

# Co zrobić z zepsutym komputerem, na którym są zapisane dane osobowe

**PROCEDURY** | Informatyk wezwany do naprawy sprzętu może się starać usunąć usterkę na miejscu w firmie, pod warunkiem że będzie to robił pod nadzorem pracownika odpowiedzialnego za bezpieczeństwo informacji. Sytuacja się komplikuje, gdy sprzęt trzeba zabrać do zewnętrznego serwisu.

MICHAŁ KOŁTUNIAK

■ W naszej firmie zepsut się komputer, na którym są przetwarzane dane osobowe. Jak powinniśmy postępować, aby nie naruszyć przepisów w zakresie ochrony danych osobowych? Czy informatyk wezwany do jego naprawy może to zrobić, jeżeli będzie miał upoważnienie od administratora bezpieczeństwa informacji (taką osobą jest u nas w firmie), czy wystarczy, że będzie dokonywał naprawy w obecności takiej osoby? A co, jeżeli nie uda się naprawić komputera i trzeba będzie przewieźć go do serwisu? Jak wówczas należy zabezpieczyć dane osobowe? – pyta czytelnik.

Obecnie większość danych osobowych, za które – przypomnijmy – uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przetwarzane są w systemach informatycznych. Do tego potrzebne są komputery, łącza, serwery i inny sprzęt. Jak wszystkie urządzenia, także one mogą ulec awarii. W każdym innym przypadku wystarczy

wezwać informatyka lub oddać sprzęt do serwisu. Jeżeli jednak na umieszczonych w nich dyskach lub innych nośnikach pamięci zawarte są dane osobowe, to sprawa się komplikuje.

## Ściśle tajne

W jaki zatem sposób należy postępować z zepsutym sprzętem, aby nie narazić się na zarzut naruszenia przepisów o ochronie danych osobowych? Generalnie można odpowiedzieć na to pytanie w ten sposób, że firma powinna postępować tak, jakby na takim komputerze lub serwerze znajdowały się najściślej chronione informacje o firmie i sposobie jej działania, stanowiące jej tajemnicę. Czy w takim wypadku prezes lub dyrektor zgodziliby się, aby komputer przeglądała obca osoba bez żadnego nadzoru? Albo czy byłiby gotowi oddać taki sprzęt do serwisu, nie upewniwszy się najpierw, że nie da się z niego odczytać żadnych kluczowych informacji? Zapewne nie. Zastosowa-

liby takie rozwiązania, aby do tego nie dopuścić. I podobnie jest w przypadku postępowania z komputerem, który służy do przetwarzania danych osobowych.

O ile jednak pierwszy przypadek wynika z samoregulacji i zasad ostrożności, o tyle drugi dodatkowo z przepisów prawa.

## Zakaz udostępniania

Przed wszystkim zgodnie z art. 26 ustawy o ochronie danych osobowych (DzU z 2014 r. poz. 1182 ze zm.) administrator danych powinien dolożyć szczególnych starań w celu ochrony interesów osób, których dane dotyczą. Z kolei art. 36 ust. 1 wskazuje, że administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez taką osobę, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Sama ustawa nie wprowadza szczególnych kryteriów i wskazówek, jak w praktyce proces ten powinien być regulowany. Nie znaczy to jednak, że takich przepisów nie ma.

Szereg minimalnych wymagań i warunków, jakie powinny być spełnione w procesie zarządzania bezpieczeństwem, zawartych jest bowiem w rozporządzeniu ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (DzU z 2004 r. nr 100, poz. 1024). W szczególności warto zwrócić uwagę na załącznik do tego rozporządzenia. W jego części A pkt VI

znajduje się następująca informacja: urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

■ likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

■ przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

■ naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

Wreszcie, w myśl art. 37 ustawy, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

## Różne scenariusze

Odpowiadając zatem na pytania dotyczące tego, jak postępować z uszkodzonym sprzętem, da się nakreślić kilka scenariuszy. Po pierwsze, naprawa takiego sprzętu może zostać wykonana przez informatyka na miejscu w firmie, pod warunkiem że będzie mu towarzyszyła osoba odpowiadająca za bezpieczeństwo danych w przedsiębiorstwie (instytucji). Przy tym chodzi tu o nadzór osoby, która ma upoważnienie do przetwarzania danych, a upoważnienie to pochodzi od administratora danych, a nie od administratora bezpieczeństwa informacji, co sugerowało pytanie czytelnika. Jeżeli ten warunek będzie spełniony, procedury postępowania będą prawidłowe.

