Annales Canonici 16 (2020) 2 • s. 45-90
DOI: http://dx.doi.org/10.15633/acan.3830

ks. Piotr Lewandowski
ORCID: 0000-0001-5473-1181

Uniwersytet im. Adama Mickiewicza w Poznaniu

Raport szacowania ryzyka doboru środków bezpieczeństwa

Szacowanie ryzyka w zakresie doboru środków bezpieczeństwa na przykładzie większych parafii opiera się na podstawie norm prawa kanonicznego, zwłaszcza dekretu KEP w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim[1], oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych[2]. Jeśli przetwarzanie danych będzie odbywać się w ramach wewnętrznej działalności Kościoła, to przetwarzający będą działać na podstawie wytycznych Dekretu, a w pozostałych przypadkach także na podstawie RODO.

Dekret stosuje się do publicznych kościelnych osób prawnych w zakresie między innymi bezpieczeństwa przetwarzania danych, ich administratora i podmiotu przetwarzającego.

---

1 Dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim wydany przez Konferencję Episkopatu Polski w dniu 13 marca 2018 r., podczas 378. Zebrania Plenarnego w Warszawie, na podstawie kan. 455 Kodeksu Prawa Kanonicznego, w związku z art. 18 Statutu KEP, po uzyskaniu specjalnego zezwolenia Stolicy Apostolskiej z dnia 3 czerwca 2017 r., http://episkopat.pl/wp-content/uploads/2018/04/13.3.2018.PL_.Dekret-ogolny-o-ochronie-danych-osobowych.pdf (3.07.2020) [dalej: Dekret]. Por. P. Kroczek, *Kilka uwag dotyczących Dekretu KEP z 13 marca 2018 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim na podstawie kazusu przedszkola*, „Annales Canonici" 14 (2018), s. 17.

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 (Dz. Urz. UE L Nr 119) [dalej: RODO].

RODO wyznacza stosunkowo niewielki katalog dokumentów obowiązkowych, do których zalicza się rejestry czynności przetwarzania, dokumentację naruszeń ochrony danych osobowych czy dokumentację oceny skutków. Regulacje RODO dotyczące polityki bezpieczeństwa pośrednio zastały wpisane w art. 24 ust 2 RODO i nr 78 preambuły RODO, a pośrednio także w art. 4 pkt 20 RODO, art. 39 ust. 1 lit b RODO[3]. Wszelkiego rodzaju polityki wewnętrzne są przewidziane przez rozporządzenie, o czym mówi także art. 17 i 32 Dekretu. Należy zaznaczyć, że nie jest to dokument, którego posiadanie jest obligatoryjnie i wymagane przez rozporządzenie, tym niemniej na administratorze spoczywa obowiązek udokumentowania przestrzegania norm w zakresie ochrony danych osobowych[4].

Obowiązek przygotowania raportu szacowania ryzyka będącego wynikiem przeprowadzonej analizy ryzyka wynika bezpośrednio z art. 24 RODO (Dz. Urz. UE L z 2016 r., Nr 119/47), zgodnie z którym administrator musi dostosować środki techniczne oraz organizacyjne do określonego ryzyka dla przetwarzanych danych osobowych. Zgodnie z motywem 76 RODO: Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko. Obowiązkiem administratora danych jest uzasadnienie podstawy doboru konkretnych środków oraz rozwiązań, co bez formalnego dokumentu z analizy ryzyka może być trudne lub niemożliwe. W przypadku naruszenia poufności przetwarzanych przez administratora danych osobowych organ nadzorczy będzie sprawdzał, czy administrator danych właściwie oszacował ryzyko dla przetwarzanych danych i dobrał do niego odpowiednie środki zapewniające poufność[5].

RODO daje administratorowi danych dowolność w zakresie wybranej metodologii oraz sposobu dokumentowania przeprowadzenia analizy. Swoje stanowisko dotyczące konieczności udokumentowania przeprowadzonej analizy ryzyka wyraził Urząd Ochrony Danych Osobowych w *Poradniku RODO. Podejście oparte na ryzyku*[6]:

3 Por. RODO (Dz. Urz. UE L Nr 119, s. 15, 34, 47, 56).
4 Por. https://uodo.gov.pl/pl/138/273 (28.05.2018).
5 Dz. Urz. UE L z 2016 r., Nr 119/15.
6 https://uodo.gov.pl/pl/file/706, s. 11 (14.07.2020).

- Uzależnienie środków ochrony przetwarzanych danych od poziomu ryzyka wymaga oszacowania ryzyka i zastosowania środków, które je wyeliminują lub zredukują do akceptowalnego poziomu, np. rezygnacja z usługi zdalnego dostępu do bazy danych osobowych.
- Zasada rozliczalności wymaga, aby proces szacowania ryzyka został przeprowadzony i udokumentowany – w celu wykazania, że ryzyko zostało oszacowane i wprowadzono odpowiednie środki ochrony.
- Zasada rozliczalności oznacza wdrożenie wewnętrznych środków (technicznych i organizacyjnych) zapewniających zgodność przetwarzania z RODO oraz pozostawania w gotowości do wykazania tej zgodności organowi nadzorczemu lub podmiotom, których dane są przetwarzane[7].

Realizacja tego przedsięwzięcia urzeczywistnia się między innymi za pośrednictwem przykładowego, dostosowanego do potrzeb większej parafii raportu szacowania ryzyka oraz doboru środków bezpieczeństwa[8]. W tym sensie są to wszelkie działania zmierzające do zabezpieczenia przetwarzania danych osobowych, których administrator wyznacza cel, podstawy prawne oraz zakres przetwarzania. Zawiera informacje o podmiotach, których dane są udostępniane i przetwarzane, analizuje ryzyko przetwarzania oraz sugeruje sposoby przeciwdziałania[9].

Rozpatrywany raport szacowania ryzyka doboru środków bezpieczeństwa w zakresie ochrony danych osobowych w parafii może przyczynić się do bezpieczniejszego przetwarzania danych osobowych w gąszczu przepisów i zagrożeń. Zwłaszcza że przetwarzanie danych musi być przedmiotem niezależnego nadzoru[10], a kwestie związane z bezpieczeństwem danych należą do kompetencji państwa[11] z wyjątkiem spraw unormowanych w kościelnym porządku prawnym.

---

7 Por. art. 24 RODO (Dz. Urz. UE L z 2016 r., Nr 119/47).

8 Przetwarzanie danych osobowych przez osoby prawne Kościoła katolickiego powinno odbywać się w ramach własnego prawa. Por. M. Poniatowski, *Przetwarzanie danych osobowych w kościelnych organizacjach pożytku publicznego*, w: *Ochrona danych osobowych w Kościele*, red. S. Dziekoński, P. Drobka, Warszawa 2016, s. 171.

9 Por. https://odo24.pl/rodo-uodo/polityka-ochrony-danych-osobowych/ (30.04.2020).

10 Por. G. Buttarelli, *Ochrona danych osobowych w Kościołach i związkach wyznaniowych w świetle ogólnego rozporządzenia o ochronie danych*, w: *Ochrona danych osobowych w Kościele*, dz. cyt., s. 16. Art. 91 RODO stanowi, że „kościoły i związki wyznaniowe [...] podlegają nadzorowi niezależnego organu [...]" (Dz. Urz. UE L z 2016 r., Nr 119/85).

11 Por. A. Mezglewski, *Perspektywa i zakres implementacji nowych przepisów Unii Europejskiej dotyczących przetwarzania danych osobowych przez związki wyznaniowe*, w: *Ochrona danych osobowych w Kościele*, dz. cyt., s. 52.

Metodyka zarządzania ryzykiem w bezpieczeństwie ochrony danych osobowych[12]

I. Definicje pojęć i skrótów stosowanych w procedurze:

- **Zasoby** – wszystko, co stanowi wartość, aktywa parafii;
- **Zagrożenie** – zdarzenie, które może wywołać negatywne skutki; czynnik ryzyka;
- **Podatność** – aspekty, które mogą być wykorzystane przez osoby nieuprawnione / sprzyjać powstaniu zagrożenia; słabość, przyczyna, słaby punkt;
- **Skutek** – efekt wystąpienia zagrożenia, następstwo;
- **Zmaterializowanie się ryzyka** – sytuacja, w której ryzyko zaistniało; wystąpienie ryzyka;
- **Zabezpieczenia** – rozwiązania, które zmniejszają ryzyko; mechanizmy kontroli, środki kontroli;
- **STI** – system teleinformatyczny;
- **KZ** – krytyczne zasoby;
- **PB** – polityka bezpieczeństwa.
- **Postępowanie z ryzykiem** – działania podejmowane w następstwie oceny ryzyka;
- **IOD** – Inspektor Ochrony Danych;
- **ASI** – Administrator Systemu Informatycznego[13];
- **AD** – Administrator Danych.

II. Cel ustanowienia procedury

Celem procedury zarządzania ryzykiem w bezpieczeństwie informacji jest wsparcie PB w zakresie ograniczania do minimum ryzyka dla bezpieczeństwa danych osobowych w parafii, a w szczególności określenie metodyki i zasad zarządzania ryzykiem.

---

12 Por. M. Więckowska, *Metodyka przeprowadzenia oceny skutków dla ochrony danych w ujęciu praktycznym*, uodo.gov.pl/pl/138/605, s. 42–45 (22.04.2020).

13 W tej procedurze przyjęto, że ASI jest organem doradczym, jednakże w innej można na ASI nałożyć określoną odpowiedzialność. Jest to organ ustanowiony wewnętrznie przez administratora danych, więc może zostać on zobligowany do bycia odpowiedzialnym za pewne procesy w zakresie danych osobowych z uwzględnieniem reguł wewnętrznych i innych przepisów – prawa kanonicznego i prawa świeckiego, a w tym kodeksu pracy, kodeksu cywilnego i innych.

III. Metodyka zarządzania ryzykiem

1. Zgodnie z powszechnie stosowanymi metodykami i systemami zarządzania bezpieczeństwem fizycznym, w tym bezpieczeństwem teleinformatycznym, do zaplanowania i realizowania adekwatnych działań zapewniających bezpieczeństwo teleinformatyczne niezbędne jest:
   - dokonanie inwentaryzacji zasobów;
   - określenie zasobów kluczowych;
   - przeprowadzenie oceny ryzyka;
   - podjęcie działań będących następstwem oceny ryzyka.
2. Ocena ryzyka obejmuje:
   - identyfikację ryzyka;
   - analizę ryzyka;
   - ewaluację ryzyka;
   - inwentaryzację ryzyka;
3. Zarządzanie ryzykiem obejmuje m.in. ocenę ryzyka i postępowanie z ryzykiem[14].

