

# Antypiracki przewodnik dla urzędów, przedsiębiorstw i innych organizacji



**Czy niebezpieczeństwo piractwa na służbowych komputerach dotyczy Twojej organizacji i Ciebie? Tak, bo co do zasady, pracodawca ponosi odpowiedzialność prawną za działania pracowników, w tym także za naruszenia praw autorskich do oprogramowania, ale także muzyki i filmów czy gier komputerowych.**

Aby sprawdzić czy pracodawca jest faktycznie zagrożony ryzykiem konsekwencji prawnych, finansowych, a także wizerunkowych, wynikających z niewłaściwego zarządzania zasobami informatycznymi, należy odpowiedzieć na jedno zasadnicze pytanie: **czy pracownicy mają zbyt dużą swobodę w zakresie korzystania ze służbowych komputerów – czy mogą samodzielnie bez wiedzy pracodawcy dokonywać instalacji oprogramowania?** Jeśli odpowiedź jest pozytywna, ryzyko piractwa, czyli naruszenia praw autorskich przez firmę, urząd czy inną organizację jest duże. Jeśli chcesz ocenić to ryzyko bardziej precyzyjnie, odpowiedz na kilka pytań w ramach krótkiego testu:

**Czy wiesz ile komputerów osobistych, laptopów i serwerów posiada Twoja firma/organizacja?**

Tak Nie

**Czy firma/organizacja posiada licencje na wszystkie programy zainstalowane w komputerach osobistych, laptopach i serwerach?**

Tak Nie

**Czy pracownicy w Twojej firmie/organizacji mogą samodzielnie instalować oprogramowanie, np. aplikacje typu P2P lub ściągnięte z Internetu?**

Tak Nie

**Czy w Twojej firmie/organizacji jest wyznaczona osoba odpowiedzialna za oprogramowanie i zasoby informatyczne?**

Tak Nie

**Czy w Twojej firmie/organizacji sformułowano zasady zarządzania zasobami informatycznymi i procedury zakupu i kopiowania oprogramowania?**

Tak Nie

**Czy praktyka ta została zatwierdzona przez kadrę zarządzającą?**

Tak Nie

**Czy Twoja firma/organizacja prowadzi rejestr licencji na oprogramowanie?**

Tak Nie

**Czy rejestr ten jest zawarty w bazie danych zarządzania oprogramowaniem?**

Tak Nie

**Czy Twoja firma/organizacja korzysta z narzędzi do audytu oprogramowania?**

Tak Nie

**Czy stosowane narzędzie do audytu oprogramowania monitoruje zasoby wszystkich komputerów w sieci lokalnej?**

Tak Nie

**Czy regularnie przeprowadzasz audyt oprogramowania pod kątem zgodności z warunkami posiadanych licencji?**

Tak Nie

Jeśli któraś z tych odpowiedzi jest negatywna, należy się poważnie zająć tematem zarządzania zasobami IT w organizacji, bo ryzyko korzystania z nielegalnych plików jest duże. Zanim się tym zajmiesz, powinieneś przeczytać jakie konsekwencje mogą spotkać organizację i Ciebie, jako pracownika, w wypadku ujawnienia faktu naruszenia praw autorskich i wszczęcia postępowania karnego lub/i cywilnego.

### **Jak piractwo na służbowych komputerach zagraża Twojej organizacji i Tobie?**

- Mówiąc o odpowiedzialności prawnej pracodawcy za działania pracowników, w tym także za naruszenia praw autorskich do oprogramowania, a także muzyki i filmów czy gier komputerowych, chodzi głównie o odpowiedzialność cywilną, w tym majątkową, bo postępowań karnych – co do zasady – nie prowadzi się wobec osób prawnych a jedynie wobec osób fizycznych. Oznacza to, że postępowanie karne może być prowadzone wobec pracowników (np. członków zarządu, kierownikowi ds. IT, innych pracowników winnych danego naruszenia) a wobec samego pracodawcy jedynie w sytuacji kiedy pracodawcą jest firma prowadzona przez osobę fizyczną w ramach indywidualnej działalności gospodarczej. Polskie prawo przewiduje jednak możliwość prowadzenia postępowania wobec pracodawcy będącego osobą prawną na

podstawie przepisów ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary. Warunkiem wszczęcia takiego postępowania jest prawomocny wyrok skazujący pracownika lub warunkowo umarzający prowadzone przeciwko niemu postępowanie karne albo karno-skarbowe (więcej informacji niżej).

