

Modele kontroli dostępu do danych telekomunikacyjnych

Prof. UMK, dr hab. Andrzej Adamski
Katedra Prawa Karnego i Polityki Kryminalnej
Wydział Prawa i Administracji
Uniwersytet Mikołaja Kopernika w Toruniu

Reglamentacja prawna danych o ruchu telekomunikacyjnym w Unii Europejskiej

Dawny model (1997, 2002) cel : potrzeby operatorów i ich klientów, ochrona prywatności użytkowników.

- „dane o ruchu” - wszelkie dane przetwarzane do celów przekazywania komunikatu w sieci łączności elektronicznej lub **naliczania opłat** za te usługi;
- muszą zostać **usunięte lub anonimizowane**, gdy nie są już potrzebne do celów transmisji komunikatu...

DYREKTYWA 2002/58/WE (art. 6): Można przetwarzać dane o ruchu niezbędne do celów naliczania opłat abonenta i opłat rozliczeń międzyoperatorских. Przetwarzanie takie jest dozwolone tylko do końca okresu, w którym rachunek może być zgodnie z prawem zakwestionowany lub w którym należy uiścić opłatę.

Nowy model (Dyrektywa 2006/24/WE) cel: potrzeby organów ścigania, wymiaru sprawiedliwości i służb specjalnych, ochrona bezpieczeństwa publicznego.

- „dane” oznaczają dane o ruchu i lokalizacji oraz powiązane dane niezbędne do **identyfikacji** abonenta lub użytkownika;
- są **zatrzymywane** na okresy nie krótsze niż 6 miesięcy oraz nie dłuższe niż 24 m-ce od daty połączenia.

Wyrok TSUE (08.04.2014) : **dyrektywa 2006/24 jest nieważna** - prawodawca Unii przekroczył granice, które wyznacza poszanowanie zasady proporcjonalności na gruncie art. 7, 8 i art. 52 ust. 1 Karty Praw Podstawowych UE.

Wyrok TSUE z dnia 8 kwietnia 2014 r.

39 Co się tyczy zasadniczej istoty prawa podstawowego do poszanowania życia prywatnego oraz innych praw wynikających z art. 7 karty, należy stwierdzić, że, mimo tego, iż obowiązek zatrzymywania danych nałożony dyrektywą 2006/24 **stanowi szczególnie poważną ingerencję w te prawa, nie narusza on ich istoty, gdyż zgodnie z art. 1 ust. 2 tej dyrektywy nie pozwala ona na zapoznawanie się z samą treścią komunikatów elektronicznych.**

40 **Owo zatrzymywanie danych nie narusza też zasadniczej istoty prawa podstawowego do ochrony danych osobowych ustanowionego w art. 8 karty, gdyż w art. 7 dyrektywy 2006/24 ustanawia regułę dotyczącą ochrony i bezpieczeństwa danych, zgodnie z którą, bez uszczerbku dla postanowień przyjętych zgodnie z dyrektywą 95/46/WE i dyrektywą 2002/58/WE, dostawcy ogólnie dostępnych usług łączności elektronicznej lub publicznej sieci łączności obowiązani są przestrzegać pewnych zasad w zakresie ochrony i bezpieczeństwa danych ustanawianych przez państwa członkowskie, które gwarantują, że w stosunku do danych stosowane będą właściwe środki techniczne i organizacyjne w celu ich ochrony przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą.**

44 ustanowiony w dyrektywie 2006/24 obowiązek zatrzymywania danych w celu ich ewentualnego udostępniania właściwym organom krajowym, w istocie realizuje cel interesu ogólnego.

