„Zeszyty Naukowe
Uczelni Jana Wyżykowskiego.
Studia z Nauk Technicznych"
2018 (7), s. 9–20. ISSN 2543-6740.

Zdzisław Pólkowski
Uczelnia Jana Wyżykowskiego

Wybrane aspekty wdrażania RODO

Streszczenie: Globalizacja i rozwój technologii informacyjnych i komunikacyjnych (ICT) spowodowały istotne zmiany w administracji publicznej i biznesie w Unii Europejskiej. Wprowadzone 25 maja 2018 r. ogólne rozporządzenie o ochronie danych (RODO) uwzględnia zachodzące zmiany, rozsądnie regulując aspekty przetwarzania i ochrony danych. RODO stosuje nowe podejście do oceny ryzyka. Celem niniejszego artykułu jest przedstawienie wybranych zagadnień związanych z wdrażaniem RODO. W pierwszej części artykułu przedstawiono podstawowe założenia RODO. W kolejnej zawarto analizę literatury i przepisów prawnych. Ostatnia część pracy koncentruje się na omówieniu wybranych rekomendacji dotyczących RODO. Opracowanie zawiera zalecenia, które wynikają z przeprowadzonych przez Autora działań związanych z wdrażeniem RODO i pełenieniem funkcji Inspektora Ochrony Danych Osobowych. Zawarte w pracy treści mogą być bezpośrednio wykorzystane zarówno przez osoby odpowiedzialne za ochronę danych, menadżerów, jak i informatyków. Ponadto opracowanie może być przydatne dla wykładowców i studentów podczas zajęć dydaktycznych na wielu kierunkach studiów.

Słowa kluczowe: RODO, ICT, przetwarzanie danych, bezpieczeństwo IT.

Selected aspects implementation of GDPR

Summary: Globalization and development of Information and Communication Technology (ICT) have caused significant changes in public administration and business in the European Union. The General Data Protection Regulation (GDPR), introduced on 25 May 2018, takes into account the implemented changes, reasonably regulating the aspects of data processing and protection. The GDPR applies a new approach to risk assessment. The purpose of this article is to present selected issues related to the implementation of the GDPR. The first part of the article presents the basic assumptions of the GDPR. The next contains an analysis of literature and legal provisions. The last part of the work focuses on discussing selected recommendations regarding the GDPR. The study contains recommendations that result from the activities carried out by the author related to the implementation of the GDPR and his experience as the Inspector of Personal Data Protection. The content contained in the work can be directly used by persons responsible for data protection, managers as well as IT specialists. In addition, the study may be useful for lecturers and students during didactic classes in many fields of study.

Keywords: GDPR, ICT, data processing, IT security.

1. Wprowadzenie

W ostatnim czasie kwestie związane z regulacjami prawnymi dotyczącymi ochrony danych w Polsce i Europie budzą wiele emocji. Postępująca i szybko rozprzestrzeniająca się digitalizacja zmusza ustawodawcę do dostosowania obowiązujących przepisów do aktualnej sytuacji i bieżących potrzeb. W rezultacie weszło w życie nowe rozporządzenie w sprawie ochrony danych osobowych osób fizycznych.

Zastąpiło ono obowiązującą ustawę o ochronie danych osobowych, wprowadzając w ten sposób nowe regulacje. Zostało przyjęte przez Parlament Europejski i Radę Unii Europejskiej w kwietniu 2016 r., a zawarte w nim przepisy są egzekwowane od 25 maja 2018 r. Dwuletni okres wdrażania, który był przewidziany, aby przygotować się na nadchodzące zmiany, został zakończony. Od tego momentu wszystkie firmy i instytucje działające w Unii Europejskiej są zobligowane do stosowania nowych wytycznych dotyczących przepływu i przetwarzania danych osobowych osób fizycznych. Nowe rozporządzenie dotyczy przetwarzania danych osobowych, a zatem ma ogromne znaczenie dla całego społeczeństwa. Każdy obywatel jest właścicielem swoich danych, takich jak: imię, nazwisko, wiek lub adres e-mail. Można stwierdzić, że **dane osobowe** to wszelkie informacje dotyczące **zidentyfikowanej lub możliwej do zidentyfikowania żyjącej osoby fizycznej**. Poszczególne informacje, które w połączeniu ze sobą mogą prowadzić do ustalenia tożsamości danej osoby także stanowią dane osobowe zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio określić, w szczególności na podstawie identyfikatora, takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników wskazujących fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej[1].

