**Szanuj prywatność**

Mimo że pracował w firmie od niedawna, Wendell lubił pracować z Belindą. Miała taki spokojny, cichy sposób bycia, a on nie bał się zadawać jej żadnych pytań. Z Alexem lub Henrym nigdy nie wiadomo, czy nie staniesz na cienkim lodzie.

– Hej, Belindo.

– Hej, Wendell, jak leci?

"Świetnie." Wendell potarł czubek głowy. – Muszę cię poprosić o przysługę. Czy możesz przygotować dla mnie miejsce do pracy? Mike poprosił mnie o poprowadzenie tego małego projektu, aby lepiej poznać klientów i potrzebuję przydzielonego miejsca na dysku.

Belinda odsunęła krzesło z pustego biurka obok siebie. "Pewnie nie ma problemu. Usiądź."

Wendell usiadł i patrzył, jak Belinda pracuje. Opakowane skrypty, których używał zespół, nie wyglądały już tak obco, a on oswoił się ze składnią i terminologią.

"Ile potrzebujesz?"

„Uch. Powiedzmy 500 GB?”

"Jasne. Wiesz co, dam ci miejsce na dysku, ale dam ci też wszystkie uprawnienia, więc będziesz właścicielem danych. Będziesz także właścicielem grupy, która ma dostęp do przestrzeni, co oznacza, że będziesz mieć także możliwość dodawania i usuwania członków grupy, jeśli będziesz potrzebować kogoś innego do pracy z Tobą nad projektem, dobrze? Nie będzie można zmienić rozmiaru obszaru, ale jeśli potrzebujesz więcej miejsca, po prostu daj mi znać, OK.”

**„Brzmi znakomicie.”**

Belinda zapisała długie polecenie. „O co chodzi w tym projekcie?” Wendell położył łokcie na kolanach i pochylił się do przodu. „Mike chce, żebym przeprowadził mały eksperyment. Chce, żebym sprawdził, czy istnieją jakieś powiązania między adresami domowymi naszych klientów a lokalizacjami sklepów. Na przykład, jeśli idą na zakupy o określonej porze, na przykład wracając z pracy, mogą wejść do sklepu, który jest bliżej miejsca pracy niż ich domu. Jeśli jednak zrobią zakupy w weekend, jest bardziej prawdopodobne, że zrobią to w lokalizacji znajdującej się w pobliżu ich adresu domowego. Coś w tym stylu. Chyba Mike chce, żebym zapoznał się z modelami danych, których używamy. To wszystko." "O fajnie. Jestem pewien, że wiele się nauczysz z tego ćwiczenia. Wiesz, pewnego dnia Alex założył dla mnie wysokie konto, żebym mógł uruchomić tę aplikację dla jednego z moich klientów. Występowały problemy z wydajnością i potrzebowałem uprawnień, aby móc je rozwiązać. Znalazłem tam również wiele przydatnych korelacji.” – Tak, powiedział mi o tym. Belinda odwróciła się w jego stronę. „Czy wiesz, jakich danych będziesz używać podczas ćwiczeń?” Wendell skrzywił się. „To jest rzecz, o której wciąż myślę. Myślałem o wygenerowaniu losowych fikcyjnych danych przy użyciu starego skryptu napisanego przez Gopala, ale nie wiem, na ile to będzie przydatne. To nie jest tak, że wykorzystamy te informacje do czegokolwiek prawdziwego”. "Powiem ci, co." Belinda pstryknęła palcami. „Może dam Ci kopię danych moich klientów? Mogę przenieść pliki do Twojego obszaru pracy, a ponieważ nie będziesz wykorzystywał analizy danych w produkcji, wszystko będzie dobrze. Tylko upewnij się, że dane są bezpieczne, dobrze?” Wendell pojaśniał. "Oczywiście. To brzmi naprawdę fajnie. Dzięki." Belinda skrzywiła się. – Czy mogę cię prosić o wielką przysługę? – Tak, jasne. „Właściwie mam problem, w którym mógłbyś mi pomóc. Mam projekt, w którym próbuję wyczyścić pełne dyski i usunąć nieużywane katalogi domowe. Na przykład, jeśli użycie wzrośnie do 95%, zarchiwizuję następnie każdy folder, w którym nie było dostępu do żadnych plików w ciągu ostatnich 3 miesięcy, lub jeśli użytkownik się nie

