Warszawa, dnia 7 września 2021 r.

Poz. 3

Z A R Z Ą D Z E N I E

P R E Z E S A U R Z Ę D U O C H R O N Y K O N K U R E N C J I I K O N S U M E N T Ó W

z dnia 7 września 2021 r.

w sprawie podstawowych zasad bezpieczeństwa informacji w Urzędzie Ochrony Konkurencji i Konsumentów (Polityka Bezpieczeństwa Informacji)

Na podstawie § 1 ust. 2 statutu Urzędu Ochrony Konkurencji i Konsumentów, stanowiącego załącznik do zarządzenia nr 272 Prezesa Rady Ministrów z dnia 20 grudnia 2019 r. w sprawie nadania statutu Urzędowi Ochrony Konkurencji i Konsumentów (M.P. poz. 1198 oraz z 2020 r. poz. 498) w związku z § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247) zarządza się, co następuje:

§ 1. 1. Zarządzenie określa podstawowe zasady bezpieczeństwa informacji tworzonych, wykorzystywanych, przechowywanych, udostępnianych, przetwarzanych w sposób zautomatyzowany lub niezautomatyzowany przez Urząd Ochrony Konkurencji i Konsumentów, zwany dalej „Urzędem”:

1) niezależnie od tego, czy stanowią własność Urzędu, czy zostały przekazane lub powierzone Urzędowi przez inne osoby lub podmioty, w szczególności w ramach umów lub porozumień,

2) niezależnie od formy ich przetwarzania lub przesyłania, w tym informacji przekazywanych pisemnie, ustnie lub z wykorzystaniem systemów informatycznych,
3) niezależnie od sposobu ich zapisania lub przechowywania, w tym informacji utrwalonych na informatycznych nośnikach danych lub w postaci papierowej, w formie nagrań audio lub video

– zwanych dalej „informacjami”.

2. Zasady ochrony informacji niejawnych określają przepisy odrębne.

3. Zasady ochrony danych osobowych określa odrębne zarządzenie Prezesa Urzędu.

4. Jeżeli przepisy odrębnych ustaw, które odnoszą się do bezpieczeństwa i ochrony informacji, przewidują dalej idącą ich ochronę, niż wynika to z Polityki Bezpieczeństwa Informacji i innych przepisów wewnętrznych określających zasady i procedury dotyczące bezpieczeństwa informacji w Urzędzie, stosuje się przepisy tych ustaw.

5. Jeżeli systemy zarządzania laboratoriami, ustanowione w celu spełnienia wymagań dotyczących kompetencji laboratoriów określonych w Polskiej Normie, zawierają zasady i procedury przewidujące dalej idącą ochronę informacji dotyczących badań prowadzonych przez laboratoria, niż wynika to z Polityki Bezpieczeństwa Informacji i innych przepisów wewnętrznych określających zasady i procedury dotyczące bezpieczeństwa informacji w Urzędzie, stosuje się zasady i procedury zawarte w systemach zarządzania laboratoriami.

§ 2. 1. Podstawowe zasady bezpieczeństwa informacji określone w niniejszym zarządzeniu stanowią Politykę Bezpieczeństwa Informacji w Urzędzie.

2. Zgodnie z § 6 zarządzenia Prezesa Urzędu Ochrony Konkurencji i Konsumentów z dnia 3 września 2021 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Ochrony Konkurencji i Konsumentów (Dz. Urz. UOKiK poz. 2), Dyrektor Generalny Urzędu określa w przepisach odrębnych szczegółowe zasady i procedury dotyczące bezpieczeństwa informacji.

3. Podstawowe zasady bezpieczeństwa informacji (Polityka Bezpieczeństwa Informacji) oraz szczegółowe zasady i procedury dotyczące bezpieczeństwa informacji zawarte w przepisach, o których mowa w ust. 2, są elementem Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie.

4. Zasady określone w Polityce Bezpieczeństwa Informacji należy uwzględniać przy opracowywaniu innych przepisów wewnętrznych określających zasady i procedury dotyczące bezpieczeństwa informacji w Urzędzie.