Retencja danych telekomunikacyjnym w Polsce

- XII 2000 r. – projekt nałożenia na operatorów obowiązku „ciągłego monitorowania użytkowników sieci telekomunikacyjnych”, w tym Internetu (rozp. MSWiA),
- I 2003 r. - obowiązek zapewnienia „uprawnionym podmiotom” dostępu do posiadanych przez operatorów danych „z ostatnich **12 miesięcy**” (Rozp. Min. Infrastruktury § 5 pkt 7),
- art. 165 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne : obowiązek przechowywania przez okres **12 miesięcy** danych transmisyjnych dotyczących abonentów i użytkowników końcowych
 - XI 2005 r. – postulat polityczny PiS : **15-letni** okres przechowywania danych
 - 2006 r. – projekt nowelizacji ustawy Prawo telekomunikacyjne : **5 letni okres retencji danych**
- 2009 – implementacja Dyrektywy 2006/24/WE do prawa telekomunikacyjnego – 24 m. okres retencji danych
- 2011 – nowelizacja prawa telekomunikacyjnego, skrócenie okresu retencji do 12 m-cy,
- 2011 – zaskarżenie przepisów o retencji danych przez oraz grupę posłów SLD (28.01.), RPO (01.08.) oraz Prokuratora Generalnego (21.06.2012) do Trybunału Konstytucyjnego.
- 30.07.2014 ogłoszenie wyroku Trybunału Konstytucyjnego.

Retencja danych - instrument inwigilacji masowej

SK RFN z 2 marca 2010

- retencja danych przez 6 miesięcy
„poważnie zwiększa ryzyko obywateli, że zaczną być śledzeni, mimo że nie zrobili nic złego. Wystarczy o niewłaściwej porze skontaktować się z określoną osobą, by zostać zmuszonym do składania na ten temat wyjaśnień”.

Badania w Polsce

- w 2009 r. 71% ankietowanych prokuratorów zlecało ekspertyzy dotyczące połączeń telekomunikacyjnych w związku ze sprawami o posiadanie narkotyków,
- na podstawie bilingu poszukiwano nowych osobowych źródeł dowodowych w celu ewentualnego rozszerzenia zarzutów osobom podejrzanym o posiadanie,
 - wzywano i przesłuchiowano jako świadków osoby „z bilingu”

Wyrok TK z 30 lipca 2014

TK : wnioskodawcy (RPO, PG) nie kwestionują istoty retencji danych, czyli przepisów prawa telekomunikacyjnego nakładających na przedsiębiorców telekomunikacyjnych obowiązek zatrzymywania danych telekomunikacyjnych.

Poza zakresem zaskarżenia jest:

- a) problem dopuszczalności i proporcjonalności tego obowiązku,
- b) zakresu danych podlegających retencji i
- c) obowiązkowego okresu ich zatrzymywania.

TK: zarzuty wnioskodawców mają stosunkowo wąski zakres. Ograniczają się do zagadnienia udostępniania służbom policji i ochrony państwa - w ramach czynności operacyjno-rozpoznawczych - danych będących przedmiotem retencji.

TK: Chodzi więc o „ocenę konstytucyjności przepisów kompetencyjnych, które upoważniają do wykorzystywania tych danych w pracy operacyjno-rozpoznawczej”.

Niezgodność przepisów ustawy o policji z konstytucją

- TK podziela zarzuty wnioskodawców o niezgodności art. 20c ust.1 ustawy o policji z art. 47 i 49 w zw. z art. 31 ust.3 Konstytucji w odniesieniu do zarzutu niedostosowania gwarancji proceduralnych zw. z brakiem ZEWNĘTRZNEJ KONTROLI UDOSTĘPNIANIA DANYCH TELEKOMUNIKACYJNYCH.

TK nadaje temu zarzutowi kluczowe znaczenie na tle innych zarzutów podniesionych przez wnioskodawców.

Zdaniem TK stwierdzenie niekonstytucyjności przepisów w zakresie braku zewnętrznej kontroli udostępniania danych „uczyni zbędnym odnoszenie się do pozostałych zarzutów sformułowanych przez wnioskodawców, a związanych z dopuszczalnością pozyskiwania danych w celu zapobiegania przestępstwom o relatywnie niewielkim stopniu społecznej szkodliwości oraz ich ścigania, czy też braku przesłanki subsydiarności”.

Stanowisko kontrowersyjne, TK nie ustosunkował się do zarzutu naruszenia zasady proporcjonalności i nie sformułował w tym zakresie swojego stanowiska/ propozycji.

Zasada proporcjonalności, zasada konieczności

PG 21.06.2012 r. w nawiązaniu do wyroku TK z 2005 r.