W przypadku gdy komputera nie będzie można naprawić na miejscu i konieczne będzie zabranie go do serwisu, wówczas przebieg postępowania powinien zależeć od tego, czy

## • KOMENTARZ EKSPERTA

Małgorzata Kałużyńska-Jasak

dyrektor zespołu rzeczni-  
kasowego generalnego  
inspektora ochrony danych  
osobowych



Zadaniem administratora danych osobowych jest niedopuszczenie do sytuacji, w której dane osobowe trafiłyby w ręce osób postronnych. Muszą być stworzone takie warunki, aby osoby trzecie nie miały dostępu do danych, nie mogły się z nimi swobodnie zapoznać, nie mówiąc już o ich skopiowaniu czy innej formie ich przejęcia. Dotyczy to danych przechowywanych nie tylko w tradycyjnej postaci papierowej, ale i zawartych na nośnikach elektronicznych, np. dyskach komputerów. Dlatego w przypadku konieczności dokonania naprawy takiego sprzętu niezbędny jest nadzór osoby upoważnionej przez administratora danych do przetwarzania danych. Jeżeli naprawa nie może zostać wykonana pod takim nadzorem, sprzęt może trafić do zewnętrznego serwisu tylko pod warunkiem, że nie będzie zawierał możliwych do odczytania danych osobowych. ©©

na nośnikach pamięci stanowiących podzespoły uszkodzonego komputera nie są zapisane żadne dane osobowe, tj. komputer wykorzystywany jest jedynie jako narzędzie dostępu do systemu, a na jego nośnikach nie są przechowywane żadne dane osobowe czy też zapisywane takie informacje. W pierwszym przypadku (gdy na nośnikach pamięci komputera nie są przechowywane dane osobowe), nie ma przeszkód, aby komputer przekazać do naprawy, pod warunkiem że były przestrzegane zasady dotyczące ustawień np. przeglądarki w zakresie niezapamiętywania danych z formularzy, haseł itp. lub zapisane dane w tym zakresie zostały usunięte przed przekazaniem sprzętu.

## Źródło informacji

W drugim przypadku, gdy dane osobowe były przechowywane na nośnikach pamięci uszkodzonego komputera, wówczas w zależności od rodzaju uszkodzenia postępowanie powinno być następujące: ■ jeśli uszkodzenie nie dotyczy nośników pamięci, należy je

wymontować i do naprawy przekazać jedynie komputer niezawierający nośników, na których są dane osobowe,

■ jeśli uszkodzony został nośnik pamięci zawierający dane osobowe, wówczas jeśli nie jest możliwa jego naprawa na miejscu, należy go wymontować i zniszczyć w sposób uniemożliwiający odczytanie zapisanych danych oraz zakupić nowy.

W ostatnim przypadku, czyli gdy pojawi się konieczność zakupu nowego sprzętu (dysku), w specyfikacji warunków dotyczących jego zakupu, i w gwarancji, warto zastrzec, by wówczas, gdy dojdzie do uszkodzenia nośników pamięci, ich wymiana nie wymagała zwrotu tych, które uległy awarii.

Inne, niewymienione w wyżej wskazanym rozporządzeniu (załączniku) działania w zakresie bezpieczeństwa powinny pozostawać w zgodzie z aktualnym stanem wiedzy w zakresie zarządzania bezpieczeństwem informacji. Można w tym celu wykorzystać m.in. dokumenty definiujące narodowe, europejskie lub międzynarodowe standardy i dobre praktyki w tym zakresie. ©©

## ➔ Strasznie kara

Po ostatniej zmianie przepisów ustawy o ochronie danych osobowych w sieci pojawiły się wprowadzające w błąd informacje m.in. o obowiązku zarejestrowania zbiorów danych osobowych do 30 czerwca 2015 roku. Co więcej, autorzy niektórych z nich straszą, że niedopełnienie tego obowiązku grozi karą w wysokości nawet 200 tys. zł. Takie informacje są niezgodne z prawdą. Data 30 czerwca dotyczy bowiem zgłoszenia do rejestracji dotychczasowych administratorów bezpieczeństwa informacji (ABI), i to pod warunkiem, że administrator danych zdecyduje, by uwzględnić ich nowe kompetencje i usytuowanie w strukturze firmy, nadal pełnił oni tę funkcję. Nie ma jednak obowiązku dokonania takiego zgłoszenia w przypadku, gdy administrator zamierza sam wykonywać wszystkie obowiązki ciążące na ABI. Jeżeli jednak administrator danych powoła ABI i zgłosi go do rejestracji generalnemu inspektorowi ochrony danych osobowych, zwolniony będzie z obowiązku rejestracji zbiorów danych (chyba że zawierają one tzw. dane wrażliwe). Warto też dodać, że GODO nie nakłada kar za niezgłoszenie zbioru do rejestracji, co nie znaczy, że takiego obowiązku nie ma. Nie należy go lekceważyć, zważywszy, że za jego niedopełnienie ustawa o ochronie danych osobowych przewiduje odpowiedzialność karną. Jednak o rodzaju kary decyduje nie GODO, lecz sąd. GODO może nałożyć jedynie grzywnę, ale tylko w celu przymuszenia, w przypadku niewykonania wydanej przez niego decyzji. ©©