IV. Założenia do działań związanych z zarządzaniem ryzykiem doboru środków bezpieczeństwa

1. Oceną ryzyka, jak również sprawozdawczością nie są objęte STI wykorzystywane przez parafię, których administratorem jest podmiot udostępniający system/usługę.
2. W celu efektywnego wykorzystania sił i środków szczegółowej ocenie ryzyka i sprawozdawczości będą poddane KZ.
3. Ocena ryzyka oraz działania z niej wynikające nie ograniczają się jedynie do zagrożeń natury technicznej, lecz uwzględniają również zagrożenia generowane przez użytkowników STI oraz inne strony zainteresowane[15].
4. Na potrzeby oceny ryzyka i przygotowania sprawozdania zidentyfikowane ryzyka dzieli się na:
   - **ryzyko wewnętrzne** – ryzyko, które jest związane z wystąpieniem zagrożenia wewnętrznego lub takiego, na które parafia ma wpływ (działanie albo

---

14 Por. L. Więcaszek-Kuczyńska, *Zagrożenia bezpieczeństwa informacyjnego*, „Obronność. Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2014 nr 2 (10), s. 218–220.

15 Por. K. Pszczółkowski, *Metodyka zarządzania ryzykiem w ochronie danych osobowych*, Warszawa 2018, s. 12–15.

zaniechanie pracownika, dostawcy, awaria urządzenia spowodowana złą eksploatacją itp.);

- **ryzyko zewnętrzne** – ryzyko, które jest związane z wystąpieniem zagrożenia zewnętrznego (działanie cyberprzestępcy, działanie sił przyrody itp.)[16].

v. Odpowiedzialność

1. Odpowiedzialność za przeprowadzenie oceny ryzyka i przygotowanie sprawozdania podsumowującego wyniki oceny ryzyka ponosi AD, dla którego organem doradczym jest IOD[17].
2. Odpowiedzialność za podejmowanie określonych działań w stosunku do zidentyfikowanego ryzyka ponosi AD, dla którego organem doradczym jest ASI / IOD i osoby, którym przypisano podjęcie odpowiedniego przeciwdziałania ryzyku[18].

vi. Sposób przeprowadzania oceny ryzyka

1. Identyfikacja zbiorów, kategorii przetwarzanych danych oraz systemów teleinformatycznych służących do przetwarzania danych osobowych[19].
2. Podział zidentyfikowanych zasobów na: krytyczne i pozostałe.
3. Wybór KZ teleinformatycznych oraz zbiorów przetwarzanych w formie nieelektronicznej.
4. Uwzględniane takich czynników, jak:

a. prawdopodobieństwo naruszenia praw lub wolności osób fizycznych, których dane przetwarzane są przez parafię[20];

---

16 Por. G. Sibiga, *Zadania administratora bezpieczeństwa informacji – wybrane zagadnienia*, w: *Polska i europejska reforma ochrony danych osobowych*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2016, s. 161–162.

17 Por. T. A. J. Banyś, *Wdrażanie nowych elementów systemu ochrony danych osobowych przez podmioty publiczne*, w: *Polska i europejska reforma ochrony danych osobowych*, dz. cyt., s. 57–60.

18 Por. M. Chodorowski, *Nowe prawa i obowiązki administratorów bezpieczeństwa informacji (inspektorów ochrony danych) w świetle najnowszych opinii wydanych przez Grupę Roboczą Art. 29*, w: *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osieja, Warszawa 2017, s. 149–152.

19 Por. M. Cwener, *Nowe obowiązki dokumentacyjne związane z przetwarzaniem danych osobowych*, w: *Ogólne rozporządzenie o ochronie danych osobowych...*, dz. cyt., s. 99–100.

20 Należy podkreślić, że art. 7, p. 2 Dekretu stanowi: „Przetwarzanie danych wrażliwych dopuszczalne jest wyłącznie w stosunku do osób ochrzczonych w Kościele katolickim i tych, którzy po chrzcie

b. ciągłość działania oraz realizowania zadań parafii, które na dzień obecny byłyby niemożliwe do realizacji bez STI;

c. możliwość realizowania konstytucyjnych praw i obowiązków obywatela;

d. zaufanie i ocena parafii.

VII. Identyfikacja ryzyka

1. Identyfikacja zagrożeń związanych z KZ

1.1. Dla każdego z KZ należy zidentyfikować związane z nim zagrożenia, które mogą spowodować m.in.:

a. niedostępność usług;

b. nieuprawniony dostęp do danych / kradzież danych;

c. nieuprawnioną modyfikację danych;

d. zniszczenie danych.

1.2. Na etapie identyfikacji zagrożeń sporządzana jest lista zidentyfikowanych zagrożeń. Identyfikacja zagrożeń dokonywana jest z zastosowaniem m.in. pracy zespołowej (z wykorzystaniem burzy mózgów i innych narzędzi wspomagających pracę zespołową) lub kwestionariuszy i ankiet. Przy identyfikacji zagrożeń wykorzystywane są m.in.:

a. prowadzony rejestr incydentów;

b. wyniki audytów i kontroli;

c. fachowa literatura;

d. specjalistyczne fora internetowe;

e. informacje udostępniane przez producentów oprogramowania i sprzętu.

1.3. Przykładowe zagrożenia dotyczące bezpieczeństwa teleinformatycznego wymieniono w Załączniku nr 1 do niniejszej procedury.

2. Wybór KZ

2.1. W celu skoncentrowania oraz efektywnego wykorzystania sił i środków wybierane są w parafii zagrożenia krytyczne, których liczba waha się od kilku do kilkunastu. Przykład działań poniżej.

---

zostali do niego przyjęci (członków Kościoła), łącznie z tymi, którzy złożyli formalne oświadczenie woli o wystąpieniu z Kościoła katolickiego, zgodnie z wewnętrznymi przepisami Kościoła („byłych członków Kościoła") oraz osób utrzymujących z nim stałe kontakty w związku z realizacją celów Kościoła w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń. Dane te nie są ujawniane poza Kościołem bez zgody osób, których dane dotyczą".

LP.	IDENTYFIKACJA KZ	RODZAJ	UWAGI
1	ZASOBY TELEINFORMATYCZNE	krytyczny	Zależne od wielkości parafii
2	UŻYTKOWNICY	pozostały	
3	ZBIORY DANYCH SZCZEGÓLNYCH	krytyczny	
4	ZBIORY DANYCH ZWYKŁYCH	pozostały	
5	SYSTEM BEZPIECZEŃSTWA FIZYCZNEGO	krytyczny	

2.2. Dokonanie selekcji zagrożeń odbywa się przez podjęcie arbitralnej decyzji osoby odpowiedzialnej za KZ.
2.3. Dopuszcza się również dokonanie wyboru zespołowo, stosując np. głosowanie, ocenę punktową.
2.4. Przeanalizowanie zagrożeń pod względem ich skutków i prawdopodobieństwa wystąpienia.
2.5. Analiza skutków zagrożeń uwzględnia:
a. skutki związane z naruszeniem praw lub wolności osób fizycznych;
b. skutki finansowe dla parafii;
c. skutki związane z nierealizowaniem zadań parafii;
d. skutki związane z zaufaniem i opinią na rynku.
2.6. Analiza prawdopodobieństwa wystąpienia zagrożeń tam, gdzie ma to zastosowanie, uwzględnia:
a. dane historyczne (informacje o zmaterializowaniu ryzyka w parafii i otoczeniu);
b. zabezpieczenia i ich skuteczność (w tym przeciwdziałające, detekcyjne, dające możliwość skutecznej reakcji po wykryciu);
c. podatności (występujące słabości);
d. ekspozycję (czas dostępności, liczba użytkowników, liczba operacji, dostępność przez Internet);

e. atrakcyjność zasobu (m.in. korzyść materialna, prestiż, korzyść polityczna);
f. potencjalnego agresora, jego wiedzę, motywację i zasoby[21].

VIII. Analiza ryzyka[22]

1. Ocena skutków zagrożeń i prawdopodobieństwa ich wystąpienia

Zgromadzone dane na temat skutków i prawdopodobieństwa zagrożeń oceniane są z zastosowaniem poniższej skali punktowej:

- **Skala oceny skutków** – poniżej znajduje się macierz, która ma ułatwić ocenę skutku na właściwym poziomie. Każde zagrożenie analizowane jest pod kątem skutków w czterech aspektach (naruszenie praw i wolności osób, finanse, funkcje i zadania parafii, zaufanie i opinia parafii).

W celu ułatwienia i zapewnienia obiektywnej i wyważonej oceny skutków dla poszczególnych aspektów przyjęto charakterystyki przypisane do odpowiednich poziomów punktowych. Ocena punktowa skutku wyrażana jest jako jedna wartość w przedziale od 1 do 5, co oznacza odpowiednio skutek oceniony jako nieznaczny (1) do bardzo duży (5).

Możliwe jest wystąpienie zagrożenia, które nie będzie oddziaływało na wszystkie cztery aspekty, przykładowo nie będzie oddziaływało na aspekt finansowy, ale jego wpływ np. na naruszenie praw i wolności osób spowoduje wysoką (4 albo 5 punktów) ocenę skutków. Może również wystąpić sytuacja, w której dane zagrożenie będzie niosło za sobą skutki, dla których opis trzech aspektów będzie wskazywał na ocenę na poziomie 1 (np. straty poniżej 100 000, krótkie i nieznaczne zakłócenia w realizacji funkcji i zadań parafii, nieznaczna utrata zaufania), natomiast bardzo

21 Por. P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2016, s. 405–409.

22 „Analiza ryzyka powinna być wykonana przez każdą organizację wdrażającą system zarządzania bezpieczeństwem informacji i mieć na celu doprowadzenie do obniżenia ryzyka do takiego poziomu, w którym organizacja będzie zdolna ponieść ciężar strat spowodowanych przez kradzież lub modyfikację danych. Podstawowymi zadaniami analizy ryzyka jest zatem zidentyfikowanie, dla danego środowiska przetwarzania (środowisko informatyczne, zabezpieczenia fizyczne do obiektów, nośników danych, serwerów, stacji roboczych, mediów transmisyjnych itp.) naturalnych zagrożeń i oszacowanie potencjalnych skutków ich wystąpienia, a następnie wyszukanie i zaproponowanie środków redukujących prawdopodobieństwo i/lub skutki ich wystąpienia. Proces taki może przebiegać według różnych schematów" (Generalny Inspektor Ochrony Danych Osobowych, *Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa*, archiwum.giodo.gov.pl/163/id_art/1063/j/p (23.04.2020), s. 67.

wysoka ocena w jednym aspekcie (np. naruszenie praw i wolności osób) spowoduje całościową ocenę skutków na poziomie 4 czy nawet 5 punktów.

