

Podsumowanie działań audytowych związanych z systemem informatycznym Legimi

Wprowadzenie

Legimi informuje, że z uwagi na zastrzeżenia niektórych dostawców treści i związane ze współpracą z Legimi S.A. (dalej: „Legimi” lub „Spółka”), Spółka niezwłocznie podjęła działania w celu zweryfikowania możliwości przeprowadzenia audytu w zakresie aspektów technologicznych związanych z tymi zastrzeżeniami. Już w drugiej połowie października 2024 r. Zarząd Legimi S.A. podjął starania w celu przeprowadzenia rzetelnego, niezależnego audytu rozwiązań informatycznych stosowanych przez Legimi, kontaktując się z różnymi podmiotami, które taką usługę mogłyby zrealizować. Intencją Spółki było wybranie podmiotu o dużej wiarygodności, renomie oraz mającego najwyższej klasy zaplecze techniczne i osobowe, jak również zapewniającego bezpieczeństwo danych i informacji przekazywanych przez Legimi S.A.

Koncepcję przeprowadzenia zewnętrznych działań audytowych przedstawiono niektórym podmiotom, wskazującym na możliwość zaistnienia błędów w rozliczeniach.

Niezwłocznie po podpisaniu listu intencyjnego dnia 30.10.2024 r., o czym spółka informowała w raporcie ESPI 12/2024, przystąpiono do sprecyzowania zakresu działań audytowych, aby przeprowadzić je możliwie najszybciej i tym samym uzyskać rzetelną wiedzę na temat funkcjonowania systemu informatycznego Legimi, w tym modułów związanych z raportowaniem czytelnictwa, a tym samym mających wpływ na skalę rozliczeń z dostawcami treści (dystrybutorami, wydawnictwami oraz self-publisherami).

Główną intencją Legimi było takie przeprowadzenie audytu, by w sposób w pełni obiektywny sama Spółka otrzymała od zewnętrznego podmiotu rzetelne informacje na temat funkcjonowania jej systemu informatycznego (co Legimi uważa za kluczowe dla dalszego planowania prac rozwojowych związanych z tym systemem), ale też by móc podzielić się z całym polskim środowiskiem związanym z czytelnictwem kluczowymi danymi, które powinny zwiększyć transparentność rynku oraz ułatwić merytoryczną dyskusję nad wyzwaniami, problemami i perspektywami polskiego rynku e-książki.

Po przeprowadzeniu wstępnej analizy prawnej i organizacyjnej, w dniu 4 lutego 2025 r. została zawarta umowa z jedną ze spółek audytorskich należących do grupy międzynarodowej firmy audytorskiej z tzw. „wielkiej czwórki”. Wybór tego podmiotu audytującego uwarunkowany był tym, że dysponował potencjałem organizacyjnym i osobowym oraz wieloletnim doświadczeniem, co daje rękojmię rzetelnego i wnikliwego procesu audytowego oraz poufność pozyskanych w ten sposób danych.

Opis założeń audytu

Przechodząc do opisu założeń audytu, wskazać należy dwa cele, które Legimi uznała za kluczowe, tj.:

- 1) Niezależne zweryfikowanie rozliczeń z wydawcami w oparciu o dużą (1.000 przypadków) próbę wypożyczeń publikacji elektronicznych oraz zidentyfikowanie indywidualnych rozbieżności i wskazanie ich przyczyn.
- 2) Zidentyfikowanie i ocena środków kontroli organizacyjnej i systemowej, obejmujących nadzorowanie, zarządzanie i weryfikację integralności danych w bazie danych rejestrujących wypożyczenia publikacji elektronicznych (ebooków i audiobooków).

Upraszczając, audyt miał dać odpowiedź na dwa pytania:

- 1) Czy istnieją wady w systemie informatycznym Legimi, które mogą wpływać na rozliczenia z dostawcami treści (a jeżeli tak, to jakie są to wady i w jakim stopniu mogą oddziaływać na rozliczenia finansowe z dostawcami treści)? oraz
- 2) Czy nadzór nad systemem informatycznym był odpowiedni i czy nie mają miejsca „ręczne” modyfikacje danych, które mogłyby wpływać na rejestrację transakcji czytelnicznych i rozliczenia z dostawcami treści?

W celu odpowiedzi na te pytania, zespół audytujący skupił się na dwóch zagadnieniach:

- 1) Bezpośrednim procesie udostępniania publikacji elektronicznych użytkownikom indywidualnym (posiadaczom aktywnego abonamentu) oraz wypożyczania publikacji elektronicznych za pośrednictwem bibliotek publicznych i zakładowych funkcjonującym w Legimi oraz powstałych wskutek tych działań zapisach w systemie informatycznym Legimi.
- 2) Weryfikacji obecnie funkcjonujących mechanizmów organizacyjnych i systemowych, zapewniających integralność danych o wypożyczeniach publikacji elektronicznych.

Obydwa te zagadnienia zostały szeroko i dokładnie omówione w otrzymanym przez Legimi Raporcie po zakończeniu audytu (dalej: „Raport”).

Warto podkreślić, że Legimi, zlecając przeprowadzenie czynności audytowych, zamówiła wykonanie ich w szerszym zakresie niż dotyczyły tego zastrzeżenia, jakie formułowane były publicznie przez dostawców treści lub w bezpośredniej komunikacji pomiędzy Legimi a dostawcami treści. Zweryfikowano bowiem także te modele rozliczeń, co do których zastrzeżenia nie występowały.

Etap działań związanych z obszarem technologicznym poprzedziło zapoznanie Audytora z wzorami umów zawieranych przez Legimi z dostawcami treści (dystrybutorami i wydawnictwami), którzy odpowiadali za znaczny wolumen transakcji czytelnicznych. W

tym kontekście kluczowe było zapoznanie Audytora z prawnymi i organizacyjnymi aspektami współpracy Legimi z tymi podmiotami, ewentualnymi odmiennościami, które mogą występować w przypadku współpracy z danym dostawcą treści (np. wynikającymi z integracji systemu Legimi z systemem stosowanym przez konkretnego dystrybutora) oraz sposobem raportowania transakcji i ich przełożeniem na finansowy wymiar rozliczeń między Legimi a dostawcami treści.

Prace audytowe zostały podzielone na 5 faz:

- Faza 0 – planowanie prac (10-14 lutego 2025 r.),
- Faza 1 – przygotowanie do audytu (17-28 lutego 2025 r.),
- Faza 2 – przeprowadzenie i udokumentowanie testów wypożyczeń i rozliczeń (24 lutego i 29 marca 2025 r.),
- Faza 3 – audyt integralności danych w bazie danych (24 lutego – 14 marca 2025 r.),
- Faza 4 – opracowanie Raportu (24 marca – 4 kwietnia 2025 r.).

Harmonogram miał charakter poglądowy i mimo znacznego zaangażowania zarówno zespołu audytującego, jak i personelu Legimi, nie udało się stworzyć ostatecznej wersji Raportu do 4 kwietnia 2025 r. Ostateczna wersja Raportu została przedstawiona Legimi w dniu 18 kwietnia 2025 r.

Intencją zarówno podmiotu audytowanego, jak i audytującego, było rzetelne przedstawienie poczynionych ustaleń oraz przygotowanie rekomendacji podjęcia działań informatycznych i organizacyjnych w Legimi zmniejszających ryzyko i podstawy do zakwestionowania działań Spółki w zakresie rozliczeń z dostawcami treści.

W tym momencie należy też zaznaczyć, że zespół Legimi na bieżąco reagował na zgłaszane uwagi wskazywane w toku prac audytowych, w tym błyskawicznie wprowadzał niektóre poprawki, o czym będzie jeszcze szczegółowo mowa w dalszej części Podsumowania.

Rolą niniejszego podsumowania przygotowanego na bazie Raportu jest przedstawienie tych ustaleń w sposób uproszczony, pozwalający zapoznać się z nimi także osobom mniej biegłym technicznie lub nieznającym niektórych realiów funkcjonowania polskiego rynku wydawniczego, jednocześnie nie naruszając wymogów poufności stosowanych przez Audytora.

Legimi ma nadzieję, że taka praktyka zainspiruje również inne podmioty obecne na polskim rynku dystrybucyjnym i wydawniczym do większej transparentności w rozliczeniach z autorami i partnerami biznesowymi.

Przygotowanie do audytu

Etap 1 służył wszechstronnemu przygotowaniu do audytu technologicznego systemu.

Podczas tego etapu Audytor zapoznał się z zasadami rozliczania się Legimi z wydawcami oraz funkcjonowania systemu informatycznego w zakresie:

- 1) Rejestrowania aktywności użytkowników w systemie – w zakresie liczby przeczytanych materiałów oraz zakresu przeczytanego materiału.
- 2) Rejestrowania zakresu tzw. „zaczycia” czyli rozpoznania progu, powyżej którego materiał uważa się za przeczytany.
- 3) Rozliczenia z wydawcami na podstawie liczby materiałów przeczytanych lub „zaczycanych” przez użytkowników systemu Legimi.
- 4) Cen stosowanych w rozliczeniach z wydawcami (i ich zróżnicowania w zależności od klasyfikacji użytkownika).
- 5) Przygotowanie przypadków testowych – ustalenie szczegółów dotyczących testowania zapisów w systemie Legimi, w zakresie:
 - (a) ustalenia wielkości próby testów,
 - (b) kont, które zostaną użyte do testów,
 - (c) czasu testowania,
 - (d) zakresu testowania.
- 6) Przeglądu umów zawieranych przez Legimi z dostawcami treści w zakresie obowiązków przechowywania danych oraz rozliczeń – w celu dostosowania testów do zapisów umownych.

Metodologia weryfikacji wypożyczeń i rozliczeń oraz integralności danych

Kolejnym etapem audytu było przeprowadzenie i udokumentowanie weryfikacji wypożyczeń i rozliczeń transakcji.