§ 3. Zasady i procedury dotyczące bezpieczeństwa informacji stosuje się w miejscach i sytuacjach, w których informacje związane z działalnością Urzędu są przetwarzane w siedzibie głównej Urzędu, budynkach delegatur i laboratoriów (zwanych dalej „budynkami Urzędu") oraz poza tymi lokalizacjami, w szczególności w ramach prowadzonych kontroli i przeszukań, zdalnego korzystania z sieci komputerowej Urzędu, w tym telepracy i pracy zdalnej.

§ 4. 1. Zasady bezpieczeństwa informacji są realizowane w szczególności przez:

1) zapewnienie odpowiedniej organizacji i niezawodności procesów przetwarzania informacji, w szczególności skuteczności i adekwatności działania zabezpieczeń chroniących przed nieuprawnionym ujawnieniem, odpowiednich warunków do ich użytkowania oraz sprawności i efektywności ich wykorzystywania;
2) zapewnienie, aby pracownicy Urzędu mający dostęp do informacji posiadali odpowiednią wiedzę i umiejętności niezbędne do stosowania zasad bezpieczeństwa informacji;
3) ochronę organizacyjną, techniczną i fizyczną informacji przed dostępem osób nieuprawnionych, w szczególności przed nieuprawnionym wykorzystaniem, kradzieżą, uszkodzeniem, nieuprawnioną modyfikacją lub zniszczeniem;
4) zabezpieczenie systemów informatycznych, w tym systemów teleinformatycznych, używanych do realizacji zadań publicznych przez Urząd;
5) zabezpieczenie informacji przed ich uszkodzeniem lub zniszczeniem w wyniku pożaru, zalania, zdarzenia o charakterze terrorystycznym, zjawisk naturalnych lub innych zagrożeń;
6) zapewnienie ciągłości działania procesów przetwarzania informacji;
7) zapewnienie możliwości sprawnego odtworzenia informacji w przypadku ich zniszczenia;
8) zapewnienie gotowości do reakcji na sytuację awaryjną lub kryzysową;
9) zapewnienie rozwiązań organizacyjnych i systemowych regulujących zasady i sposób zarządzania bezpieczeństwem informacji;
10) zapewnienie spójnej polityki informacyjnej;
11) określenie i stosowanie odpowiednich zasad i procedur w zakresie bezpieczeństwa informacji w umowach i porozumieniach;
12) zapewnienie pracownikom Urzędu szkoleń oraz organizowanie akcji informacyjnych i edukacyjnych z zakresu bezpieczeństwa informacji;

13) zapewnienie działań kontrolnych w zakresie przestrzegania zasad i procedur określonych w Urzędzie.

2. W celu ochrony bezpieczeństwa informacji mogą być podejmowane działania lub stosowane rozwiązania ograniczające prawdopodobieństwo wystąpienia zagrożenia lub minimalizujące jego negatywne skutki, które mogą mieć charakter zabezpieczeń:

1) organizacyjnych, w tym polegających na określeniu zasad i procedur dotyczących bezpieczeństwa informacji, wyznaczeniu osób odpowiedzialnych za organizację ochrony bezpieczeństwa informacji, określeniu obowiązków i uprawnień poszczególnych osób w zakresie ochrony bezpieczeństwa informacji, organizowaniu szkoleń oraz organizowaniu kontroli i audytu ustalonych zasad i procedur;
2) technicznych, w tym obejmujących środki zabezpieczające systemy informatyczne przed szkodliwym oprogramowaniem, elektroniczne urządzenia i systemy alarmowe sygnalizujące zagrożenie osób lub mienia, urządzenia wykorzystywane do monitoringu, środki i oprogramowanie zarządzające uprawnieniami w zakresie dostępu do budynków Urzędu i poszczególnych pomieszczeń, systemy podtrzymania zasilania oraz środki zapewniające bezpieczeństwo okablowania i odpowiednią temperaturę w serwerowni;
3) fizyczne, w tym środki mechanicznego zabezpieczenia dostępu do budynków Urzędu, poszczególnych pomieszczeń oraz wyposażenia i mebli wykorzystywanych do przechowywania dokumentów i informatycznych nośników danych.