1. *wyważenie właściwej proporcji w prawnej ochronie obu sfer, obejmuje: z jednej strony, **regulację materialnoprawną** (określającą granice stawiane przez system prawa wkroczeniu przez władzę w poszczególne sfery prywatności jednostki); z drugiej zaś - **gwarancje proceduralne**, tj. konieczność zgłoszenia kontroli organowi pozapolicyjnemu i jej legalizacji przez ten organ, przesłanki i procedury legalizacji - przez organ zewnętrzny* (wyrok TK z dnia 12 grudnia 2005 r., sygn. K 32/04)
2. Analizowane uprawnienia służb dotyczą nie tylko przestępstw ściganych z urzędu (w tym również ściganych na wniosek pokrzywdzonego), ale również wszystkich **przestępstw ściganych z oskarżenia prywatnego**.
3. *należałoby zakwestionować wyposażenie służb przez ustawodawcę w uprawnienie do pozyskiwania i przetwarzania billingów, w kontekście zasady konieczności wkraczania przez te służby w sferę praw i wolności jednostki. **Trudno sobie wyobrazić, by dane telekomunikacyjne mogły pozwolić służbom na zapobieżenie lub wykrycie większości omawianych wyżej czynów określonych przez ustawodawcę jako przestępstwa.***

Reasumując tę część rozważań, zawartych w uzasadnieniu niniejszego wniosku, należy stwierdzić, że przepisy art. 20c ust. 1 ustawy z o Policji (....) **są niezgodne z art. 2, art. 47 oraz art. 49 w związku z art. 31 ust. 3 Konstytucji RP.**

Propozycje Trybunału Konstytucyjnego dotyczące modelu kontroli dostępu do danych telekomunikacyjnych w toku czynności operacyjno-rozpoznawczych

1. **Kontrola następcza** – co do zasady
2. Sąd lub inny organ niezależny od rządu i „*niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności*”
3. **Kontrola uprzednia** zalecana w dwóch przypadkach:
 - a. udostępniania danych osób wykonujących zawody zaufania publicznego,
 - b. gdy „*nie ma konieczności pilnego działania służb*”

Organy kontroli dostępu do danych w krajach UE

Sąd	Sąd lub prokurator	Sędzia śledczy lub prokurator	Prokurator	Organ administracyjny	brak kontroli uprzedniej	brak organu kontroli zewnętrznej
Bułgaria Dania Finlandia Grecja Hiszpania Litwa Luksemburg Niemcy Portugalia Słowenia	Belgia Cypr	Estonia Holandia	Węgry Włochy	Francja Irlandia Malta UK	Irlandia Malta UK	Czechy Łotwa Polska Słowacja

Model francuski

Ściganie przestępstw

- **brak organu kontroli dostępu;**
- policjant sądowy, prokurator i sędzia śledczy uzyskują dane bezpośrednio od dostawców usług (art. 60-1 kpk);
- **prokurator** upoważniony przez sędziego wolności i detencji w przypadku wniosku policji o „zamrożenie” przez dostawcę usługi informacji dostępnych *online* (art.60-2 kpk)
- **kontrola uprzednia**

Zapobieganie przestępstwom

- **urzędnik MSW** (*personnalité qualifiée*)
- **uprzednia kontrola** wniosków policji i organów bezpieczeństwa publicznego (art. L34-1-1 CPCE)

Liczba wniosków o udostępnienie danych telekomunikacyjnych złożonych przez francuskie służby specjalne do *personnalité qualifiée* (2008-2012).

Rok	Liczba wniosków skierowanych do <i>personnalité qualifiée</i>	Wnioski uznane za prawidłowe	Wnioski załatwione odmownie
2008	38.306	34.911	93
2009	43.559	39.070	30
2010	45.716	38.566	90
2011	34.081	31.637	16
2012	29.322	26.569	23

W 2009 r. 76% wniosków dotyczyło identyfikacji abonenta lub użytkownika usługi telekomunikacyjnej. Znacznie rzadziej (23%) pytano o połączenia telekomunikacyjne inwigilowanych osób. Znikoma była liczba zapytań o dane geolokacyjne (mniej niż 1 % ogólnej liczby wniosków).