Ocenę skutków można przeprowadzić, stosując metody matematyczne, np. dokonując oceny punktowej w poszczególnych aspektach i wyliczenia średniej. Jednakże wyrażona punktowo ocena jest wynikiem analizy, zaś poniższa macierz ma charakter jedynie wspomagający. Określając wartość skutku, zakładany jest możliwy, ale najbardziej negatywny scenariusz wystąpienia zagrożenia. Przy ocenie skutków uwzględniane są zabezpieczenia, które mają na celu zmniejszenie skutków[23].

Ocena	Poziom (S)	Skutki związane z naruszeniem praw i wolności osób, których dane są przetwarzane	Skutki finansowe dla parafii	Skutki związane z nierealizowaniem funkcji i zadań parafii	Skutki związane z zaufaniem i opinią dot. parafii
1	nieznaczny	Nieznaczne naruszenie	Straty nieznacznie wpływające na działanie parafii	Krótkotrwałe i nieznaczne zakłócenia w realizacji funkcji i zadań	Nieznaczna utrata zaufania i opinii
2	mały	Niewielkie naruszenie	Straty mające mały wpływ na działanie parafii	Niewielkie zakłócenia w realizacji funkcji i zadań	Niewielka utrata zaufania i opinii
3	średnie	Poważne naruszenie	Straty średnio wpływające na działanie parafii	Poważne zakłócenia w realizacji funkcji i zadań	Poważna utrata zaufania i opinii

23 Por. M. Mazur, *Analiza ryzyka a ocena skutków dla ochrony danych*, https://uodo.gov.pl/pl/138/605 (29.04.2020), s. 34–38; D. Lubasz, *Europejska reforma ochrony danych osobowych – nowe obowiązki administratorów w ogólnym rozporządzeniu o ochronie danych*, w: *Polska i europejska reforma ochrony danych osobowych*, dz. cyt., s. 80–82.

Ocena	Poziom (S)	Skutki związane z naruszeniem praw i wolności osób, których dane są przetwarzane	Skutki finansowe dla parafii	Skutki związane z nierealizowaniem funkcji i zadań parafii	Skutki związane z zaufaniem i opinią dot. parafii
4	duży	Poważne i trwałe naruszenie	Straty mające duży wpływ na działanie parafii	Poważne i trwałe zakłócenia w realizacji funkcji i zadań	Poważna i trwała utrata zaufania i opinii
5	bardzo duży	Bardzo poważne naruszenie praw i wolności	Straty paraliżujące działalność parafii	Poważny i długotrwały brak realizacji funkcji i zadań	Poważna i długotrwała utrata zaufania i opinii

- **Skala oceny prawdopodobieństwa** – przy ocenie prawdopodobieństwa analizowane jest zagrożenie uwzględniające charakterystyki umieszczone w kolumnie *Opis wspomagający*. W przypadku wystąpienia sytuacji, w której poszczególne charakterystyki występują w różnych przedziałach punktowych, ocena oparta jest na osądzie oceniających prawdopodobieństwo. W przypadku oceny danych historycznych uwzględniane są dane posiadane w parafii, jak również informacje z otoczenia. Analiza podatności uwzględnia znane i występujące w rzeczywistości podatności. W sytuacji, w której jedna albo więcej charakterystyk nie miała zastosowania, nie jest uwzględniana, np. zagrożenie może nie być wywołane celowym działaniem pracownika lub innej strony zainteresowanej (w tym wypadku nie odnosi się do cyberprzestępcy)[24].

24 Por. M. Więckowska, *Stosowanie technicznych środków bezpieczeństwa w aspekcie zgłoszeń naruszeń do* UODO *oraz ocena wagi naruszenia w oparciu o zalecenia Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (*ENISA*)*, www.uodo.gov.pl (21.04.2020), s. 42–44.

OCENA	POZIOM (P)	OPIS WSPOMAGAJĄCY
1	BARDZO MAŁO PRAWDOPODOBNE	Dane historyczne: Nie występują Zabezpieczenia: Liczne i bardzo skuteczne Podatności: Brak Atrakcyjność: Bardzo mała Ekspozycja: Nieistotna Cyberprzestępca: Przypadkowy
2	MAŁO PRAWDOPODOBNE	Dane historyczne: Bardzo nieliczne wystąpienia Zabezpieczenia: Liczne i skuteczne Podatności: Bardzo nieliczne Atrakcyjność: Mała Ekspozycja: Bardzo małe znaczenie Cyberprzestępca: Nieprofesjonalny, mający małą wiedzę
3	PRAWDOPODOBNE	Dane historyczne: Nieliczne wystąpienia Zabezpieczenia: Liczne i częściowo skuteczne Podatności: Nieliczne Atrakcyjność: Średnia Ekspozycja: Małe znaczenie Cyberprzestępca: Profesjonalny, mający odpowiednią wiedzę
4	BARDZO PRAWDOPODOBNE	Dane historyczne: Wystąpienia Zabezpieczenia: Nieliczne i mało skuteczne Podatności: Liczne Atrakcyjność: Duża Ekspozycja: Duże znaczenie Cyberprzestępca: Profesjonalny, mający odpowiednią wiedzę i zmotywowany
5	PEWNE	Dane historyczne: Liczne wystąpienia Zabezpieczenia: Brak albo nieliczne i nieskuteczne Podatności: Bardzo liczne Atrakcyjność: Bardzo duża Ekspozycja: Bardzo duże znaczenie Cyberprzestępca: Profesjonalny, mający odpowiednią wiedzę, zmotywowany i wyposażony w niezbędne zasoby, w tym finansowe

2. Ustalenie PR

PR jest obliczany jako iloczyn skutków (S) i prawdopodobieństwa (P), tj. PR= S x P

3. Ewaluacja ryzyka dokonywana jest według poniższej tabeli

KRYTERIA		EWALUACJA RYZYKA
WARTOŚĆ PUNKTOWA PR	PR	
1-5	**MAŁE**	Akceptowalne
6-9	**ŚREDNIE**	Akceptowalne, wymagające decyzji AD i IOD
10-16 oraz 5 gdzie: P = 1, a S = 5	**DUŻE**	Nieakceptowalne, wymagające decyzji AD i IOD w zakresie dalszego postępowania z ryzykiem
18-25	**BARDZO DUŻE**	Nieakceptowalne, wymagające decyzji AD w zakresie dalszego postępowania z ryzykiem

IX. Podjęcie decyzji dotyczącej postępowania z ryzykiem

W stosunku do ryzyka podejmowane są następujące decyzje:

- zapobieganie, czyli działania polegające na zmniejszeniu PR;
- przeniesienie ryzyka na inną jednostkę (przenosząc ryzyko, należy pamiętać, że jego przeniesienie najczęściej nie zmniejsza odpowiedzialności za jego wystąpienie, co ma istotne znaczenie z punktu widzenia działania parafii);
- unikanie, czyli m.in. zaprzestanie działań powodujących ryzyko;
- tolerowanie (akceptowanie) ryzyka w przypadku, gdy istnieją określone trudności w przeciwdziałaniu ryzykom lub gdy koszty planowanych działań doskonalących mogą przekroczyć przewidywane korzyści.

X. Monitorowanie ryzyka

1. Podstawowym celem monitorowania ryzyka jest uzyskanie potwierdzenia, że wdrożona procedura jest skuteczna.

2. Równie ważne jest wykrywanie sytuacji, gdy środki ochrony są niewystarczające bądź funkcjonowanie procedury sytuuje się poniżej przyjętych standardów.
3. W obu przypadkach konieczne jest podejmowanie zdecydowanych działań doskonalących.
4. Proces monitorowania ryzyka składa się z następujących elementów:
   a. Wejście: wszystkie uzyskane informacje z systemu zarządzania ryzykiem,
   b. Działanie: obserwacja ryzyka i czynników ryzyka[25],
   c. Wyjście: ciągłe dostrajanie systemu zarządzania ryzykiem.
5. Proces monitorowania ryzyka ma charakter ciągły.
6. Podczas etapu monitorowania powinny być zbierane również informacje o tym, jak zmieniają się ryzyka:
   • Czy zmieniły się zagrożenia?
   • Czy zmieniły się podatności?
   • Czy zmieniło się prawdopodobieństwo wystąpienia ryzyka?
   • Czy zmienił się wpływ skutków zaistniałego ryzyka?
   • Czy działania dla złagodzenia ryzyka są nadal odpowiednie?

XI. Informowanie o ryzyku

Komunikowanie ryzyka polega na wzajemnej wymianie informacji dotyczących ryzyka między odpowiedzialnymi za zarządzanie ryzykiem a zainteresowanymi stronami[26].

Powinno prowadzić do wzrostu świadomości ryzyka wśród obsługi parafii, co może wspierać naturalne mechanizmy kontroli wewnętrznej.

XII. Działania związane z zarządzaniem ryzykiem

1. Na podstawie przedstawionej powyżej metodyki przynajmniej raz w roku podczas przeglądu PB oraz po każdej istotnej zmianie w parafii mogącej mieć wpływ na ryzyko dokonuje się identyfikacji i oceny ryzyka oraz określa metody przeciwdziałania ryzyku.

---

25 Por. M. Więckowska, *Stosowanie technicznych środków bezpieczeństwa w aspekcie zgłoszeń naruszeń do UODO oraz ocena wagi naruszenia w oparciu o zalecenia Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)*, www.uodo.gov.pl (21.04.2020).

26 Zob. art. 8 Dekretu.

2. Wykonywany jest także przegląd procesu zarządzania ryzykiem w celu jego usprawnienia.
3. Na podstawie wyników powyższych działań sporządza się arkusz sprawozdania podsumowującego wyniki analizy ryzyka zgodnie z wzorem stanowiącym Załącznik nr 2 do niniejszej procedury.
4. Jednocześnie stale realizowany jest proces monitorowania ryzyka.
5. Podstawowym źródłem danych do monitorowania ryzyka jest proces zarządzania incydentami związanymi z bezpieczeństwem informacji.

Załącznik nr 1

Przykładowe zagrożenia dotyczące bezpieczeństwa informacji. Zagrożenia z Załącznika nr 2 – analiza ryzyka winny być tożsame ze wszystkimi rodzajami ryzyka z Załącznika nr 1. Jednakże dla celu artykułu postanowiono zaprezentować wariacje ryzyka, które mogłyby być analizowane w tabeli z Załącznika nr 2.

1. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) przez korespondencję elektroniczną.
2. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) przez stronę www.
3. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) przez nośniki zewnętrzne.
4. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) w instalowanym oprogramowaniu.
5. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) w trakcie naprawy lub serwisu.
6. Wykorzystanie luk w systemach urządzeń mobilnych.
7. Atak zewnętrzny ograniczający dostęp typu DDoS.
8. Przejęcie informacji przesyłanych pocztą elektroniczną.
9. Podsłuchanie informacji przesyłanych siecią radiową (informatyczną).
10. Podsłuchanie informacji przesyłanych siecią tradycyjną.
11. Włamanie do STI.
12. Atak socjotechniczny w celu przejęcia danych (*phishing*).
13. Przekierowanie – *pharming*.
14. Nieuprawniony fizyczny dostęp do urządzeń.

15. Nieuprawniony dostęp do nośników danych (m.in. optycznych, magnetycznych).
16. Brak zasilania energetycznego.
17. Zalanie wodą lub innymi substancjami z instalacji wewnętrznych.
18. Pożar.
19. Powódź.
20. Przegrzanie sprzętu.
21. Awaria sprzętu.
22. Zły stan techniczny sprzętu.
23. Niewydolne urządzenia (zbyt wolne, nieodpowiadające wymaganiom programowym).
24. Niestabilność łącza w usłudze dostępu do internetu.
25. Niewystarczająca przepustowość łącza w usłudze dostępu do internetu.
26. Używanie oprogramowania niemającego wsparcia producenta.
27. Kradzież sprzętu z siedziby parafii.
28. Kradzież sprzętu mobilnego.
29. Podejrzenie informacji w siedzibie parafii.
30. Podejrzenie informacji przetwarzanej na sprzęcie mobilnym.
31. Błędy uprawnionych użytkowników – niezapisanie danych.
32. Błędy uprawnionego użytkownika – skasowanie danych.
33. Błąd uprawnionego użytkownika – wysłanie informacji pocztą elektroniczną do nieuprawnionej osoby.
34. Błąd uprawnionego użytkownika – administratora – błędna konfiguracja dająca nadmierne uprawnienia.
35. Celowe działanie uprawnionych użytkowników – zniszczenie informacji.
36. Celowe działanie uprawnionych użytkowników – sprzedaż informacji.
37. Celowe działanie uprawnionych użytkowników – sabotaż.
38. Celowe działanie uprawnionych użytkowników – nadużycie uprawnień.
39. Celowe działanie – zniszczenie sprzętu.
40. Brak świadomości użytkowników STI na temat ryzyka (zagrożeń, podatności, skutków).
41. Brak znajomości zasad i procedur bezpieczeństwa.
42. Zbyt rzadko zmieniane hasła.
43. Zbyt słabe hasła.
44. Zbyt często zmieniane hasła.
45. Nieprzestrzeganie przez użytkowników STI zasad i procedur bezpieczeństwa.

46. Nieprawidłowe zarządzanie uprawnieniami użytkowników – nadanie nadmiernych uprawnień.
47. Nieprawidłowe zarządzanie uprawnieniami użytkowników (brak cofnięcia albo zbyt późne cofnięcie uprawnień).
48. Źle skonfigurowane, w tym otwarte porty.
49. Źle skonfigurowane systemy operacyjne.
50. Brak zabezpieczeń protokołów komunikacyjnych.
51. Kradzież zbiorów danych szczególnych.
52. Kradzież zbiorów danych zwykłych.
53. Zniszczenie zbiorów danych szczególnych.
54. Zniszczenie zbiorów danych zwykłych.
55. Udostępnienie zbiorów danych przetwarzanych w formie papierowej osobom nieuprawnionym[27].

27 Por. M. Mazur, *Analiza ryzyka a ocena skutków dla ochrony danych*, dz. cyt., s. 25–28.

Załącznik nr 2

Raport z oceny ryzyka i doboru środków bezpieczeństwa

KZ	Identyfikacja ryzyka			Analiza ryzyka			Ewaluacja ryzyka	Sposób postępowania z ryzykiem przyjętym w parafii
	Rodzaj ryzyka	Zdarzenie (dodatkowo można krótko opisać jego skutki i prawdopodobieństwo)	Podatność	Ocena (S)	Ocena (P)	PR = S x P		
KZ – 1	Zgodnie z Załącznikiem 1	Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) przez korespondencję elektroniczną.	Stacje robocze Użytkownicy	1	3	3	Akceptowalne	Zabezpieczenie stacji roboczych oprogramowaniem antywirusowym skanującym pocztę elektroniczną, wdrożenie instrukcji korzystania z Internetu oraz poczty elektronicznej.
KZ – 1	Zgodnie z Załącznikiem 1	Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) przez stronę www.	Stacje robocze Użytkownicy	1	3	3	Akceptowalne	Zabezpieczenie stacji roboczych oprogramowaniem antywirusowym skanującym przeglądarkę internetową oraz ściągane treści, wdrożenie instrukcji korzystania z Internetu oraz poczty elektronicznej.

KZ – 1	Zgodnie z Załącznikiem 1	Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) przez nośniki zewnętrzne.	Stacje robocze Użytkownicy	1	3	3	Akceptowalne	Zabezpieczenie stacji roboczych poprzez blokowanie portów USB, stacji CD, wdrożenie instrukcji korzystania z Internetu oraz poczty elektronicznej.
KZ – 1	Zgodnie z Załącznikiem 1	Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) w instalowanym oprogramowaniu.	Stacje robocze Użytkownicy	1	3	3	Akceptowalne	Zabezpieczenie stacji roboczych poprzez blokowanie portów USB, stacji CD. Zabezpieczenie instalowania oprogramowania przez hasło AD, wdrożenie instrukcji korzystania z Internetu oraz poczty elektronicznej.
KZ – 1	Zgodnie z Załącznikiem 1	Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) w trakcie naprawy lub serwisu.	Stacje robocze, nośniki danych	1	3	3	Akceptowalne	Umowa powierzenia oraz umowa na wykonywanie usług serwisowych IT.
KZ - 1	Zgodnie z Załącznikiem 1	Przejęcie informacji przesyłanych pocztą elektroniczną.	Stacje robocze Użytkownicy	1	3	3	Akceptowalne	Potwierdzenie tożsamości odbiorcy poprzez weryfikację adresu email, korzystanie

KZ	Identyfikacja ryzyka			Analiza ryzyka			Ewaluacja ryzyka	Sposób postępowania z ryzykiem przyjętym w parafii
	Rodzaj ryzyka	Zdarzenie (dodatkowo można krótko opisać jego skutki i prawdopodobieństwo)	Podatność	Ocena (S)	Ocena (P)	PR = S x P		
								z zatwierdzonych przez AD usług świadczonych drogą elektroniczną, korzystanie z szyfrowanych łączy i stron WWW.
KZ – 1	Zgodnie z Załącznikiem 1	Przekierowanie – *pharming*.	Stacje robocze Użytkownicy	1	3	3	Akceptowalne	Potwierdzenie tożsamości nadawcy, nieotwieranie załączników poczty pochodzącej od nieznanego nadawcy, wdrożenie instrukcji korzystania z Internetu oraz poczty elektronicznej.
KZ – 1	Zgodnie z Załącznikiem 1	Nieuprawniony fizyczny dostęp do urządzeń.	Stacje robocze	1	3	3	Akceptowalne	Właściwe zabezpieczenie fizyczne pomieszczeń, procedura przebywania osób trzecich w strefach przetwarzania.

KZ – 1	Zgodnie z Załącznikiem 1	Nieuprawniony dostęp do nośników danych (m.in. optycznych, magnetycznych).	Nośniki danych Stacje robocze	1	3	3	Akceptowalne	Właściwe zabezpieczenie fizyczne pomieszczeń, procedura przebywania osób trzecich w strefach przetwarzania, polityka czystego biurka.
KZ – 1	Zgodnie z Załącznikiem 1	Brak zasilania energetycznego.	Stacje robocze	1	3	3	Akceptowalne	Stacje robocze zabezpieczone urządzeniami UPS, procedura zakończenia pracy w przypadku utraty zasilania.
KZ – 1	Zgodnie z Załącznikiem 1	Pożar.	Pomieszczenia biurowe Budynek	4	2	8	Średnie	Wyznaczenie inspektora ppoż., szkolenia ppoż., wyposażenie budynku w sprzęt gaśniczy oraz procedury ewakuacji na wypadek pożaru.
KZ – 1	Zgodnie z Załącznikiem 1	Niestabilność łącza w usłudze dostępu do Internetu.	Stacje robocze	1	2	2	Akceptowalne	Umowa na świadczenie usług serwisowych.
KZ – 1	Zgodnie z Załącznikiem 1	Używanie oprogramowania niemającego wsparcia producenta.	Stacje robocze	1	2	2	Akceptowalne	Aktualizacja oprogramowania, używanie programów mających wsparcie producenta, zmiana oprogramowania.

KZ	Identyfikacja ryzyka			Analiza ryzyka			Ewaluacja ryzyka	Sposób postępowania z ryzykiem przyjętym w parafii
	Rodzaj ryzyka	Zdarzenie (dodatkowo można krótko opisać jego skutki i prawdopodobieństwo)	Podatność	Ocena (S)	Ocena (P)	PR = S x P		
KZ – 1	Zgodnie z Załącznikiem 1	Błędy uprawnionych użytkowników – niezapisanie danych.	Użytkownik	1	3	3	Akceptowalne	Włączenie funkcji autozapisu w używanym oprogramowaniu.
KZ - 1	Zgodnie z Załącznikiem 1	Błędy uprawnionego użytkownika – skasowanie danych.	Użytkownik	1	3	3	Akceptowalne	Procedura archiwizowania danych na stacjach roboczych i zewnętrznych nośnikach.
KZ – 1	Zgodnie z Załącznikiem 1	Błąd uprawnionego użytkownika – wysłanie informacji pocztą elektroniczną do nieuprawnionej osoby.	Użytkownik	1	3	3	Akceptowalne	Weryfikacja odbiorcy przed wysłaniem poczty, wdrożenie instrukcji korzystania z Internetu oraz poczty elektronicznej.
KZ – 1	Zgodnie z Załącznikiem 1	Źle skonfigurowane, w tym otwarte porty.	Administrator Informatyk	1	4	4	Akceptowalne	Zamknięcie dostępu do portów przez urządzenia zewnętrzne, przypisanie urządzeń adresami IP do określonych stacji roboczych.
ŚREDNIA OCENA RYZYKA W OBSZARZE KZ – 1				**1,17**	**2,88**	**3,36**	**Akceptowalne**	

KZ – 2	Zgodnie z Załącznikiem 1	Nieuprawniony dostęp do nośników danych (m.in. optycznych, magnetycznych).	Nośniki danych Stacje robocze	1	3	3	Akceptowalne	Właściwe zabezpieczenie fizyczne pomieszczeń, procedura przebywania osób trzecich w strefach przetwarzania, polityka czystego biurka.
KZ – 2	Zgodnie z Załącznikiem 1	Kradzież sprzętu z siedziby parafii.	Stacje robocze Nośniki danych	1	3	3	Akceptowalne	Właściwe zabezpieczenie fizyczne pomieszczeń, procedura przebywania osób trzecich w strefach przetwarzania, umowy z firmami świadczącymi usługi, np. sprzątania pomieszczeń, instrukcja wydawania kluczy, polityka czystego biurka.
KZ – 2	Zgodnie z Załącznikiem 1	Celowe działanie uprawnionych użytkowników – zniszczenie informacji.	Użytkownik	1	2	2	Akceptowalne	Okresowe szkolenia podnoszące świadomość pracownika, przyjęcie oświadczenia o zachowaniu poufności.