Wykorzystane zostały do tego celu konta użytkowników, które były w pełni zarządzane przez zespół audytowy (tzn. zespół sam określał, jak i kiedy dany użytkownik zapoznaje się z publikacją elektroniczną, na jakiego rodzaju urządzeniu, ile testów jest przeprowadzanych za pomocą danego konta itp.). Konta te system traktował jako posiadające indywidualny abonament lub uprawnionych do zapoznawania się z książkami jako czytelnicy bibliotek.

Próbę 900 testów „zwykłych” opracowano tak, aby w sposób reprezentatywny oddała udział w czytelnictwie, na platformie Legimi:

- poszczególnych wydawców,
- kanałów sprzedaży (rozumianych tutaj jako dostęp abonamentowy, dostęp za pośrednictwem biblioteki publicznej, dostęp za pośrednictwem biblioteki korporacyjnej),
- modeli rozliczeń (jednoprogowy, wieloprogowy, biblioteczny (OCA), proporcjonalny),

- typów urządzeń końcowych (urządzenia z systemami operacyjnymi: iOS, Android, Windows, urządzenia: Kindle, Pocketbook, inkBook) oraz
- formatów czytanych dzieł (ebook, audiobook, “TTS” (text to speech)).

Część kont użytkowników zgrupowano w ramach „biblioteki”, by w ten sposób zweryfikować poprawność raportowania publikacji elektronicznych przez czytelników bibliotecznych.

W toku audytu nie udostępniano żadnych danych autoryzacyjnych ani innych danych użytkowników usług Legimi (w szczególności danych osobowych). Pozwoliło to zapewnić bezpieczeństwo tych danych, ale też skutkowało tym, że sam audyt nie prowadził do zaburzeń statystyk systemu Legimi. Pomimo tego, że weryfikacja systemu miała charakter wyłącznie testowy, transakcje te uwzględnione zostały w ramach rozliczeń z dostawcami treści i wygenerowały dla nich wynagrodzenie.

W ramach etapu weryfikacji przeprowadzono 100 testów “specjalnych”, których celem było sprawdzenie poprawności funkcjonowania modeli rozliczeniowych. Testy te miały dać odpowiedź na pytanie, jak zachowuje się system Legimi w następujących obszarach:

- składanie się postępów czytania różnych użytkowników na fakt zaraportowania w modelu wieloprogowym,
- czytanie egzemplarza przez jednego użytkownika zarówno w modelu wieloprogowym, jak i jednoprogowym;
- “zacztywanie” egzemplarza wypożyczonego w ramach modelu bibliotecznego (OCA);
- czytanie jednocześnie w modelu bibliotecznym (OCA);
- powrót egzemplarza do puli “wolnych” egzemplarzy w modelu bibliotecznym (OCA);
- czytanie i słuchanie w ramach synchrobook® w modelu proporcjonalnym.

W ramach przyjętej metodologii zadbano o to, by czytanie/słuchanie książek odbywało się przez wyselekcjonowane w tym celu osoby, które uruchamiały swoje urządzenie (np. czytnik e-booków) i czytały lub słuchały książkę. Miało to zapewnić warunki możliwie jak najbliższe tym, jakie towarzyszą typowemu użytkownikowi usług Legimi. Niemniej z uwagi na ograniczony czas trwania testów niezbędne okazało się stosowanie pewnych rozwiązań, które wpłynęły na specyfikę korzystania z publikacji przez testerów, a w rezultacie zaowocowały zwiększeniem częstotliwości występowania niektórych błędów niż ma to miejsce w ogóle populacji użytkowników.

Testerzy działali zgodnie z przyjętą procedurą. Tester oznaczał swoją aktywność (początek i koniec testu) w specjalnym systemie. Następnie logował się do aplikacji na odpowiednie konto na urządzeniu, które służyło do testów, wykonywał test, ręcznie wymuszał synchronizację aplikacji po każdym ukończonym teście i dokumentował zdjęciem

realizację testu. Pozyskane w ten sposób dane można było zweryfikować z danymi przekazywanymi następnego dnia przez Legimi i wychwycić zdarzenia, które mogły skutkować różnicami w tych zestawieniach danych.

Niezależnie od tego Legimi podjęła również działania, aby w procedurę audytową zaangażować dostawców treści. W tym celu zwrócono się do dostawców treści kierujących pytania do Legimi o rozliczenia transakcji z propozycją, aby wskazali konkretne publikacje lub dane, które ich szczególnie interesują do uwzględnienia w ramach audytu. Wszelkie otrzymane w ten sposób sugestie przekazano zespołowi audytującemu. Pośredniczono też w organizacji spotkania przedstawicieli Audytora z przedstawicielami jednego z dystrybutorów treści, gdyż uznano takie spotkanie za pomocne dla opracowania należytej metodyki działań audytowych. Intencją Legimi było stworzenie jak najbardziej reprezentatywnej próbki danych, które miały być poddane weryfikacji.

Ostatecznie, bazując na danych dotyczących dystrybucji przez Legimi publikacji elektronicznych w styczniu 2025 r. oraz statystykach dotyczących popularności formatów publikacji elektronicznych i kanałów sprzedaży w okresie od 17 do 23 lutego 2025 r., podmiot audytujący wybrał publikacje elektroniczne dostawców treści, którzy łącznie otrzymują 95% wynagrodzeń dla dostawców treści wypłacanych przez Legimi. Umożliwiło to dywersyfikację form publikacji elektronicznych i rodzajów treści, a więc pozwoliło możliwie jak najbardziej zbliżyć się podczas audytu do faktycznej popularności publikacji wśród użytkowników usług Legimi.

Posiadając tę wiedzę oraz dostęp do kont użytkowników, zespół audytowy mógł przejść do Etapu 2 działań audytowych, czyli przeprowadzenia i udokumentowania weryfikacji wypożyczeń i rozliczeń.

Weryfikacja wypożyczeń i rozliczeń publikacji elektronicznych

Etap weryfikacji wypożyczeń i rozliczeń publikacji odbywał się w okresie od 6 do 27 marca 2025 r.

Zgodnie z założeniami etap ten polegał na:

- 1) Wykonaniu zaplanowanych czynności czytania i odsłuchu materiałów Legimi.
- 2) Zebraniu detalicznych danych z systemów informatycznych Legimi dla uczestników biorących udział w weryfikacji z przypisanych do nich kont.
- 3) Niezależnym zweryfikowaniu kwalifikacji transakcji przez system i powiązania z nimi rozliczeń wraz z odniesieniem do uzgodnionych zasad rozliczeń z wydawcami.

Sesje czytania/słuchania realizowano w taki sposób, aby tester przeczytał/przesłuchał co najmniej taki fragment publikacji elektronicznej, który stanowił tzw. darmowy fragment danej publikacji. Zapoznanie się przez czytelnika z fragmentem publikacji elektronicznej mniejszym lub równym darmowemu fragmentowi nie powoduje uwzględniania takiej

styczności z książką jako wliczającej się do przychodu należnego dostawcy treści. Dlatego też czytano/słuchano książki w większym wymiarze, zazwyczaj na poziomie kilkunastu procent publikacji elektronicznej, by mieć pewność, że darmowy fragment został przeczytany/przesłuchany. W przypadku urządzeń Kindle czytano 100% dzieła.

Testerzy korzystali z książek w różny sposób, w tym z kilku tytułów jednocześnie na różnych urządzeniach. Audiobooki słuchano w od 3- do 3,5-krotnym przyspieszeniu.

Dane pozyskane przez Audytora podczas tego etapu zostały zarchiwizowane na potrzeby ich analizy i przygotowania Raportu poaudytowego.

Audyt integralności danych

Podczas kolejnego Etapu 3 kluczowym aspektem był tzw. audyt integralności danych w bazie danych. Upraszczając, podczas tego etapu badano, jakie istniały możliwości pracy na bazie danych statystyk czytelnich i ingerencji w nią, czego rezultatem mogłoby być modyfikowanie liczby książek, za które dostawca treści powinien otrzymać wynagrodzenie.

Punktem wyjścia do przeprowadzenia działań w ramach tego etapu było:

- 1) zrozumienie przez Audytorów działania systemu IT zarządzającego bazą danych wypożyczeń ebooków (ocena kontroli dostępu użytkowników na poziomie aplikacji oraz ocena kontroli i rozliczalności dostępu użytkowników aplikacji do bazy danych) oraz
- 2) zrozumienie przez Audytorów działania bazy danych wypożyczeń ebooków (zrozumienie, w jaki sposób logika biznesowa została zaimplementowana w bazie danych, ocena kontroli dostępu użytkowników uprzywilejowanych, ocena rozliczalności czynności wykonanych przez użytkowników uprzywilejowanych, w tym: integralności śladu audytowego na poziomie bazy danych, logów bazy danych, logów systemu operacyjnego; zasad wdrażania uzasadnionych korekt danych na podstawie zleceń typu „data fix”; zasad przeglądu śladów audytowych w celu wykrywania i usuwania wykrytych nieprawidłowości).

Elementem działań była także ocena ustawień bezpieczeństwa środowiska bazy danych (np. polityka haseł, kontrola dostępu do systemu operacyjnego, kontrola dostępu do bazy danych, itp.), ocena aplikacyjnych (automatycznych) i organizacyjnych mechanizmów kontrolnych zapewniających integralność danych.

Aby zweryfikować te aspekty, zespół audytowy przeprowadził następujące działania:

- 1) Analizę polityki bezpieczeństwa i procedur bezpieczeństwa, w tym dostępu uprzywilejowanego, monitorowania aktywności użytkowników.
- 2) Analizę procedury zarządzania uprawnieniami użytkowników.
- 3) Ocenę zasad nadawania / odbierania uprawnień użytkowników.