- Odpowiedzialność cywilna, w tym majątkowa, pracodawcy wynika przede wszystkim z przepisów ustawy o prawie autorskim i prawach pokrewnych, obejmując m. in. obowiązek zapłaty kwoty równej wynagrodzeniu (opłaty licencyjnej) w potrójnej wysokości, jeśli naruszenie ma charakter zawiniony lub podwójnej wysokości, jeśli jest niezawinione, a także obowiązek wydania uzyskanych korzyści.
- Dodatkowo sąd może zobowiązać pracodawcę do publikacji w prasie stosownego oświadczenia, w którym firma, urząd czy inna organizacja przyznaje się publicznie do naruszenia praw autorskich przysługującym konkretnym twórcom czy producentom. Z pewnością nie jest to nigdy powód do chluby i może bardzo niekorzystnie wpłynąć na wizerunek i renomę pracodawcy.
- Ponadto pracodawca musi się liczyć z odpowiedzialnością przewidzianą w ustawie o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary. Zgodnie z art. 7 tej ustawy, w sytuacji kiedy pracownik został skazany prawomocnym wyrokiem karnym za naruszenie praw autorskich w ramach wykonywania swoich obowiązków pracowniczych, sąd może wobec pracodawcy orzec karę pieniężną w wysokości od 1.000 do 20.000.000 złotych, nie wyższą jednak niż 10 % przychodu osiągniętego w roku obrotowym, w którym popełniono czyn zabroniony będący podstawą odpowiedzialności podmiotu zbiorowego. Wobec podmiotu zbiorowego – zgodnie z art. 9 ww. ustawy – sąd może orzec dodatkowo:
  - 1) zakaz promocji lub reklamy prowadzonej działalności, wytwarzanych lub sprzedawanych wyrobów, świadczonych usług lub udzielanych świadczeń;
  - 2) zakaz korzystania z dotacji, subwencji lub innych form wsparcia finansowego środkami publicznymi;
  - 3) zakaz korzystania z pomocy organizacji międzynarodowych, których Rzeczpospolita Polska jest członkiem;
  - 4) zakaz ubiegania się o zamówienia publiczne;
  - 5) zakaz prowadzenia określonej działalności podstawowej lub ubocznej;
  - 6) podanie wyroku do publicznej wiadomości.
- Warto wiedzieć, że pracodawca ponosząc konsekwencje majątkowe (finansowe) wynikające z działań lub zaniechań swoich pracowników w związku z naruszeniem przez nich praw autorskich, może dochodzić od nich naprawienia szkody, którą poniósł. Jeśli zatem, będąc pracownikiem, jesteś członkiem zarządu lub np. pracownikiem odpowiedzialnym za dział IT

albo, po prostu, pracownikiem z którego winy pracodawca poniósł szkodę, musisz się liczyć, że pracodawca będzie dochodził od Ciebie tych roszczeń. Jeśli jesteś zatrudniony na podstawie umowy o pracę, Twoja odpowiedzialność jest ograniczona, zgodnie z Kodeksem pracy, do potrójnej wysokości Twojego wynagrodzenia. Jeśli jednak pracodawca dowiedzie, że pracownik naruszył prawa autorskie i naraził go na szkodę umyślnie, to odpowiedzialność materialna pracownika nie jest ograniczona. Odpowiedzialność można ponieść również wypadku świadczenia usług na podstawie umowy cywilnoprawnej przez osobę prowadzącą działalność gospodarczą (w tym też w ramach tzw. samozatrudnienia) czy w wypadku wykonania umowy o dzieło przez osobę fizyczną nieprowadzącą działalności gospodarczej przy użyciu komputera należącego do zamawiającego: zgodnie z art. 415 Kodeksu cywilnego, kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia.

- Co do postępowania karnego w sprawie o naruszenie praw autorskich do utworów (w tym: oprogramowanie, muzyka i filmy), to postępowania takie nie są prowadzone wobec firmy, choć w przypadku indywidualnej działalności prowadzonej przez osobę fizyczną, to zazwyczaj właściciel firmy będzie w polu zainteresowania organów ścigania. W wypadku spółek, urzędów i innych organizacji, w tym organizacji pozarządowych, akt oskarżenia może zostać skierowany przeciw członkom zarządu lub pracownikom odpowiedzialnym za dział IT lub pracownikom winnym (nawet nieumyślnie) danego naruszenia praw autorskich.
- Mówiąc o odpowiedzialności karnej, należy pamiętać, że zgodnie z Kodeksem karnym, karalne jest nie tylko sprawstwo, ale także **pomocnictwo i podżeganie**, a w niektórych przypadkach także **przygotowanie**, jako forma stadialna przestępstwa.