Model włoski kontroli dostępu do danych

Ściganie przestępstw	Zapobieganie przestępstwom
- prokurator publiczny przy sądzie I inst. (art. 132 (1) KODO) - kontrola uprzednia	- prokurator publiczny przy sądzie I inst. zatwierdza wniosek policji o „zamrożenie danych” (art.132 (4) KODO) - prokurator publiczny przy sądzie apelacyjnym zatwierdza wniosek służb wywiadu o dostęp do danych (art. 4 dekretu antyterrorystycznego z 27.07.2005)

Włochy – przesłanki dostępu do danych

- **Retencja danych telekomunikacyjnych stanowi element systemu ustawowej ochrony danych osobowych**
- **Włoski Kodeks ochrony danych osobowych** (art.132 ust. 3) zapewnia dostęp do danych osobom mającym w tym uzasadniony interes prawny, w szczególności w celach procesowych związanych z ochroną indywidualnych dóbr prawnych.
- przewiduje też możliwości udostępniania danych :
 - policji (ściganie przestępstw) - na podstawie postanowienia prokuratora,
 - na podstawie wniosku obrońcy, podejrzanego, osoby pokrzywdzonej lub każdej innej osoby prywatnej, przy czym obrońca oskarżonego lub podejrzanego może bezpośrednio zwrócić się dostawcy usług o udostępnienie danych na warunkach określonych przepisami Kodeksu postępowania karnego i Kodeksu ochrony danych osobowych(art. 391 ust.4 KPK w zw. z art. 8 (2) lit. f Kodeksu ochrony danych osobowych).

Model niemiecki

Ściganie przestępstw	Zapobieganie przestępstwom
- sąd, uprzednia kontrola wniosków o udostępnianie danych na temat połączeń i lokalizacji (art. 100g (2) StPO) - brak kontroli udostępniania danych osobowych abonentów usług (art.113 TKG) - brak kontroli udostępniania „danych statycznych” (art.112 TKG)	- komisje parlamentarne: - Komisja G 10 – kontrola zarządzeń uzyskania danych przed ich wykonaniem (kontrola uprzednia) - Parlamentarne Gremium Kontrolne – kontrola następcza

Niemcy – zakres kontroli sądowej ze względu na rodzaj danych

1. ustawodawstwo RFN nie przewiduje sądowej kontroli udostępniania tzw. „danych statycznych” (art. 113 TKG) , ani danych osobowych użytkowników usług telekomunikacyjnych, w tym danych umożliwiających identyfikację adresów IP;
2. dane osobowe abonentów usług telekomunikacyjnych są udostępniane podmiotom uprawnionym w sposób zautomatyzowany przez Federalną Agencję Sieci (art. 112 (1) TKG) > Die Bundesnetzagentur <
3. w 2013 r. FAS otrzymała od 102 podmiotów uprawnionych*/ **35,15** mln zapytań, z czego **26,7** mln dotyczyło nazwiska abonenta i **8,45** mln numeru telefonu. Odpowiedzi pochodziły od 127 przedsiębiorców telekomunikacyjnych.

*/ Podmioty uprawnione obejmują oprócz sądów i organów ścigania także organy celne, cywilne i wojskowe służby wywiadu , organy ochrony konstytucji, służby ratunkowe , federalne instytucje nadzoru i kontroli finansów oraz inne podmioty publiczne.

RFN – statystyka spraw i zezwoleń sądu na korzystanie z danych w postępowaniu karnym

Rok	Liczba spraw, w których korzystano z danych telekomunikacyjnych o połączeniach lub lokalizacji	Liczba zezwoleń sądu na podst. § 100g ust.1 zd.1 StPO (przestępstwa poważne)	Liczba zezwoleń sądu na podst. § 100g ust.1 zd.2 StPO (przestępstwa popełnione z wykorzystaniem sieci telekomunikacyjnej)
2008	8.123	12.469	1.414
2009	9.459	14.714	1.456
2010	6.828	11.663	835
2011	7.986	13.236	921
2012	10.070	17.020	1.011

Polskie statystyki zapytań o dane telekomunikacyjne

rok	Liczba zapytań o udostępnienie danych telekomunikacyjnych
2009	1 059,089
2010	1 399,144
2011	1 874,107
2012	1 762,620
2013	1,75 mln

Dane UKE

ABW - operatorzy komórkowi	2010
Zapytań ogółem:	138 tys. tj. 13% ogólnej liczby
O dane abonentów	70 tys.
O dane o połączeniach	63,5 tys.
O dane o lokalizacji	4,5 tys.