Dane osobowe są nieprzerwanie przetwarzane przez różnego rodzaju instytucje i firmy: począwszy od publicznych ośrodków zdrowia, a skończywszy na sieciach społecznościowych.

Przetwarzanie danych osobowych oznacza czynność, która obejmuje m.in.: zbieranie, ich utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie albo łączenie, ograniczanie, usuwanie lub niszczenie. Czynności te mogą być wykonywane w sposób zautomatyzowany lub niezautomatyzowany[2].

Wszystkie jednostki zajmujące się przetwarzaniem danych osobowych w zakresie przedstawionym powyżej są grupą, do której zostały skierowane nowe przepisy. Realizacja RODO i jego aktywne wykorzystanie daje uprzywilejowaną pozycję obywatelom, którym zostały przyznane nowe prawa. Podczas wprowadzania danych osobowych do

systemów informacyjnych i informatycznych będą otrzymywać one bardziej przejrzyste informacje od administratorów danych o celach, dla których dane będą wykorzystywane. Jest to jeden z nowych obowiązków nałożonych przez RODO na przedsiębiorstwa i instytucje.

Warto wspomnieć, że rosnąca popularność umów zawieranych drogą elektroniczną sprawiła, że podpisywanie papierowych wersji podczas fizycznego spotkania obu stron transakcji stało się „przestarzałe". Umowy te są często zawierane między obywatelami różnych krajów, w których przetwarzanie danych osobowych odbywa się na innej podstawie. RODO obowiązuje we wszystkich 28 krajach Unii Europejskiej, tym samym standaryzując obecnie obowiązujące przepisy dotyczące ochrony danych. Na decyzję Komisji Europejskiej o wdrożeniu RODO miały również wpływ przeprowadzone badania dotyczące ochrony danych osobowych, w których respondenci wyrazili zaniepokojenie bezpieczeństwem swoich danych osobowych.

Mimo znacznego zaangażowania i wysiłku ogólne rozporządzenie o ochronie danych z dnia 27 kwietnia 2016 r., tj. RODO, pozostawiło niedookreślonymi wiele istotnych z punktu widzenia pracodawców kwestii związanych z przetwarzaniem ich danych osobowych[3].

Zdaniem wielu ekspertów polskie firmy w kontekście nowych przepisów najczęściej narzekają na to, że:

- źle wdrożone RODO ogranicza możliwość działań marketingowych i sprzedażowych, a tym samym wzrost ich przychodów, proces wejścia produktów i usług na rynek znacznie się wydłuża, następuje nadużywanie praw, a w szczególności prawa do zapomnienia,
- niewielu jest odpowiednich kandydatów na Inspektorów Ochrony Danych w firmach, co powoduje problemy z ich zatrudnieniem,
- funkcjonują niejasne zasady zgłaszania naruszeń do Prezesa Urzędu Ochrony Danych Osobowych, co stwarza wyzwania w praktycznym stosowaniu tego obowiązku,
- nie maleje fala fałszywych kontroli – oszuści powołują się na Urząd Ochrony Danych Osobowych[4].

Wdrożenie RODO nie polega na jednorazowym działaniu związanym ze stworzeniem odpowiedniej papierowej dokumentacji. To stały i cykliczny monitoring procesów biznesowych występujących w firmie poprzez wykonywanie m.in. działań takich jak:

- prowadzenie analizy ryzyka,
- prowadzenie i aktualizacja rejestru czynności przetwarzania,
- stałe podnoszenie świadomości pracowników w zakresie ochrony danych osobowych poprzez ich systematyczne szkolenia,
- prowadzenie rejestru incydentów i zgłaszanie naruszeń do organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych),
- realizowanie praw osób, których dane dotyczą,

- dopuszczanie do przetwarzania danych wyłącznie osób posiadających nadane upoważnienia oraz okresowe weryfikowanie i aktualizowanie rejestru osób upoważnionych do przetwarzania danych osobowych,
- włączenie umów dotyczących powierzenia danych osobowych w obowiązującą w firmie procedurę zawierania umów z kontrahentami[5].