- 4) Weryfikację procesu okresowego przeglądu uprawnień użytkowników.
- 5) Weryfikację procesu nadawania / odbierania uprawnień użytkowników.
- 6) Analizę ustawień bezpieczeństwa IT badanego systemu na poziomie aplikacji, systemu operacyjnego i bazy danych w zakresie zapewnienia odpowiedniego poziomu kontroli i rozliczalności dostępu.
- 7) Weryfikację istniejących ustawień dotyczących kontroli i rozliczalności dostępu na poziomie systemu operacyjnego, bazy danych i aplikacji, w tym ustawienia dotyczące haseł, logów i retencji danych.
- 8) Ocenę bezpieczeństwa fizycznego, tj. mechanizmów kontroli dostępu fizycznego do pomieszczeń centrum przetwarzania danych.

Poddano analizie dokumentację definiującą mechanizmy kontrolne oraz przetestowano te mechanizmy na próbie czynności z obszaru zarządzania uprawnieniami użytkowników, monitorowania aktywności użytkowników, transakcji i logów systemowych.

Podstawowe informacje o Raporcie

Ostatnim etapem prac audytowych było przygotowanie Raportu, którego ostateczną wersję Legimi otrzymała w dniu 18 kwietnia 2025 r.

Zgodnie z umową zawartą z Audytorem, Raport zaprezentował wykonane prace oraz ich rezultat. Przedstawiono w nim szczegółowo metodykę testowania, cel i zakres testów, sposób ich organizacji oraz przeprowadzania, a także wnioski z testów wraz z wyliczeniami. Ponadto, w Raporcie opisano wyniki weryfikacji mechanizmów kontrolnych, które funkcjonują w Legimi S.A. i są dedykowane do zapewnienia integralności danych w bazie danych dotyczących wypożyczeń i rozliczeń z dostawcami treści.

Raport zawiera również rekomendacje zmian w systemie Legimi, których wdrożenie Legimi uznała za priorytetowe. Wszystkie zalecenia audytowe zostały zaaplikowane niezwłocznie po ich przekazaniu.

Legimi wskazuje, że Raport zawiera informacje poufne, które stanowią tajemnicę przedsiębiorstwa Legimi S.A. oraz także jej kontrahentów (w szczególności dostawców treści). Z tego względu sam Raport nie może być dostępny publicznie, a niniejsze podsumowanie stanowi szczegółowe omówienie treści Raportu, który liczy 35 stron oraz zawiera 7 załączników. Legimi ma nadzieję, że przygotowane podsumowanie pozwoli rozwiązać wszystkie wątpliwości osób zainteresowanych wynikami audytu.

W tym miejscu zespół Legimi pragnie podziękować wszystkim dostawcom treści, którzy w ostatnich miesiącach wyrazili w różny sposób swoje zaufanie względem Legimi. Personel działu obsługi dostawców treści otrzymał od Państwa wiele wyrazów wsparcia.

W toku komunikacji staraliśmy się możliwie sprawnie i kompleksowo odpowiedzieć na otrzymywane od Państwa pytania. Legimi ma nadzieję, że niniejsze podsumowanie jest dobrym uzupełnieniem tych odpowiedzi, pokazującym „od kuchni” specyfikę współpracy z Legimi.

Przebieg weryfikacji systemu

Przechodząc do podsumowania rezultatów audytu, wskazać należy, że w ramach wspomnianych 900 testów „zwykłych” zweryfikowano 23 kombinacje urządzeń końcowych, modeli rozliczeniowych, kanałów sprzedaży i form utworu literackiego.

Testowano m.in. na urządzeniach końcowych działających na systemie Android dystrybucję za pomocą abonamentu indywidualnego e-booków i audiobooków, za pomocą dystrybucji bibliotecznej e-booków i audiobooków, dystrybucję e-booków obydwu tych kanałów sprzedaży na urządzeniach inkBook oraz Pocketbook oraz na urządzeniach końcowych działających na systemie iOS dystrybucję za pomocą abonamentu indywidualnego e-booków i audiobooków oraz za pomocą dystrybucji bibliotecznej.

W przypadku testów „specjalnych” - z uwagi na ograniczony czas trwania projektu – nie wszystkie z parametrów modelu bibliotecznego były możliwe do zweryfikowania. Należał do nich m.in. czas, po którym egzemplarz uznaje się za „zaczytany” i nie jest możliwe jego dalsze wypożyczanie kolejnym użytkownikom. Czas dostępności takiego pliku cyfrowego wynosi 12 miesięcy.

W ramach weryfikowanych sesji koncentrowano się m.in. na przypadkach, które mogły prowadzić do rozbieżności pomiędzy tym, jak faktycznie przebiegały sesje czytania/słuchania, a tym co zostało zaraportowane przez system Legimi. Dzięki wprowadzeniu mechanizmu, że Legimi codziennie automatycznie dostarczała informacje na temat zarejestrowanych sesji użytkowników testujących, w tym informacje o: 1) identyfikatorze konta użytkownika, 2) czytany/słuchany dzieło, 3) początku i zakończeniu sesji, 4) liczbie przeczytanych słów/przesłuchanych sekund, 5) liczbie unikalnych, wcześniej nieprzeczytanych słów, 6) liczbie słów/sekund liczonych na poczet raportowania, 7) osiągniętemu w ramach sesji tempie czytania, a także o „zaczytanych” dziełach w modelu proporcjonalnym, modelu stosowanym dla użytkowników bibliotek oraz w modelu jednoprogowym i wieloprogowym wraz z ID zaraportowanej transakcji związanej z „zaczyciem”, można było na bieżąco wychwycić takie przypadki brzegowe i zidentyfikować ich naturę oraz wpływ na funkcjonowanie systemu.

W toku działań audytowych zidentyfikowano możliwych 5 problemów, którym przyporządkowano oznaczenia od 1 do 5. Dotyczyły one następujących zagadnień, które poniżej zostaną omówione:

- problem nr 1 – problem, który wyniknął wskutek naprawy błędu nr 2 i 4;

- problem nr 2 – problem związany z „nakładaniem się” czasu sesji czytelniczych w przypadku audiobooków,
- problem nr 3 – problem związany z brakiem synchronizacji danych podczas aktualizacji platformy serwerowej,
- problem nr 4 – problem związany z kompresowaniem danych synchronizacyjnych przy dużych sesjach czytania/słuchania,
- problem nr 5 – problem związany z rejestracją czytania e-booka przy wysokim tempie czytania przez użytkownika

W próbie audytowej tzw. 900 testów „zwykłych” wystąpiło łącznie 114 przykładów jednego z powyższych przypadków.

Z tej liczby z perspektywy Legimi nie stanowi błędu 71 przypadków dotyczących problemu nr 5, tj. w sytuacji niespełnienia kryterium czasu spędzonego na stronie/ekranie książki, gdy aplikacja wychwyciła, że tempo czytania osób testujących wykraczało poza wprowadzony przez Legimi mechanizm weryfikacji naturalnego tempa czytania użytkownika (tzw. zabezpieczenie przed zliczaniem stron wskutek ich „wertowania”). Powtórzenie czytania przez testerów z uwzględnieniem kryterium minimalnego czasu wyświetlenia strony prowadziło za każdym razem do zaraportowania czytania w systemie. W ocenie Legimi mechanizm ten ma istotny walor chroniący interesy twórców i dostawców treści. Zabezpieczenie przed przewijaniem treści („kartkowaniem”) pozwala wychwycić wyłącznie te formy interakcji czytelnika z książką, kiedy faktycznie ją czyta, a nie tylko próbuje dotrzeć do interesującego go fragmentu. Zapobiega też sztucznemu zawyżaniu czytelnictwa (a przez to wynagrodzenia konkretnego dostawcy treści) przez użytkowników dokonujących nienaturalnych aktywności w aplikacji, trudnych do zidentyfikowania w inny sposób.

Jak wspomniano powyżej, wprowadzony limit nie zakwalifikował do rozliczenia części sesji czytelniczych rozpoznanych w systemie jako „kartkowanie” (nienaturalnie szybkie tempo czytania).

Konieczne jest w tym miejscu zastrzeżenie, że na zaraportowanie transakcji jako rozliczonej składa się wiele sesji czytelniczych, zatem niezakwalifikowanie pojedynczej sesji czytelniczej może oznaczać nieprawidłowość w funkcjonowaniu systemu, ale nie oznacza automatycznie braku zaraportowania danej transakcji. W praktyce tylko niewielki odsetek pojedynczych sesji czytelniczych stanowi o zakwalifikowaniu tytułu do objęcia rozliczeniem, jako pochodna stosowanych modeli rozliczeń.

Z dotychczasowych wieloletnich doświadczeń Legimi związanych z analizą czytania publikacji elektronicznych wynika, że czytelnicy zazwyczaj czytają często, ale w małych porcjach tekstu (średnio po ok. 15 min), a wszelkie przerwy w lekturze (wywołane choćby odebraniem połączenia na telefonie) powodują automatyczne zakończenie sesji i rozpoczęcie kolejnej. Dane na temat sesji zależą oczywiście od wielu parametrów, ale

aktualnie Legimi na podstawie próbki rzeczywistych przypadków książek porzuconych (czyli nieczytanych od co najmniej 60 dni) o liczności 79246 przypadków dla 100 różnych tytułów była w stanie ustalić, że średnia długość jednej sesji czytania to „objętość” 1,6% książki, zatem sytuacje, gdy czytelnicy zapoznają się z dużymi fragmentami książek na raz (podczas jednej sesji) zdarzają się niezwykle rzadko. Z tego względu omawiany przypadek brzegowy nie ma istotnego wpływu na działanie systemu rozliczeń. Szacując zatem częstość wystąpienia takiej sytuacji, w przypadku typowego korzystania z aplikacji Legimi, Spółka - bazując na posiadanych danych – może ocenić, w skali rozliczeń, wpływ takiego „zabezpieczenia przed kartkowaniem” na poziomie promila.