3. Stosowanie zabezpieczeń powinno uwzględniać następujące zasady:

1) zabezpieczenia powinny być adekwatne do wymogów prawnych oraz wyników audytów i analizy ryzyka bezpieczeństwa informacji (zasada adekwatności zabezpieczeń);
2) zabezpieczenia organizacyjne, techniczne i fizyczne powinny wzajemnie się uzupełniać i zapewniać wymagany poziom bezpieczeństwa informacji (zasada kompleksowości ochrony);
3) zabezpieczenia powinny być dobierane z uwzględnieniem zasad racjonalnego gospodarowania środkami publicznymi oraz ograniczeń i uwarunkowań prawno-organizacyjnych w Urzędzie;
4) przy doborze zabezpieczeń należy kierować się w szczególności:
   a) wymaganiami wynikającymi z przepisów prawa, w tym przepisów rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany

informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,

b) zaleceniami Polskiej Normy PN-ISO 27001,

c) adekwatnością zabezpieczeń,

d) wynikami szacowania ryzyka;

5) poziom bezpieczeństwa informacji wyższy niż minimalny poziom wynikający z obowiązujących przepisów może zostać zastosowany, jeżeli uzasadniają to szczególne potrzeby Urzędu lub wyniki szacowania ryzyka (zasada ochrony niezbędnej);

6) przy doborze zabezpieczeń należy uwzględnić zagrożenia związane ze świadomymi lub nieświadomymi działaniami lub zaniechaniem pracowników Urzędu, jak i innych osób mających lub mogących uzyskać dostęp do informacji;

7) wiedza pracowników Urzędu w zakresie bezpieczeństwa informacji powinna być stale i regularnie doskonalona, w tym poprzez różne formy podnoszenia kwalifikacji.

§ 5. 1. Do przestrzegania zasad bezpieczeństwa informacji są obowiązane wszystkie osoby mające dostęp do informacji, w szczególności:

1) pracownicy Urzędu – w zakresie odpowiednim do nałożonych na nich obowiązków i posiadanych uprawnień, zgodnie z przepisami prawa, w tym przepisami wewnętrznymi obowiązującymi w Urzędzie;

2) osoby świadczące usługi, w tym realizujące umowy serwisowe dotyczące systemów informatycznych, wykonujące dostawy lub roboty budowlane na rzecz Urzędu na podstawie umów cywilnoprawnych, w tym umów zlecenia lub umów o dzieło – w zakresie i na zasadach określonych w tych umowach;

3) osoby odbywające praktykę, staż lub wolontariat – w zakresie i na zasadach określonych odpowiednio w umowie dotyczącej praktyki lub stażu albo w porozumieniu zawartym przez Urząd z wolontariuszem;

4) eksperci oraz pracownicy podmiotów zewnętrznych realizujący inne niż określone w pkt 1–3 zadania na rzecz Urzędu – w zakresie i na zasadach określonych w dokumentach regulujących zasady współpracy tych osób z Urzędem;

5) pracownicy urzędów obsługujących organy, z którymi Prezes Urzędu zawarł porozumienia dotyczące współpracy, jeżeli porozumienia te dotyczą także wymiany informacji – w zakresie i na zasadach określonych w tych porozumieniach.

2. W przypadku, gdy umowy i porozumienia, o których mowa w ust. 1 pkt 2–5, wiążą się z możliwością dostępu do informacji przez osoby inne niż pracownicy Urzędu, umowy

i porozumienia powinny regulować zagadnienia dotyczące ochrony informacji. Zakres zagadnień dotyczących ochrony informacji, które powinny zostać określone w umowach i porozumieniach, o których mowa w ust. 1 pkt 2–5, oraz podstawowe zasady wymiany informacji określa § 10.

3. Biuro Kadr, Szkolenia i Organizacji zapoznaje nowo zatrudnionego pracownika Urzędu z zasadami i procedurami ochrony informacji, w szczególności z Polityką Bezpieczeństwa Informacji, oraz weryfikuje wiedzę w tym zakresie.