2. Przegląd literatury

Głównym dokumentem źródłowym jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz uchylające dyrektywę 95/46/WE (ogólne rozporządzenie o ochronie danych)[6]. Ponadto ważnym dokumentem jest Konstytucja Rzeczypospolitej Polskiej przyjęta przez Zgromadzenie Narodowe 2 kwietnia 1997 r., a także przez Naród w referendum konstytucyjnym z 25 maja 1997 r. podpisanym przez Prezydenta RP 16 lipca 1997 r. Ponadto ważnym dokumentem dla wdrażania RODO jest Ustawa z 10 maja 2018 r. o ochronie danych osobowych[7, 8].

Warto wspomnieć, że 25 maja 2018 r. uruchomiono nowy portal Urzędu Ochrony Danych Osobowych, który jest rzetelnym źródłem informacji[9]. Ostatnio opracowano wiele wartościowych publikacji dotyczących RODO, większość z nich to rozwiązania zaproponowane przez Urząd Ochrony Danych Osobowych (UODO) i firmy wdrożeniowe[10, 11, 12, 13, 14, 15, 16]. Niestety, nie znaleziono zbyt wielu opracowań naukowych, w tym posiadających wartości empiryczne.

Ponadto podczas wdrożeń RODO okazało się, że niektóre kwestie są niejasne, występują problemy z interpretacją określonych przepisów. W wielu przypadkach decyzje musiały być podejmowane przez inspektorów ochrony danych mimo braku wystarczających informacji. Powoduje to pewne obawy i stres. Głównym problemem w zakresie wdrożenia RODO jest brak zaleceń, które mogą być bezpośrednio stosowane w firmach i administracji publicznej. Niniejsza publikacja może być wykorzystana nie tylko w środowisku akademickim, ale również przez praktyków informatyki i inspektorów ochrony danych.

W pierwszej części artykułu przedstawiono podstawowe założenia RODO. W kolejnej części zawarto analizę literatury i przepisów prawnych. Ostatnia część pracy koncentruje się na zilustrowaniu wybranych rekomendacji dotyczących właściwej obsługi sprzętu informatycznego, świadczenia pomocy metodą zdalną oraz zasad przekazywania sprzętu komputerowego do serwisu. Opracowanie zawiera zalecenia, które wynikają z przeprowadzonych przez Autora działań związanych z wdrażeniem RODO i pełnienia funkcji Inspektora Ochrony Danych Osobowych w administracji publicznej oraz biznesie w 2017 i 2018 r.

3. Podstawy prawne

- Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
- Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. nr 101, poz. 926 – tekst jedn. ze zm.),
- Rozporządzenie z 29 kwietnia 2004 r. Ministra Spraw Wewnętrznych i Administracji (Dz.U. z 2004 r. nr 100, poz. 1024),
- Ustawa o ochronie danych osobowych z dnia 10 maja 2018 (Dz.U. z 2018 r. poz. 1000),
- przepisy sektorowe.

4. Metodologia

Opierając się na przeglądzie literatury, praktycznych doświadczeniach Autora i coraz bardziej widocznych tendencjach w obszarze ochrony danych osobowych, można stwierdzić, że liczba opracowań dotyczących RODO wciąż jest niewystarczająca.

Artykuł został przygotowany przede wszystkim z myślą o inspektorach ochrony danych osobowych, ponieważ prezentowany materiał może być zastosowany przez nich w codziennej pracy. Artykuł, o czym wspomniano wyżej, może być również wykorzystywany na uniwersytetach, zarówno przez profesorów, jak i studentów bardzo wielu kierunków, takich jak informatyka, prawo, zarządzanie itd.