Celem uniknięcia ewentualnych przyszłych sytuacji spornych, Legimi w dniu 8 kwietnia 2025 r. zmniejszyła wymagany przez system limit czasu spędzonego na stronie. W rezultacie Legimi zastosowała się do rekomendacji Audytora przyjętej w Raporcie. Efekt tej zmiany pozostał niezauważalny w bieżących rozliczeniach (wspomniany ułamek rzędu promila), jest jednak wyrazem dbałości spółki o podnoszenie standardów funkcjonowania platformy.

W 16 na 900 przypadków testów dotyczących wyłącznie audiobooków system Legimi nie uwzględnił sesji czytelniczych. Przypadki te dotyczyły odstępu audiobooka nie z jego normalną prędkością, lecz w znacznym przyspieszeniu (od 3- do 3,5-krotnym) w sytuacji, gdy po zakończeniu odsłuchiwanie takiego audiobooka czytelnik od razu przechodził do słuchania kolejnej publikacji. Prędkości takie zazwyczaj nie są stosowane przez użytkowników, którzy słuchają książek z prędkością normalną lub zbliżoną do normalnej. Prędkości te jednak funkcjonują w aplikacji Legimi, służą np. przewijaniu dłuższych fragmentów i dlatego system nie rozpoznawał ich jako słuchanie, niemniej jednak nie można wykluczyć sytuacji, że istnieją użytkownicy, którzy z taką prędkością słuchają audiobooków. Wychwycony przypadek związany był z rejestracją czasu słuchania książek, gdyż aplikacja Legimi raportowała, że użytkownik zakończył sesję czytelniczą pierwszej książki później niż faktycznie rozpoczął słuchanie kolejnej książki, a tym samym sesje czytelnicze nakładały się i późniejsza (do momentu oznaczonego przez system jako moment zakończenia słuchania pierwszej książki) nie była uwzględniana. Zespół audytujący odnotował ten przypadek i 11 marca 2025 r. poinformowała o tym Legimi. Legimi dokonało poprawki w rozpoznawaniu sesji z przyspieszeniem 3- i 3,5-krotnym zgodnie z zaleceniem.

Podmiot audytujący zarekomendował Legimi oszacowanie skali występowania zjawiska i jego wpływu na rozliczenia z dostawcami treści. 1 kwietnia 2025 r. Legimi poinformowała Audytora, że przeprowadziła w tym zakresie wewnętrzną analizę. Legimi dysponowała niezagregowanymi logami od stycznia 2025 r. i znając już sytuację, w których taki błąd mógł występować, na bazie tych logów do 11 kwietnia 2025 r. uwzględniono w raportach wszystkie sesje, których taki błąd mógł dotyczyć. Legimi podjęła decyzję o rozstrzygnięciu wszelkich wątpliwości na korzyść dostawców treści, co znalazło już swoje

odzwierciedlenie w rozliczeniach Legimi z dostawcami treści (skala rozbieżności pomiędzy danymi przed i po uwzględnieniu tych sesji osiągnęła okolice poniżej jednego promila). Legimi wskazuje, że sytuacja ta występowała jedynie w ściśle określonych przypadkach, tj.: 1) dotyczyła słuchania audiobooków, a nie dotyczyła czytania e-booków, 2) prędkości słuchania musiały być bliskie maksymalnym, które oferowała aplikacja Legimi, 3) użytkownik po zakończeniu słuchania musiał w krótkim odstępie czasu rozpocząć kolejną sesję czytelnictwa, co w praktyce zachodzi niezwykle rzadko.

Z drugiej strony, zauważono w toku testów, że system Legimi raportował w przypadku modelu bibliotecznego większą liczbę egzemplarzy niż faktycznie przesłuchana. Wynikało to z faktu, że wskutek słuchania książek na maksymalnej prędkości, sesje słuchania różnych czytelników nakładały się, co wpływało na uwzględnianie większej liczby egzemplarzy danego tytułu do transakcji rozliczeniowych. W praktyce jednak ta kwestia również ma niewielkie znaczenie na funkcjonowanie systemu Legimi, gdyż popularność u faktycznych użytkowników słuchania audiobooków z tak wysokim przyspieszeniem i praktyka słuchania całych tytułów w ten sposób przez dłuższy czas jest znikoma.

Audytor zdiagnozował również inny przypadek, który w Raporcie określono jako problem nr 3. Wystąpił on, gdy mimo wymuszenia ręcznej synchronizacji dane nie zostały zarejestrowane przez serwer, na którym wówczas odbywała się synchronizacja platformy serwerowej. Aplikacja Legimi okresowo przesyła dane synchronizacyjne na serwer Legimi, co pozwala zbierać dane o sesjach czytania i przekłada się na rozliczenia z dostawcami treści. Niemniej w toku testów odnotowano 2 przypadki na 900 (czyli 0,22%), gdy dane nie zostały przesłane na serwer. Po wylogowaniu się użytkownika (co poprzedzało często zalogowanie się testera na nowe konto użytkownika), aplikacja nie mogła ich wysłać ponownie, a tym samym pojawiła się rozbieżność pomiędzy sesjami, jakie realizowali testerzy, a dziennymi danymi, jakie dla porównania przekazywała Legimi.

Omawiane przypadki w pewnym stopniu były bliskie więc sytuacjom, gdy np. pewien użytkownik przeczytał offline publikację w aplikacji, wylogował się i więcej aplikacji nie uruchomił. W takich okolicznościach dane o sesjach czytelnictwa nie są przysyłane na serwer ze względu na brak możliwości technicznych. Jednocześnie, gdyby użytkownik skorzystał z aplikacji ponownie po zakończeniu wdrożenia aktualizacji serwera, aplikacja przestałaby te dane na serwer. W testowym przypadku użytkownik jednak wylogował się i nie korzystał więcej z aplikacji, toteż dane nie zostały ponownie wysłane do serwera. W praktyce zatem dane, jakie wygenerował ponownie logujący się do aplikacji użytkownik zostałyby przyjęte przez serwer Legimi i uwzględnione do rozliczeń przysługujących dostawcy treści, choć dotarłyby z pewnym opóźnieniem.

Zespół audytowy zdiagnozował również inny problem, który określono w Raporcie jako problem nr 4. Każdy utwór jest w systemie Legimi podzielony na zakresy. Informacja o części dzieła przeczytanej przez użytkownika w danej sesji jest zapisana z wykorzystaniem powyższych zakresów. W przypadku, gdy liczba przeczytanych przez użytkownika w

ramach jednej sesji zakresów była na tyle duża, że informacja ta przekraczałaby maksymalną wielkość określoną w systemie, była ona dodatkowo kompresowana. Z powodu błędu przy implementacji kompresji możliwe było, że sesja nie została prawidłowo zarejestrowana na serwerze Legimi, a przez to nie była brana pod uwagę przy rozliczeniu z wydawcami.

Zaistnienie tego błędu związane było ze specyfiką przypadków testowych, która polegała na doborze długich fragmentów tekstu w ramach sesji czytelniczych. W pewnym momencie wolumen danych powodował, że dane poddane serializacji, a następnie kompresji, przekraczały dostępny limit dla tego typu informacji. Zdarzenia takie wystąpiły w 21 testach na 900 czyli w 2,33% przypadków. Jednak, jak zostało już wskazane powyżej, czytelnicy zwyczajowo sięgają po publikację, dzieląc zapoznanie się z nią na krótsze fragmenty (przeciętnie wynoszące około 15 minut), co powoduje, że sesja czytelnicza obejmuje mniejszy zakres danych. Przypadek ten pojawiał się więc zatem w szczególnych sytuacjach brzegowych poddanych analizie na potrzeby audytu, choć możliwych do wystąpienia podczas korzystania z aplikacji Legimi przez mającego nadzwyczajnie dużo czasu na lekturę czytelnika.

Audytor przekazał Legimi informację w dniu 11 marca 2025 r. a Legimi niezwłocznie zweryfikowała to zgłoszenie i już następnego dnia wdrożyła zalecaną zmianę w trybie hotfix.

Audytor zarekomendował oszacowanie skali występowania problemu i jego wpływ na rozliczenia z dostawcami treści. Przeprowadzono weryfikację sesji zapisanych w bazie danych („surowych” danych, jakie posiada Legimi, za okres od stycznia 2025 r.). Wszystkie przypadki, które mogłyby podlegać pod problem nr 4 uwzględniono jako prawidłowe sesje czytelnicze i rozliczono z dostawcami treści.

Z uwagi na to, że powszechną praktyką jest zapoznanie się z książką w wielu pojedynczych sesjach, z danych niezagregowanych posiadanych przez Legimi wynika, iż takie przypadki miały marginalny charakter, pozostające bez wyraźnego wpływu na rozliczenia z dostawcami treści.

Wdrożenie hotfixów w dniu 12 marca 2025 r. miało pierwotnie poboczny skutek w postaci niewłaściwego zachowania systemu Legimi, co określono w Raporcie jako problem nr 1. W wyniku zmian w oprogramowaniu systemu sesje czytania z 2 testów na 900 (czyli w 0,22% testów) nie zarejestrowały się z uwagi na fakt, że dwa równoległe działające procesy podejmowały próbę wprowadzenia zmian do tej samej tabeli w bazie danych zbierającej informacje o aktywności użytkowników w tym samym czasie. 20 marca 2025 r. Audytor poinformował Legimi o tym problemie i już następnego dnia otrzymał informację od Legimi, że błąd został naprawiony. Legimi dokonała też niezbędnej korekty (dodała brakujące sesje i transakcje rozliczeniowe) dla wszystkich użytkowników platformy.