zalogował, mogę po prostu zmniejszyć jego przydział do kilku MB . Ale jest kilka katalogów, które stale się rozwijają. Są to katalogi domowe kilku użytkowników z tymczasowo zablokowanymi kontami w systemie Linux, ale muszą tam istnieć procesy, które nadal zapisują te pliki. Wendell potarł brodę. „Hm. Cóż, myślę, że możemy uruchomić skrypt obejmujący całe środowisko, który sprawdzi, czy jakieś procesy przechowują otwarte uchwyty plików do tych katalogów domowych, a następnie zobaczymy, co możemy zrobić dalej. Belinda poruszała palcami, jakby pisała na klawiaturze. "Mógłbyś?" Wendell podszedł do krawędzi biurka, żeby móc pracować na laptopie. „Daj mi jakieś 10 minut na napisanie scenariusza. Potem sprawdź, czy niczego nie zniszczę, i wtedy to uruchomimy. Wendellowi podobało się to wyzwanie. Lubił doskonalić swoje umiejętności pisania scenariuszy. Co więcej, uznał to za najlepszy sposób na poznanie nowego środowiska. Mimo że pod maską znajdowała się znajoma technologia, wszystko wyglądało nieco inaczej niż w jego ostatnim miejscu pracy. „OK, myślę, że mam to" – powiedział Wendell. „Scenariusz znajduje się w naszym obszarze pracy grupowej". Spojrzała na kod. „Uruchommy to." Kilka minut później otrzymała raport i zaczęła przeglądać wyniki. „Tutaj nie ma nic zbyt oczywistego." Wendell zmarszczył brwi. „Więc coś zapisuje do tych plików, ale nie jest to jeden, stale działający proces. Więc myślę, że musi być jakieś zaplanowane zadanie, które uruchamia się od czasu do czasu, zapisuje trochę, a następnie kończy się. Spróbujmy czegoś innego. Zmapujmy rozmiar wszystkich plików znajdujących się na tych zablokowanych kontach. Następnie sprawdzamy ponownie co 5 minut, powiedzmy co godzinę, i sprawdzamy, czy są jakieś zmiany. – W takim razie w sam raz na lunch. Belinda uśmiechnęła się. „O tak, umieram z głodu. Pozwól mi przepisać ten scenariusz i wtedy możemy iść. Po lunchu Belinda miała do przejrzenia nowy zestaw kłód, ale tym razem udało jej się osiągnąć postęp. Jedno z kont miało dużą pulę poczty, która stale rosła. Wendell wskazał i przypadkowo dotknął monitora Belindy. Nienawidził, kiedy to się działo. Nie lubił zostawiać śladów odcisków palców na ekranie. „Wydaje mi się, że w środowisku działają zautomatyzowane zadania wysyłające wiadomości e-mail do użytkownika. Podobnie jak w przypadku zakończenia zadania wsadowego. Chyba nadal są włączone. Belinda podniosła wzrok znad danych dziennika. „Czy możemy sprawdzić, które procesy to robią?" Wendell zapiszczał. "Zdradliwy. Nie ma sposobu, aby dowiedzieć się, w jaki sposób te procesy faktycznie wysyłają wiadomość e-mail. Ciężko powiedzieć." Belinda uniosła brwi. „Ale… może moglibyśmy zajrzeć do skrzynki odbiorczej użytkowników i dowiedzieć się, co wysyła e-maile. BTW, czy masz pomysł, jak otworzyć pocztę?" Wendell skinął głową. „Tak, możemy spróbować. Jest taki mały, schludny, tekstowy parser poczty, którego możemy użyć." Uruchomił na swoim komputerze nowe okno terminala i pokazał jej, jak go używać z własną lokalną skrzynką pocztową. "Świetnie." Belinda raz czy dwa obejrzała się, przyglądając się strukturze dowodzenia i flagom. Następnie otworzyła pocztę klienta. „OK, więc to są rzeczywiste raporty od klienta" – mruknęła Belinda. „Może to jakiś test, który przeprowadzili jakiś czas temu i po prostu o nim zapomnieli". "Najprawdopodobniej. Posortujmy e-maile według rozmiaru." Belinda ponownie wyświetliła dane. „O tak, zdecydowanie. Znam imię tego gościa. Współpracowaliśmy z nimi nad stworzeniem planu odzyskiwania po awarii. Dlatego co godzinę tworzą statystyki dotyczące logowań użytkowników, pakują je i wysyłają pocztą elektroniczną. Dzięki temu w przypadku awarii głównego centrum danych mogą mieć pewność, że zapasowe serwery internetowe są poprawnie skonfigurowane i że nie ma problemu z łącznością zewnętrzną". Wendell westchnął. „No cóż, mogą potrzebować tych danych. Prawdopodobnie powinniśmy porozmawiać z menadżerem użytkownika i zobaczyć, co chce z tym zrobić". Belinda uśmiechnęła się. „Dziękuję, Wendell." "Jasne. To mi bardzo pomaga." Belinda skinęła głową. „Zawsze najwięcej nauczysz się, pracując z rzeczywistymi danymi produkcyjnymi. Któregoś tygodnia Cezar poprosił mnie o pomoc. Polecił swoim klientom błędne wprowadzenie pewnych wartości do swojej bazy danych i zapytał mnie, czy mogę mu w tym pomóc. Robimy tak wiele z naszymi klientami, ale nie zawsze wiesz, co tak naprawdę robią ze swoimi danymi. Ale kiedy już dokonasz prawdziwej zmiany środowiska produkcyjnego, wszystko działa jak należy". Wendell był w optymistycznym nastroju, szczęśliwy, że mógł pomóc Belindzie w rozwiązaniu zagadki wzrostu danych.

„Wyślijmy e-mail do menedżera. Kto to napisze, ty czy ja?" – Cóż, to moi klienci. Zrobię to" – powiedziała Belinda. Dlaczego należy szanować prywatność?

Prywatność to jedna z tych rzeczy, które są z natury intuicyjne i oczywiste, a mimo to wymagają głębszej analizy, gdy temat jest poruszany. Rdzeń słowa prywatność oznacza pewne indywidualne odosobnienie i wolność, co na pozór stoi w sprzeczności z oczekiwaniami publicznego miejsca pracy, w którym współpracujemy z dziesiątkami i setkami osób. Rzeczywiście dopiero niedawno, w epoce cyfrowej, pojęcie prywatności zaczęto wiązać z kontrolą publiczną. Powstanie maszyny zmieniło sposób, w jaki wchodzimy w interakcję z otoczeniem. W przeszłości dzielenie się wiadomościami było sprawą trudną, komplikowaną przez wyzwania związane z podróżami na duże odległości i niskim poziomem umiejętności czytania i pisania w populacji ogólnej, co czyniło komunikatorów cennym, szanowanym i zaufanym elementem społeczności. Wynalazek i zastosowanie elektryczności niemal z dnia na dzień zaprzestały mechanicznego rozpowszechniania wiadomości, umożliwiając ludziom oddalonym o tysiące mil (lub, jeśli wolicie) kilometry, komunikowanie się między sobą z jedynie krótkim opóźnieniem. Pojawienie się komputera sprawiło, że odległości i upływ czasu stały się jeszcze mniejsze, czego kulminacją była rzeczywistość czasu niemal rzeczywistego, którą cieszymy się dzisiaj. Rzeczy, które dzieją się na jednym końcu globu, są natychmiast rejestrowane, rejestrowane i udostępniane milionom ludzi na całym świecie, niemal bez barier i filtrów. Rozprzestrzenianie się i wszechobecność współczesnych informacji stworzyło również potężny efekt uboczny. W przeszłości ludzie mieli większą swobodę w wyborze informacji, które chcą wykorzystać. Gdyby nie chcieli czytać gazety, po prostu by tego nie robili. W dzisiejszych czasach jest to prawie niemożliwe, ponieważ każde medium cyfrowe to niemal nieograniczone źródło nowych informacji, czy tego chcemy, czy nie. Nasza chęć wchłaniania informacji jest w pewnym sensie odwrotnie proporcjonalna do naszego narażenia i dostępności do tych informacji. A wraz z kurczeniem się przestrzeni osobistej, do której możemy pozwolić, aby informacje przedostały się do środka, potrzeba prywatności wysunęła się na pierwszy plan naszych priorytetów. Ponieważ każde urządzenie cyfrowe jest wektorem wymiany danych, granice między tym, co uważamy za przestrzeń prywatną, a domeną publiczną, zacierają się. Potrzebujemy sposobów i metod ograniczenia ujawniania informacji, które uważamy za prywatne. Potrzeba ta nie przekłada się jednak od razu na to, co postrzegamy jako funkcje publiczne, takie jak nasze miejsce pracy. Jednak koncepcje prywatności obowiązują tam tak samo rygorystycznie, jak w przypadku każdej osoby. W związku z tym prywatności nie należy już traktować jako nośnika tożsamości. Jest to miara narażenia, na skutek której dowolna osoba, grupa lub zbiór danych może zostać skrzywdzona w przypadku udostępnienia ich poza określonymi granicami. Jeśli pracujesz w branży IT, Twoje życie jest o wiele trudniejsze. Informacje stały się podstawą praktycznie bardzo wielu biznesów. Nawet firmy, które nie mają nic wspólnego z technologią informatyczną, zatrzymają jakąś kadrę IT lub dzierżawią takie usługi. Administracja systemami w praktyce oznacza niemal nieograniczony dostęp do sprzętu, oprogramowania, własności intelektualnej (IP) i ogromnych ilości danych generowanych przez przedsiębiorstwa, zarówno wewnętrznie, jak i zewnętrznie. Każdy z nich jest potencjalną pułapką, czekającą, aby usidlić nieostrożnych. A wtedy prywatność staje się czymś więcej niż miarą narażenia. Staje się kluczowym filarem, dzięki któremu przedsiębiorstwa mogą zostać zniszczone. Nie pomaga masowa liczba naruszeń danych, których byliśmy świadkami w ciągu ostatniej dekady. Niemal co tydzień ukazuje się biuletyn informacyjny na temat tej i tej firmy, której dane zostały skradzione. Od danych kart kredytowych po adresy e-mail, adresy i historię zakupów – całe archiwa i bazy danych są usuwane z siedziby firmy i uwalniane na wolność. Obawy dotyczące prywatności rosną, ponieważ ludzie udostępniają swoje dane osobowe firmom takim jak Google, Facebook i Microsoft w zamian za bezpłatne lub tanie informacje i usługi. Warunki prywatności są jasno określone pod względem prawnym, którego niestety przeciętny użytkownik tych usług nie czyta lub nie jest w stanie w pełni zrozumieć. Po zdefiniowaniu warunków dotyczących prywatności firmy muszą podjąć wszelkie środki