Odpowiada za podżeganie, kto chcąc, aby inna osoba dokonała czynu zabronionego, nakłania ją do tego a za pomocnictwo, kto w zamiarze, aby inna osoba dokonała czynu zabronionego, swoim zachowaniem ułatwia jego popełnienie, w szczególności dostarczając narzędzie, środek przewozu, udzielając rady lub informacji a także ten, kto wbrew prawnemu, szczególnemu obowiązkowi niedopuszczenia do popełnienia czynu zabronionego swoim zaniechaniem ułatwia innej osobie jego popełnienie. Przygotowanie natomiast zachodzi wtedy, gdy sprawca w celu popełnienia czynu zabronionego podejmuje czynności mające stworzyć warunki do przedsięwzięcia czynu zmierzającego bezpośrednio do jego dokonania, w szczególności w tymże celu wchodzi w porozumienie z inną osobą, uzyskuje lub przysposabia środki, zbiera informacje lub sporządza plan działania.

Więcej o zasadach odpowiedzialności karnej i cywilnej w **przewodniku dla osób prywatnych i pracowników**.

- Oprócz konsekwencji prawnych i finansowych, pracodawca musi się liczyć z ryzykiem w zakresie bezpieczeństwa informatycznego. Jak dowodzą specjalistyczne badania\*, pirackie oprogramowanie czy inne nielegalne pliki (muzyka, filmy, gry komputerowe) są siedliskiem złośliwych dodatków (wirusy, trojany, oprogramowanie szpiegujące, key loggery etc), które mogą zainfekować komputery służbowe i umożliwić osobie z zewnątrz (intruzowi):

- (1) dostęp do poufnych danych, w tym np. haseł dostępu do bankowości internetowej czy do informacji stanowiących tajemnicę przedsiębiorstwa;
- (2) przejęcie kontroli nad naszym komputerem i wykorzystanie go jako tzw. komputer-zombie do ataku hackerskiego;
- (3) kradzież tożsamości umożliwiającej podszywanie się przestępcy pod nas w ramach działalności przestępczej lub wykorzystanie komputera służbowego jako tzw. komputera-zombie do ataków hackerskich.

\* badania IDC „Ryzyko związane z pozyskiwaniem i korzystaniem z pirackiego oprogramowania”, 2006

Podsumowując, z punktu widzenia pracodawcy, ryzyko korzystania z nielegalnego oprogramowania oraz nielegalnych plików muzycznych i filmowych np. wskutek korzystania przez pracowników z aplikacji P2P instalowanych na służbowych komputerach, należy postrzegać w pięciu zasadniczych kategoriach:

1. ryzyko odpowiedzialności karnej pracowników, np. członków kadry zarządzającej a także właściciela w wypadku firm osób prowadzących działalność gospodarczą, włącznie z karami finansowymi wobec pracodawcy przewidzianymi w ustawie o odpowiedzialności zbiorowej podmiotów za czyny zabronione pod groźbą kary;
2. odpowiedzialność cywilna pracodawcy, w tym majątkowa, włącznie z obowiązkiem zapłaty potrójnej lub podwójnej wysokości wynagrodzenia (opłaty licencyjnej) oraz obowiązkiem wydania uzyskanych korzyści;
3. ryzyko dostępu osoby nieupoważnionej do tajemnic przedsiębiorstwa oraz innych wrażliwych i poufnych danych, włącznie z niebezpieczeństwem kradzieży tożsamości i wykorzystania jej przez przestępcę do prowadzenia działalności przestępczej;
4. inne konsekwencje finansowe wynikające z przypadku komputerów a także powstałych wskutek przestoju pracy wynikającego z zatrzymania przez Policję sprzętu komputerowego;
5. utrata reputacji i wiarygodności w oczach klientów i kontrahentów.

Warto także pamiętać, że zwolnieni **pracownicy są najczęściej źródłem zawiadomień o nieprawidłowościach u ostatniego pracodawcy** w zakresie oprogramowania i innych plików. Zawiadomienia takie są składane bezpośrednio do organów ścigania lub za pośrednictwem organizacji zajmujących się ochroną praw autorskich. W Polsce zawiadomienia o przypadkach piractwa komputerowego mogą być zgłaszane telefonicznie lub mailem do BSA, organizacji zrzeszającej czołowych producentów oprogramowania ([www.bsa.org/polska](http://www.bsa.org/polska)).