Dzięki natychmiastowemu wychwyceniu tego błędu możliwe było przy okazji jego zweryfikowanie w odniesieniu do skali faktycznych transakcji z dostawcami treści. Porównując liczbę książek, która stanowiła podstawę do rozliczenia się z dostawcami treści w okresach od 6 do 11 marca 2025 r. i od 13 do 18 marca 2025 r. stwierdzono, że liczba sztuk książek była praktycznie identyczna (różnica w liczbie sesji na poziomie 0,002%). Zdaniem Legimi, wskazuje to na okoliczność, że błąd miał charakter marginalny, a na liczbę transakcji, jaką raportuje Legimi wpływ mają wyłącznie wybory czytelników, a nie kwestie błędów technologicznych.

Z kolei przeprowadzenie wszystkich 100 testów “specjalnych” (które służyć miały weryfikacji, czy system Legimi prawidłowo łączy dane dotyczące statystyk czytelnicznych użytkowników w różnych modelach rozliczeń i udostępniania publikacji) dało wynik pozytywny, tj. zweryfikowano, że system Legimi łączy dane w sposób poprawny. Nie stwierdzono tym samym błędów, co wskazuje na właściwe funkcjonowanie systemu pod tym kątem.

Jednocześnie zgłaszane w ramach audytu scenariusze zdarzeń, stanowiących przypadki brzegowe, zostały pokryte dodatkowo testami automatycznymi w ramach procedury wytwarzania oprogramowania, co stanowi wykraczającą poza zalecenia audytowe praktykę należytej staranności podnoszenia standardów organizacyjnych.

Weryfikacja rozliczeń

Poczynione do tego momentu testy pozwoliły ponadto przystąpić do weryfikacji poprawności rozliczeń w modelu proporcjonalnym.

Audytora otrzymało od Legimi dane dotyczące generalnych parametrów modelu proporcjonalnego, wyliczanych dla ogółu użytkowników Legimi na potrzeby codziennego przeliczania modelu proporcjonalnego za okres od 1 do 27 marca 2025 r., a także dane dotyczące „zacytania” wszystkich użytkowników Legimi dotyczących dzieł rozliczanych w modelu proporcjonalnym dla dzieł „zacytanych” przez testerów za okres od 1 do 27 marca 2025 r. Legimi przedstawiła też swoje wyliczenia kwot należnych wydawcom dla dzieł „zacytanych” przez testerów z tytułu „zacytań” wszystkich użytkowników Legimi na dzień 27 marca 2025 r. Dostarczono również zestawienie transakcji rozliczeniowych dla dzieł „zacytanych” przez testerów z tytułu „zacytań”.

Zespół audytowy sprawdził, czy publikacje faktycznie czytane/słuchane przez testerów znalazły się w zestawieniu przedstawionym przez Legimi w zakresie i we właściwej ilości, jak również w odpowiedniej liczbie. Liczba zaraportowanych transakcji zgadzała się z liczbą przeczytanych dzieł, przy uwzględnieniu dwóch warunków: 1) liczba transakcji rozliczeniowych dotyczących danego dzieła za dany okres przeliczania modelu nie może przekraczać liczby „zacytań” tego dzieła w tym okresie, oraz 2) w codziennych kalkulacjach modelu proporcjonalnego w ramach danego miesiąca, wyliczona na dany dzień liczba transakcji rozliczeniowych danego dzieła, nie może być mniejsza niż

wyliczona w poprzedzające dni. Podczas testów „specjalnych” przestuchano i przeczytano dzieło udostępnione jako synchrobook®. Zidentyfikowano dwie osobne transakcje rozliczeniowe z dostawcą treści, zapewniającym tę publikację.

Kolejnym zagadnieniem poruszonym w toku audytu była poprawność rejestrowania zdarzeń, które mają wpływ na rozliczenie z wydawcami działającymi w ramach modelu jednoprogowego (czyli takiego, w którym po przekroczeniu darmowego fragmentu przez czytelnika, dostawca treści otrzymuje wynagrodzenie w określonej kwocie przyporządkowanej tej publikacji). W tym modelu rozliczone są aktualnie książki w ramach „Katalogu Klubowego”. Każda poprawnie zarejestrowana sesja czytania/słuchania dzieła w modelu jednoprogowym wygenerowała powiązaną transakcję rozliczeniową. Zweryfikowano również okoliczność, gdy użytkownik przeczytał jakąś książkę częściowo na urządzeniu Kindle, a częściowo na innym urządzeniu. W wyniku testu potwierdziło się, iż publikacja ta została zarejestrowana zgodnie z dostarczoną przez Legimi dokumentacją systemu rozliczeniowego.

Analizę poprawności funkcjonowania systemu Legimi w kontekście modelu wieloprogowego przeprowadzono, weryfikując następujące dane otrzymane od Legimi:

- Zestawienie prezentujące dla każdego z ebooków czytanych przez osoby testujące w modelu wieloprogowym sumaryczny procent jej czytania przez wszystkich użytkowników Legimi łącznie - na moment przed i na moment po ukończonych testach;
- Zestawienie prezentujące dla wszystkich użytkowników czytających wyżej wymienione ebooki ich procent postępu czytania w ramach danego ebooka na moment przed i na moment po ukończonych testach;
- Zestawienie prezentujące wszystkie transakcje rozliczeniowe w modelu wieloprogowym dotyczące wyżej wymienionych ebooków za czas trwania testów.

Testy wykazały 100% poprawność rejestracji postępu czytania przez system informatyczny Legimi. Zweryfikowano w tym celu sumaryczny przyrost punktów procentowych czytania w okresie od początku do końca testów. Testy „specjalne” potwierdziły, że system właściwie „zlicza” dane wygenerowane przez czytelników (dokonuje składania się postępów czytań poszczególnych czytelników) i znajduje to właściwe przełożenie na wygenerowanie transakcji rozliczeniowej dla danego dzieła. ***Dla testów „zwykłych” odnotowano dla każdej z sesji „zaczynania” powiązaną transakcję rozliczeniową.***

Pojawił się natomiast błąd w zakresie zliczenia audiobooków (problem nr 1), który - jak się okazało - związany był z wyżej omówioną kwestią nakładania się na siebie czasów zapoznawania się z tą publikacją. Błąd ten zatem nie wynikał z zasad modelu, lecz innej niedoskonałości technicznej, która została już poprawiona.

Mając dane na temat wszystkich modeli dystrybucji i rozliczeń oraz dane związane z czytaniem/słuchaniem każdej publikacji, możliwe było potwierdzenie przez zespół audytujący, że ***wszystkie z transakcji rozliczeniowych wygenerowanych przez prawidłowe sesje i wiążące się z przekroczeniem darmowego fragmentu dzieła zostały prawidłowo odzwierciedlone w końcowym zestawieniu wszystkich transakcji rozliczeniowych.***

W toku analizy dokumentacji rozliczeniowej stwierdzono także, że ***niezależnie od tego, czy dany użytkownik objęty był jakąś formą odpłatnej usługi (np. abonamentem), czy też przysługiwał mu bezpłatny okres próbny, to dana publikacja elektroniczna, z jaką się zapoznał, podlegała uwzględnieniu przy kształtowaniu wynagrodzenia dla dostawcy treści.***

Zespół audytujący zweryfikował też postanowienia umów łączących Legimi z dostawcami treści w aspektach, które są dla tych dostawców treści specyficzne, np. okres dostępności danego tytułu w “Katalogu Klubowym” zanim dany tytuł stanie się dostępny dla pozostałych użytkowników usług abonamentowych.

Porównanie tych umów pozwoliło wychwycić kilka błędów:

- W przypadku umowy zawartej z jednym z wydawców miało miejsce błędnie przypisany okres karencji w modelu jednoprogowym, czyli czas, po którym dana publikacja powinna być przeniesiona do modelu proporcjonalnego. Legimi, po uzyskaniu informacji od Audytora, o wychwyconym błędzie, wprowadziła właściwe dane, o czym poinformowała Audytora 01.04.2025 r. Jednocześnie Legimi wskazuje, że ta sytuacja nie miała wpływu na rozliczenie z tym wydawców. Nie zidentyfikowano bowiem żadnych dzieł, które byłyby niepoprawnie zaraportowane w wyniku tego błędu.
- W przypadku umowy zawartej z innym wydawcą pojawiła się niespójność pomiędzy zawartym w umowie parametrem dotyczącym wynagrodzenia przysługującego danemu dostawcy treści a danymi przekazanymi przez Legimi. Właściwa wartość parametru powinna mieć zastosowanie w systemie Legimi od lutego 2025 r., ale omyłkowo nie została wprowadzona do bazy danych systemu w badanym okresie. Legimi skontaktowała się z dostawcą treści celem uwzględnienia poprawnej wartości w fakturach, jakie ten podmiot będzie wystawiał w związku z dystrybucją swoich publikacji elektronicznych za pomocą usług Legimi.

Wskazano również, że system rejestrując wartość darmowego fragmentu w liczbach całkowitych, kwalifikował jako przeczytanie/przesłuchanie darmowego fragmentu dopiero taką sytuację, gdy przekroczone o cały 1% wartość darmowego fragmentu. Powyższe mogło mieć wpływ na kwalifikację danej publikacji jako uwzględnianej przy rozliczeniach z dostawcami treści.

Analiza autonomiczności i rozliczalności systemu

Następny obszar działań audytowych związany był z audytem integralności baz danych. System informatyczny Legimi posiada mechanizmy związane z nadawaniem uprawnień użytkownikom oraz rejestrowaniem ich działań na bazach danych. Dostęp osób do systemu podzielony jest pod względem skali uprawnień tak, aby osoby te nie mogły zarówno przypadkiem, jak i intencjonalnie, naruszyć struktury bazy danych oraz dokonywać nieraportowanej aktywności.