ostrożności, aby nie tylko przestrzegać własnych warunków, ale także przepisów dotyczących prywatności obowiązujących w każdym ze związków/krajów/stanów/regionów, w których prowadzą działalność. Mimo że w Stanach Zjednoczonych nie obowiązują szczegółowe przepisy dotyczące cyberbezpieczeństwa, dyrektor generalny Facebooka został wezwany przed Kongres, aby wyjaśnić, w jaki sposób dane osobowe użytkowników są udostępniane firmie zewnętrznej. Ta zewnętrzna firma została następnie zatrudniona do pomocy w kampanii prezydenckiej w USA, w której dane osobowe mogły zostać wykorzystane do kierowania reklam. Najprawdopodobniej zespół zbierający dane dotyczące osobowości nie planował, że będą one dostępne do innych zastosowań poza pierwotnym zamierzeniem. Najprawdopodobniej został przekazany zewnętrznej firmie z najlepszymi intencjami. Ale czy użytkownicy Facebooka, którzy wzięli udział w teście, zostali powiadomieni o zmianie sposobu użytkowania? Czy pierwsi badacze zostali powiadomieni? Kto został poinformowany po zauważeniu błędu? Czy podjęto próbę natychmiastowego naprawienia błędu? Etyczne zachowanie nie tylko pomaga zapobiegać przypadkowemu i niezgodnemu z prawem udostępnianiu prywatnych danych, ale także promuje działania mające na celu zaangażowanie odpowiednich osób w celu szybkiego rozwiązania problemów związanych z prywatnością. Każde naruszenie tego rodzaju podważa zaufanie i reputację zaangażowanych firm, może skutkować wysokimi grzywnami i odszkodowaniami pieniężnymi dla osób, których to dotyczy, a czasami wiąże się z odpowiedzialnością karną dla właścicieli firm, kadry kierowniczej, a nawet pracowników. Naruszenia prywatności i zacieranie się granic między tym, co uważamy za domeny osobiste i publiczne, wywołały ostry sprzeciw w całej branży, ponieważ kraje wdrażają zasady i regulacje mające na celu zapewnienie użytkownikom większej kontroli nad ich danymi. Ogólne rozporządzenie UE o ochronie danych (RODO)1 opracowane w 2016 r. i wdrożone na początku 2018 r. to doskonały przykład przyjęcia przez pozarządowy Parlament Europejski rozporządzenia mającego na celu ochronę prywatnych obywateli Unii Europejskiej i Europejskiego Obszaru Gospodarczego. Podobnie w Stanach Zjednoczonych stan Kalifornia właśnie przyjął ustawę o ochronie prywatności konsumentów2, która ma na celu rozwiązanie wielu problemów związanych z prywatnością cyfrową i ma wejść w życie w 2020 r. Z drugiej strony wiele krajów albo nadal tego nie robi, posiadają przepisy definiujące prywatność cyfrową lub korzystają z przestarzałych przepisów, które nie są zgodne z krajobrazem nowoczesnych technologii, co powoduje niespójność i zamieszanie w sposobie traktowania danych. Nie ma nic prostszego niż wysłanie kilku plików w drugi koniec globu, ale konsekwencje prawne takiego działania mogą być ogromne. Jako administrator systemu, programista lub po prostu niewinny pracownik pomocy technicznej jesteś cienką linią klina. Zamierzonym celem tego rozdziału nie jest zwiększenie poczucia paranoi. Daleko stąd. Zamierzamy zapewnić proste i jasne wskazówki, jak postępować etycznie w złożonym, niejednoznacznym i niebezpiecznym świecie danych. Często nie masz wpływu na dane, ale możesz kontrolować swoje zachowanie i reakcję na sytuacje, w których zetkniesz się z danymi.

**Szanuj prywatność**

Prywatność jest jednostką miary zaufania. Jeśli otrzymasz dane, otrzymasz zaufanie.

Jeśli potrzebujesz dostępu do prywatnych informacji, uzyskaj pozwolenie. Rozmowa Wendella i Belindy to historia opowiadana tysiące razy w całej branży IT. Pracę rzadko wykonuje się w izolacji i może zaistnieć potrzeba polegania na pomocy współpracowników. Dość często będziesz narażony na nowe wektory danych, niezależnie od tego, czy będą to rutynowe dzienniki systemowe, czy analizy klientów. Każde takie spotkanie jest okazją do nauczenia się nowych rzeczy, ale jest też sprawdzianem etycznego postępowania, nawet jeśli ludzie niekoniecznie tak to traktują. Niezależnie od tego, z jaką konkretną sytuacją się spotykasz, jeśli musisz przetwarzać dane prywatne, powinieneś poprosić o zgodę właściciela danych – osobę lub podmiot odpowiedzialny za dane.

**Jeśli przypadkowo ujawnisz informacje prywatne, powiadom o tym .**

Mogą wystąpić wycieki danych. Stanie się. Nawet mając najlepsze intencje, praktyki i narzędzia, możesz przypadkowo ujawnić prywatne informacje. Czasami narażenie może być niewielkie, a szkody minimalne lub żadne, ale mimo to należy upewnić się, że właściciel danych został powiadomiony. Jeśli ktoś powierzy Ci swoje dane, Twoim obowiązkiem będzie zarządzanie tymi danymi w sposób jasny i przejrzysty.