Główny wysiłek Autora został skupiony na próbie znalezienia odpowiedzi na następujące pytania:

- Jakie zasady powinny być stosowane podczas świadczenia pomocy metodą zdalną?
- Jakie zasady powinny obowiązywać w zakresie dostępu i wykonywania prac w serwerowni?
- Jakie zasady właściwej obsługi systemu informatycznego powinny być stosowane zarówno w biznesie, jak i administracji publicznej?
- Jakie zasady należałoby uwzględnić podczas przekazania sprzętu komputerowego do serwisu?

5. Rezultaty

Administrator danych osobowych powinien zapewnić odpowiednie techniczne i organizacyjne środki ochrony danych.

Podmiot przetwarzający powinien zagwarantować:

- dostępność – dyspozycję do wykorzystania danych na żądanie, w założonym czasie, przez autoryzowany podmiot,

- poufność – informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
- integralność – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany,
- autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),
- niezaprzeczalność – uczestnictwo w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
- niezawodność – zamierzone zachowania i skutki są spójne.

W dalszej części opracowania zostały zawarte rekomendacje i zalecenia dotyczące właściwego świadczenia pomocy metodą zdalną, zasad dostępu i wykonywania prac w serwerowni, zasad obsługi sprzętu informatycznego oraz zasad przekazywania sprzętu komputerowego do serwisu.

5.1. Zasady świadczenia pomocy metodą zdalną

Pomoc zdalna pozwala na nawiązanie połączenia z komputerem klienta (pracownika) bez względu na odległość w celu usunięcia usterek technicznych. Po nawiązaniu połączenia pracownik firmy informatycznej (bądź zatrudniony informatyk) może za zgodą klienta rozwiązać niektóre problemy związane z oprogramowaniem komputerowym.

Systemy zdalnej pomocy z reguły korzystają z szyfrowania przez wymianę klucza prywatnego/publicznego RSA i 256-bitowego szyfrowania sesji AES. Ta technologia bazuje na tych samych standardach co protokoły https/SSL. Według obowiązujących standardów ta metoda jest uważana za całkowicie bezpieczną. Wymiana klucza gwarantuje ponadto pełną ochronę danych na całej trasie przesyłu danych. Oznacza to, że serwery trasujące nie są w stanie odczytać strumienia danych.

Oprócz identyfikatora klienta system zdalnej pomocy generuje hasło sesji zmieniane przy każdym uruchomieniu programu, które stanowi dodatkowe zabezpieczenie przed nieuprawnionym dostępem do systemu. Warto zauważyć, że nie może istnieć możliwość sterowania komputerem w sposób niewidoczny.

Regulamin zdalnej pomocy:

a) usługi serwisu zdalnego i konsultacji zdalnych mogą być świadczone przez firmę informatyczną (bądź zatrudnionego informatyka) na podstawie dostępnych i odpowiednio bezpiecznych systemów. Szczegółowe informacje o systemie znajdują się na stronie internetowej danego producenta, np. w przypadku systemu Teamviewer: http://www.teamviewer.com/pl/;
b) usługa zdalnej pomocy odbywa zgodnie z instrukcją zamieszczoną poniżej:
   - osoba prosząca o wsparcie informatyczne musi pobrać oprogramowanie klienta ze strony internetowej firmy informatycznej (bądź innego wskazanego, odpowiednio zabezpieczonego miejsca) po podaniu identyfikatora osoby zwracającej się o wsparcie,

- następnie należy zaakceptować regulamin,
- klient udostępnia swój komputer konsultantowi każdorazowo wyłącznie na podstawie klucza (numeru sesji) oraz hasła (generowanego automatycznie) otrzymanego uprzednio od klienta telefonicznie bądź za pomocą poczty elektronicznej. Hasło jest ważne tylko na czas trwania czynności serwisowych;