§ 6. 1. Osoby mające dostęp do informacji są obowiązane do:

1) przestrzegania zasad i procedur dotyczących bezpieczeństwa informacji;
2) zabezpieczania informacji przed ich udostępnieniem osobie nieuprawnionej, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem informacji;
3) niezwłocznego reagowania w przypadku wystąpienia lub podejrzenia wystąpienia incydentu naruszenia bezpieczeństwa informacji, zgodnie z zasadami określonymi w przepisach odrębnych.

2. Zgodnie z przepisami prawa pracy, pracownicy Urzędu są obowiązani w szczególności zachować w tajemnicy informacje, których ujawnienie mogłoby narazić Urząd na szkodę oraz przestrzegać tajemnicy określonej w przepisach odrębnych.

§ 7. 1. W Urzędzie przyjmuje się następujące kategorie klasyfikacji informacji:

1) informacje jawne;
2) informacje prawnie chronione;
3) informacje wewnętrzne.

2. Informacja jawne to informacje, których udostępnienie nie podlega ograniczeniom, w szczególności informacje powszechnie dostępne oraz informacje publiczne w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 r. poz. 2176 oraz z 2021 r. poz. 1598) z wyłączeniem informacji, do których dostęp podlega ograniczeniom wskazanym w tej ustawie.

3. Informacje prawnie chronione to informacje, których udostępnienie podlega ograniczeniom wynikającym z przepisów prawa powszechnie obowiązującego, w szczególności dane osobowe, informacje stanowiące tajemnicę przedsiębiorstwa, informacje objęte tajemnicą skarbową lub bankową, informacje chronione na mocy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742) oraz

informacje chronione na podstawie ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r. poz. 275).

4. Informacje wewnętrzne to informacje, które nie należą do kategorii informacji jawnych ani informacji prawnie chronionych, wytworzone w ramach Urzędu lub na jego rzecz i przeznaczone wyłącznie do użytku w ramach Urzędu, w tym informacje o charakterze roboczym, porządkowym, ewidencyjnym oraz korespondencja robocza w ramach Urzędu (dokumenty wewnętrzne), lub informacje, których ujawnienie mogłoby narazić Urząd na szkodę.

§ 8. W ramach ochrony bezpieczeństwa informacji w ramach Urzędu stosuje się następujące ogólne zasady:

1) osoby powinny posiadać dostęp tylko do takiego rodzaju informacji oraz systemów informatycznych i baz danych, które są konieczne do prawidłowej realizacji powierzonych im zadań (zasada wiedzy koniecznej);
2) za bezpieczeństwo informacji odpowiadają konkretne osoby, w zakresie nałożonych obowiązków i nadanych uprawnień (zasada indywidualnej odpowiedzialności);
3) stosowane zabezpieczenia nie mogą nadmiernie utrudniać realizacji celów i zadań Urzędu;
4) dokumenty zawierające informacje prawnie chronione i informacje wewnętrzne powinny być przechowywane w miejscach zabezpieczonych przed dostępem osób nieuprawnionych (zasada nadzorowania dokumentów);
5) monitory i inne urządzenia służące do wyświetlania informacji powinny być ustawiane w sposób, który nie pozwala na zapoznanie się z wyświetlanymi informacjami przez osoby postronne lub nieuprawnione (zasada bezpiecznego ustawienia monitora);
6) na czas nieobecności osoby w Urzędzie, dokumenty oraz informatyczne nośniki danych należy przechowywać w odpowiednio zabezpieczonych meblach biurowych, szafach metalowych lub sejfach (zasada czystego biurka);
7) wydruki powinny być sporządzane w sposób uniemożliwiający osobom nieuprawnionym zapoznanie się z treścią drukowanych informacji, w szczególności osoba dokonująca wydruku powinna zapewnić bezpieczeństwo dokumentów drukowanych z wykorzystaniem drukarek umieszczonych w pomieszczeniach, w których przebywają lub do których dostęp mają inne osoby (zasada bezpiecznych wydruków);

