nich funkcjami. Co do zasady członkowie organów Spółdzielni (Rada Nadzorcza i Zarząd) przetwarzają dane osobowe zgodnie z ogólnymi przepisami w ramach obowiązujących w Spółdzielni regulacji - Polityki Bezpieczeństwa i Instrukcją zarządzania Systemem Informatycznym, a także innymi

dokumentami wewnętrznymi i procedurami związanymi z przetwarzaniem danych osobowych.

Rada Nadzorcza – na podstawie wyjaśnień Przewodniczącego Rady Nadzorczej oraz przedłożonej przez Radę do badania dokumentacji w postaci protokołu z posiedzenia Rady Nadzorczej wraz z załącznikami (protokołami Komisji stałych działających przy Radzie – stwierdzam, że Rada Nadzorcza nie posiada odrębnych regulacji w zakresie ochrony danych osobowych dedykowanych temu organowi. W ramach sprawowania funkcji nadzorczych przestrzega ogólnych procedur związanych z bezpieczeństwem ochrony danych osobowych obowiązujących w Spółdzielni.

Dokumenty z posiedzeń Rada prowadzi w formie papierowej, dokumentacja z prac członków pracujących w poszczególnych Komisjach przy Radze i Prezydium prowadzona jest również w formie papierowej, Rada otrzymuje tylko część dokumentów w postaci elektronicznej, które są umieszczane przez Prezesa Zarządu na stronie internetowej Spółdzielni w zakładce „Rada Nadzorcza". Każdy z członków Rady posiada własny login i hasło z dostępem do w/w zakładki. W pozostałym zakresie dokumenty przekazywane są w formie papierowej Radzie, jak również poszczególnym Komisjom zgłaszającym zapotrzebowanie. Rada prowadzi korespondencje mailowo z członkami Zarządu z wykorzystaniem służbowych adresów mailowych.

Jeżeli chodzi o protokoły Rady jak i poszczególnych Komisji stałych działających przy Radzie Nadzorczej – Komisji Technicznej, Komisji Rewizyjnej i Komisji Członkowsko-Windykacyjnej – nie mam zastrzeżeń do treści protokołów podlegających badaniu (zwracam jedynie uwagę na konieczność składania odpowiedniej ilości podpisów w sprawozdaniach), w sposób prawidłowy Komisja Członkowsko-Windykacyjna operuje danymi dotyczącymi zadłużeń, bez możliwości identyfikacji dłużników. Co prawda, Komisja posługuje się numerami lokali mieszkalnych bez wskazywania nazwisk, to jednak należy każdorazowo badać czy ten sposób oznaczenia nie będzie naruszał przepisów RODO, o ile nie będzie można określić tożsamości właściciela będzie to prawidłowe. Numer lokalu mieszkalnego może zostać

uznany za dane osobowe w rozumieniu ustawy *o ochronie danych osobowych*, jeżeli na jego podstawie będzie można określić tożsamość właściciela lokalu mieszkalnego. Zgodnie z art. 4 RODO za dane osobowe uważa się informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej). Numer lokalu w określonych sytuacjach może stanowić dane osobowe, gdyż pośrednio na tej podstawie można określić tożsamość właściciela lokalu. Za dane osobowe nie można natomiast uznać informacji określającej ogólną sumę zaległości z tytułu opłat wnoszonych do spółdzielni z danego budynku bez wskazywania numerów lokali mieszkalnych. Identyfikacja konkretnej osoby w takim przypadku nie jest możliwa. Wątpliwości budzi upublicznianie ogólnej informacji o wysokości zadłużenia osób, którym przysługują prawa do lokali w określonej klatce schodowej lub na określonym piętrze bez wskazania dłużników. Dozwolone będzie udostępnienie tych informacji, jeżeli nie, będzie możliwe zidentyfikowanie konkretnego dłużnika. Spółdzielnia jest dobrowolnym zrzeszeniem nieograniczonej liczby osób, która w interesie swoich członków prowadzi wspólną działalność gospodarczą. Majątek spółdzielni jest prywatną własnością jej członków, dlatego informacje o zadłużeniach czynszowych poszczególnych członków są istotne dla każdego z jej członków.

W związku z powyższym, Spółdzielnia powinna w Statucie szczegółowo uregulować tryb i formę ich udostępniania.

Audytor rekomenduje w każdym przypadku ograniczanie posługiwania się danymi wrażliwymi, jeżeli jest to wystarczające dla osiągnięcia celu w ramach prowadzenia statutowej działalności organu nadzoru.