c) usługa nawiązywana połączenia z klientem w każdej chwili może zostać przez niego zakończona;
d) wymiana danych pomiędzy komputerem klienta i konsultanta powinna być zabezpieczona szyfrowaniem bazującym na wymianie kluczy publicznych i prywatnych RSA oraz szyfrowaniu sesji 256-bitowym kodem AES;
e) klient zobowiązany jest przed podjęciem czynności przez konsultanta określić wyczerpująco problem, jaki należy rozwiązać;
f) usługa może być wykonywana po uprzednim telefonicznym określeniu terminu połączenia przez klienta;
g) w czasie trwania czynności klient decyduje o wszystkich akcjach, jakie może podjąć osoba udzielająca wsparcia. Ponadto nadzoruje proces świadczenia usługi zdalnej poprzez obserwację działań widocznych na ekranie monitora;
h) konsultant jest zobowiązany do zachowania w całkowitej tajemnicy informacji o zawartości dysku twardego obsługiwanego komputera klienta oraz do niezmieniania zawartości plików stanowiących dokumenty, zbiory multimedialne, zbiory fotograficzne, dane itd.;
i) zainstalowane oprogramowanie może być być używane podczas następnych sesji;
j) sesja zdalnej pomocy może zostać nagrana w celu udokumentowania przeprowadzonych czynności;
k) reklamacja przeprowadzonych prac może zostać zgłoszona w okresie 14 dni od daty wykonania. Po tym też czasie powinny zostać usunięte ewentualne nagrania wykonanych prac;
l) firma informatyczna (bądź zatrudniony informatyk) ponosi całkowitą odpowiedzialność z tytułu czynności dokonanych przez konsultanta.

5.2. Zasady dostępu i wykonywania prac w serwerowni

Pod pojęciem serwerowni rozumie się wydzielone pomieszczenie, będące środowiskiem pracy komputerów pełniących rolę serwerów, a także aktywnych i pasywnych elementów sieci komputerowych. Urządzenia są najczęściej umieszczane w szafach stelażowych (rackowych) wewnątrz serwerowni[17].

Obowiązują następujące zasady:

a) w serwerowni (pomieszczeniu, w którym znajduje się serwer) mogą przebywać tylko uprawnione osoby;
b) serwerownia musi być każdorazowo zamykana na klucz;

c) klucz do serwerowni musi znajdować się u osoby uprawnionej w odpowiednio zabezpieczonym miejscu o ograniczonym dostępie, takim jak kaseta zamykana na klucz lub sejf z szyfratorem;
d) w serwerze mogą być wykonywane tylko prace związane z działalnością podmiotu przetwarzającego i wyłącznie przez upoważnione osoby;
e) w przypadku posiadania szafy serwerowej dostęp kluczy do niej także musi być ograniczony;
f) zaleca się użytkowanie klimatyzacji, która powinna być poddawana okresowym przeglądom;
g) bardzo wysoki poziom bezpieczeństwa należy zachować w przypadku konieczności wykonywania czynności serwisowych metodą zdalną.

5.3. Zasady właściwej obsługi systemu informatycznego

Obowiązują następujące zasady:

a) za bezpieczeństwo przetwarzania danych osobowych w określonym procesie przetwarzania indywidualną odpowiedzialność ponosi każdy pracownik mający dostęp i upoważnienie do przetwrzania danych osobowych;
b) nie wolno prosić osoby, której dane dotyczą o podanie danych osobowych, które wykraczają poza zakres niezbędny do wykonania zamierzonego celu;
c) zabrania się wykorzystywania danych osobowych w celach innych niż te, do których zostały zebrane i na które osoba zainteresowana wyraziła zgodę;
d) osobę, której dane dotyczą, należy informować o jej prawach i obowiązkach w sposób jasny i zrozumiały, dotyczy to również kwestii zgód;
e) nie należy utrudniać osobie, której dane dotyczą, realizacji jej praw wynikających z RODO;
f) pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem związanym z zakresem obowiązków służbowych w ramach udzielonego upoważnienia do przetwarzania danych;
g) pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym;
h) dane osobowe w formie papierowej muszą być przechowywane w szafach zamykanych na klucz. Klucze należy przechowywać w sposób bezpieczny bez możliwości dostępu do nich osób nieuprawnionych – zawsze przy opuszczaniu stanowiska pracy (nawet na chwilę) należy pamiętać o zabezpieczeniu dokumentów oraz komputera;
i) zawsze istnieje ryzyko, że osoby niepowołane/trzecie mogą podsłuchać rozmowę, w której podawane są dane osobowe, dlatego zawsze należy być ostrożnym i świadomym otoczenia, gdy omawiane są sprawy poufne;