KZ	Identyfikacja ryzyka			Analiza ryzyka			Ewaluacja ryzyka	Sposób postępowania z ryzykiem przyjętym w parafii
	Rodzaj ryzyka	Zdarzenie (dodatkowo można krótko opisać jego skutki i prawdopodobieństwo)	Podatność	Ocena (S)	Ocena (P)	PR = S x P		
KZ – 2	Zgodnie z Załącznikiem 1	Celowe działanie uprawnionych użytkowników – sprzedaż informacji.	Użytkownik	3	2	6	Średnie	Okresowe szkolenia podnoszące świadomość pracownika, przyjęcie oświadczenia o zachowaniu poufności.
KZ - 2	Zgodnie z Załącznikiem 1	Celowe działanie uprawnionych użytkowników – nadużycie uprawnień.	Użytkownik	2	2	4	Akceptowalne	Okresowe szkolenia podnoszące świadomość pracownika, przyjęcie oświadczenia o zachowaniu poufności.
KZ – 2	Zgodnie z Załącznikiem 1	Brak świadomości użytkowników STI na temat ryzyk (zagrożeń, podatności, skutków).	Użytkownik	1	3	3	Akceptowalne	Okresowe szkolenia podnoszące świadomość pracownika, doraźne kontrole przestrzegania procedur.
KZ – 2	Zgodnie z Załącznikiem 1	Brak znajomości zasad i procedur bezpieczeństwa.	Użytkownik Pracownicy	1	3	3	Akceptowalne	Szkolenia podnoszące świadomość pracownika, doraźne kontrole przestrzegania procedur.

KZ – 2	Zgodnie z Załącznikiem 1	Zbyt rzadko zmieniane hasła.	Użytkownik Stacje robocze	1	4	4	Akceptowalne	Wdrożenie procedur zmiany haseł, ustawienie STI wymuszające zmianę haseł.
KZ – 2	Zgodnie z Załącznikiem 1	Zbyt słabe hasła.	Użytkownik Stacje robocze	1	4	4	Akceptowalne	Wdrożenie procedur zmiany haseł, ustawienie STI wymuszające ustawienia odpowiedniej siły haseł.
KZ – 2	Zgodnie z Załącznikiem 1	Nieprzestrzeganie przez użytkowników STI zasad i procedur bezpieczeństwa.	Użytkownik Stacje robocze	1	4	4	Akceptowalne	Szkolenia podnoszące świadomość pracownika, doraźne kontrole przestrzegania procedur.
KZ – 2	Zgodnie z Załącznikiem 1	Nieprawidłowe zarządzanie uprawnieniami użytkowników (brak cofnięcia albo zbyt późne cofnięcie uprawnień).	Administrator Informatyk	1	2	2	Akceptowalne	Szkolenia podnoszące świadomość pracownika, doraźne kontrole przestrzegania procedur nadawania i usuwania uprawnień.
KZ – 2	Zgodnie z Załącznikiem 1	Kradzież zbiorów danych szczególnych.	Pracownik	3	2	6	Średnie	Szkolenia podnoszące świadomość pracownika, doraźne kontrole przestrzegania procedur. Wdrożenie

KZ	Identyfikacja ryzyka			Analiza ryzyka			Ewaluacja ryzyka	Sposób postępowania z ryzykiem przyjętym w parafii
	Rodzaj ryzyka	Zdarzenie (dodatkowo można krótko opisać jego skutki i prawdopodobieństwo)	Podatność	Ocena (S)	Ocena (P)	PR = S x P		
								procedur zmiany haseł, ustawienie STI wymuszające zmianę haseł. Zabezpieczenie fizyczne pomieszczeń, w których przetwarzane są zbiory w formie papierowej.
KZ - 2	Zgodnie z Załącznikiem 1	Kradzież zbiorów danych zwykłych.	Pracownik	3	2	6	Średnie	Szkolenia podnoszące świadomość pracownika, doraźne kontrole przestrzegania procedur; Wdrożenie procedur zmiany haseł, ustawienie STI wymuszające zmianę haseł; Zabezpieczenie fizyczne pomieszczeń, w których przetwarzane są zbiory w formie papierowej.

KZ – 2	Zgodnie z Załącznikiem 1	Zniszczenie zbiorów danych szczególnych.	Pracownik	2	2	4	Akceptowalne	Szkolenia podnoszące świadomość pracownika, doraźne kontrole przestrzegania procedur. Wdrożenie procedur zmiany haseł, ustawienie STI wymuszające zmianę haseł. Zabezpieczenie fizyczne pomieszczeń, w których przetwarzane są zbiory w formie papierowej.
KZ - 2	Zgodnie z Załącznikiem 1	Zniszczenie zbiorów danych zwykłych.	Pracownik	2	2	4	Akceptowalne	Szkolenia podnoszące świadomość pracownika, doraźne kontrole przestrzegania procedur. Wdrożenie procedur zmiany haseł, ustawienie STI wymuszające zmianę haseł. Zabezpieczenie fizyczne pomieszczeń, w których przetwarzane są zbiory w formie papierowej.

KZ	Identyfikacja ryzyka			Analiza ryzyka			Ewaluacja ryzyka	Sposób postępowania z ryzykiem przyjętym w parafii
	Rodzaj ryzyka	Zdarzenie (dodatkowo można krótko opisać jego skutki i prawdopodobieństwo)	Podatność	Ocena (S)	Ocena (P)	PR = S x P		
KZ – 2	Zgodnie z Załącznikiem 1	Udostępnienie zbiorów danych przetwarzanych w formie papierowej osobom nieuprawnionym.	Użytkownik przetwarzający / Pracownik	2	2	4	Akceptowalne	Szkolenia podnoszące świadomość pracownika, doraźne kontrole przestrzegania procedur. Wdrożenie procedur zmiany haseł, ustawienie STI wymuszające zmianę haseł. Zabezpieczenie fizyczne pomieszczeń, w których przetwarzane są zbiory w formie papierowej.
Średnia ocena ryzyka w obszarze KZ – 2				1,62	2,62	4,24	Akceptowalne	
KZ – 3	Zgodnie z Załącznikiem 1	Kradzież sprzętu z siedziby parafii zawierających na dysku dane „szczególne”.	Stacje robocze Nośniki danych	1	3	3	Akceptowalne	Właściwe zabezpieczenie fizyczne pomieszczeń, procedura przebywania osób trzecich w strefach przetwarzania, umowy z firmami świadczącymi usługi

								np. sprzątania pomieszczeń, instrukcja wydawania kluczy, polityka czystego biurka. Nadzór nad nośnikami.
KZ – 3	Zgodnie z Załącznikiem 1	Kradzież zbiorów danych szczególnych.	Nośniki Bazy	3	2	6	Średnie	Planowane i doraźne kontrole przestrzegania procedur przez ASI. Wdrożenie procedur zmiany haseł, ustawienie STI wymuszające zmianę haseł. Zabezpieczenie fizyczne pomieszczeń, w których przetwarzane są zbiory w formie papierowej.
KZ – 3	Zgodnie z Załącznikiem 1	Zniszczenie zbiorów danych szczególnych.	Bazy, zbiory danych	2	2	4	Akceptowalne	Szkolenia podnoszące świadomość pracownika, doraźne kontrole przestrzegania procedur. Wykonywanie kopii zgodnie z procedurą. Polityka antywirusowa.

KZ	Identyfikacja ryzyka			Analiza ryzyka			Ewaluacja ryzyka	Sposób postępowania z ryzykiem przyjętym w parafii
	Rodzaj ryzyka	Zdarzenie (dodatkowo można krótko opisać jego skutki i prawdopodobieństwo)	Podatność	Ocena (S)	Ocena (P)	PR = S x P		
KZ – 3	Zgodnie z Załącznikiem 1	Udostępnienie zbiorów danych szczególnych przetwarzanych w systemie informatycznym i formie papierowej osobom nieuprawnionym.	Zbiory danych szczególnych Zbiory danych szczególnych w formie papierowej	2	2	4	Akceptowalne	Szkolenia podnoszące świadomość pracownika, doraźne kontrole przestrzegania procedur. Zasada „dwóch par oczu”.
KZ – 3	Zgodnie z Załącznikiem 1	Nieprawidłowe zarządzanie uprawnieniami użytkowników (brak cofnięcia albo zbyt późne cofnięcie uprawnień do systemów informatycznych) do zbiorów szczególnych.	Zbiory szczególne w systemie informatycznym	1	2	2	Akceptowalne	Szkolenia podnoszące świadomość ASI. Nadzór IOD. Komunikacja pomiędzy: kadry–IOD–ASI.
KZ – 3	Zgodnie z Załącznikiem 1	Nieprawidłowe zarządzanie uprawnieniami do wejścia w obszar przetwarzania danych szczególnych.	Zbiory szczególne w formie papierowej, informatycznej nośniki	1	2	2	Akceptowalne	Polityka uprawnień do pobierania kluczy, systemów alarmowych. Okresowe kontrole przełożonych, IOD.

KZ – 3	Zgodnie z Załącznikiem 1	Nieprawidłowe zabezpieczenie przesyłek (dokumentów w dowolnej formie) zawierających dane szczególne poza obszarem przetwarzania	Zbiory szczególne w formie papierowej, informatycznej nośniki	1	2	2	Akceptowalne	Przestrzeganie procedur dot. zgód na przetwarzanie poza obszarem przetwarzania, świadomość pracowników, okresowe szkolenia, przestrzeganie procedury przetwarzania danych na urządzeniach mobilnych. Brak umów powierzenia.
ŚREDNIA OCENA RYZYKA W OBSZARZE KZ – 3				1,57	2,14	3,29	Akceptowalne	
KZ – 4	Zgodnie z Załącznikiem 1	Kradzież sprzętu z siedziby parafii zawierających na dysku dane zwykłe.	Stacje robocze Nośniki danych	1	2	2	Akceptowalne	Właściwe zabezpieczenie fizyczne pomieszczeń, procedura przebywania osób trzecich w strefach przetwarzania, umowy z firmami świadczącymi usługi np. sprzątania pomieszczeń, instrukcja wydawania kluczy, polityka czystego biurka. Nadzór nad nośnikami.