**Ochrona prywatnych danych dzięki wyraźnym właścicielom**

W tej historii było kilka rzeczy zrobionych dobrze. Wendellowi przydzielono prywatną przestrzeń na dane, a Belinda zapewniła Wendellowi odpowiednie uprawnienia do zarządzania danymi. Dam ci miejsce na dysku, ale dam ci też wszystkie uprawnienia, więc będziesz właścicielem danych. Wendell poprosił o miejsce na dysku dla swojego projektu roboczego, a Belinda również odpowiedziała, przypisując mu wszystkie niezbędne uprawnienia, aby mógł być właścicielem danych. Jest to ważne, ponieważ wszystkie dane muszą być własnością w sposób jednoznaczny. Musi być wyznaczona osoba, która będzie odpowiedzialna – i to odpowiedzialna – za przetwarzanie odpowiednich danych. Odpowiedzialność będzie się różnić w zależności od rodzaju wykorzystywanych danych i konkretnych działań z nimi związanych. Będziesz mieć także możliwość dodawania i usuwania członków grupy. Jako właściciel danych Wendell staje się również odpowiedzialny za wszelkie prace wykonane z danymi tam przechowywanymi. Ponownie eliminuje to niejasności. Wendell jest jedyną osobą kontaktową w zakresie przetwarzania danych i w razie potrzeby może delegować swoje obowiązki. To także usprawnia procedury pracy, gdyż nie ma już potrzeby kontaktowania się z Belindą i proszenia o dodatkowe zmiany w przydzielonej przestrzeni dyskowej. Jako właściciel Wendell ponosi odpowiedzialność, a dzięki możliwości dodawania i usuwania członków obszaru dysku jest także odpowiedzialny za wszelką pracę tu wykonaną. Z kolei jeśli ludzie będą potrzebować dostępu do danych przechowywanych na terenie Wendella, będą musieli poprosić go o pozwolenie.

**Bez autoryzacji dane prywatne są podatne na zagrożenia**

Właściciele danych muszą kontrolować wszystkie punkty dostępu do danych. Należy zidentyfikować takie punkty i uzyskać wyraźne zezwolenie na dostęp do nich i korzystanie z nich. Znalazłem tam również wiele przydatnych korelacji. Historia Belindy ujawnia wiele delikatnych problemów związanych z rozwiązywaniem problemów z wydajnością aplikacji jej klientów. Chociaż ma dobre intencje, a rozwiązywanie problemów związanych z przepływem klientów jest nawet obowiązkiem zawodowym, naraziła się na potencjalne naruszenie prywatności klientów, uruchamiając ich aplikacje oraz przeglądając i przetwarzając dane, a następnie wyciągając wnioski bez ich wyraźnej wiedzy i pozwolenie.

**A może dam Ci kopię danych moich klientów?**

Belinda może uzyskać zgodę swoich klientów na przechowywanie i dostęp do niektórych ich danych, ale jest mało prawdopodobne, że ma taką samą zgodę na udostępnianie tych danych swoim współpracownikom. Akceptując kopię, Wendell nieumyślnie przejmuje odpowiedzialność za dane klientów Belindy. Co więcej, ani Belinda, ani on nie zapytali klienta, czy wyrażają zgodę na taki ruch. Co więcej, choć wcześniej Belinda rzeczywiście postępowała zgodnie z właściwymi procedurami, przypisując Wendellowi własność i kontrolę nad przestrzenią dyskową na potrzeby swojego projektu testowego, ona sama postąpiła odwrotnie w przypadku własnych danych. Postanowiła stworzyć kopię i tym samym wprowadzić do systemu niejednoznaczność. Być może za kopię danych klientów odpowiada teraz Wendell, ale czy odpowiada on również za klientów Belindy? Mogę przenieść pliki do Twojego obszaru pracy, a ponieważ nie będziesz wykorzystywał analizy danych w produkcji, wszystko będzie dobrze. Tylko upewnij się, że dane są bezpieczne, dobrze? Belinda przyjmuje tutaj kilka założeń. Wendell może w rzeczywistości wykorzystać część analizy danych do celów innych niż test. Wendell

nie określił w pełni zakresu swojego eksperymentu, w związku z czym nie wie, co może zrobić z danymi. Wyniki mogą okazać się na tyle cenne, że pozwolą na wprowadzenie zmian w środowisku. W takim przypadku Wendell potrzebuje wyraźnej zgody Klienta na wykorzystanie jego danych w celach innych niż zakres uzgodniony z Belindą. Klient może nawet wyrazić chęć takiego wykorzystania, ale ramy muszą być jasno określone i wyraźna zgoda. Bezpieczeństwo danych to zupełnie inny wymiar. Dbając o bezpieczeństwo danych, Wendell przejmuje za nie odpowiedzialność. Co więcej, Wendell nie wie, jaki poziom bezpieczeństwa jest wymagany. Jak wrażliwe są dane? Czy istnieją jakieś wytyczne lub wymagania? Czy są jakieś klauzule pozatechniczne, o których powinien wiedzieć? W rzeczywistości, w sposób dorozumiany przejmując odpowiedzialność za bezpieczeństwo danych, Wendell stawia się poza strefą administrowania systemem w strefie prawnej, do której nie ma ani uprawnień, ani wiedzy specjalistycznej. Jako administrator systemu Wendell nie może być prawnikiem. Jego interpretacja tego, co uważa się za bezpieczne, może nie być zgodna z polityką firmy – lub, co ważniejsze, polityką klienta. Nieautoryzowana kopia danych klienta, nawet dobrze zabezpieczona, stanowi dodatkową lukę w zabezpieczeniach firmy. Co się stanie, jeśli haker uzyska dostęp do danych uwierzytelniających Wendella? A co jeśli dał dostęp grupowy innej osobie, która następnie skopiowała go na swój laptop? Zanim szyfrowane laptopy stały się normą, największą obawą firmy była kradzież laptopa HR. Jednak nawet jeśli Wendell stanie w obliczu potencjalnie złożonej sytuacji, która wymaga bezpieczeństwa danych, jest coś, co może zrobić, aby zapewnić maksymalnie etyczne zachowanie w imieniu swoim i wszystkich osób. Najlepsze podejście do prywatności i bezpieczeństwa danych omówimy później. Wendell i Belinda nie postanowili otwarcie przeglądać prywatnych danych. Czy kiedykolwiek można przeglądać prywatne dane? Rozważmy ten przykład z życia wzięty: Menedżer menedżera administratora systemu poprosił ją, aby skorzystała ze swojego uprzywilejowanego dostępu w celu uzyskania informacji z pliku, którego żadne z nich nie posiadało. Następnie menedżer wysokiego szczebla powiedział administratorowi systemu, aby nikomu nie mówił nic na temat dostępu do pliku, zwłaszcza bezpośredniemu menedżerowi. Chociaż administrator systemu nie czuł się komfortowo w związku z dostępem do tych plików, uważała, że ten menedżer wysokiego szczebla był upoważniony do wykonania połączenia. Czy menedżer wysokiego szczebla był właściwą osobą, od której można było uzyskać pozwolenie przed uzyskaniem dostępu do prywatnych danych? Czy administrator systemu powinien powiedzieć komuś innemu o przeglądaniu prywatnego pliku? Jakie jest etyczne postępowanie w tej sytuacji? Menedżer nie był właścicielem danych, ponieważ wyraźnie nie miał wyraźnych praw/pozwoleń na uzyskanie dostępu do danych. A co, jeśli stanowiłoby to część jego pracy, np. dyrektora ds. bezpieczeństwa informacji (CISO)? Nadal powinna istnieć osoba trzecia zatwierdzająca zastąpienie uprawnień. Jeśli CISO będzie musiało to zmienić, zgodę musi wydać menedżer stojący nad właścicielem danych. Jeśli menedżer potrzebuje dostępu, musi uzyskać zgodę działu HR lub CISO. Chęć zobaczenia danych, a następnie wyrażenie zgody na zastąpienie uprawnień to poważny konflikt interesów. Jako administrator systemu, nawet jeśli Twój menedżer tego od Ciebie wymaga, musisz uzyskać autoryzację od właściciela danych, zanim uzyskasz dostęp do prywatnych danych. Ponadto przydatne jest również sprawdzenie polityki firmy, aby upewnić się, że zasady procedury dostępu do danych są jasno określone. Ponieważ nieautoryzowany dostęp do danych może mieć poważne konsekwencje, administrator systemu powinien upewnić się, że ma spisane zasady ochrony, aby uniknąć zwolnienia za odmowę dostępu do danych menedżerowi. Jeżeli właściciel danych jest niedostępny, osobą uchylającą uprawnienia tego właściciela nie może być osoba wnioskująca o dostęp do danych prywatnych.