W przypadku stwierdzenia błędu lub otrzymania informacji o problemach (np. od osób z działu pomocy technicznej) praktyką przyjętą w Legimi jest stworzenie ticketu (zadania/zgłoszenia) przez osobę, która dowiedziała się o problemie, by przyspieszyć procedurę analizy błędu i – jeśli rzeczywiście występują problemy techniczne – określa się ważność błędu, a potem jest naprawiany. Zdarzenia te znajdują swoje odzwierciedlenia w narzędziach zarządzania pracami informatycznymi (systemach ticketowych), z których korzysta Legimi, a których stosowanie jest globalnym standardem w pracy działów IT. Umożliwia to prześledzenie prac informatycznych w systemie oraz zdiagnozowanie np. takich sytuacji, gdy naprawa jednego błędu wywołała zjawiska niepożądane w innym obszarze systemu. Dodatkowo w trakcie audytu wprowadzono mechanizm powiązywania zdarzeń w systemie z określoną osobą odpowiedzialną za rozwój systemu, co umożliwia dokładniejszą analizę działań podejmowanych przez zespół IT. Wskazać należy, że Legimi rozwija równocześnie system na kilku obszarach, w tym w zakresie funkcjonowania aplikacji Legimi w kilku różnych systemach operacyjnych. Oznacza to, że pewien błąd lub inne negatywne zjawisko występujące w ramach jednej wersji aplikacji Legimi (np. na system Android) nie musi przekładać się na istnienie takiego błędu lub zjawiska w innych wersjach aplikacji (np. iOS). Błąd mający przełożenie na różne wersje aplikacji zaistnieć może tylko na poziomie serwerowym, a więc podczas odbierania danych (np. statystyk czytelniczych) od urządzeń, z których korzystają użytkownicy usług Legimi. Dlatego też w toku prac audytowych członkowie zespołu audytowego dokonali weryfikacji zaczytania książek wybranych do próby w powiązaniu z szerokim spektrum wersji aplikacji i urządzeń, aby możliwe było zweryfikowanie, czy pewne błędy nie występują np. tylko w określonych wersjach aplikacji Legimi (takie jak błędy z synchronizacją danych między aplikacją a serwerem).

Prace w tym obszarze rozpoczęto od dwóch spotkań z dwoma przedstawicielami Legimi odpowiedzialnymi za środowisko IT. Omówiono wówczas zagadnienia związane z: 1) logiką działania aplikacji, 2) łączeniem się aplikacji z bazą danych, 3) architekturą aplikacji, 4) autoryzacją dostępu użytkowników do bazy danych aplikacji, 5) wykorzystaniem dostępu za pośrednictwem konta technicznego, 6) procesem monitorowania działań użytkowników oraz śladzie audytowym przy procesie monitorowania akcji wykonywanych przez użytkowników, 7) dostępem fizycznym do

pomieszczeń serwerowych, 8) procesem rozliczania przeczytanych/przestuchanych książek.

Poddano analizie zarządzanie zmianą w systemach IT, zarządzanie dostępem logicznym oraz monitorowanie aktywności użytkowników. Na tej podstawie Audytor w Raporcie sformułował obserwacje, implikacje i rekomendacje. Raport prezentuje wyniki przeglądu procesów bezpieczeństwa IT obsługujących system Legimi.

Ustalono, że system ticketowy stosowany przez Legimi (i wiele innych podmiotów z branży IT do zarządzania projektami i śledzenia problemów) nie wymagał obowiązkowego wskazania informacji o developerze, testerze i osobie akceptującej zmiany oraz nie wymagał potwierdzenia poprawności wdrożenia przez stronę biznesową. Uwzględniane były natomiast w tablicy przepływu zgłoszeń i odpowiadały regułom metodyki zwinnej, do której stosowała się Legimi. Ta okoliczność w ocenie audytorów zwiększa ryzyko wdrożenia zmiany niewystarczająco przetestowanej lub zatwierdzonej, a tym samym zwiększa ryzyko błędów i awarii w ramach całego systemu. Ta uwaga w zakresie zarządzania zmianą dotyczyła obszarów zmian typu hotfix i wdrożeń planowych oraz zmian typu data fix.

W odpowiedzi na spostrzeżenia zespołu audytującego, w lutym 2025 r. Legimi wdrożyła również bardziej zaawansowany mechanizm rejestracji logów dostępu do baz danych, co pozwoli przeanalizować (w ramach tzw. śladu audytowego) zmiany w bazach danych. Stosowane rozwiązania w zakresie zarządzania uprawnieniami użytkowników również zostaną w najbliższym czasie usprawnione, co powinno przyczynić się korzystnie do zapewnienia integralności i rozliczalności systemu stosowanego przez Legimi.

W obszarze monitorowania aktywności użytkowników zauważono, że opisy procedur były niekompletne lub nieaktualne, a tym samym mogły nie odzwierciedlać rzeczywistych praktyk. Legimi podjęła działania w celu aktualizacji tych procedur, w tym w obszarze wdrożenia dodatkowego mechanizmu logującego zdarzenia związane z działaniami użytkowników i zmian w systemie.

W toku audytu stwierdzono również, że nad prawidłowym funkcjonowaniem systemu Legimi, w tym w obszarze bazy danych, pieczę sprawują pracownicy Legimi na 4 poziomach dostępu, różniących się uprawnieniami. Z uwagi na okoliczność, że publiczne poinformowanie o skali dostępu każdego stanowiska zaangażowanego w pracę na bazie danych, mogłoby generować zwiększone ryzyko dla bezpieczeństwa informatycznego bazy danych oraz samego funkcjonowania Legimi, w niniejszym podsumowaniu pominięto dokładne informacje o uprawnieniach poszczególnych stanowisk / ról. Sesje użytkowników zapisywane są w modelu kolejkowym, co może powodować pewne opóźnienia w zapisie w sytuacjach większego obciążenia systemu. System zbiera takie dane jak informacje na temat użytkownika, czytanej/słuchanej książki i ilości przeczytanych słów oraz czasie, jaki użytkownik na nią poświęcił. Drugie konto techniczne

utworzono dla użytkownika, który procesuje zadania techniczne (np. przygotowuje raporty). Personel Legimi zapisuje dane autoryzacyjne w uznanym i cenionym w środowisku informatycznym menedżerze haseł, który zawiera również dane autoryzacyjne do konta technicznego. Dotyczy to również danych niezbędnych do zalogowania i pracy w systemie informatycznym dla osób mających uprawnienia administracyjne, z których każdy posiada własne imienne konto, co pozwala określić skalę ingerencji tych osób w przetwarzane dane. Przywołany menedżer haseł umożliwia weryfikację, kto wnioskował o dane autoryzacyjne i na tej podstawie mógł mieć dostęp do kont technicznych. W praktyce jednak takie zjawisko nie występuje, bo konto techniczne zapisujące dane w bazie danych służy wyłącznie do komunikacji aplikacji z serwerem, czyli rejestrowania danych związanych z tym, jak czytelnicy (użytkownicy usług Legimi) korzystają ze świadczonych przez Legimi usług udostępniania publikacji elektronicznych.

Na potrzeby audytu Legimi przedstawiło zespołowi audytowemu następujące obowiązujące w spółce procedury związane z systemem IT:

- “Procedurę monitorowania aktywności użytkowników”,
- “Standard - zarządzanie uprawnieniami”,
- “Standard - zarządzanie kontami technicznymi”,
- “Procedura - wdrażania zmian na bazie danych – FIX”,
- Polityka ochrony danych – POD_LEGIMI,
- dokumentacja systemu rozliczeniowego Legimi (dokument ten przedstawia kluczowe informacje dotyczące zasad rejestrowania aktywności użytkowników w aplikacji Legimi, opisów algorytmów rozliczeń z wydawcami oraz przykładowych danych rozliczeniowych),
- dokument opisujący kontrolę dostępu karty wejścia/wyjścia,
- dokument opisujący blokowanie uprawnień po odejściu pracownika.

Analiza brzmienia tych dokumentów skłoniła Audytora do sformułowania rekomendacji, że brzmienie tych procedur powinno - oprócz ich aktualizacji - również rozszerzone o pewne zagadnienia.

Przykładowo, zdaniem Audytora, w “Procedurze monitorowania aktywności użytkowników” powinien znaleźć się opis procedur dotyczących przechowywania, dostępu i ochrony danych uzyskanych z monitorowania. W dokumencie tym powinny być też obecne szczegółowe instrukcje dotyczące instalacji i korzystania z narzędzi do monitorowania. Legimi wskazała w toku audytu, że informacje dotyczące wspomnianych narzędzi uwzględnione zostały w dokumencie “Standard - przygotowanie stacji roboczej”. Odnosnie zaś do przetwarzania danych osobowych przez pracowników Legimi, Legimi wskazuje, że każda osoba z dostępem do danych osobowych podpisuje upoważnienie do przetwarzania danych osobowych w zakresie wynikającym z zadań służbowych pracownika oraz poleceń służbowych przełożonego. Widnieje tam również informacja o

tworzeniu, posiadaniu ewidencji czy rejestrów z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w spółce.

Odnosnie do dokumentu “Standard - zarządzanie uprawnieniami” sformułowano m.in. uwagę, iż dokument ten nie wyjaśnia, jak powinien wyglądać proces zatwierdzania zmian w uprawnieniach przez przełożonego. Wskazano też, że choć przegląd uprawnień jest wymieniony, brakuje szczegółowych informacji na ten temat. Mimo zatem faktu, że przegląd uprawnień odbywa się co kwartał, to nie sprecyzowano, jak ten przegląd powinien się odbywać.

