Warszawa, dnia 3 września 2021 r.

Poz. 2

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 3 września 2021 r.

w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Ochrony Konkurencji i Konsumentów

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 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. Zarządzenie określa ogólne zasady organizacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Ochrony Konkurencji i Konsumentów, zwanym dalej „Urzędem”, w szczególności:

1) sposób określania zasad i procedur dotyczących bezpieczeństwa informacji;
2) działania podejmowane w celu wdrożenia i eksploatacji, monitorowania i przeglądu oraz utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie;
3) strukturę organizacyjną zapewniającą właściwe zarządzanie bezpieczeństwem informacji w Urzędzie i osoby odpowiedzialne za realizację działań, o których mowa w pkt 2.

§ 2. 1. Celem Systemu Zarządzania Bezpieczeństwem Informacji jest zapewnienie poufności, dostępności i integralności informacji, z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

2. System Zarządzania Bezpieczeństwem Informacji dotyczy informacji tworzonych, wykorzystywanych, gromadzonych, udostępnianych, przetwarzanych w sposób zautomatyzowany lub niezautomatyzowany przez Urząd:

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”.

3. Zasady dotyczące bezpieczeństwa informacji określone w ramach Systemu Zarządzania Bezpieczeństwem Informacji nie naruszają zasad określonych w przepisach o ochronie informacji niejawnych i przepisach o ochronie danych osobowych.

§ 3. Użyte w zarządzeniu określenia oznaczają:

1) poufność – właściwość zapewniającą, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom fizycznym;
2) system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2021 r. poz. 576).

§ 4. 1. System Zarządzania Bezpieczeństwem Informacji uwzględnia procesy zapewnienia i utrzymania odpowiedniego poziomu bezpieczeństwa, w tym:

1) zarządzanie ryzykiem;
2) zarządzanie dostępem do zasobów;
3) monitorowanie poziomu bezpieczeństwa;
4) zarządzanie incydentami naruszenia bezpieczeństwa informacji.

2. Nakłady ponoszone na zapewnienie i utrzymanie bezpieczeństwa informacji powinny być poprzedzone analizą ryzyka i kosztów oraz powinny być adekwatne do potencjalnych strat spowodowanych naruszeniem bezpieczeństwa informacji.

§ 5. 1. Podstawowe zasady dotyczące bezpieczeństwa informacji w Urzędzie, w tym zasady klasyfikacji informacji, określa Polityka Bezpieczeństwa Informacji.

2. Politykę Bezpieczeństwa Informacji wprowadza w drodze odrębnego zarządzenia Prezes Urzędu, na wniosek Dyrektora Generalnego Urzędu.

§ 6. 1. Dyrektor Generalny Urzędu określa, w drodze zarządzenia, szczegółowe zasady i procedury dotyczące bezpieczeństwa informacji oraz zasady i procedury bezpieczeństwa informatycznego w Urzędzie.

2. Przepisy, o których mowa w ust. 1, obejmują:

1) zasady ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, realizowanej przez:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
2) zasady zabezpieczania informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
3) zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
4) zasady postępowania z informacjami klasyfikowanymi do poszczególnych kategorii i zasady dokonywania zmian kategorii informacji, a także zasady ochrony, oznaczania, przetwarzania, przechowywania, przekazywania, udostępniania, niszczenia poszczególnych kategorii informacji, w zakresie w jakim kwestie te nie są uregulowane w przepisach prawa powszechnie obowiązującego;
5) zasady nadawania, zmiany i cofania uprawnień w zakresie przetwarzania informacji oraz dostępów do baz danych i systemów informatycznych;
6) zasady korzystania ze sprzętu komputerowego i systemów informatycznych, w tym zasady bezpieczeństwa w systemach teleinformatycznych, z uwzględnieniem Polskiej Normy PN-ISO/IEC 27001;

7) podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
8) zasady zgłaszania incydentów naruszenia bezpieczeństwa informacji i podejmowania działań korygujących;
9) zasady inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmujące ich rodzaj i konfigurację, z uwzględnieniem ogólnych zasad inwentaryzacji majątku Urzędu;
10) zasady przeprowadzania przez dyrektorów komórek organizacyjnych Urzędu okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, w szczególności zasady dokonywania oceny takiego ryzyka, z uwzględnieniem Polskiej Normy PN-ISO/IEC 27005;
11) plan wdrożenia i egzekwowania Polityki Bezpieczeństwa Informacji;
12) inne zasady i procedury dotyczące bezpieczeństwa informacji, jeśli jest to niezbędne do sprawnego i prawidłowego działania Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie.