Warunki wstępne wprowadzenia kontroli udostępniania danych telekomunikacyjnych w Polsce

1. Ograniczenie korzystania z danych telekomunikacyjnych dotyczących połączeń i lokalizacji do ścigania przestępstw poważnych (np. zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata) oraz przestępstw popełnianych z wykorzystaniem sieci telekomunikacyjnych.
2. Wyłączenie z definicji legalnej tajemnicy telekomunikacyjnej danych osobowych abonentów.
3. Zapewnienie osobom mającym w tym uzasadniony interes prawny, w szczególności w celach procesowych związanych z ochroną dóbr osobistych, dostępu do danych umożliwiających identyfikację sprawców naruszeń / „prawo do sądu”.
4. Powołanie niezależnego organu kontrolującego pracę operacyjną służb specjalnych, sprawującego m.in. kontrolę następczą nad gromadzeniem i przetwarzaniem danych telekomunikacyjnych przez służby specjalne.



Uniwersytet
Kardynała Stefana Wyszyńskiego
w Warszawie



Narodowe Centrum
Badań i Rozwoju



NAUKOWE
CENTRUM
PRAWNO
INFORMATYCZNE

Dziękuję za uwagę

Konstytucja RP

Art. 51.

Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.

Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Mapa mobilności użytkownika telefonu komórkowego w dniach 25-27.04.2013 r. na podstawie danych uzyskanych od operatora.



Niemieckie przepisy procesowe

- 1 Wykorzystywanie w postępowaniu karnym **danych o połączeniach** telekomunikacyjnych bez wiedzy osoby, której te dane dotyczą, jest dopuszczalne, jeżeli jest to konieczne dla wyjaśnienia sprawy albo w celu ustalenia miejsca pobytu podejrzanego, gdy inne środki byłyby nieskuteczne a wykorzystanie danych jest proporcjonalne ze względu na wagę sprawy (art. 100g (1) 2, zd. 2 StPo).

Ponadto (zd.3) - korzystanie z **danych lokalizacyjnych gromadzonych w czasie rzeczywistym** jest dopuszczalne tylko w przypadku istnienia uzasadnionego podejrzenia dokonania, usiłowania lub przygotowania w drodze innego czynu zabronionego przestępstwa, które nawet w indywidualnym przypadku jest przestępstwem poważnym, w szczególności jednego z tych, które wymienia w art. 100a (2).

0

1 Zasada proporcjonalności:

z uwagi na rosnące znaczenie środków komunikacji elektronicznej, dane, które mają być zatrzymywane na podstawie tej dyrektywy, dają krajowym organom ścigania dodatkowe możliwości w zakresie wyjaśniania okoliczności poważnych przestępstw i z tego względu stanowią dla nich cenne narzędzie przy prowadzeniu czynności dochodzeniowo-śledczych. Można zatem uznać, że **zatrzymywanie tego rodzaju danych jest odpowiednie dla realizacji celów, jakie zakłada ta dyrektywa.**

2. Warunek środka koniecznego:

cel interesu ogólnego, mimo ma on fundamentalne znaczenie, **sam w sobie nie uzasadnia** stwierdzenia, że system zatrzymywania danych taki jak ten ustanowiony przez dyrektywę 2006/24, **jest konieczny** do celów tej walki.

3. Konieczny sensu stricte?

Co się tyczy kwestii, czy ingerencja, którą zakłada dyrektywa 2006/24, jest ograniczona do tego, co ściśle niezbędne, należy zauważyć, że zgodnie z art. 3 w związku z art. 5 ust. 1 dyrektywa ta zobowiązuje do zatrzymywania wszystkich danych o ruchu związanych z telefonią stacjonarną i mobilną, dostępem do Internetu, pocztą elektroniczną oraz telefonią internetową. **Ingeruje więc w prawa podstawowe prawie wszystkich mieszkańców Unii Europejskiej.**

test proporcjonalności dot. retencji danych telekomunikacyjnych

Pytania

➔ ustalenie, czy ograniczenie w interesie publicznym konstytucyjnie gwarantowanych praw i wolności jest usprawiedliwione.