j) upoważnienie dostępu do danych osobowych musi być wydane na piśmie. Osoba, której dane dotyczą, wypisując upoważnienie, musi wskazać z imienia i nazwiska oraz podać nr dokumentu potwierdzającego tożsamość osoby, której dane mogą być udostępnione. Nie wolno przekazywać danych w żadnej formie (elektronicznej, papierowej) osobom trzecim, które nie są uprawnione do dostępu do nich;
k) ze względu na fakt, iż nigdy nie mamy pewności co do tożsamości osoby, z którą rozmawiamy przez telefon, nie wolno udzielać informacji, w których podawane są dane osobowe w formie zapytania telefonicznego;
l) wszystkie zbędne dane w formie kopii, powstałe w procesie przetwarzania muszą zostać niezwłocznie zniszczone w sposób uniemożliwiający ich odczytanie;
m) przy przetwarzaniu danych osobowych podczas kontaktu z klientami na biurku mogą znajdować się dokumenty z danymi osobowymi wyłącznie osoby, z którą w danym momencie załatwiamy formalności;
n) nie wolno pozostawiać bez kontroli dokumentów z danymi osobowymi. Zawsze przy opuszczaniu stanowiska pracy (nawet na chwilę) dokumenty należy schować do szafki i zamknąć na klucz (zabrać klucz), uniemożliwiając w ten sposób dostęp do danych osobom trzecim; komputer należy zablokować (klawisze windows + L);
o) pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu w godzinach pracy, jak i po jej zakończeniu; klucze nie mogą być pozostawione w zamku;
p) przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem;
q) ujawnianie przez użytkownika osobie trzeciej haseł tymczasowych, haseł osobistych lub innych powierzonych mu haseł jest zabronione;
r) zabrania się wynoszenia dokumentów, zarówno w formie papierowej, jak i elektronicznej, zawierających dane osobowe poza miejsce pracy lub jeśli to konieczne, należy uzyskać na to zgodę przełożonego;
s) po zakończeniu pracy należy uporządkować biurko i zamknąć w szafach na klucz pod) ufne dokumenty (klucz zabrać) oraz sprawdzić, czy w portach USB lub napędzie DVD nie pozostały nośniki z danymi.

Zasady korzystania ze służbowej poczty elektronicznej (e-mail):

a) zabrania się przesyłania przez pracownika dokumentów firmowych na swoje prywatne adresy e-mailowe;
b) niezaszyfrowana poczta elektroniczna może służyć wyłącznie do przesyłania dokumentów, które nie zawierają danych osobowych, danych wrażliwych czy poufnych;

c) nie wolno przesyłać niezaszyfrowaną pocztą elektroniczną żadnych danych osobowych klientów oraz pracowników, informacji o wysokości wynagrodzenia itp.;
d) nie wolno prosić o przesłanie danych osobowych lub innych danych wrażliwych e-mailem, należy poprosić ewentualnie o dostarczenie danych bez określenia sposobu – jeżeli osoba, której dane dotyczą, wyśle je e-mailem, robi to na własną odpowiedzialność (my jej o to nie prosiliśmy);
e) nigdy nie należy otwierać załączników ani klikać na linki przesłane pocztą elektroniczną od nieznanych nadawców lub w wiadomościach, których się nie spodziewamy.

5.4. Zasady korzystania ze służbowego komputera:

a) obowiązkiem pracownika jest korzystanie ze służbowego komputera oraz oprogramowania wyłącznie w celach wykonywania obowiązków pracowniczych;
b) nie wolno podłączać do portów USB lub wkładać do napędów DVD nośników zewnętrznych prywatnych lub pochodzących z nieznanego źródła; nośniki te mogą zawierać wirusy komputerowe, które stwarzają zagrożenie dla bezpieczeństwa komputera, sieci firmowej, i co się z tym wiąże – również przetwarzanych w firmie danych osobowych;
c) w przypadku zaistnienia konieczności podłączenia ww. urządzenia należy skontaktować się z administratorem sieci komputerowej w celu uprzedniego przeskanowania sprzętu pod kątem obecności złośliwego oprogramowania;
d) podczas użytkowania komputera zabrania się wchodzenia na strony internetowe, które mogą stwarzać zagrożenie dla systemu informatycznego i bezpieczeństwa danych (nie serfuj po internetowych stronach o niewłaściwej treści, nie ściągaj stamtąd żadnych plików);
e) monitor komputera należy usytuować w taki sposób, aby osoby nieupoważnione wchodzące do pomieszczenia nie miały wglądu do danych na nim wyświetlanych.