§ 7. W ramach Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie zadania dotyczące wdrożenia i eksploatacji, monitorowania i przeglądu oraz utrzymania i doskonalenia tego systemu realizują:

1) Prezes Urzędu,
2) Wiceprezesi Urzędu,
3) Dyrektor Generalny Urzędu,
4) Zespół do spraw Systemu Zarządzania Bezpieczeństwem Informacji, zwany dalej „Zespołem ds. SZBI”,
5) Dyrektor Biura Informatyki i Ochrony,
6) Dyrektor Biura Kadr, Szkolenia i Organizacji,
7) dyrektorzy komórek organizacyjnych Urzędu w sprawach należących do zakresu zadań tych komórek,
8) gestorzy systemów informatycznych, administratorzy aplikacji i administratorzy techniczni systemów informatycznych, zgodnie z zasadami określonymi w odrębnych przepisach wewnętrznych,
9) Inspektor Ochrony Danych,
10) Pełnomocnik do spraw ochrony informacji niejawnych

– zgodnie z zasadami określonymi w § 8–17.

§ 8. Prezes Urzędu określa ogólne zasady działania Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie, w tym określa Politykę Bezpieczeństwa Informacji, a także nadzoruje działania podejmowane w celu wdrożenia i eksploatacji, monitorowania i przeglądu oraz utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie.

§ 9. Wiceprezesi Urzędu oraz Dyrektor Generalny Urzędu odpowiadają za bezpieczeństwo informacji w zakresie powierzonych im zadań i nadzorowanych komórek organizacyjnych Urzędu.

§ 10. Dyrektor Generalny Urzędu:

1) określa zasady i procedury, o których mowa w § 6;
2) zapewnia zawieranie w umowach cywilnoprawnych, w tym umowach serwisowych dotyczących systemów informatycznych, podpisywanych ze stronami trzecimi, zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
3) zapewnia organizowanie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok;
4) zapewnia podejmowanie działań kontrolnych w zakresie przestrzegania zasad i procedur określonych w Polityce Bezpieczeństwa Informacji i innych przepisach wewnętrznych określających zasady i procedury dotyczące bezpieczeństwa informacji w Urzędzie.

§ 11. 1. Zespół ds. SZBI wspiera Dyrektora Generalnego Urzędu w realizacji zadań związanych z bezpieczeństwem informacji.

2. Do zadań Zespołu ds. SZBI należy w szczególności:

1) analizowanie wykrytych incydentów naruszenia bezpieczeństwa informacji i przygotowywanie rekomendacji dotyczących działań w tym zakresie;
2) przygotowywanie rekomendacji w zakresie rozwiązań organizacyjno-technicznych dotyczących wdrożenia i eksploatacji, monitorowania i przeglądu oraz utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie;
3) przygotowywanie rekomendacji w zakresie organizacji szkoleń dotyczących bezpieczeństwa informacji i współpraca w tym zakresie z Biurem Kadr, Szkolenia i Organizacji;
4) opracowanie projektów zasad i procedur, o których mowa w § 6;

5) analizowanie wyników kontroli przestrzegania zasad i procedur określonych w Polityce Bezpieczeństwa Informacji oraz przygotowywanie rekomendacji dotyczących zmian Polityki;
6) wspieranie działań podejmowanych w ramach procesu zarządzania ryzykiem w obszarze bezpieczeństwa informacji, w szczególności w zakresie identyfikacji ryzyka, analizy ryzyka i dokonywania oceny ryzyka oraz stosowanych zabezpieczeń.

3. W skład Zespołu ds. SZBI wchodzą:

1) Dyrektor Biura Informatyki i Ochrony, pełniący funkcję przewodniczącego Zespołu;
2) Zastępca Dyrektora Biura Informatyki i Ochrony, pełniący funkcję zastępcy przewodniczącego Zespołu;
3) Inspektor Ochrony Danych;
4) Pełnomocnik do spraw ochrony informacji niejawnych,
5) przedstawiciele następujących komórek organizacyjnych Urzędu, wskazani przez dyrektorów tych komórek:
   a) Biura Prezesa,
   b) Biura Kadr, Szkolenia i Organizacji,
   c) Biura Budżetu i Administracji,
   d) Departamentu Komunikacji,
   e) Departamentu Ochrony Konkurencji,
   f) Departamentu Monitorowania Pomocy Publicznej,
   g) Departamentu Inspekcji Handlowej,
   h) Departamentu Rozwoju Analiz,
   i) Departamentu Postępowań w Sprawach Zatorów Płatniczych.

4. Przewodniczący Zespołu ds. SZBI może występować do dyrektorów komórek organizacyjnych Urzędu w sprawie przedstawienia opinii lub udzielenia pomocy w realizacji zadań Zespołu.

5. Dyrektor Generalny Urzędu, po zasięgnięciu opinii Prezesa Urzędu, określa w drodze zarządzenia tryb pracy i harmonogram pracy Zespołu ds. SZBI.