KZ	Identyfikacja ryzyka			Analiza ryzyka			Ewaluacja ryzyka	Sposób postępowania z ryzykiem przyjętym w parafii
	Rodzaj ryzyka	Zdarzenie (dodatkowo można krótko opisać jego skutki i prawdopodobieństwo)	Podatność	Ocena (S)	Ocena (P)	PR = S x P		
KZ – 4	Zgodnie z Załącznikiem 1	Kradzież zbiorów danych zwykłych.	Nośniki Bazy	2	2	4	Akceptowalne	Planowane i doraźne kontrole przestrzegania procedur przez ASI. Wdrożenie procedur zmiany haseł, ustawienie STI wymuszające zmianę haseł. Zabezpieczenie fizyczne pomieszczeń, w których przetwarzane są zbiory w formie papierowej.
KZ - 4	Zgodnie z Załącznikiem 1	Zniszczenie zbiorów danych zwykłych.	Bazy, zbiory danych	2	2	4	Akceptowalne	Szkolenia podnoszące świadomość pracownika, doraźne kontrole przestrzegania procedur. Wykonywanie kopii zgodnie z procedurą. Polityka antywirusowa.

KZ – 4	Zgodnie z Załącznikiem 1	Udostępnienie zbiorów danych szczególnych przetwarzanych w systemie informatycznym i formie papierowej osobom nieuprawnionym.	Zbiory danych szczególnych Zbiory danych szczególnych w formie papierowej	2	2	4	Akceptowalne	Szkolenia podnoszące świadomość pracownika, doraźne kontrole przestrzegania procedur. Zasada „dwóch par oczu”.
KZ – 4	Zgodnie z Załącznikiem 1	Nieprawidłowe zarządzanie uprawnieniami użytkowników (brak cofnięcia albo zbyt późne cofnięcie uprawnień do systemów informatycznych) do zbiorów zwykłych.	Zbiory szczególne w systemie informatycznym	1	2	2	Akceptowalne	Szkolenia podnoszące świadomość ASI. Nadzór IOD. Komunikacja pomiędzy: kadry–IOD–ASI.
KZ – 4	Zgodnie z Załącznikiem 1	Nieprawidłowe zarządzanie uprawnieniami do wejścia w obszar przetwarzania danych zwykłych.	Zbiory szczególne w formie papierowej, informatycznej	1	2	2	Akceptowalne	Polityka uprawnień do pobierania kluczy, systemów alarmowych. Okresowe kontrole przełożonych, IOD.
KZ – 4	Zgodnie z Załącznikiem 1	Nieprawidłowe zabezpieczenie przesyłek (dokumentów w dowolnej formie) zawierających dane zwykłe poza obszarem przetwarzania.	Zbiory szczególne w formie papierowej, informatycznej Nośniki	1	2	2	Akceptowalne	Przestrzeganie procedur dot. zgód na przetwarzanie poza obszarem przetwarzania, świadomość pracowników, okresowe szkolenia, przestrzeganie procedury przetwarzania danych

KZ	Identyfikacja ryzyka			Analiza ryzyka			Ewaluacja ryzyka	Sposób postępowania z ryzykiem przyjętym w parafii
	Rodzaj ryzyka	Zdarzenie (dodatkowo można krótko opisać jego skutki i prawdopodobieństwo)	Podatność	Ocena (S)	Ocena (P)	PR = S x P		
								na urządzeniach mobilnych. Brak umów powierzenia.
Średnia ocena ryzyka w obszarze KZ – 4				1,29	2,00	2,86	Akceptowalne	
KZ – 5	Zgodnie z Załącznikiem 1	Nieprawidłowe przydzielenie uprawnień do wejścia w strefy przetwarzania danych osobowych.	Pracownicy Zbiory danych Sprzęt informatyczny	2	2	4	Akceptowalne	Polityka uprawnień. Świadomość pracowników – szkolenia. Okresowe szkolenia.
KZ – 5	Zgodnie z Załącznikiem 1	Brak nadzoru nad personelem sprzątającym.	Zbiory danych Sprzęt informatyczny Nośniki	1	2	2	Akceptowalne	Świadomość pracowników. Procedury nadzoru nad wejściem do stref przetwarzania. Okresowe kontrole.
KZ – 5	Zgodnie z Załącznikiem 1	Brak stosowania certyfikowanych zabezpieczeń – Systemu Sygnalizacji Napadu i Włamania.	Zbiory danych Sprzęt informatyczny	2	1	2	Akceptowalne	Stosowanie norm dla systemów alarmowych.

		Brak monitorowania systemów monitorujących.						Umowa z Agencją ochrony (Strażą Miejską).
KZ – 5	Zgodnie z Załącznikiem 1	Umożliwienie wejścia osób nieuprawnionych gości (personelu technicznego) w strefy przetwarzania danych osobowych.	Zbiory danych osobowych	2	2	4	Akceptowalne	Świadomość pracowników. Procedury nadzoru nad wejściem do stref przetwarzania. Okresowe kontrole.
KZ – 5	Zgodnie z Załącznikiem 1	Nieprzestrzeganie polityki wydawania (posiadania) kluczy do stref przetwarzania.	Zbiory danych Sprzęt informatyczny	2	2	4	Akceptowalne	Szkolenie. Okresowe kontrole polityki wydawania kluczy.
KZ – 5	Zgodnie z Załącznikiem 1	Nieprawidłowe zabezpieczenie serwerowni.	Zbiory danych przetwarzanych w systemie informatycznym	3	2	6	Średnie	Nadzór ASI. Kontrola IOD. Kontrola przełożonych. Zastosowanie adekwatnych systemów bezpieczeństwa dla pomieszczeń specjalnych.
ŚREDNIA OCENA RYZYKA W OBSZARZE KZ – 5				2,4	2,4	4,4	Średnie	
ŚREDNIA OCENA RYZYKA				1,61	2,41	3,63	Akceptowalne	

XIII. Opis doboru środków bezpieczeństwa

Z przeprowadzonej analizy zagrożeń wewnętrznych i zewnętrznych wypływają wnioski dotyczące organizacji systemu ochrony danych osobowych w parafii wraz z opisem czynności, jakie winny po sobie następować. Najbardziej prawdopodobne zagrożenie wewnętrzne to możliwość ujawnienia danych osobowych. Zagrożenie to wymusiło wprowadzenie systemu kontroli dostępu do obszarów (stref) przetwarzania danych, system fizycznego zabezpieczenia obszarów, procedurę nadzorowania personelu technicznego i innych osób oraz politykę zarządzania kluczami. Szczególnej ochronie podlegają pomieszczenia / obszary przetwarzania danych, w których znajdują się stacje robocze do przetwarzania danych osobowych i urządzenia rejestrujące monitoring wizyjny[28].

Analiza ryzyka pozwoliła na określenie właściwych potrzeb w zakresie zabezpieczenia materiałów zawierających dane osobowe, w tym zasobów systemu teleinformatycznego, co będzie istotnym czynnikiem wpływającym na efektywność zastosowanych środków ochrony. Prowadzenie szkoleń ma na celu podniesienie ogólnej świadomości w zakresie bezpieczeństwa i ukształtowania właściwych nawyków w zakresie ochrony danych osobowych[29].

Poziom zagrożeń i podatności związanych z bezpieczeństwem systemu teleinformatycznego w środowisku bezpieczeństwa elektronicznego nie przekracza przeciętnego, a wdrożony system ochrony podstawowej skutecznie minimalizuje ryzyko do poziomu akceptowalnego.

Mając na uwadze wyniki z szacowania ryzyka, należy podkreślić, że utrzymanie założonego poziomu bezpieczeństwa danych osobowych przetwarzanych, udostępnianych i przechowywanych w parafii organizacyjnej zostało uzyskane poprzez:

- Wprowadzenie przeglądów ryzyka w okresie nieprzekraczającym jednego roku;
- Wprowadzenie cyklicznych przeglądów systemu teleinformatycznego realizowane przez podmiot wspierający parafię w zakresie zabezpieczenia IT;
- Uaktualnianie procedur i zastosowanych środków zabezpieczających na bieżąco;
- Wprowadzenie zasad niszczenia wszystkich nośników zawierających dane osobowe;

---

28 Por. M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016, s. 53–76.

29 Por. M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie...*, dz. cyt., s. 53–76.

- Wprowadzenie zasady stosowania zarejestrowanych nośników danych (pendrive) i szyfrowania dysków komputerów przenośnych, jak również zabezpieczenia łączy;
- Wdrożenie odpowiednich zabezpieczeń systemu teleinformatycznego poprzez blokadę napędu cd/dvd, zbędnych portów usb itd., co gwarantuje odpowiedni poziom bezpieczeństwa;
- Zobligowanie ASI / informatyka do bieżącego nadzoru oraz analizy dziennika zdarzeń;
- Wyjaśnianie i reagowanie na incydenty naruszenia bezpieczeństwa w momencie wystąpienia incydentu;
- Wprowadzenie obowiązku systematycznego tworzenia kopii zapasowych oraz backupów[30].

Przeprowadzona analiza ryzyka wykazuje, że najsłabszym ogniwem bezpieczeństwa w systemie ochrony danych osobowych może być „czynnik ludzki". Główny nacisk na bezpieczeństwo danych winien być położony na bezpieczeństwo osobowe realizowane przez szkolenia, nadanie upoważnień i doraźne kontrole przestrzegania wdrożonych procedur[31].

W celu zminimalizowania zagrożeń główny ciężar odpowiedzialności za bezpieczeństwo systemu teleinformatycznego będzie spoczywał na AD. IOD stanowi organ doradczy, podobnie jak ASI oraz inne osoby prowadzące systematyczne kontrole stanu faktycznego ochrony danych osobowych, w tym stosujące procedurę okresowego audytu bezpieczeństwa, zabezpieczeń, sprzętu i oprogramowania, jak również szkoleń z użytkownikami systemu. Takie działania służą zminimalizowaniu ryzyka. Zdefiniowane w analizie ryzyko występujące w systemie jest znane i akceptowalne[32].

---

30 Por. A. Bajorek, *Ochrona i bezpieczeństwo danych osobowych organizacji*, „De Securitate" 2016 nr 1 (2), s. 45–46.

31 Por. M. Mazur, *Nowe podejście do stosowania przepisów określających wymogi w zakresie bezpieczeństwa danych osobowych, analizy ryzyka oraz ocena skutków dla ochrony danych osobowych*, https://mkadministrators.pl/wp-content/uploads/2020/01/Prezentacja.pdf (28.04.2020), s. 10–19, 63–64.