8) po zakończeniu spotkania, osoby odpowiedzialne za organizację tego spotkania są obowiązane do uprzątnięcia lub zabezpieczenia materiałów zawierających informacje oraz wyczyścić tablice (zasada czystej tablicy);
9) na czas nieobecności osoby na stanowisku pracy, dostęp do komputera jest blokowany, a po zakończeniu pracy komputer jest wyłączany, chyba że dany komputer musi pracować w trybie ciągłym (zasada blokowania dostępu do komputera);
10) wykonywanie krytycznych zadań nie powinno być powierzane w całości pojedynczym osobom (zasada separacji obowiązków);
11) prawo do przebywania w miejscach istotnych dla bezpieczeństwa informacji powinny mieć tylko osoby upoważnione (zasada obecności koniecznej);
12) miejsca istotne dla bezpieczeństwa informacji powinny być zabezpieczone przed dostępem osób nieuprawnionych; w uzasadnionych przypadkach miejsca te mogą być oznaczone jako miejsca o ograniczonym dostępie;
13) pomieszczenia służbowe (pokoje) powinny być zabezpieczone przed dostępem osób nieuprawnionych, w szczególności na zakończenie dnia pracy ostatnia osoba wychodząca z pomieszczenia powinna zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia w sposób określony w przepisach odrębnych (zasada zamykania pomieszczeń służbowych na czas nieobecności);
14) systemy funkcjonujące w Urzędzie powinny być sprawne i przygotowane na zidentyfikowane zagrożenia; niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających bez zastosowania alternatywnych zabezpieczeń (zasada stałej gotowości systemów);
15) zabronione jest udostępnianie imiennych kont w systemach informatycznych osobom innym niż użytkownik danego konta, z wyjątkiem przypadków przewidzianych przez przepisy odrębne przewidujące udostępnianie takich kont przez administratora danego systemu informatycznego i w szczególnych sytuacjach (zasada zachowania prywatności kont w systemach);
16) osoby są obowiązane do zachowania poufności i nieudostępniania innym osobom haseł i kodów dostępu, w tym haseł i kodów umożliwiających dostęp do systemów informatycznych; zasada ta dotyczy także kart dostępu do pomieszczeń, depozytorów kluczy, tokenów i innych urządzeń służących do uwierzytelniania (zasada poufności haseł);

17) na stacjach roboczych może być zainstalowane wyłącznie legalne oprogramowanie (zasada legalnego oprogramowania);
18) oprogramowanie zainstalowane na stacjach roboczych powinno być stale aktualizowane, w tym poprzez automatyczne aktualizacje (zasada aktualnego oprogramowania);
19) osoby, w szczególności użytkownicy systemów informatycznych, są obowiązane do niezwłocznego zgłoszenia wystąpienia lub podejrzenia wystąpienia incydentu bezpieczeństwa informacji (zasada zgłaszania incydentów bezpieczeństwa informacji);
20) procesy tworzenia kopii zapasowych powinny być zautomatyzowane oraz niemożliwe do przerwania przez osobę (zasada automatyzacji tworzenia kopii zapasowych);
21) w szczególnie uzasadnionych przypadkach zbiór informacji może być bardziej chroniony niż poszczególne informacje, które się na niego składają (zasada podwyższonego poziomu ochrony zbiorów informacji);
22) dokumenty papierowe, z wyjątkiem materiałów promocyjnych, marketingowych i zawierających wyłącznie informacje jawne, powinny być niszczone w sposób uniemożliwiający ich odczytanie (zasada czystego kosza).

§ 9. 1. Dokumenty w postaci papierowej lub utrwalone na informatycznych nośnikach danych mogą być tymczasowo wynoszone poza Urząd przez pracowników Urzędu za zgodą dyrektora komórki organizacyjnej Urzędu lub zastępcy dyrektora. Zgoda ta nie jest wymagana w przypadku gdy:

1) dokumenty te są jednoznacznie związane z rodzajem wykonywanych obowiązków służbowych i jeżeli ich wyniesienie poza Urząd jest niezbędne do wykonania tych obowiązków;
2) dokumenty te zawierają wyłącznie informacje jawne.

2. Dokumenty wynoszone poza Urząd powinny być zabezpieczone przed ich utratą, w szczególności przez bezpośredni nadzór oraz przechowywanie dokumentów w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.