Czy retencja danych jest środkiem:

- odpowiednim do osiągnięcia określonego celu;
- **koniecznym** do osiągnięcia celu (tzn. środkiem najmniej restrykcyjnym spośród dostępnych);
- **proporcjonalnym** w ścisłym rozumieniu (tj. właściwej proporcji pomiędzy celem ingerencji i określonymi prawami jednostki)

Odpowiedzi

TAK

NIE

NIE

Kryterium środka koniecznego do osiągnięcia celu

Badania niemieckie nt. efektywności zabezpieczenia danych *lquick freeze*

Wg analizy *Bundeskriminalamt* w 2005 r. policja nie uzyskała dostępu do danych w 381 sprawach (dane nie były już dostępne u operatorów)

- 381 w stosunku do 6.4 mln spraw w 2005 r. to **0.001%**

Wg badań Instytutu Maxa Plancka : w 99,99% postępowaniach karnych rocznie dostęp do danych o ruchu i lokalizacji gwarantuje organom ścigania procedura „quick freeze”*

A zatem , w 99,99% śledztw w sprawach karnych rocznie, **zabezpieczenie danych aktualnie dostępnych mogłoby być realną alternatywą dla reżimu retencji danych**

* Zob. art. 218a polskiego k.p.k. oraz art. 16 konwencji RE o cyberprzestępczości

Wyrok TK z 3 października 2000 r. (K. 33/99)

zastosowanie środków niezbędnych (koniecznych) w tym sensie, że będą one chronić określone wartości w sposób, bądź w stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych środków, a jednocześnie winny to być środki jak najmniej uciążliwe dla podmiotów, których prawo bądź wolność ulegają ograniczeniu

Czy retencja danych jest środkiem proporcjonalnym?

Kwestia 1

Czy przechowywanie danych o połączeniach telekomunikacyjnych wszystkich obywateli na wypadek ich ewentualnej przydatności dla organów ścigania i wymiaru sprawiedliwości spełnia warunek proporcjonalności?

Wyrok Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r. (K 32/04)

„W demokratycznym państwie prawnym **nie jest konieczne** przechowywanie informacji na temat obywateli, uzyskanych w toku czynności operacyjnych **ze względu na potencjalną przydatność tych informacji.**”

Czy retencja danych jest środkiem proporcjonalnym?

Kwestia 2

Kiedy korzystanie z danych telekomunikacyjnych przez organy ścigania spełnia kryterium proporcjonalności?

Wyrok Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r. (K 32/04)

„Może to być stosowane **tylko w związku z konkretnym postępowaniem**, prowadzonym na podstawie ustawy dopuszczającej ograniczenie wolności ze względu na bezpieczeństwo państwa i porządek publiczny.”

0

1

Uchylenie wyrokiem Sądu Konstytucyjnego RFN z 2 marca 2010 r. art. 113b TKG nie pozbawiło służb specjalnych możliwości korzystania z danych o ruchu w telekomunikacji.

Wszystkie służby specjalne mają „**szczególne uprawnienia w zakresie żądania informacji**” (art. 8a BVerfSchG). Dotyczą one dostępu do danych telekomunikacyjnych i danych o ruchu na serwerach dostawców usług internetowych – gromadzonych i przechowywanych przez przedsiębiorców w celach komercyjnych (art. 2 ustawy G 10).

Co do zasady, kontrola dostępu do tych danych przez Komisję G 10 ma charakter uprzedni.

Osoba odpowiedzialna w Ministerstwie Federalnym każdego miesiąca informuje Komisję G 10 o zarządzeniach dotyczących udostępnienia danych, przed ich wykonaniem, chyba że zachodzą okoliczności niecierpiące zwłoki i zarządzenie trzeba wykonać natychmiast. W zwykłym trybie postępowania, legalność takiego zarządzenia i konieczność jego wykonania jest przedmiotem oceny Komisji.

Jeżeli jest to ocena negatywna, Minister Federalny unieważnia wydane zarządzenie, a uzyskane na jego podstawie dane są niezwłocznie niszczone (art. 8 (5) BVerfSchG).