**Chroń się, szybko informując właścicieli**

Żaden system nie jest hermetyczny. Za każdym razem, gdy manipulujesz danymi, ryzykujesz popełnienie błędów. Wyeliminowanie błędów jest niemożliwe. Można je zminimalizować poprzez wydajne procesy i automatyzację. Kiedy jednak zdarzają się błędy i wiążą się one z ujawnieniem

prywatnych danych, konieczne jest poinformowanie wszystkich zaangażowanych osób – od właściciela danych po osoby, grupy lub firmy, na których dane ma to wpływ.

**Unikaj dostępu do prywatnych danych**

Belinda dołożyła wszelkich starań, aby chronić prywatność swoich klientów. Jest to ważna zasada, która powinna kierować względami technicznymi i logiką stosowaną w narzędziach i skryptach potrzebnych do pracy. Następnie zarchiwizuję każdy folder, w którym nie otwierano żadnych plików w ciągu ostatnich 3 miesięcy lub jeśli użytkownik się nie zalogował. Logika sprawdzania czyszczenia dysku stosowana przez Belindę jest metodyczna i szanuje także prywatność właścicieli danych. Jej skrypt sprawdza jedynie, czy uzyskano dostęp do folderu najwyższego poziomu i nie sprawdza zawartości pliku w nim zawartego. Skrypt obejmujący całe środowisko, który sprawdza, czy jakieś procesy trzymają otwarte uchwyty plików. Wendell wie, że jest to praktyczna i dokładna metoda analizy wykorzystania danych. Skrypt działa w całym środowisku, co zapewnia jeden, wspólny zestaw wyników. Eliminuje to ryzyko błędów i zapewnia dobrą widoczność ogólnego stanu centrum danych. Logika skryptu szanuje również prywatność danych; uchwyty plików nie są identyfikowalne i jedynie wskazują, że określone procesy aktywnie korzystają z określonych obszarów dysku, ale w żaden sposób nie ujawniają zawartości tych obszarów ani odpowiednich plików.

**Poinformuj właścicieli danych, jeśli ujawnione zostaną dane prywatne**

Ogólnie rzecz biorąc, należy unikać dostępu do prywatnych danych bez zgody właściciela danych. Z drugiej strony, jeśli potrzebujesz dostępu do uzasadnionych celów biznesowych, powinieneś uzyskać to pozwolenie przed próbą uzyskania dostępu do danych. Na koniec, jeśli ujawniono prywatne dane, należy poinformować o tym właścicieli danych. Jeśli to nie Ty ujawniłeś dane, zachęć osobę odpowiedzialną za ich ujawnienie, aby o tym powiedziała. W najbardziej ekstremalnych przypadkach, zwłaszcza gdy prywatne dane zostały ujawnione w złośliwy sposób, musisz wziąć na siebie odpowiedzialność i poinformować właściciela danych, jeśli nikt inny nie jest dostępny lub nie chce tego zrobić. Kiedy duże firmy otrzymują reprymendę za brak ochrony prywatnych danych, to zwykle opóźnienia w raportowaniu powodują zdenerwowanie większości ludzi, a nie samo naruszenie.

**Zajrzyj do skrzynki odbiorczej użytkownika i dowiedz się, co wysyła e-maile.**

Próbując wykazać się sumiennością i wydajnością, Belinda po raz kolejny zdecydowała się pójść o krok dalej w rozwiązywaniu problemów i uzyskać dostęp do danych klientów. Jest to podobny wzorzec do tego, co zrobiła w przypadku analizy wydajności aplikacji. Jej skrypt danych był anonimowy i unikał dostępu do zawartości plików, co właśnie zdecydowała się teraz zrobić. Wendell prawdopodobnie nie zdawał sobie sprawy, że był współwinny tego wykroczenia, udostępniając Belindzie narzędzia do analizowania danych w skrzynce pocztowej. Pochłonięty chwilą, pełen pasji i ciekawości aktualnego problemu, Wendell zapomniał cofnąć się i sprawdzić, czy jego działania prowadzą do niewłaściwego, niesankcjonowanego wykorzystania danych klientów. Może nie jest to coś naturalnego, ale ważne jest, aby posegmentować pracę wokół wszelkich manipulacji danymi. Na każdym kroku Wendell musi zadać sobie pytanie, czy praca została zatwierdzona przez właściciela danych i czy klient wyraził zgodę na taki dostęp.

**Są to rzeczywiste raporty od klienta.**

Belinda i Wendell w końcu dotarli do sedna problemu związanego ze wzrostem ilości miejsca na dysku. Po drodze ujawnili także dane klientów. Otworzyli skrzynkę pocztową i sprawdzili raporty danych, które mogą zawierać wrażliwe, uprzywilejowane informacje, które nie są przeznaczone do udostępniania i zdecydowanie nie powinny być widoczne dla administratorów systemu. Rozwiązując jeden problem,