W zakresie prowadzenia korespondencji z mieszkańcami osiedla (osobami zainteresowanymi, albo osobami będącymi w zainteresowaniu Rady) - na podstawie oświadczenia Przewodniczącego - stwierdzam, że korespondencja

jest archiwizowana jedynie w niezbędnym zakresie w formie papierowej i przechowywana wraz z dokumentacją Rady w miejscu do tego przeznaczonym. Przewodniczący Rady zwrócił uwagę na potrzebę ujednolicenia dostępu form komunikacji porozumiewania się na odległość z Radą poprzez założenie wspólnego adresu e-mail dla wszystkich członków Rady Nadzorczej, a w następstwie dekretowania korespondencji przychodzącej do poszczególnych komisji w ramach ich kompetencji. Wdrożenie procedury pozwoli ograniczyć obieg dokumentów niezwiązanych z pracami poszczególnych Komisji, wszelką decyzyjność obiegu i organizacji pracy należy pozostawić Prezydium Rady.

Zarząd Spółdzielni – na podstawie wyjaśnień Prezesa Zarządu oraz przedłożonej przez Zarząd do badania dokumentacji w postaci protokołu z posiedzenia Zarządu – stwierdzam, że Zarząd w ramach sprawowania swojej funkcji przestrzega ogólnych procedur związanych z bezpieczeństwem ochrony danych osobowych obowiązujących w Spółdzielni. Z podziału obowiązków członków Zarządu wynika sposób przetwarzania danych przez poszczególnych członków, kwestia związana z archiwizacją dokumentów faktycznie realizowana jest w ramach obowiązków służbowych pracowników.

Spółdzielnia spełnia obowiązek informacyjny.

Zarząd Spółdzielni przeprowadza systematyczne audyty stanu ochrony danych osobowych. Z dokumentów wynika, że przeprowadzono w latach 2018 – 2020 łącznie 5 audytów wewnętrznych. Analiza przeprowadzona w ramach badania w latach początkowych zmierzała do wdrożenia nowych procedur związanych z ochroną danych osobowych, systematycznie Zarząd kontrolował ów proces. W badanym okresie odnotowano dwa incydenty naruszenia ochrony danych osobowych, należy poprawić jakość zabezpieczania informacji nie tylko dotyczących danych wrażliwych, ale również informacji poufnych, stanowiących tajemnicę Spółdzielni.

Szczególna sytuacja związana z wprowadzeniem w roku 2020 stanu zagrożenia epidemicznego i w jego następstwie stanu epidemii koronawirusa SARS-COV19 na terenie całego kraju stanowiła podstawę do zmian trybu

pracy pracowników Spółdzielni (i nie tylko) oraz innych ograniczeń np. w zakresie przyjmowania interesantów. W związku z koniecznością wprowadzenia pewnych obostrzeń i ograniczeń – Zarząd wprowadził hybrydowy tryb pracy dla pracowników, zgodnie z oświadczeniem Zarządu wprowadzone zostały dodatkowe zabezpieczenia umożliwiające również świadczenie przez pracowników pracy zdalnej w domach, o bezpieczeństwo informatyczne zadbał współpracujący ze Spółdzielnią informatyk. Pracownicy zostali na tą okoliczność wprowadzeni w nowy tryb pracy, nie zgłaszali żadnych problemów. Obsługa interesantów została usystematyzowana, a bezpośredni kontakt możliwy jest wyłącznie po umówieniu wizyty w ważnych sprawach. Brak możliwości, osobistego załatwiania spraw przez członków spółdzielni i pozostałych mieszkańców, wymaga od pracowników zachowania szczególnej dbałości i ostrożności podczas ujawniania informacji zawierających dane wrażliwe.

Spółdzielnia posiada rozwiązania techniczne, które zapewniają dostęp do dokumentów zawartych na stronie internetowej Spółdzielni tylko osobom uprawnionym - członkom spółdzielni i organom poprzez system logowania się na stronie za pomocą określonego hasła. Pracownicy spółdzielni oraz członkowie organów posiadają indywidualne loginy i hasła (których system wymusza okresowe zmiany), pracują na dokumentach zawierających dane wrażliwe i w sposób zgodny z obowiązującymi procedurami zabezpieczają dokumenty i komputery. Dodatkowo, pracownicy oraz członkowie Zarządu stosują politykę czystego biurka w szczególności: podczas dyżurów z interesantami, a Zarząd także w czasie spotkań z kontrahentami. Polityka czystego biurka ma na celu zabezpieczenie dokumentów wykorzystanych w trakcie wykonywania obowiązków służbowych przed nieuprawnionym dostępem do nich przez osoby trzecie (interesantów, kontrahentów itp.). W ramach polityki dostosowano sposób lokalizacji komputerów (ekranów monitorów) oraz wyznaczono godziny urzędowania dla interesantów (dyżury).