Legimi przyjęła te sugestie i rekomendacje i stopniowo będzie je wdrażała, precyzując w ten sposób obowiązujące procedury i uzupełniając je o brakujące zagadnienia. Rozważone zostanie także przesunięcie pewnych zagadnień do innych procedur. Przykładowo, dotąd tematyka działań w przypadku naruszenia zasad dotyczących uprawnień stanowiła element załącznika nr 9 do polityki bezpieczeństwa Legimi, podczas gdy zespół audytowy zarekomendował uwzględnienie tego tematu w dokumencie “Standard - zarządzanie uprawnieniami”.

Również w przypadku takich dokumentów jak “Standard - zarządzanie kontami technicznymi” czy “Procedura - wdrażanie zmian bazy danych – FIX” wprowadzone zostaną sugestie i rekomendacje. Aktualnie, choć pewne działania związane z zarządzaniem bazą danych i dostęпами do niej są realizowane, nie znajdowało to swojego odzwierciedlenia w procedurach. Zwiększenie precyzji procedur umożliwi zmniejszenie ryzyk informatycznych i zwiększy rozliczalność działań podejmowanych przez osoby z działu IT i innych pracowników Legimi, którzy przeprowadzają operacje na danych.

W przypadku “Polityki ochrony danych – POD_LEGIMI” dostrzeżono brak danych w dokumentacji, które:

- odpowiadałyby na pytania, *“jak często polityka ma być przeglądana i aktualizowana oraz kto jest odpowiedzialny za ten proces”,*
- prezentowałyby opis *“programów szkoleniowych dla pracowników dotyczących ochrony danych osobowych oraz ich roli w realizacji polityki”,*
- dotyczyłyby *“informacji o procesie regularnego przeprowadzania analiz ryzyka związanych z przetwarzaniem danych osobowych oraz dokumentowania wyników tych analiz”,*
- opisywałyby procedury *“postępowania w przypadku incydentów związanych z bezpieczeństwem danych, w tym komunikacji z osobami, których dane dotyczą”.*

To ostatnie zagadnienie uwzględnione zostało w Załączniku nr 9 do polityki bezpieczeństwa, niemniej faktycznie nie było obecne w Polityce ochrony danych.

Kolejnym zagadnieniem podejmowanym w Raporcie jest opis zarządzania uprawnieniami użytkowników. Zespół audytujący przedstawia w nim, jakie grupy administracyjne

funkcjonują w ramach działu IT, jak dokonywany jest przegląd użytkowników, blokowanie dostępu do nich czy zarządzanie zleceniami lub incydentami. Jak wskazano wyżej, Legimi korzysta z platformy - systemu ticketowego służącego zarządzaniu zadaniami realizowanymi przez personel IT. W przypadku zleceń typu data fix na bazie danych, proces inicjuje często osoba, która nie realizuje zadania (np. osoba z personelu działu obsługi klienta, która informuje o braku danej funkcjonalności). Zleceniem zajmuje się dyżurny programista, mający wyłącznie dostęp 'read-only' do produkcyjnej bazy danych i tylko do wybranych kolumn bądź tabel. W przypadku incydentów (takich jak globalne awarie w postaci niedziałającej aplikacji czy niepoprawnego działania kluczowej z perspektywy użytkowników funkcjonalności), proces inicjowany jest przez zarejestrowanie incydentu. Incydent koordynuje dyżurny programista, który dokonuje jego weryfikacji i ocenia go w skali istotności. Po tej wstępnej analizie potrzeba podjęcia reakcji na incydent kierowana jest do odpowiednich administratorów.

Zaudytowano również dostęp fizyczny do pomieszczeń serwerowych. Dostęp do nich jest ograniczony tylko do upoważnionych osób, których wejścia i wyjścia są rejestrowane i wymagają również zastosowania środków autoryzacyjnych będących w ich posiadaniu.

W zakresie zarządzania zmianą zaobserwowano stałą cykliczność dokonywania zmian i wdrażania ich do środowiska produkcyjnego zarówno w obszarze aplikacji mobilnych, jak i wersji webowo-serwerowej. Funkcjonowanie mechanizmów zarządzania zmianą zweryfikowano za pomocą dwóch testów.

W pierwszym z nich wybrano 18 zleceń data fix (z puli 172 zleceń) i stwierdzono, że dla wszystkich złożono wnioski w systemie ticketowym. W 4 przypadkach po realizacji zlecenia nie zostało ono zamknięte przez osobę, która złożyła wniosek w systemie ticketowym, co powinno stanowić potwierdzenie, że zlecenie zrealizowano prawidłowo. W 15 przypadkach informacja o tym, że dokonano zmiany odnotowana była w sekcji komentarzy we wnioskach. Legimi wskazuje, że dotąd nie praktykowała, by zlecenie musiało być zamykane przez wnioskodawcę. Legimi prowadziła zatem monitoring zgłoszenia w sposób dorozumiany (przez zamknięcie zlecenia przez uprawnionego użytkownika w systemie ticketowym), zgodnie z obowiązkami służbowymi tej osoby. Pozwalało to powiadamiać osoby zaangażowane w dany temat (zlecenie) o postępach prac nad rozwiązaniem zlecenia wyłącznie za pomocą zmian statutu zadań w systemie ticketowym. W ocenie Audytora proces zarządzania zmianą funkcjonuje w Legimi w wystarczający sposób według podejścia Agile. Zasadne jest jednak wprowadzenie dodatkowych mechanizmów kontroli, co Legimi będzie chciała wdrożyć w najbliższym czasie.

W przypadku zleceń typu hotfix, z puli 69 zleceń wybrano 7, na których przeprowadzono testy. Również w tym przypadku stwierdzono, że dla każdej zmiany został złożony wniosek w systemie ticketowym oraz każda została zawnioskowana i rozwiązana. W dwóch przypadkach wdrożenie produkcyjne wymagało zmiany w bazie danych. W testowanych

zleceniach również nie praktykowano zamykania zleceń w systemie ticketowym przez osobę wnioskującą o przeprowadzenie zmiany. Test pozwolił potwierdzić, że miał miejsce poprawny przebieg procesu wdrażania wybranych do badania zmian, a wnioski zostały zamknięte zgodnie z ustalonymi wewnętrznymi zasadami, co również jest zgodne w wystarczającym stopniu z działaniem organizacji według metodyki Agile.

W tym momencie Legimi wskazuje, że w przypadku kwestii technologicznych nie zawsze osoba zgłaszającą potrzebę zmian w systemie Legimi ma wystarczające kompetencje lub możliwości, by sprawdzić zmiany w kontekście funkcjonowania całego systemu. Stąd też dotąd przyjmowano, że istotne jest, by “zamknięcie” zadania (uznanie ticketu w systemie ticketowym za zakończony) dokonywane było przez osobę weryfikującą tę kwestię, którą niekoniecznie była osoba inicjująca potrzebę zmiany.

Obserwacje poczynione podczas tego etapu audytu pozwalają stwierdzić, że procedury wymagają aktualizacji i sprecyzowania i takie działanie rekomenduje Audytor. Zasadnym byłoby przeprowadzenie szczegółowego przeglądu istniejących procedur w celu identyfikacji luk oraz uzupełnienia ich o brakujące informacje i szczegółowe opisy procesów. Zmiany w procedurach powinny być dokumentowane i komunikowane do wszystkich pracowników do wszystkich pracowników, których one dotyczą. Dotąd praktyką Legimi było stosowanie systemu ticketowego i za jego pomocą wersjonowanie procedur.

W Raporcie jako rekomendację wskazano również wdrożenie polityki okresowej zmiany haseł. Dotąd w Legimi nie stosowano tego rozwiązania z uwagi na dyskusyjność tej strategii (wielu użytkowników, np. zmienia hasła, modyfikując tylko jeden lub kilka znaków, wskutek czego na bazie “wyciekłych” przeszłych haseł istnieje możliwość łatwego określenia aktualnego hasła). W tym zakresie Legimi dotąd stosowało oficjalne rekomendacje firmy Microsoft, które przede wszystkim postulują wieloelementowy proces autoryzacji, np. z wykorzystaniem różnych narzędzi autoryzacyjnych, co przy okazji ułatwia pracę personelowi, który nie jest zobowiązany do zapamiętywania aktualnego hasła. Rekomendacja poddana jednak zostanie analizie wewnętrznej przez Legimi i na pewno stanowić będzie element rozważań nad procedurami zabezpieczenia dostępu do systemu informatycznego przy najbliższej aktualizacji procedur.

W Raporcie wskazano również, że administratorzy, którzy mają dostęp do edycji bazy danych, mają również dostęp do edycji logów bazy danych. Aktualnie taki dostęp ma tylko jedna osoba, zatem ewentualna edycja logów pozwala bez cienia wątpliwości zidentyfikować, kto taką operację przeprowadził. Pomimo tego faktu, w rekomendacjach zasugerowano “ograniczenie dostępu do logów wyłącznie dla wyznaczonych administratorów oraz wprowadzenie ról i uprawnień, które precyzyjnie regulują, kto może mieć możliwość modyfikacji lub usuwania logów oraz aby administratorzy edytujący bazę danych nie mieli uprawnień do edycji logów”. Legimi wskazuje jednakże, że w ramach Content Security Policy przynajmniej jedno konto w ramach kierowania zmian do

środowiska produkcyjnego musi mieć określony poziom uprawnień, stąd też takie konto utworzono.

Drugą rekomendacją było “opracowanie i wdrożenie polityki zarządzania logami, która określi zasady dotyczące przechowywania, modyfikacji i usuwania logów, a także procedury postępowania w przypadku naruszeń”. Legimi uwzględni tę rekomendację w ramach przeglądu i aktualizacji procedur, zaznaczając przy okazji, że dotąd procedurę postępowania w przypadku naruszeń normował załącznik nr 9 do Polityki bezpieczeństwa.