Naruszenie któregoś z powyższych punktów może doprowadzić do wycieku danych, co z kolei wiąże się z bardzo poważnymi konsekwencjami prawnymi, z odpowiedzialnością finansową i karną włącznie.

Zasady przekazania sprzętu komputerowego do serwisu:

a) w przypadku awarii sprzętu komputerowego, na którym znajdują się dane osobowe należy postępować zgodnie z procedurami zapewniającymi bezpieczeństwo informatyczne i informacyjne;
b) przed rozpoczęciem czynności serwisowych należy sprawdzić, czy urządzenie jest na gwarancji. W przypadku obowiązywania gwarancji trzeba zweryfikować, czy na komputerze znajdują się dane osobowe. W sytuacji stwierdzenia braku danych w uszkodzonym sprzęcie można zgłosić reklamację i przekazać urządzenie do gwaranta. Jeśli

w uszkodzonym sprzęcie komputerowym znajdują się dane osobowe, wówczas nośnik z danymi należy wymontować i skopiować dane na inny – nawet jeżeli wiąże się to z utratą gwarancji na dane urządzenie. Po skopiowaniu plików konieczne jest sformatowanie na niskim poziomie nośnika danych przed przekazaniem sprzętu do gwaranta;

c) zaleca się formatowanie na niskim poziomie (ang. *low level format* – LLF);
d) zabezpieczeniem danych powinien zająć się specjalista ds. informatycznych zatrudniony w firmie bądź zewnętrzna firma informatyczna obsługująca system informatyczny. Ponadto zaistniałą sytuację należy zgłosić do inspektora ochrony danych osobowych;
e) w przypadku gdy sprzęt nie jest objęty okresem gwarancyjnym, naprawą komputera zajmuje się specjalista ds. informatycznych zatrudniony w firmie. Jeśli naprawa wymaga oddania komputera do firmy zewnętrznej obsługującej system informatyczny, wówczas warunkiem koniecznym jest posiadanie podpisanej z tą firmą umowy powierzenia danych. W takim przypadku uprawniony pracownik firmy informatycznej może zabrać sprzęt do siedziby firmy w celu usunięcia awarii. Ważne jest, aby zachować szczególne zasady ochrony danych;
f) każdy przypadek wyniesienia sprzętu zawierającego dane osobowe poza miejsce jego użytkowania musi być niezwłocznie zgłoszony do inspektora ochrony danych.

6. Wnioski

Celem artykułu było zaprezentowanie wybranych zaleceń i rekomendacji dotyczących RODO. Wybór analizowanych obszarów i zagadnień był podyktowany bieżącymi potrzebami, które pojawiły się podczas wdrożeń RODO. Niniejsze opracowanie posiada znaczną wartość praktyczną, ponieważ zaprezentowany materiał zawiera zestaw zasad i regulaminów, które mogą być bezpośrednio wykorzystane przez inspektorów ochrony danych osobowych.

Warto wspomnieć, że przeprowadzone audyty wewnętrze wykazały kilka słabych punktów w systemie ochrony danych osobowych. Natychmiast podjęto decyzję o ich wyeliminowaniu. Zbiór wspomnianych rekomendacji jest wynikiem audytu, którego przeprowadzenie w znacznym stopniu może może wyeliminować słabe punkty w systemie ochrony danych. Istotny wydaje się również fakt, iż zastosowanie rekomendacji nie wiąże się z dużymi nakładami finansowymi.

Na podstawie wdrożonych rozwiązań można stwierdzić, że dalsze badania i analizy mogą być ukierunkowane zarówno na aspekty etyczne, jak i organizacyjne związane z ochroną danych. Rozsądnym podejściem byłoby zaprojektowanie, opracowanie i późniejsza implementacja użytecznych narzędzi informatycznych (systemów eksperckich lub systemów DSS), które z kolei mogłyby wspierać wdrażanie procesu RODO.