stworzyli inny. Wendell zdał sobie sprawę, że Belinda i on nie mają wystarczających uprawnień, aby samodzielnie rozwiązać ten problem i że powinni porozmawiać z menadżerem użytkownika. Powinien był zasugerować, aby przed otwarciem skrzynki pocztowej uzyskali taką zgodę od menedżera i nie udostępniać żadnych narzędzi, które umożliwiłyby koledze dostęp do danych klientów bez pozwolenia. Co ważniejsze, ponieważ uzyskali już dostęp do danych klienta, powinni powiadomić klienta i wyjaśnić, co zostało zrobione. Jest tu jeszcze jeden ważny element. Wendell i Belinda zdecydowały się skontaktować z kierownikiem, co wydaje się słuszne (etyczne) posunięcie. Nie wiemy jednak, czy chcą skontaktować się z menadżerem, aby poinformować ich o przypadkowym dostępie do prywatnych danych, czy po prostu zapytać, co z nimi zrobić (uzyskać dodatkowe informacje i/lub uprawnienia do obsługi poczty elektronicznej). Jeśli Wendell i Belinda proszą jedynie o wyjaśnienia, mogą nawet nie być świadomi, że zrobili coś złego. Jeśli „mówią", że uzyskali dostęp do prywatnych danych, postępują słusznie, ale kwestia etyczna dotycząca początkowego dostępu nadal pozostaje otwarta. W obu przypadkach najprawdopodobniej menedżer wyjaśni, że to, co zrobił, nie było właściwe. Co więcej, powinni byli najpierw poprosić o pozwolenie na dostęp do wiadomości e-mail, a następnie przejść kolejną rundę zatwierdzania w celu zajęcia się jej zawartością. Niezbędny może być tutaj łańcuch zezwoleń na dostęp do danych, zaczynając od menedżera użytkownika, aż do klienta. Czasami ten sposób działania może nie być jasny. Identyfikacja właściciela danych może nie być możliwa, klient może być nieosiągalny, a komplikacje mogą wystąpić z dziesiątek innych powodów. Następna sekcja powinna pomóc w uproszczeniu.

**Prywatność od podstaw**

Jak zaprojektować „idealne" środowisko pracy, które szanuje prywatność wszystkich zaangażowanych podmiotów, we wszystkich wektorach danych? Brzmi to jak koncepcja bardzo amorficzna i przez to trudna. Odpowiedź kryje się w danych. Względy techniczne dotyczące infrastruktury środowiska IT i zarządzania danymi w oparciu o prywatność będą zależeć bezpośrednio od danych. Innymi słowy, powinieneś zacząć od mapowania danych. Dane wymagają dwóch podstawowych atrybutów: własności i klasyfikacji.

• Własność – każda część danych, niezależnie od jej formy i treści, musi mieć właściciela. Właścicielem danych będzie podmiot gospodarczy, który będzie ostatecznie odpowiedzialny za dane. Właściciel danych może być także opiekunem danych, w ramach którego zarządza danymi (lub ich częścią) i zapewnia możliwość wykorzystania ich przez osoby, które ich potrzebują, oraz bezpieczeństwo przed osobami, które nie muszą ich znać. Obie te funkcje rozumieją zawartość danych oraz sposób, w jaki one są i mogą być wykorzystywane. W wielu przypadkach będzie to główny użytkownik danych (takich jak poczta e-mail).

• Klasyfikacja – ten atrybut będzie miał wpływ na sposób zarządzania danymi, w tym na przesyłanie danych, przechowywanie, przechowywanie, kopie zapasowe, archiwizację, dostęp i każdy inny rodzaj możliwego wykorzystania. Klasyfikacja danych zostanie ustalona przez właściciela danych w porozumieniu z inspektorem ds. bezpieczeństwa informacji. W niektórych przypadkach właściciel danych określi jedynie wrażliwość danych, a techniczną realizację pozostawi inspektorowi ds. bezpieczeństwa informacji. W innych przypadkach właściciel danych może narzucić określone zasady dotyczące wykorzystania lub przechowywania danych. W całej branży dane będą zazwyczaj klasyfikowane na poziomach takich jak publiczny, poufny, tajny lub ściśle tajny (nie film). Każdy poziom ma własne metody ochrony. Na przykład poufne dane mogą być dostępne dla każdego w firmie, ale ich wykorzystanie poza firmą może nadal wymagać zgody biura prasowego. Tajne informacje najprawdopodobniej będą wymagały szyfrowania. Pełny zakres klasyfikacji i bezpieczeństwa danych wykracza poza zakres tej książki.

Po zdefiniowaniu tych dwóch atrybutów możliwe jest zaprojektowanie konfiguracji pracy, która będzie spełniać wymagania. Na przykład w większości jurysdykcji na całym świecie dane medyczne pacjentów mogą być przechowywane wyłącznie w placówkach znajdujących się na terenie danej jurysdykcji, co uniemożliwia ich przesyłanie do innych krajów. W takim scenariuszu na przykład zaprojektujesz kopie zapasowe, dostępność, przywracanie po awarii i inne rozwiązania w oparciu o te rygorystyczne wymagania. Inne typy danych, w zależności od ich klasyfikacji, mogą wymagać szyfrowania, nieograniczonego przechowywania kopii zapasowych, sprawdzania personelu przez departamenty rządowe i nie tylko. Po zdefiniowaniu danych należy nimi zarządzać. Zarządzanie danymi obejmuje cały zestaw operacji na danych. Ta podróż obejmuje każdy etap, od utworzenia danych po ich przechowywanie, a czasem także późniejsze usunięcie. Musisz wyznaczyć szlak (postępować zgodnie ze wskazówkami) i zrozumieć, w jaki sposób dane przemieszczają się i zmieniają z jednego punktu do drugiego. Choć nie da się określić każdego możliwego rodzaju zarządzania danymi, można ująć to zarządzanie w sposób szeroki, obejmujący przechowywanie, przesyłanie i wykorzystywanie.

• Przechowywanie – dane nieulotne będą przechowywane jako trwały zapis. Sposób przechowywania będzie podyktowany klasyfikacją. Technologia używana do przechowywania zostanie również określona na podstawie typu danych, ich objętości i zawartości. Przechowywanie danych zorientowane na prywatność wymaga, aby każda kopia danych była rejestrowana, a dostęp do nich monitorowany i regulowany. W tym celu, podobnie jak dane potrzebują swojego właściciela, tak też nośnik danych go potrzebuje. Właściciel danych wyznaczy następnie jednego lub więcej opiekunów danych, którzy będą mogli wyznaczać i udzielać członkom danych zgody na dostęp do miejsca na dysku i danych. W niektórych firmach właścicielem danych będzie ta sama osoba, co opiekun danych. Z firmami, które mają klientów, klienci  często będą także opiekunami danych lub członkami danych.

• Transfer – dane rzadko będą przechowywane bez dostępu i zostaną przeniesione z jednego nośnika na drugi. Każdy ruch danych wymaga rozliczenia. Jeśli nie kontrolujesz przepływu danych (tak jak miało to miejsce w przypadku, gdy Belinda skopiowała dane klientów na dysk Wendella), nie możesz zagwarantować prywatności. Jeśli nie możesz kontrolować przepływu, musisz zadbać o utrzymanie integralności danych. Na przykład ruch e-mailowy wysyłany od jednej osoby do drugiej często przechodzi przez wiele węzłów serwerów pocztowych, do niektórych z których możesz nie mieć dostępu lub nie być ich właścicielem. Szyfrowanie poczty i stosowanie podpisów cyfrowych może zapewnić, że dane nie zostaną naruszone. Takie zasady i praktyki zostaną określone w oparciu o klasyfikację danych przez właściciela i specjalistę ds. bezpieczeństwa informacji.