Inną obserwacją poczynioną przez zespół audytujący była kwestia braku mechanizmu logującego zdarzenia w 2024 r. Legimi wskazuje, że mechanizm ten istniał, ale z retencją danych na poziomie dwóch tygodni, a w połowie lutego 2025 r. został rozbudowany w obecnie funkcjonujący sposób. Zawarte w Raporcie rekomendacje będą stanowić podstawę do dalszych prac projektowych i informatycznych w tym zakresie tak, by mechanizm logujący zdarzenia był najbardziej efektywny, funkcjonalny i nie wpływał istotnie na obciążenie operacjami innych elementów środowiska informatycznego. Rekomendacjami były wdrożenie mechanizmu logującego, który będzie rejestrować wszystkie zdarzenia w systemie oraz bazie danych. Uzasadnione jest również opracowanie polityki dotyczącej logowania zdarzeń, która precyzyjnie określi, jakie zdarzenia powinny być rejestrowane, jak długo logi będą przechowywane oraz kto może mieć do nich dostęp. Polityka ta powinna także zawierać procedury przeglądania i analizy logów. Trzecią rekomendacją jest wprowadzenie regularnych przeglądów logów przez zespół bezpieczeństwa, co pozwoli na identyfikację nietypowych lub podejrzanych działań. Przeglądy te powinny być udokumentowane, a wszelkie nieprawidłowości powinny być analizowane i raportowane, co przyczyni się do zwiększenia bezpieczeństwa systemu.

Podczas prac nad wprowadzaniem zmian w systemie Legimi podstawą do określenia osób, które dokonywały zmian, były statusy na tablicy Agile. W ocenie Audytora, rekomendowanym działaniem jest poszerzenie raportowania w taki sposób, by przeprowadzić szczegółowy przegląd procedur dotyczących zarządzania zmianami, wymusić obowiązkowe wypełniania informacji o developerze, testerze i osobie akceptującej zmianę oraz przeprowadzać regularne szkolenia dla pracowników zaangażowanych w proces zarządzania zmianą. Wskazane jest również regularne przeglądanie przez kierownictwo raportów dotyczących wprowadzanych zmian w celu oceny skuteczności procesu zarządzania zmianą.

Bardzo zbliżone rekomendacje sformułowano również w obszarze potwierdzania poprawności wdrażania zmian, które nie są wynikiem dostrzeżenia przez dział IT niedoskonałości systemu lub chęci wprowadzenia usprawnień, ale inicjowane były przez osoby z personelu odpowiadającego za kontakt z użytkownikami lub partnerami biznesowymi. Jak wskazano, Legimi wiele zmian w systemie inicjowanych jest przez dział

pomocy technicznej (np. otrzymujący informację od użytkowników usług Legimi, że występuje określony problem) lub przez osoby odpowiedzialne za relacje z dostawcami treści (np. wskutek aktualizacji uregulowań umownych pomiędzy Legimi a konkretnym dostawcą treści, co musi znaleźć swoje odzwierciedlenie w rozwiązaniach technologicznych systemu Legimi). W ocenie Audytora rekomendowanym działaniem byłoby uzyskiwanie również potwierdzeń ze strony osoby inicjującej, że wprowadzona zmiana odpowiada jej zapotrzebowaniom. Brak takiego potwierdzenia potraktowany został przez zespół audytujący jako stwarzający ryzyko wprowadzenia rozwiązań, które nie odpowiadają rzeczywistym potrzebom i wymaganiom operacyjnym.

Audyt zwrócił również uwagę na brak okresowego przeglądu uprawnień użytkowników w minionym (2024) roku. Brak takiego przeglądu mógł zwiększać ryzyko posiadania przez niektórych użytkowników nadmiarowych uprawnień, a “okresowy przegląd uprawnień pozwala na wykrycie i zniwelowanie” błędów polegających np. na omyłkowym przyznaniu takich uprawnień lub ich brak odebrania osobie, która zmieniła stanowisko lub zakończyła pracę. Legimi wdrożyła mechanizm okresowego przeglądu uprawnień przed rozpoczęciem audytu i założono przegląd uprawnień co kwartał.

Uwagi końcowe

W toku działań audytowych zespół wyłoniony przez Audytora poddał analizie różnorodne aspekty funkcjonowania systemu Legimi, aby zweryfikować zarówno pewne kwestie techniczne, jak i związane z rozliczeniami z dostawcami treści.

Wychwycenie wyżej wskazanych przypadków brzegowych oraz zastosowanie przez Legimi zaleceń poaudytowych nie miało istotnego wpływu na wysokość wynagrodzenia dla dostawców treści, a jakiegokolwiek wątpliwości (dotyczące przypadków wychwyconych w testach) Legimi rozstrzygała zawsze na ich korzyść, akceptując je jako zdarzenia, które powinny znaleźć swoje pozytywne przełożenie na wynagrodzenie dostawców treści. System zaprojektowano, by dane o transakcjach przetwarzał w sposób dokładny i odzwierciedlający faktyczne czytelnictwo, a następnie by dane pozwalały wyliczyć wynagrodzenie dla poszczególnych dostawców treści zgodnie z zawartymi z nimi umowami.

Legimi pozyskała istotną wiedzę, którą zamierza wykorzystać w celu podwyższenia poziomu zabezpieczeń i rozliczalności systemu Legimi. Sugestie i rekomendacje zostaną uwzględnione w najbliższych miesiącach podczas kolejnych prac technologicznych oraz będą uwzględnione w planach rozwoju systemu. O gotowości Legimi do zapewnienia możliwie jak najwyższej jakości systemu informatycznego oraz zarządzania tym systemem świadczy fakt, że w toku audytu w trybie pilnym podejmowano działania, by wdrożyć wskazywane przez Audytora postulaty. Pokazuje to wysoki poziom merytoryczny personelu działu IT Legimi oraz jego zaangażowanie w doskonalenie systemu.

Legimi ma nadzieję, że niniejsze podsumowanie pozwala zaspokoić zainteresowanie osób oczekujących prezentacji wyników audytu. Przygotowując to Podsumowanie staraliśmy się w sposób możliwie precyzyjny i przystępny przedstawić przebieg audytu oraz poczynione ustalenia i rekomendacje. Mamy nadzieję, że niniejsze podsumowanie pozwala zaspokoić zainteresowanie osób oczekujących prezentacji wyników audytu.

Zastrzeżenie

Celem pełnej prezentacji poczynionych przez zespół audytujący obserwacji i rekomendacji uzasadnione jest w tym miejscu wskazanie założeń i ograniczeń, jakie wiązały się z audytem. Należy podkreślić, że Audytor przygotował Raport w oparciu o przekazane Audytorowi przez Legimi dane i dokumenty oraz informacje uzyskane podczas rozmów z pracownikami Legimi do dnia 1 kwietnia 2025 roku. Audytor nie podejmował innych prac poza tymi, jakie opisał w Raporcie. Nie dokonywał też analizy kompletności, prawdziwości ani wiarygodności danych, jakie przekazywała Legimi, chyba że w Raporcie zaznaczono inaczej. Raportu nie można traktować jako badania sprawozdania finansowego, opinii czy porady prawnej lub podatkowej. Usługi Audytora objęły przede wszystkim procedury analityczne przeprowadzone w oparciu o udostępnione Audytorowi informacje, dane oraz wyjaśnienia. Żadne stanowisko czy ustalenie Audytora nie powinno być analizowane czy interpretowane w oderwaniu od całości Raportu. Legimi nie jest uprawniona do ujawniania Raportu osobom trzecim bez uprzedniej pisemnej zgody Audytora poza przypadkami i zgodnie z trybem opisanym w umowie łączącej Legimi z Audytorem.

Wszelkie informacje, stanowiska i wyjaśnienia zawarte w niniejszym podsumowaniu stanowią informacje, stanowiska i wyjaśnienia sformułowane przez Legimi. Jedynym dokumentem, który prezentuje stanowisko i ustalenia Audytora jest Raport wraz z załącznikami.

Niniejszy dokument powstał jako dokument Spółki w celu wywiązania się z deklaracji złożonej w raporcie ESPI z dnia 12/2024, jak również by uprzystępnąć zainteresowanym zawarte w Raporcie ustalenia. Wnioski w nim prezentowane bazują na Raporcie audytora oraz stanowiskach doradców uczestniczących w procesie audytu i stanowią ich podsumowanie. Warto jednak zaznaczyć, że dokument ten nie jest autorstwa którejkolwiek z firm doradczych zaangażowanych w proces ani nie może być traktowany jako ich stanowisko lub ustalenie.

Legimi, przygotowując podsumowanie, podjęła starania, by zawarte w tym podsumowaniu sformułowania były możliwie jak najbliższe brzmieniu sformułowań zawartych w Raporcie (i załącznikach do niego), a ewentualne komentarze i odniesienia się co do treści Raportu służą wyłącznie wyjaśnieniu pewnych zagadnień, w szczególności osobom mającym nieco mniejszą wiedzę na temat funkcjonowania środowiska informatycznego lub zagadnień branżowych. Za wszystkie ewentualne

różnice interpretacyjne lub jakiegokolwiek błędy lub niedociągnięcia w zreferowaniu treści Raportu lub cytowaniu jego fragmentów odpowiedzialna jest Legimi. Legimi zastrzega, że podsumowanie to, podobnie jak Raport, nie mogą i nie powinny stanowić opinii lub porady podatkowej lub prawnej, jak również służyć podejmowaniu decyzji inwestycyjnych. Audyt nie obejmował badania sprawozdania finansowego, zatem nie może być traktowany w ten sposób. Podobnie wykonane przez Audytora w toku działań audytowych czynności nie obejmowały analizy prawnej oraz technicznej zidentyfikowanych kwestii, jak również wyceny majątku Legimi (za przypadkami opisanymi wprost w Raporcie).

Podpisy:

Mikołaj Małaczyński – Prezes Zarządu

Mateusz Frukacz – Członek Zarządu

Georgi Gruew – Przewodniczący Rady Nadzorczej