32 Bezpieczeństwo przetwarzania szerzej reguluje art. 22 Dekretu: „1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. 2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego

- Kopiowanie danych z dysku twardego na nośniki zewnętrzne. W związku z tym, że istnieje potrzeba utrzymania w systemie komputerowym napędu DVD-R/W oraz istnieje stały nadzór przez uprawniony personel nad wykorzystaniem tych napędów, przyjmuje się założenie, że użytkownicy nie wykonują nielegalnych kopii danych osobowych[33].
- Ponieważ w systemie teleinformatycznym używane są nośniki elektroniczne, istnieje niebezpieczeństwo zainfekowania systemu wirusem przenoszonym na tych nośnikach, w związku z powyższym zainstalowano oprogramowanie antywirusowe, aktualizowane przez ASI lub osobę upoważnioną[34].
- Pomimo wprowadzonych zabezpieczeń oraz akceptacji podwyższonego ryzyka pozostają sytuacje wynikające ze zbiegu kilku zagrożeń w jednym czasie. Sytuacja ta może nastąpić w przypadku, gdy nastąpi awaria zasilania, a użytkownik nie prowadzi okresowego zapisywania danych. Najtrudniejsze do przewidzenia i zdefiniowania ryzyko jest związane z brakiem wiedzy użytkownika. W celu eliminacji takich przypadków należy prowadzić cykliczne szkolenia z użytkownikami systemu.
- Kolejnym trudnym do przewidzenia elementem jest ujawnienie informacji zawierających dane osobowe, uzyskanych w związku z wykonywaną pracą. Sprawcami ujawnienia takiej informacji mogą być zarówno byli pracownicy znający osoby i miejsce wytwarzania i przechowywania oraz znający funkcjonujący system ochrony, jak i obecni pracownicy, którzy dla korzyści materialnych mogą takie informacje zdobyć i ujawnić innym źródłom[35].

XIV. Informacje dodatkowe o środkach bezpieczeństwa teleinformatycznego oraz fizycznego stosowanych w parafii

System zabezpieczeń danych. Środki organizacyjno-techniczne

1. Ochrona zbiorów danych polega na zabezpieczeniu informacji wprowadzonej, przetwarzanej, przesyłanej w systemie informatycznym oraz na nośnikach

ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych [...]".

33 Por. A. Bajorek, *Ochrona i bezpieczeństwo...*, dz. cyt., s. 47–48.

34 Por. M. Cwener, *Nowe obowiązki dokumentacyjne...*, dz. cyt., s. 107–108.

35 Por. Generalny Inspektor Ochrony Danych Osobowych, *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych*, Warszawa 2009, s. 7–8.

informacji przed nielegalnym ujawnieniem, kradzieżą oraz nieuprawnioną modyfikacją lub usunięciem.

2. W celu ochrony danych przechowywanych w systemach informatycznych wykorzystuje się, wchodzące w ich skład mechanizmy zarówno sprzętowe, jak i programowe oraz inne rozwiązania zwiększające bezpieczeństwo danych.

3. Dane osobowe przetwarzają wyłącznie osoby posiadające upoważnienia do przetwarzania danych osobowych nadane przez AD – zgodnie z procedurą lub wynikające z przepisów prawa. Osoby upoważnione do przetwarzania danych mają obowiązek zachować w tajemnicy dane, które przetwarzają oraz sposoby ich zabezpieczenia.

4. Przebywanie osób nieupoważnionych w obszarach przetwarzania danych osobowych jest monitorowane przez uprawnione osoby parafii.

5. Wszystkie pomieszczenia, w których przetwarza się dane osobowe, są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy.

6. Sprzątanie pomieszczeń, gdzie przetwarzane są dane osobowe, odbywa się przez personel sprzątający, który jest przeszkolony i zaufany. Sprzątanie odbywa się z założeniem, że zostaną zachowane przez osoby przetwarzające dane osobowe zasady „czystego biurka i ekranu". Personel sprzątający może odmówić wykonywania czynności sprzątających w przypadku niezachowania ww. zasady.

7. Przy przetwarzaniu danych osobowych w STI przestrzega się zasad „czystego biurka i ekranu", realizowane poprzez stosowanie wygaszaczy ekranu, klawiatury odwieszanych za pomocą indywidualnych haseł lub kodów oraz ustawianie monitorów w taki sposób, aby nie była widoczna informacja dla osób postronnych. Zasada „czystego biurka" sprowadza się do zabezpieczenia w czasie i po pracy danych osobowych w formie papierowej w taki sposób, aby uniemożliwiało ich odczyt przez osoby nieuprawnione oraz ograniczyć skutki uszkodzenia lub zniszczenia w wyniku zdarzeń, takich jak pożar, zalanie, zabrudzenie, częściowe uszkodzenie.

8. Zabronione jest usuwanie danych przez wyrzucenie ich do kosza na odpadki. Jeżeli podczas usuwania odpadków z koszy pracownik sprzątający stwierdzi obecność trwale niezniszczonych dokumentów, to zgłasza ten fakt do AD lub IOD, a kosz na odpadki zabezpiecza na czas wyjaśnienia zdarzenia.

9. Przeglądanie sieci publicznej w zakresie tematyki niezwiązanej z zakresem wykonywanych czynności następuje za zgodą AD, który określa tematykę stron WWW,

z których można korzystać. ASI może po uzgodnieniu z AD wprowadzić domyślne filtrowanie stron WWW.
10. Zabrania się publicznego wyrażania oświadczeń w imieniu parafii z wykorzystaniem portali internetowych bez pisemnej zgody proboszcza/AD, a w szczególności zabronione jest ujawnianie informacji prawnie chronionych. Publikowanie wszelkich informacji na stronach WWW wymaga anonimizacji danych osobowych, chyba że osoba, której dane dotyczą, wyrazi zgodę na publikację danych.
11. W przypadku żądania udostępniania danych pracownicy postępują zgodnie z przepisami Dekretu. Decyzję podejmuje AD, a w razie wątpliwości co do zasadności udostępnienia danych zwraca się o opinię do proboszcza lub IOD.
12. Udostępnianie danych powinno być odnotowywane w systemach informatycznych, a w przypadku zbiorów danych w formie tradycyjnej odnotowanie informacji o udostępnianiu przechowuje pracownik merytoryczny w aktach sprawy.
13. Dokumenty zawierające dane osobowe sporządzane ze względów technicznych (notatki, zapiski, opisy, niejednolite rejestry) nie są trwale przechowywane, a po ich wykorzystaniu niezwłocznie są usuwane lub poddawane anonimizacji.
14. Sprzęt informatyczny rozlokowuje się tak, aby zminimalizować niepożądany dostęp do obszaru przetwarzania danych osobowych i wprowadza się odpowiednie zabezpieczenia w stosunku do potencjalnych zagrożeń[36].

System zabezpieczeń danych – podstawowe środki teleinformatyczne

1. Dla danych osobowych przetwarzanych w systemach informatycznych stosuje się:
   a. kontrolę dostępu do zbiorów danych osobowych;
   b. indywidualne identyfikatory użytkowników (osób przetwarzających dane osobowe);
   c. uwierzytelnianie użytkowników – hasła (potwierdzanie ich tożsamości).
2. W celu zabezpieczenia danych osobowych przed ich utratą lub uszkodzeniem:
   a. dla wszystkich systemów wdrożono procedury tworzenia kopii zapasowych;
   b. wszystkie systemy informatyczne przetwarzające dane osobowe wyposażono w awaryjne zasilanie;
   c. wdrożono oprogramowanie antywirusowe;
   d. dostęp do systemów z sieci publicznej kontroluje się za pomocą zapory sieciowej oraz filtrów antyspamowych i oprogramowania antywirusowego oraz

36 Por. D. Lubasz, *Europejska reforma ochrony danych osobowych – nowe obowiązki administratorów w ogólnym rozporządzeniu o ochronie danych*, dz. cyt., s. 73–76.

zaawansowanego urządzenia typu UTM (unified threat management – wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia);

e. przy przesyłaniu danych osobowych przez sieć publiczną użytkowników zobowiązuje się do korzystania z oprogramowania umożliwiającego połączenie szyfrujące lub stosowania kompresji ZIP zabezpieczonej hasłem przesyłanym innym kanałem łączności;

f. **AD zastrzega prawo kontroli** prawidłowości wykorzystania zasobów informatycznych. W szczególności dotyczy to działań użytkowników w Internecie, przeglądania zarchiwizowanych historii, katalogów zawierających dane prywatne utworzone bez zgody AD, zawartości twardych dysków i innych informacji przechowywanych w systemie informatycznym parafii;

g. **zabrania się** zapisu na dyskach twardych, stałych i przenośnych, nośnikach wymiennych wszelkich plików i baz danych, które nie są bezpośrednio związane z powierzonym zakresem czynności, takich jak filmy video, nagrania muzyczne, oprogramowanie do gry i zabawy, oprogramowanie szpiegowskie, hackerskie, pirackie oraz inne oprogramowanie, które może znacząco obniżyć poziom bezpieczeństwa danych osobowych;

h. **zabrania się** udostępniania indywidualnego kodu dostępu i haseł do systemu informatycznego nieupoważnionym osobom;

i. **zabrania się korzystania** z prywatnych elektronicznych wymiennych nośników informacji (tj. urządzeń wykorzystujących pamięć USB, jak pendrive, aparaty fotograficzne, telefony, przenośne dyski usb itp.) w systemach przetwarzających dane osobowe bez zgody proboszcza lub ASI;

j. **zabronione jest** przenoszenie danych osobowych na niezarejestrowanych nośnikach elektronicznych (tj. urządzeniach wykorzystujących pamięć USB, jak pendrive, aparaty fotograficzne, telefony, przenośne dyski usb itp.);

k. dokumenty zawierające dane osobowe powinny być zaszyfrowane przynajmniej z poziomu używanego oprogramowania, hasłem składającym się z minimum 8 znaków;

l. każda osoba ponosi pełną odpowiedzialność za zagubienie ww. nośnika z danymi osobowymi;

m. **zabronione jest** korzystanie z tzw. chmur obliczeniowych dostępnych w sieci internetowej (do przetwarzania danych osobowych w postaci umieszczania na serwerach nieznanych dostawców plików z danymi osobowymi parafii);

n. **Zabronione jest** korzystanie z sieci publicznej WWW do przeglądania witryn internetowych, których treść bezpośrednio lub pośrednio wskazuje na możliwość

występowania złośliwego oprogramowania, tj. witryn związanych z przemocą, uzależnieniami, promujących działania nielegalne, pirackie oprogramowanie itp.

XV. Opis ryzyk szczątkowych, które pozostają niezabezpieczone

Na podstawie analizy zagrożeń i podatności czynników związanych z bezpieczeństwem danych osobowych zdefiniowano elementy ryzyka, które występują w systemie ochrony danych osobowych z zaznaczeniem, że jest ono znane i akceptowalne przez AD.