• Wykorzystanie – wykorzystanie danych oznacza dostęp do przechowywanych informacji i ich przetwarzanie. Może to zrobić sam właściciel lub może to być wykonane w ramach projektu roboczego, w którym przetwarzane są dzienniki aplikacji lub zebrane dane analityczne w celu uzyskania wglądu i kierowania logiką biznesową. Ważne jest, aby mapować wykorzystanie danych i uwzględniać wszelkie takie zdarzenia. Jeśli nie masz pełnej wiedzy na temat sposobu wykorzystania danych, nie możesz zagwarantować, że prywatność będzie szanowana lub zachowana będzie klasyfikacja danych (poufność). Mapowanie musi wykonać właściciel danych, opiekun danych i klient. Wreszcie dane można przetwarzać z jednej klasyfikacji do drugiej lub mogą pozostać w tej samej klasyfikacji. Na przykład poufne dane klientów można analizować i przetwarzać oraz prezentować je w postaci liczby klientów na region, co następnie można przedstawić jako dane publiczne.

**Jaka jest Twoja rola w tym wszystkim?**

Administratorzy systemu odnajdą się na każdym etapie przepływu i wykorzystania danych. Będą odpowiedzialni za stan i wykorzystanie miejsca na dysku. Utworzą i przypiszą początkową własność danych w oparciu o zasady (np. nowy właściciel danych płaci za przydzielony limit). Będą mogli

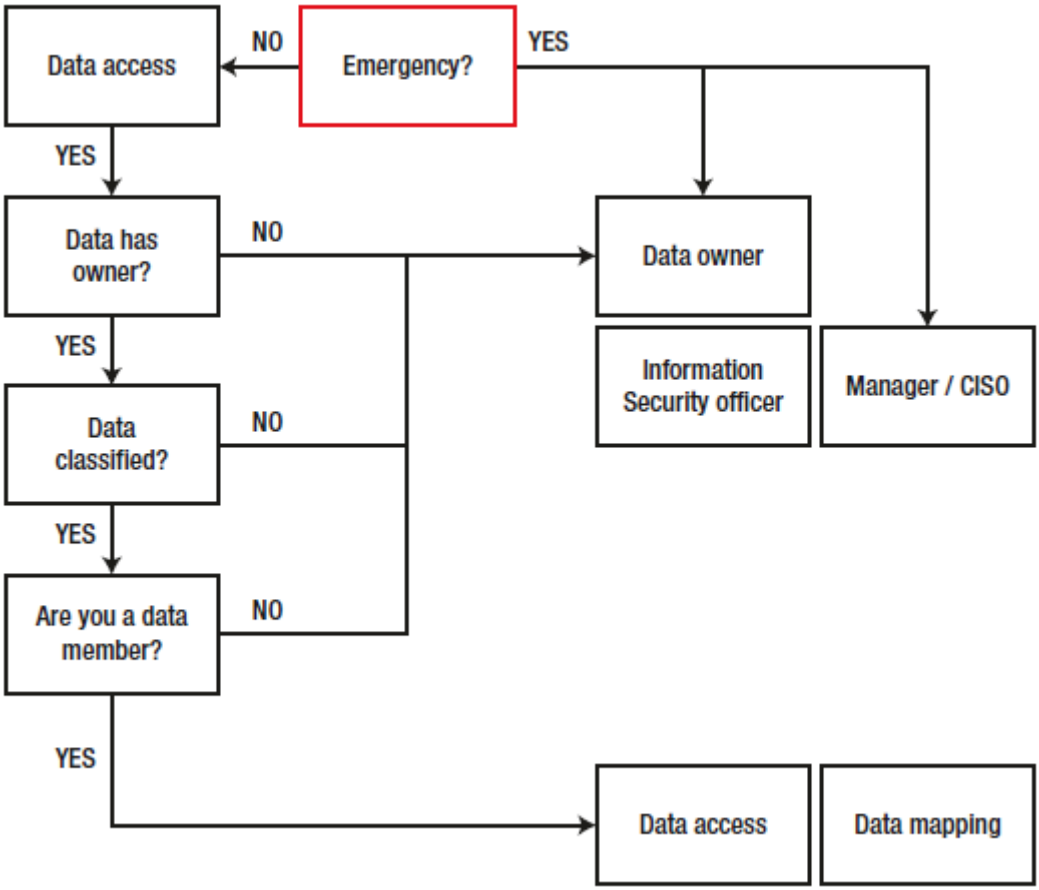
wprowadzać zmiany dotyczące dysku i własności w oparciu o polecenia osoby odpowiedzialnej za przechowywanie danych. Jeśli musisz obchodzić się z danymi i mieć pewność, że nie złamiesz tego przykazania, musisz upewnić się, że:

• Dane mają właściciela i są tajne – przestrzegasz zasad.

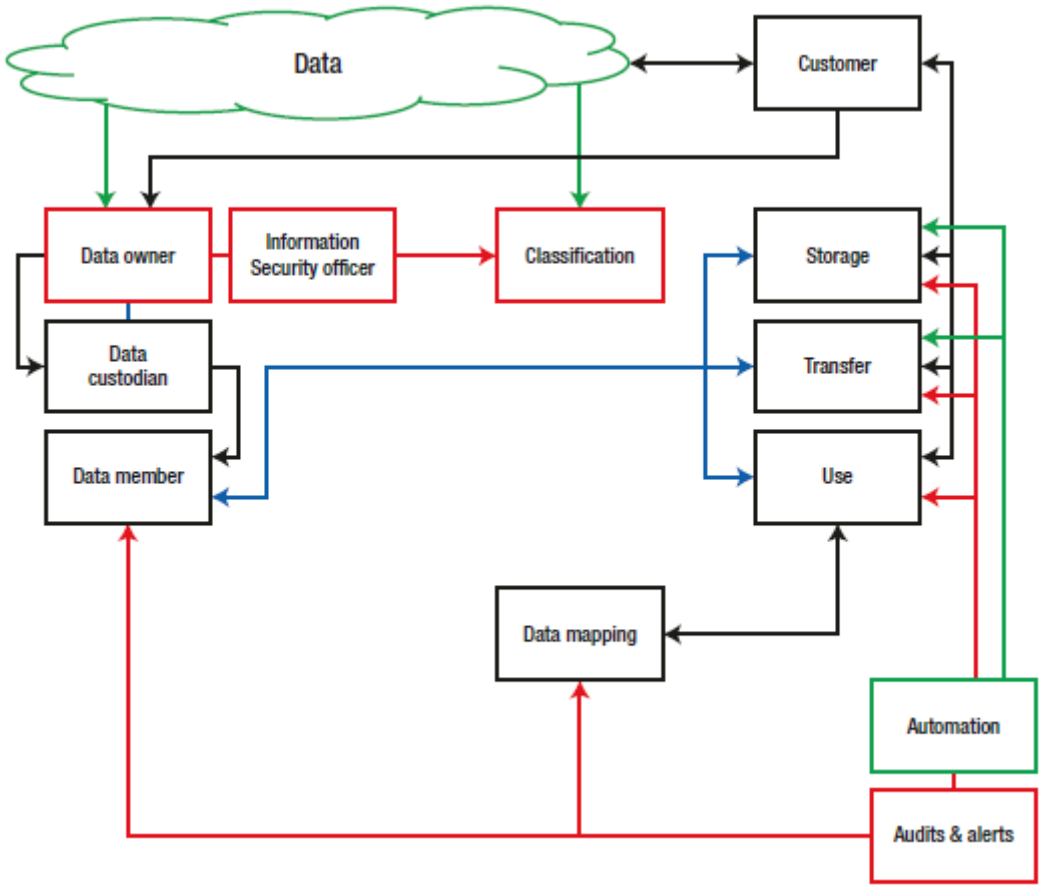
• Jeśli potrzebujesz dostępu do danych w sytuacji, gdy nie zostałeś wyraźnie wyznaczony, nie powinieneś przeglądać danych bez obecności właściciela danych lub dostarczenia konkretnych instrukcji.