## **Jak uchronić Twoją organizację i Ciebie przed piractwem na służbowych komputerach?**

Jak pokazuje praktyka, w Polsce dość często właściciel firmy lub członkowie kadry zarządzającej urzędu, spółki czy innej organizacji, nie zdają sobie sprawy z problemu niewłaściwego zarządzania zasobami informatycznymi w organizacji. A od świadomości i zrozumienia tego problemu zależy wprowadzenie środków zaradczych i naprawienia sposobu zarządzania zasobami informatycznymi. Profesjonalne zarządzanie zasobami informatycznymi (ang. Software Asset Management) to zbiór zasad i procedur pozwalających – wskutek wdrożenia – na optymalizację zarządzania komputerami i ich zawartością. Wdrożenie tych zasad i procedur pozwala na osiągnięcie korzyści, które trudno przecenić:

1. zapewnienie bezpieczeństwa prawnego dla organizacji i pracowników, w tym przedstawicieli kadry zarządzającej,
2. zmniejszenie ryzyka zagrożeń bezpieczeństwa informatycznego, w tym podniesienie poziomu bezpieczeństwa informacji, włącznie z danymi drażliwymi i ściśle poufnymi;
3. zwiększenie efektywności technologicznej poprzez korzystanie z optymalnych rozwiązań w zakresie oprogramowania, sprzętu i innych narzędzi informatycznych;
4. redukcja kosztów IT.

W czasach recesji ten ostatni argument ma szczególne znaczenie. Warto wiedzieć, że wdrożenie procedur SAM może pozwolić w pierwszym roku osiągnąć oszczędności na poziomie 30% budżetu IT, a w następnych latach na poziomie 5-10% rocznie\*

\* *“IT Asset Management: Moving to Higher Ground,” Frances O’Brien, Gartner ITAM Conference 2003*

Aby organizacja – niezależnie czy jest to firma, urząd czy inna organizacja – rozpoczęła zarządzać zasobami informatycznymi w sposób profesjonalny i efektywny, należy najpierw podjąć osiem pierwszych kroków:

### **1. Zielone światło w organizacji**

Bez zrozumienia przez kadre zarządzającej znaczenia problemu i korzyści płynących z właściwego zarządzania zasobami informatycznymi, nie sposób mówić o jakiegokolwiek perspektywie zmiany podejścia i poprawy sytuacji. Zielone światło ze strony zarządu wydaje się warunkiem koniecznym prawidłowego zarządzania zasobami informatycznymi, ich legalności oraz efektywności pod względem technicznym, jak i ekonomicznym.

### **2. Wyznaczenie osoby odpowiedzialnej za zasoby IT**

Zadaniem takiej osoby powinien być przede wszystkim nadzór nad zawartością wszystkich służbowych komputerów i instalacją oprogramowania, a także kontrola przestrzegania przez pracowników regulaminu korzystania ze służbowych komputerów oraz innych zasad i procedur zarządzania zasobami IT.

### **3. Audyt oprogramowania**

Audyt oprogramowania to nic innego jak inwentaryzacja wszystkich aplikacji zainstalowanych w służbowych komputerach, w tym także na serwerach. Audyt można przeprowadzić samodzielnie lub przez firmę zewnętrzną świadcząca tego rodzaju usługi. W wypadku samodzielnego audytu można go przeprowadzić „ręcznie” poprzez spisanie wszystkich aplikacji, jakkolwiek stosowanie takiej „ręcznej” metody ma sens jedynie w wypadku małej liczby komputerów. Jeśli organizacja posiada więcej niż 5 komputerów a nie chce wynajmować w tym celu firmy zewnętrznej, najlepszym rozwiązaniem jest skorzystanie ze specjalistycznego oprogramowania do audytu zasobów informatycznych. Wykaz tego rodzaju narzędzi informatycznych, jak i firm świadczących usługi audytu i zarządzania oprogramowaniem można znaleźć pod adresem: [www.zrobtosamo.pl](http://www.zrobtosamo.pl)

Jeśli audyt wykaże, że część oprogramowania zainstalowanego w służbowych komputerowych nie jest legalna (organizacja nie posiada na nie licencji), a także jeśli w komputerach służbowych znajdują się filmy, pliki muzyczne i gry komputerowe, należy je usunąć. Po usunięciu nielegalnego oprogramowania i nielegalnych plików, należy zainstalować legalne oprogramowanie potrzebne organizacji do prowadzenia swojej działalności. W ramach poaudytowych działań naprawczych rozsądne jest usunięcie także tych aplikacji, które – co prawda – nie są nielegalne, ale zupełnie niepotrzebne organizacji. Dotyczy to np. oprogramowania typu P2P. Tego rodzaju oprogramowanie może okazać się źródłem kłopotów organizacji i pracowników.