W efekcie przeprowadzonej analizy przyjęto, że istnieje możliwość wystąpienia następujących zagrożeń zakwalifikowanych jako ryzyko szczątkowe:

1. nieautoryzowane kopiowanie danych przez autoryzowany personel;
2. nieuprawnione zapoznanie się z treścią danych przechowywanych przez AD, przez gości lub personel techniczny pozostawiony w strefie przetwarzania danych osobowych bez nadzoru upoważnionego pracownika parafii;
3. błędy użytkownika – możliwość uszkodzenia systemu do przetwarzania danych osobowych przez użytkownika w związku z różnorodną znajomością obsługi sprzętu komputerowego;
4. wybuch pożaru w pomieszczeniu komputerowym lub w jego bezpośrednim otoczeniu, co może spowodować termiczne bądź chemiczne (działanie agresywnych gazów i produktów spalania) uszkodzenie systemu i utratę przechowywanych w nim danych;
5. zalanie pomieszczenia wodą w przypadku prowadzonej akcji gaśniczej.

Za pogodzeniem się z wyżej wymienionym ryzykiem przemawiają niżej podane założenia:

1. Użytkownicy (osoby uprawnione do przetwarzania danych osobowych) – jako osoby mające prawo do przebywania stałego na terenie parafii zostały pozytywnie zweryfikowane, są stale uświadamiane i okresowo kontrolowane – nie powinny kopiować danych osobowych.
2. Wymóg towarzyszenia w pomieszczeniach z danymi osobowymi osobom nieuprawnionym przez upoważnione osoby parafii – z uwagi na specyfikę parafii – traktowany jest priorytetowo, w związku z czym rzeczywista możliwość zaistnienia opisanego zagrożenia jest niska.
3. W celu zapobieżenia wystąpieniu krytycznych awarii systemu mogących wynikać z błędu obsługi ze strony użytkowników, ASI / IOD prowadzą okresowe szkolenia

użytkowników (osób mających dostęp do przetwarzania danych osobowych) oraz dokonują doraźnych kontroli stosowania się przez użytkowników do obowiązujących procedur[37].

4. W parafii przestrzegane są instrukcje ppoż. oraz utrzymuje się sprawny podręczny sprzęt gaśniczy.

Podsumowanie

Postulowane środki bezpieczeństwa, w oparciu o normy prawa kanonicznego i RODO, mogą przyczynić się do zwiększenia bezpieczeństwa przetwarzania danych osobowych zwłaszcza w większych parafiach, gdzie mamy do czynienia ze znaczną liczbą interesantów, których dane są przedmiotem czynności prawnych.

Raport szacowania ryzyka doboru środków bezpieczeństwa uwzględnia wszelkie okoliczności związane z przetwarzaniem danych w parafii, wskazuje na zagrożenia w zakresie bezpieczeństwa informacji oraz możliwy dobór środków bezpieczeństwa, to jest sposobów postępowania w konkretnych sytuacjach zapobiegających ich naruszeniu. Sugerowane działania zmniejszające ryzyko mogą przyczynić się do organizacji systemu ochrony danych osobowych w parafii, zwłaszcza przez ściśle określony i przestrzegany system zabezpieczeń danych.

SUMMARY

Risk assessment report for the selection of security measures

The article shows the profile of risk management in the range of selection of security solutions.

It presents procedures for limiting the risk related to the security of personal data protection in a parish, and in particular defines the methodology and principles of risk management connected with data processing and storage. The analysis of the effects of threats and the likelihood of their occurrence assesses the scale of these effects, indicates examples

37 Por. M. Gumularz, E. Laskowska, *Wpływ ogólnego rozporządzenia o ochronie danych na zasady prowadzenia baz danych – problemy praktyczne na styku prawa prywatnego i publicznego*, w: *Ogólne rozporządzenie o ochronie danych osobowych...*, dz. cyt., s. 87–90.

of threats in the area of information security and selection of security measures, i.e. ways to act in specific situations to prevent their loss. Suggested risk reduction measures can contribute to the organization of a personal data protection system in a parish, especially through a clearly-defined and observed data security system.

Keywords: personal data in a parish, GDPR, risk analysis, security system, information security threats, Decree

Raport szacowania ryzyka doboru środków bezpieczeństwa

Artykuł ukazuje zarys zarządzania ryzykiem w zakresie doboru środków bezpieczeństwa. Postuluje procedury w zakresie ograniczania ryzyka względem bezpieczeństwa ochrony danych osobowych w parafii, a w szczególności określa metodykę i zasady zarządzania ryzykiem związanym z przetwarzaniem danych i ich przechowywaniem. Analiza skutków zagrożeń i prawdopodobieństwa ich wystąpienia ocenia skalę tychże skutków, wskazuje na przykładowe zagrożenia na płaszczyźnie bezpieczeństwa informacji oraz dobór środków bezpieczeństwa, czyli sposobów postępowania w konkretnych sytuacjach zapobiegających ich utracie. Sugerowane działania zmniejszające ryzyko mogą przyczynić się do organizacji systemu ochrony danych osobowych w parafii, zwłaszcza przez ściśle określony i przestrzegany system zabezpieczeń danych.

Słowa kluczowe: dane osobowe w parafii, RODO, analiza ryzyka, system zabezpieczeń, zagrożenia bezpieczeństwa informacji, Dekret

Bibliografia

1. Bajorek A., *Ochrona i bezpieczeństwo danych osobowych organizacji*, „De Securitate" 2016 nr 1 (2), s. 40–50.

2. Banyś T. A. J., *Wdrażanie nowych elementów systemu ochrony danych osobowych przez podmioty publiczne*, w: *Polska i europejska reforma ochrony danych osobowych*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2016, s. 53–62.

3. Barta P., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2016.

4. Buttarelli G., *Ochrona danych osobowych w Kościołach i związkach wyznaniowych w świetle ogólnego rozporządzenia o ochronie danych*, w: *Ochrona danych osobowych w Kościele*, red. S. Dziekoński, P. Drobka, Warszawa 2016, s. 11–18.

5. Chodorowski M., *Nowe prawa i obowiązki administratorów bezpieczeństwa informacji (inspektorów ochrony danych) w świetle najnowszych opinii wydanych*

przez Grupę Roboczą Art. 29, w: *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osieja, Warszawa 2017, s. 141–158.

6. Cwener M., *Nowe obowiązki dokumentacyjne związane z przetwarzaniem danych osobowych*, w: *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osieja, Warszawa 2017, s. 97–110.

7. Dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim wydany przez Konferencję Episkopatu Polski w dniu 13 marca 2018 r., podczas 378. Zebrania Plenarnego w Warszawie, na podstawie kan. 455 Kodeksu Prawa Kanonicznego, w związku z art. 18 Statutu KEP, po uzyskaniu specjalnego zezwolenia Stolicy Apostolskiej z dnia 3 czerwca 2017 r., http://episkopat.pl/wp-content/uploads/2018/04/13.3.2018.PL_.Dekret-ogolny-o-ochronie-danych-osobowych.pdf (3.07.2020).

8. Generalny Inspektor Ochrony Danych Osobowych, *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych*, Warszawa 2009.

9. Generalny Inspektor Ochrony Danych Osobowych, *Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa*, archiwum.giodo.gov.pl/163/id_art/1063/j/p (23.04.2020).

10. Gumularz M., Laskowska E., *Wpływ ogólnego rozporządzenia o ochronie danych na zasady prowadzenia baz danych – problemy praktyczne na styku prawa prywatnego i publicznego*, w: *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osieja, Warszawa 2017, s. 79–95.

11. Kroczek P., *Kilka uwag dotyczących Dekretu KEP z 13 marca 2018 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim na podstawie kazusu przedszkola*, „Annales Canonici 14 (2018), s. 9–22.

12. Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016.

13. Lubasz D., *Europejska reforma ochrony danych osobowych – nowe obowiązki administratorów w ogólnym rozporządzeniu o ochronie danych*, w: *Polska i europejska reforma ochrony danych osobowych*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2016, s. 63–85.

14. Madej J., *Klasyfikacja zagrożeń bezpieczeństwa systemu informatycznego*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2010 nr 814, s. 77–86.

15. Mazur M., *Analiza ryzyka a ocena skutków dla ochrony danych*, https://uodo.gov.pl/pl/138/605 (29.04.2020).

16. Mazur M., *Nowe podejście do stosowania przepisów określających wymogi w zakresie bezpieczeństwa danych osobowych, analizy ryzyka oraz ocena skutków dla ochrony danych osobowych*, https://mkadministrators.pl/wp-content/uploads/2020/01/Prezentacja.pdf (28.04.2020).
17. Mezglewski A., *Perspektywa i zakres implementacji nowych przepisów Unii Europejskiej dotyczących przetwarzania danych osobowych przez związki wyznaniowe*, w: *Ochrona danych osobowych w Kościele*, red. S. Dziekoński, P. Drobka, Warszawa 2016, s. 35–52.
18. *Ochrona danych osobowych w działalności Kościoła katolickiego w Polsce.* Instrukcja opracowana przez Generalnego Inspektora Ochrony Danych Osobowych oraz Sekretariat Konferencji Episkopatu Polski z dnia 23 września 2009 r., https://giodo.gov.pl/data/filemanager_pl/wsp_krajowa/KEP.pdf (14.04.2020).
19. Poniatowski M., *Przetwarzanie danych osobowych w kościelnych organizacjach pożytku publicznego*, w: *Ochrona danych osobowych w Kościele*, red. S. Dziekoński, P. Drobka, Warszawa 2016, s. 171–191.
20. Pszczółkowski K., *Metodyka zarządzania ryzykiem w ochronie danych osobowych*, Warszawa 2018.
21. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz. Urz. UE L Nr 119).
22. Sibiga G., *Zadania administratora bezpieczeństwa informacji – wybrane zagadnienia*, w: *Polska i europejska reforma ochrony danych osobowych*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2016, s. 157–169.
23. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, http://www.dziennikustaw.gov.pl/DU/2018/1000 (19.04.2020).
24. Więcaszek-Kuczyńska L., *Zagrożenia bezpieczeństwa informacyjnego*, „Obronność. Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2014 nr 2 (10), s. 210–233.
25. Więckowska M., *Metodyka przeprowadzenia oceny skutków dla ochrony danych w ujęciu praktycznym*, uodo.gov.pl/pl/138/605 (22.04.2020).
26. Więckowska M., *Stosowanie technicznych środków bezpieczeństwa w aspekcie zgłoszeń naruszeń do UODO oraz ocena wagi naruszenia w oparciu o zalecenia Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)*, uodo.gov.pl (21.04.2020).