3. Informatyczne nośniki danych powinny być odpowiednio zabezpieczone w czasie transportu i przechowywania, w szczególności przez szyfrowanie.

§ 10. 1. Umowy i porozumienia, które wiążą się z możliwością dostępu do informacji przez osoby inne niż pracownicy Urzędu, powinny regulować zasady dostępu do informacji, w szczególności powinny określać:

1) zakres przekazywanych informacji;

2) sposoby przekazania informacji lub bezpiecznej wymiany informacji;
3) zasady ochrony przekazywanych informacji;
4) dopuszczalny cel przetwarzania przekazywanych informacji;
5) zasady bezpiecznego korzystania z infrastruktury informatycznej Urzędu oraz dostępu do tej infrastruktury, jeżeli jest to niezbędne do realizacji umowy lub porozumienia;
6) zasady odpowiedzialności za naruszenie bezpieczeństwa informacji;
7) tryb postępowania w przypadku wystąpienia incydentu naruszenia bezpieczeństwa informacji;
8) zasady zwrotu otrzymanych nośników informacji przed lub w momencie zakończenia obowiązywania umowy, usunięcia informacji wytworzonych w związku z realizacją umowy lub otrzymanych od Urzędu, w tym drogą elektroniczną, oraz zasady dokumentowania usunięcia informacji;
9) pracownika Urzędu i komórkę organizacyjną Urzędu, którzy są odpowiedzialni za przekazywanie lub odbieranie informacji oraz których należy powiadomić w przypadku wystąpienia incydentu naruszenia bezpieczeństwa informacji;
10) zasady przebywania w budynkach Urzędu, jeżeli jest to niezbędne do realizacji umowy lub porozumienia;
11) zasady składania deklaracji o zapoznaniu się z Polityką Bezpieczeństwa Informacji w Urzędzie.

2. Zagadnienia, o których mowa w ust. 1, nie stanową katalogu zamkniętego i w umowie lub porozumieniu mogą zostać ustalone dodatkowe zasady, jeśli wynika to ze specyfiki umowy lub porozumienia, w szczególności przedmiotu lub sposobu ich realizacji.

3. Wymiana informacji prawnie chronionych i informacji wewnętrznych pomiędzy Urzędem a podmiotem zewnętrznym wymaga odpowiedniego zabezpieczenia informacji, w szczególności szyfrowania plików lub zastosowania zabezpieczeń w odniesieniu dokumentów w postaci papierowej, które wykluczą dostęp osób nieuprawnionych do informacji.

4. Zasady, o których mowa w ust. 1–3, mogą być określone w umowie głównej albo w odrębnym porozumieniu.

5. Projekty umów i porozumień, w zakresie zasad, o których mowa w ust. 1–3, mogą zostać przekazane do zaopiniowania przez Inspektora Ochrony Danych lub Biuro Informatyki i Ochrony.

§ 11. Dyrektor Generalny Urzędu nie rzadziej niż raz w roku dokonuje oceny działania Polityki Bezpieczeństwa Informacji oraz innych zasad i procedur dotyczących bezpieczeństwa informacji w Urzędzie, uwzględniając w szczególności wnioski z audytu, zmieniające się zewnętrzne okoliczności faktyczne i prawne, w tym zmiany przepisów, oraz pojawianie się nowych zagrożeń dla bezpieczeństwa informacji. Jeśli wyniki dokonanej oceny wskazują na potrzebę dokonania zmian, Dyrektor Generalny Urzędu opracowuje projekt zmiany Polityki Bezpieczeństwa Informacji i przedstawia go Prezesowi Urzędu lub dokonuje zmian w zakresie szczegółowych zasad i procedur dotyczących bezpieczeństwa informacji w Urzędzie.

§ 12. Komórki organizacyjne Urzędu, w terminie 12 miesięcy od dnia wejścia w życie zarządzenia, dokonają przeglądu umów i porozumień, za których realizację odpowiadają, w celu ustalenia, czy wymagają one dostosowania do zasad i procedur dotyczących ochrony bezpieczeństwa informacji.

§ 13. Zarządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES URZĘDU OCHRONY

KONKURENCJI I KONSUMENTÓW

Tomasz Chróstny