

# Backup z zanikami pamięci

**PRYWATNOŚĆ** Żądanie usunięcia danych dotyczy również kopii zapasowych – uważa GODO. Eksperti przekonują jednak, że nie oznacza to konieczności kasowania informacji na bieżąco

Sławomir Wikariak  
slawomir.wikariak@infor.pl

Nie tylko w dużych korporacjach, takich jak banki, ale nawet w mikrofirmach zapisywanie kopii zapasowych (ang. backup) jest dzisiaj standardem. W zależności od rodzaju i skali działalności robi się to z różną częstotliwością i używając różnych narzędzi. Wiele firm nie kasuje od razu starych kopii i ma ich po kilka czy kilkadziesiąt. Powszechnie stosowanym rozwiązaniem jest też tworzenie kopii przyrostowych, czyli takich, w których uwzględniane są jedynie zmiany, jakie zaszły od poprzedniego zapisu.

Już dzisiaj firmy mają problem, co zrobić, gdy klient żąda wykasowania swoich danych, choćby przez cofnięcie zgody na ich przetwarzanie. Dużo poważniejszego wymiaru nabiera on jednak 25 maja, kiedy to zacznie być stosowane unijne rozporządzenie o ochronie danych osobowych (RODO). Nie tylko ze względu na przewidziane w nim wprost prawo do bycia zapomnianym, ale również na wysokie kary finansowe, które grozić będą przedsiębiorcom.

## Kopia to też przetwarzanie

Problem nie jest nowy. Już w 2009 r. Naczelny Sąd Administracyjny wydał wyrok utrzymujący decyzję generalnego inspektora ochrony danych osobowych, nakazującą usunięcie danych osobowych z kopii zapasowych banku (sygn. akt I OSK 633/08). Skład orzekający doszedł do wniosku, że przechowywanie tych danych w backupie jest niczym innym, jak ich przetwarzaniem, a to możliwe jest tylko po spełnieniu przesłanek ustawowych. Jeśli więc one wygasną (np. osiągnięty zostanie cel przetwarzania lub klient cofnie zgodę na ich przetwarzanie), dane trzeba usunąć nie tylko z systemu, który na bieżąco jest używany, ale również ze wszystkich kopii zapasowych.

GODO podtrzymuje swe stanowisko.

– W odniesieniu do danych przetwarzanych przy użyciu systemów informatycznych obo-

## Coraz mniej czasu na sprostanie nowym obowiązkom

### Artykuł 17 RODO

Prawo do usunięcia danych („prawo do bycia zapomnianym”)

*Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:*

- dane osobowe **nie są już niezbędne** do celów, w których zostały zebrane lub w inny sposób przetwarzane;*
- osoba, której dane dotyczą, **cofnęła zgodę**, na której opiera się przetwarzanie danych*
- osoba, której dane dotyczą, **wnosi sprzeciw wobec przetwarzania** i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania*
- dane osobowe były przetwarzane **niezgodnie z prawem**;*
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;*
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.*

wiązek ich usuwania dotyczy również nośników informatycznych stanowiących kopie bezpieczeństwa – mówi Agnieszka Świątek-Druś, rzecznik prasowy GODO.

– Czynności te należy jednak wykonywać, uwzględniając uwarunkowania techniczne takiego działania, przy jednoczesnym zapewnieniu bezpieczeństwa przetwarzania danych innych osób w ramach tego samego systemu informatycznego – dodaje.

W tym leży sedno problemu. Kopie bezpieczeństwa spełniają swą rolę tylko wówczas, gdy zachowana jest ich integralność. Nie można więc po prostu kasować w nich pojedynczych wpisów.

– Jeżeli ingerencja w kopię zapasową oznacza zagrożenie dla jej integralności, to mamy do czynienia z konfliktem dwóch wartości. Pierwszą jest indywidualne prawo do zapomnienia, przysługujące pojedynczej osobie. Drugie to prawo do bezpieczeństwa danych przysługujące wszystkim osobom, których dane zgromadzono w kopii zapasowej. W tej sytuacji oczywiście jest dla mnie, że priory-

tetem powinna być ochrona danych większości – przekonuje Wojciech Dziomdziora, radca prawny z kancelarii Domański Zakrzewski Palinka i ekspert Polskiej Izby Informatyki i Telekomunikacji.