Audyt oprogramowania nie powinien być działaniem jednorazowym. W organizacjach profesjonalnie zarządzającymi zasobami informatycznymi, przeprowadzany jest regularnie – np. raz w roku.

### **4. Stworzenie bazy danych posiadanego oprogramowania**

Jedną z głównych korzyści płynących z audytu jest stworzenie bazy danych posiadanego oprogramowania. Baza taka powinna być uzupełniana na bieżąco. Poprawność uaktualnienia tej bazy weryfikować powinien coroczny audyt.

### **5. Centralizacja zakupów i dystrybucji oprogramowania**

Tak jak wyznaczenie osoby odpowiedzialnej za IT pozwala określić KTO jest odpowiedzialny za zasoby informatyczne organizacji, tak wprowadzenie zasady centralizacji zakupów i dystrybucji oprogramowania pozwala określić JAK to następuje w organizacji. Często osobie odpowiedzialnej za IT powierza się także to zadanie, ale zdarza się, że osoba ta zgłasza jedynie zapotrzebowanie na instalację konkretnego oprogramowania, a decyzję o nabyciu go podejmuje osoba odpowiedzialna za finanse organizacji – często jest to członek kadry zarządzającej organizacji. Warto pamiętać, aby zakupów dokonywać tylko i wyłącznie u autoryzowanych dostawców i żeby każda nabyta licencja została wykazana w fakturze VAT.

### **6. Ustalenie zasad i procedur SAM**

Zasady i procedury SAM to istota profesjonalnego zarządzania zasobami informatycznymi. Ogólne zasady korzystania ze służbowych komputerów można określić w specjalnym regulaminie. Należy zadbać o to, żeby z regulaminem zapoznał się każdy pracownik – najlepiej poprzez pisemne potwierdzenie, włącznie ze zobowiązaniem do przestrzegania regulaminu. Często zdarza się, że zasady korzystania ze służbowych komputerów zawarte są wprost w umowach o pracę lub w odrębnych porozumieniach cywilnoprawnych zawieranych pomiędzy pracodawcą a pracownikiem.

Do najważniejszych zasad i procedur w zakresie zarządzania zasobami informatycznymi zaliczyć należy:

- sposób składania wniosków o instalację oprogramowania;
- wyznaczenie osób odpowiedzialnych za decyzje, za zakup, za zabezpieczenie finansów;
- obowiązki służb IT, np. zapoznanie się z treścią licencji na oprogramowanie, nadzór nad pracownikami i zawartością komputerów służbowych, audyty, ewidencja, szkolenia itd.);
- przechowywanie oryginalnych nośników, instrukcji i innych oryginalnych materiałów w jednym wydzielonym i zabezpieczonym miejscu;
- obowiązki pracowników: zakaz samodzielnej instalacji, zakaz kopiowania programów do prywatnych celów itd.

## **7. Stały monitoring i regularne audyty oprogramowania**

Podstawą powodzenia zmiany sposobu zarządzania zasobami informatycznymi jest ciągłość działania w tym zakresie. Dla zachowania tej ciągłości niezbędna jest cykliczność przeprowadzania audytów (np. raz w roku) i stały monitoring zawartości służbowych komputerów.

## **8. Profesjonalne wsparcie**

Przez profesjonalne wsparcie należy rozumieć zarówno pomoc dostawców usług SAM (audytu i zarządzania zasobami IT), ale i stałego korzystanie przez osoby wyznaczone do sprawowania opieki nad zasobami IT ze źródeł wiedzy na ten temat. Technologie informatyczne to bodaj najszybciej rozwijająca się dziedzina życia. W ślad za rozwojem technologii, dochodzi do zmian w prawie. A to oznacza, że zarządzanie zasobami informatycznymi wymaga ciągłego dostępu do wiedzy. Wiele przydatnych informacji na temat profesjonalnego zarządzania zasobami informatycznymi można znaleźć na polskiej stronie BSA: [www.bsa.org/polska](http://www.bsa.org/polska) lub na stronie programu Zrób to SAMo: [www.zrobtosamo.pl](http://www.zrobtosamo.pl)