§ 12. Dyrektor Biura Informatyki i Ochrony odpowiada za:

1) utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację;

2) koordynowanie przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
3) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami w szczególności przez:
   a) monitorowanie dostępu do informacji,
   b) podejmowanie czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
4) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
   a) dbałości o aktualizację oprogramowania,
   b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
   e) zapewnieniu bezpieczeństwa plików systemowych,
   f) redukcji ryzyka wynikającego z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
   g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
   h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
5) zapewnienie ciągłości działania procesów przetwarzania informacji;
6) zapewnienie możliwości sprawnego odtworzenia informacji w przypadku ich zniszczenia;
7) zapewnienie gotowości do reakcji na sytuację awaryjną lub kryzysową.

§ 13. Dyrektor Biura Kadr i Szkolenia zapewnia pracownikom Urzędu szkolenia w zakresie bezpieczeństwa informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
1) zagrożenia bezpieczeństwa informacji;
2) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna;

3) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i programowanie minimalizujące ryzyko błędów ludzkich;
4) analiza ryzyka utraty integralności, dostępności lub poufności informacji.

§ 14. Dyrektorzy komórek organizacyjnych Urzędu, w zakresie zadań realizowanych przez te komórki, odpowiadają za:

1) zapewnienie aktualizacji przepisów wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia, w szczególności zapewnienie, że zarządzenia określające zasady i procedury postępowania w sprawach należących do zakresu działania tych komórek uwzględniają zmiany w przepisach prawa powszechnie obowiązującego, nowe metody komunikacji oraz inne zmiany wynikające z informatyzacji działalności podmiotów realizujących zadania publiczne;
2) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy, we współpracy z Biurem Informatyki i Ochrony;
3) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
4) zapewnienie ciągłości działania procesów przetwarzania informacji;
5) realizację innych działań dotyczących bezpieczeństwa informacji, wynikających z regulaminu organizacyjnego Urzędu oraz przepisów wewnętrznych określających zasady i procedury dotyczące bezpieczeństwa informacji w Urzędzie oraz zasady i procedury bezpieczeństwa informatycznego, a także z umów cywilnoprawnych, porozumień i innych form współpracy Urzędu lub Prezesa Urzędu z innymi podmiotami.

§ 15. Zadania:

1) komórek organizacyjnych Urzędu zarządzających merytorycznymi funkcjami systemów informatycznych (gestorów systemów informatycznych) i pracowników tych komórek pełniących funkcje administratorów merytorycznych systemów informatycznych,
2) administratorów technicznych systemów informatycznych

– określa Dyrektor Generalny Urzędu w ramach zasad i procedur, o których mowa w § 6.

§ 16. 1. Inspektor Ochrony Danych w ramach Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie realizuje zadania w zakresie ochrony danych osobowych, na zasadach i zgodnie z przepisami dotyczącymi ochrony danych osobowych.

2. Inspektor Ochrony Danych opracowuje projekt zasad i procedur dotyczących postępowania w zakresie przetwarzania danych osobowych oraz środków technicznych i procedur zapewniających przetwarzanie danych osobowych zgodnie z prawem, monitoruje i analizuje oraz kontroluje przestrzeganie tych zasad i procedur, a także przygotowuje rekomendacje dotyczące zmian tych zasad i procedur.

§ 17. Pełnomocnik do spraw ochrony informacji niejawnych w ramach Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie realizuje zadania w zakresie ochrony informacji niejawnych za zasadach i zgodnie z przepisami dotyczącymi ochrony informacji niejawnych, w szczególności uczestniczy w pracach Zespołu ds. SZBI w celu zapewnienia kompatybilności zasad i procedur dotyczących bezpieczeństwa informacji z zasadami i procedurami dotyczącymi ochrony informacji niejawnych.

§ 18. 1. Dyrektor Generalny Urzędu wyda zarządzenia, o których mowa w § 6, w terminie 12 miesięcy od dnia wejścia w życie niniejszego zarządzenia.

2. Inspektor Ochrony Danych dokona przeglądu „Polityki Bezpieczeństwa Przetwarzania Danych Osobowych” i opracuje propozycje zmian niezbędnych dla zapewnienia zgodności z zasadami i procedurami określonymi w ramach Systemu Zarządzania Bezpieczeństwa Informacji, w terminie 12 miesięcy od dnia wejścia w życie niniejszego zarządzenia.

3. Dyrektor Biura Informatyki i Ochrony dokona przeglądu „Instrukcji Zarządzania Systemem Informatycznym” i opracuje propozycje zmian niezbędnych dla zapewnienia zgodności z zasadami i procedurami określonymi w ramach Systemu Zarządzania Bezpieczeństwa Informacji, w terminie 12 miesięcy od dnia wejścia w życie niniejszego zarządzenia.

§ 19. Traci moc zarządzenie nr 26/2018 Prezesa Urzędu Ochrony Konkurencji i Konsumentów z dnia 27 listopada 2018 r. w sprawie powołania Zespołu do spraw Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Ochrony Konkurencji i Konsumentów, zmienione zarządzeniem nr 12/2020 z dnia 26 czerwca 2020 r.

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

PREZES URZĘDU OCHRONY

KONKURENCJI I KONSUMENTÓW

Tomasz Chróstny