Kopie zapasowe nie służą tylko temu, by odzyskać dane w razie problemów. Mogą również stanowić dowód, np. gdy okazuje się, że ktoś kradnie bądź zmienia dane. Warunkiem jest jednak ich integralność, czyli pewność, że nikt ich nie zmienił.

Dostrzega to również GODO, który przyznaje, że są sytuacje, w których przechowywanie danych w kopiach zapasowych będzie uzasadnione.

– GODO ma świadomość, że przeszkodą w określaniu krótkiego okresu przechowywania kopii bezpieczeństwa może być potrzeba ich dłuższego przechowywania w celu analizy incydentów naruszenia ochrony danych, w tym oceny ich przyczyn i skutków. Termin przechowywania danych w takich celach jest trudny do ustalenia. Statystyka wskazuje, że średni czas od zaistnienia incydentu do momentu jego wykrycia sięga

ok. 100 dni – przyznaje Agnieszka Świątek-Druś.

## Nie taki diabeł straszny

Co zatem zrobić, by sprostać prawu do bycia zapomnianym, a jednocześnie nie tracić integralności kopii zapasowych?

– Zadanie nie jest trywialne, jak większość zadań, przed którymi stawia nas RODO. Usuwanie danych powinno być procesem, który może wymagać paradoksalnie pamiętania o tym, że należy zapomnieć. Jak inaczej Google mogłoby się wywiązać z obowiązku niepokazywania wyników wyszukiwania w odniesieniu do zakazanych wyników niż przez stworzenie listy wyjątków – zauważa Maciej Gawroński, partner zarządzający w kancelarii Gawroński & Partners s.k.a.

Jego zdaniem optymalnym rozwiązaniem jest wprowadzenie listy wyjątków. Upraszczając – dane na bieżąco są kasowane z systemu, na którym pracuje firma. Jednocześnie jest tworzona lista danych, które mają być usunięte w przypadku odtworzenia bazy z kopii zapasowej. Prowadzi to do pewnego paradoksu, gdyż trzeba pamiętać to,

co musi zostać zapomniane. Nie musi to jednak oznaczać mnożenia danych osobowych.

– Informacja o danych usuniętych nie musi być tożsama z ich treścią. Może np. obejmować kategorie danych i okres, za który nie powinny one być przetwarzane – tłumaczy Maciej Gawroński.

– Rekord podlegający usunięciu można oznaczyć unikalnym identyfikatorem. Wtedy, dokonując pierwotnego usunięcia, wystarczy zapisać identyfikator rekordu w liście wyjątków, a w razie przywrócenia kopii zapasowej automatycznie usunąć lub nadpisać zidentyfikowany rekord pierwotnie określoną zawartością zastępczą. Można też zastosować klucz złożony z ID systemowego i np. PESEL osoby. Wtedy system będzie wiedział, co kasować w razie przywrócenia danych – dodaje ekspert.

## Bez zbędnej zwłoki

Kwestie związane z usuwaniem danych z backupów bez wątpienia będą przysparzać administratorom wielu kłopotów. Plusem jest to, że nie muszą tego robić natychmiast. Zgodnie z art. 17 ust. 1 RODO powinni sprostać żądaniom usunięcia danych bez zbędnej zwłoki, ale ostateczny termin to miesiąc. W razie potrzeby można go przedłużyć o kolejne dwa miesiące, z uwagi na skomplikowany charakter żądań lub ich liczbę.

– Najczęściej popełnianym błędem w odniesieniu do tworzenia i przechowywania kopii bezpieczeństwa jest jednak to, że kolejno wykonywane kopie przechowywane są nie tylko w celu odtworzenia danych na wypadek awarii, ale również w celach archiwalnych. Tymczasem takie łączenie różnych celów przetwarzania danych jest niezgodne z prawem, a przez to niemożliwe do pogodzenia – podkreśla Agnieszka Świątek-Druś.

## PISALIŚMY O TYM

Większość firm nie poinformuje o przetwarzaniu danych – DGP nr 12/2018  
www.prawo.gazetaprawna.pl



114

za tyle dni zacznie być stosowane RODO



184 tys.

zbiorów danych zarejestrowano u GODO