Literatura

[1] Komisja Europejska, *Czym są dane osobowe?*, europa.eu, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pl.

[2] biznes.gov.pl, *RODO – przetwarzanie danych osobowych – poradnik,* biznes.gov.pl, //www.biznes.gov.pl/pl/firma/obowiazki-przedsiebiorcy/chce-chronic-dane-osobowe/guide_205-PRZETWARZANIE_DANYCH_OSOBOWYCH_RODO.

[3] Rączkowiak K., *RODO – co nowego dla pracodawców przyniesie 2019 rok*, Grant Thornton, https://grantthornton.pl/publikacja/rodo-co-nowego-dla-pracodawcow-przyniesie-2019-rok/.

[4] Forbes, *RODO przerosło polskie firmy. Połowa miała problem z wdrożeniem*, „Forbes", https://www.forbes.pl/prawo-i-podatki/polowa-polskich-firm-ma-problem-z-wdrozeniem-rodo-analiza-pwc/q8w38jv.

[5] Stępniewska A., *Dlaczego wciąż boimy się RODO, czyli pierwsze doświadczenia i najczęstsze pomyłki,* politykabezpieczenstwa.pl, https://www.politykabezpieczenstwa.pl/pl/a/dlaczego-wciaz-boimy-sie-rodo-czyli-pierwsze-doswiadczenia-i-najczestsze-pomylki.

[6] GIODO, https://giodo.gov.pl/, stan z dnia z dnia 18.04.2018.

[7] UODO, https://uodo.gov.pl/, stan z dnia z dnia 12.05.2018.

[8] Microsoft, *Jak RODO wpłynie na twoją firmę?,* https://www.microsoft.com/pl-pl/rethink-IT-security/GDPR/default.aspx?&qsg_sem_219240&WT.srch=1&WT.mc_id=AID657619_SEM_dgCiTV92, stan z dnia 14.05.2018.

[9] *Rejestracja i bezpieczeństwo danych osobowych,* https://rbdo.pl/wdrozenie-ue-rodo/?utm_source=b2bhello&utm_medium=b2b-ad-512&utm_campaign=b2b-ad-512&gclid=EAIaIQobChMIuPuGqO_I2wIVAomyChoi_AsNEAAYAiAAEgItyfD_BwE, stan z dnia 18.04.2018.

[10] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, http://www.dziennikustaw.gov.pl/DU/2018/1000, stan z dnia 21.05.2018.

[11] Kaczmarski M., *Aby realnie wdrożyć RODO potrzebna jest sprawdzona metodyka,* 7.04.2018, https://odo24.pl/blog-post.zegar-rodo-tyka-potrzebna-jest-sprawdzona-metodyka, stan z dnia 18.01.2018.

[12] Litwiński P., *Przewpodnik po RODO dla małych i średnich przedsiębiorców,* https://www.mpit.gov.pl/media/50521/PrzewodnikMSP_RODO_2018.pdf, stan z dnia 28.04.2018.

[13] IBM, *GDPR signals big data protection changes worldwide,* https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGB03053USEN&, stan z dnia 18.01.2018.

[14] ICO, *Preparing for the General Data Protection Regulation (GDPR),* https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf, stan z dnia 11.04.2018.

[15] Jasmontaite L., Kamara I., Leucci S., Zanfir-Fortuna G., *Implementation of Data Protection by Design and by Default: Framing guiding principles into applicable rules*, https://edps.europa.eu/sites/edp/files/publication/17-06-09_lina_jasmontaite_stefano_leucci_dpbddpbdf_ipen_en.pdf, stan z dnia 18.04.2018.

[16] Jasmontaite L., Kamara I., Leucci S., Zanfir-Fortuna G., *Implementation of Data Protection by Design and by Default: Framing guiding principles into applicable rules,* https://edps.europa.eu/sites/edp/files/publication/17-06-09_lina_jasmontaite_stefano_leucci_dpbddpbdf_ipen_en.pdf, stan z dnia 18.04.2018.

[17] http://sicd.pl/teoria/serwerownia/.