III. Wnioski i rekomendacje:

Kontrola i ocena stanu faktycznego związanego z realizacją wymagań proceduralnych i prawnych z zakresu ochrony danych osobowych prowadzi do wniosku, że standardy i wdrożone procedury wymagają ujednolicenia i aktualizacji oraz drobnych korekt (co zostało szczegółowo omówione powyżej w rekomendacjach audytora).

Jak już wskazano powyżej, w badanym okresie odnotowano dwa incydenty naruszenia ochrony danych osobowych, należy poprawić jakość zabezpieczania informacji i dokumentów. Rekomenduję, wprowadzenie stosownych procedur obiegu dokumentów, w tym w szczególności dokumentów zawierających dane w wrażliwe, ze wskazaniem daty i osoby (stanowiska), które czasowo dysponują dokumentami. Umożliwienie lokalizacji dokumentów zawierających dane osobowe na każdym etapie prac z w/w dokumentami wzmocni kontrolę, a w przypadku nieuprawnionego ujawnienia informacji zakreśli zarówno ramy czasowe jak i osobowe, a także pozwoli na ocenę ryzyk z tym związanych, by zapobiec podobnej sytuacji w przyszłości.

Mając powyższe na uwadze, stwierdzić należy że Spółdzielnia gromadzi i przetwarza dane osobowe stosując się do aktualnie obowiązujących przepisów prawa, cele ich gromadzenia i przetwarzania mieszczą się w działalności statutowej Spółdzielni, a w pozostałym zakresie wynikają z zatrudnienia i współpracy z podmiotami zewnętrznymi wspomagającymi działalność Spółdzielni.

W tym miejscu, zwracam uwagę na zmiany przepisów *Kodeksu Pracy* dotyczące pracowników i kandydatów do pracy – zmianie uległ katalog danych, które pracodawca pozyskuje od pracownika i od osoby biorącej udział w rekrutacji. Przepisy kodeksu pracy różnicują dane osobowe pod względem podstawy ich pozyskiwania – na żądanie pracodawcy zgodnie z kodeksem pracy lub na podstawie zgody pracownika.

Rekomendacje co do dalszego postępowania są następujące:

1. wprowadzenie systematyki zbiorów danych – poprzez opracowanie wykazu zbioru danych, wraz ze wskazaniem rodzaju danych osobowych tam gromadzonych,

2. ograniczenie liczby zbiorów danych,

3. wprowadzenie cyklicznych inwentaryzacji danych wraz z ich bieżącą aktualizacją,

4. analiza ryzyka i ocena skutków dla wybranych zbiorów propozycja środków w celu zmniejszenia ryzyka,

5. opracowanie ewidencji osób posiadających upoważnienia do gromadzenia i przetwarzania danych osobowych,

6. wprowadzenie cyklicznych szkoleń dla pracowników z zasad ochrony danych osobowych wraz z omówieniem bieżących problemów i wypracowaniem rozwiązań, w szczególności w przedmiocie udzielania informacji wnioskodawcom, poprzez właściwą ocenę ich interesu prawnego oraz zbadania podstawy prawnej wniosku,

7. wprowadzenie regulacji dotyczących pracy w oparciu o dokumenty zawierające dane osobowe w wersji papierowej w związku z pełnieniem funkcji w organie nadzoru, w tym także podczas prac poszczególnych Komisji działających przy Radzie Nadzorczej,

8. wprowadzenie regulacji dotyczących pracy zdalnej w zakresie realizowania obowiązków służbowych przez pracowników w oparciu o dokumenty zawierające dane osobowe w formie papierowej.

Stan faktyczny ustalono na podstawie dokumentów przekazanych w toku czynności związanych z badaniem oraz ustnych wyjaśnień i oświadczeń organów Spółdzielni (Rady Nadzorczej i Zarządu) oraz innych informacji mających istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami *o ochronie danych osobowych,* a także po przeprowadzeniu oględzin.

Stan prawny ustalono na podstawie powołanych w treści audytu aktów prawnych obowiązujących przepisów w dacie przeprowadzenia badania.

---

adwokat Kamila Klepas - Kraszka

Podstawa prawna:

1. ustawa z dnia 10 maja 2018 r. *o ochronie danych osobowych*
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
3. ustawa z dnia 16 września 1982 r. *Prawo spółdzielcze*
4. ustawa z dnia 15 grudnia 2000 r. *o spółdzielniach mieszkaniowych*
5. akty wewnętrzne Polityka Bezpieczeństwa, Instrukcja Bezpieczeństwa Informatycznego, Polityka czystego biurka