• Jeśli zajdzie potrzeba zmiany danych – przechowywania ich, przeniesienia lub wykorzystania w jakiś sposób – utworzysz nową warstwę nawigacyjną na ścieżce danych. Należy to zmapować i dlatego wymagana jest wyraźna zgoda właściciela danych.

Jednak w niektórych sytuacjach podjęcie decyzji nie będzie takie proste. Będą zdarzać się scenariusze, w których będziesz musiał poradzić sobie z kryzysem i będziesz musiał wprowadzić zmiany, które nie będą zgodne z pisemnymi zasadami. Kiedy tak się stanie, możesz poprosić o pozwolenie osoby posiadające uprawnienia do zastąpienia istniejących zasad lub procesów. Czasami może to być menedżer, który pod pewnymi warunkami będzie w stanie działać w imieniu niektórych z wcześniej określonych ról. Może to być także dyrektor oddziału lub działu, który w sytuacji awaryjnej będzie mógł ustalić nowe zasady lub zastąpić istniejące. Podobnie dyrektor ds. bezpieczeństwa informacji (CISO) w firmie prawdopodobnie byłby w stanie zrobić to samo. Jeśli sytuacja dotyczy danych osobowych, menedżer HR może wkroczyć i wraz z menedżerem udzielić niezbędnych uprawnień do zastąpienia istniejących procesów i uzyskania dostępu do prywatnych plików pracowników. W idealnym przypadku byłby to proces zastępowania, a nie wyjątek. Z mojego doświadczenia wynika, że najczęstszą przyczyną konieczności pominięcia procesu jest niedostępność właściciela danych, na przykład długi urlop naukowy. Gdy wymagany był dostęp do danych projektu, wymagana była zmiana ze strony menadżera tego projektu, a także menadżera pracownika, aby administrator systemu pozwolił innemu członkowi projektu uzyskać dostęp do prywatnych danych. Innym, mniej powszechnym zjawiskiem była potrzeba dostępu menedżera do plików znajdujących się na dysku osobistym jednego z pracowników w ramach pracy. W takich przypadkach do wydania zgody potrzebne były zasoby ludzkie. Jako administrator systemu nigdy nie musisz podejmować decyzji o tym, czy prywatny plik może zostać ujawniony. Przepływ ten możemy zobaczyć na rysunku




Jeżeli któraś z funkcji nie istnieje, możesz pominąć proces przechodząc do innych funkcji w organizacji; na przykład na drugim etapie procesu, jeśli nie ma dostępnego właściciela danych, własność danych zostanie następnie przekazana funkcjonariuszowi IS, menedżerowi lub CISO. Wreszcie, możemy użyć oprogramowania, które pomoże na wszystkich etapach procesu zarządzania danymi. W Rozdziale 1 (Oddzielne role) wspomnieliśmy o narzędziach do audytu, alertów, logowania, a także kontroli wersji i zarządzania konfiguracją. Wszystko to można wykorzystać, aby zapewnić wgląd w sposób przetwarzania danych i sprawić, że zarządzanie będzie łatwiejsze, bardziej przejrzyste i wydajne. Na przykład, jeśli transfery danych są powtarzalne, można je w pełni oskryptować. Ukończone operacje można kontrolować pod kątem powodzenia, w tym parametrów takich jak integralność danych, manifest danych i inne atrybuty. Awarie mogą być oznaczane, co umożliwia sprawdzenie ich pod kątem ewentualnych problemów. Można monitorować przechowywanie danych, w tym wykorzystanie i przydziały obszaru dysku, nieaktywne miejsce na dysku, własność obszaru dysku i uprawnienia. Jeśli to możliwe, prowadzona będzie historia zmian i wykorzystania danych, a kontrola wersji zapewni pełne mapowanie dostępu. Ogólnie rzecz biorąc, każdy dostęp do danych powinien być w pełni rejestrowany. Dokładne procesy będą zależeć od ustawienia środowiska, konkretnych typów danych i wykorzystania danych. Pokazano to na rysunku.




**Wniosek**

Prywatność brzmi jak koncepcja amorficzna, a jej wdrożenie może być trudne w żywych, oddychających środowiskach IT. Administratorzy bezpieczeństwa i programiści stają przed codziennym dylematem za każdym razem, gdy w ramach swoich obowiązków muszą wchodzić w interakcję z prywatnymi danymi. Nie da się przewidzieć ani przewidzieć każdego scenariusza, w którym dane mogą zostać niewłaściwie wykorzystane lub wycieknięte. Rozwiązaniem jest nie. Etyczne podejście do prywatności polega na tym, że nie należy przyjmować założeń ani samodzielnie decydować, jak obchodzić się z prywatnymi danymi. Zamiast tego, jeśli musisz obchodzić się z takimi danymi, możesz przestrzegać kilku prostych, ogólnych zasad, które mają zastosowanie we wszystkich przypadkach użycia. Dane muszą być własnością i klasyfikowane. ATA należy mapować i dokumentować, czasami za pomocą zautomatyzowanych narzędzi. Zgodnie z klasyfikacją potrzebujesz wyraźnego pozwolenia na dostęp do danych i ich zmianę od odpowiednich właścicieli. Jeśli przypadkowo uzyskasz dostęp do prywatnych danych, musisz powiadomić właściciela danych. W sytuacjach awaryjnych może być konieczne skorzystanie z innego łańcucha zatwierdzeń, aby wykonać pracę. Takie postępowanie zapewni, że będziesz się zachowywać i pracować w sposób etyczny, z poszanowaniem prywatności. Dane muszą być własnością i klasyfikowane. Wykorzystanie danych należy mapować i dokumentować, czasami za pomocą zautomatyzowanych narzędzi. A skoro już wiemy, jak możemy uzyskać dostęp do danych w sposób szanujący prywatność ich właściciela.