Polityka bezpieczeństwa ochrony i przetwarzania danych osobowych wraz z instrukcją zarządzania systemem informatycznym w firmie

KIKGEL Sp. z o.o.
ul. Skłodowskiej 7, 97-225 Ujazd

wydana w dniu 08.02.2017r

Podstawa prawna:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 1997, Nr 133, poz. 883 z późn. zm.).

2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004, Nr 100,poz. 1024).

§ 1

Tworzy się Politykę bezpieczeństwa ochrony danych osobowych celem zabezpieczania w sposób fizyczny dostępu do informacji będących w posiadaniu pracowników KIKGEL Sp. z o.o. oraz polegających na zwiększeniu świadomości pracowników o wartości posiadanych i przetwarzanych danych osobowych.

Przetwarzanie danych osobowych w firmie KIKGEL Sp. z o.o. odbywa się za pomocą systemów informatycznych.

Administratorem Danych Osobowych (ADO) jest Kierownik Zaopatrzenia i Zbytu.

§ 2

Wykaz pomieszczeń w firmie KIKGEL Sp. z o.o., w których przetwarza się dane osobowe

W budynku firmy KIKGEL Sp. z o.o. mieszczącego się przy ul. Skłodowskiej 7, 97-225 Ujazd znajdują się następujące pomieszczenia w których przetwarza się dane osobowe pracowników oraz kontrahentów firmy oraz sklepu internetowego na stronie www.kikgel.com.pl:

1. Biuro znajdujące się na I piętrze budynku,
2. Pokój biurowy znajdujący się w budynku mieszkalnym Prezesa zarządu na terenie firmy przy ul. Skłodowskiej 7, 97-225 Ujazd.

Pomieszczenia, w których przetwarzane są dane osobowe chronione są systemem alarmowym. Dostęp do stref przetwarzania danych osobowych mają jedynie upoważnieni pracownicy oraz ADO. System jest wyłączany przez ostatniego pracownika opuszczającego pomieszczenie, w którym przetwarzane są dane osobowe.

Zabrania się przebywania osób postronnych w pomieszczeniach, w których przetwarzane są dane osobowe bez obecności osób upoważnionych.

§ 3

Wykaz zbiorów danych osobowych oraz programów komputerowych stosowanych do przetwarzania tych danych w firmie KIKGEL Sp. z o.o. oraz opis struktury zbioru i zawartości

W firmie KIKGEL Sp. z o.o. znajdują się następujące zbiory danych przetwarzane przez pracowników biurowych:
Zbiór nr 1 – Akta osobowe pracowników w wersji papierowej.
Zbiór nr 2 - Akta osobowe pracowników – rejestr elektroniczny.
Zbiór nr 3 – Baza danych kontrahentów firmy oraz sklepu internetowego kikgel.com.pl – rejestr elektroniczny.
Poszczególne stanowiska pracowników biurowych są wyposażone w programy komputerowe służące do przetwarzania danych osobowych firmy Comarch. Każdy z komputerów zabezpieczony jest hasłem dostępu, składającym się z co najmniej pięciu znaków, w skład których wchodzą zarówno litery jak i cyfry

1) Stanowisko kadrowo-płacowe przetwarza dane osobowe wykorzystując program „Optima – Kadry i Płace”. Program ten zawiera wszystkie dane osobowe pracowników firmy KIKGEL

Sp. z o.o. Stanowią one odzwierciedlenie pracowniczych akt osobowych prowadzone w formie papierowej. Zawierają one:
- Wszystkie dane personalne pracowników
- Wszelkie dane kadrowe wynikające ze stosunku pracy
- Wszelkie dane dotyczące wynagrodzeń za płacę pracowników oraz wypłat z tytułu umów cywilnoprawnych

Na tym stanowisku wykorzystuje się dodatkowo program „Płatnik", w którym dokonuje się przetwarzania danych dotyczących składek pracowniczych przekazywanych do ZUS.

2) Stanowisko Handlowca wyposażone jest w program „Optima Handel", który zawiera następujące bazy danych:
- Baza danych kontrahentów
- Baza rejestrów księgowych

3) Stanowisko pracownika od Gospodarki magazynowej wyposażone jest w program „Optima Handel", który przetwarza wszelkie dane dotyczące magazynów firmy KIKGEL Sp. z o.o.

4) Stanowisko Kierownika Zaopatrzenia i Zbytu wyposażone jest w programy „Optima – Kadry i Płace" oraz „Optima Handel", które przetwarzają wszystkie dane dotyczące pracowników oraz kontrahentów firmy KIKGEL Sp. z o.o.

5) Stanowisko Prezesa zarządu wyposażone jest w programy „Optima – Kadry i Płace", który przetwarza wszystkie dane dotyczące pracowników.

§ 4

Sposób przepływu danych pomiędzy poszczególnymi systemami

1) W firmie KIKGEL Sp. z o.o. we wszystkich programach komputerowych przepływ informacji pomiędzy zbiorem danych a systemem informatycznym jest dwukierunkowy (do odczytu i do zapisu).

2) Następuje przesyłanie danych za pomocą teletransmisji przy wykorzystaniu funkcji eksport/import danych w obrębie następujących programów:
Optima Kadry i Płace → Płatnik

Firma KIKGEL Sp. z o.o. posiada połączenie sieciowe pomiędzy komputerami znajdującymi się w firmie.
Wszelkie informacje, jakie są pozyskiwane bądź tworzone przez poszczególnych pracowników biurowych są udostępniane w sposób pisemny bądź w sposób ustny na wyraźne polecenie Kierownika Zaopatrzenia i Zbytu, bądź na prośbę osób zainteresowanych za wyraźną zgodą Kierownika Zaopatrzenia i Zbytu zgodnie z zasadami uregulowanymi Ustawą o ochronie danych osobowych Dz. U. 1997, Nr 133 poz. 883 tekst jednolity).

§ 5

Środki techniczne i organizacyjne niezbędnych dla zapewnienia poufności, bezpieczeństwa, integralności i rozliczalności przetwarzanych danych

Wszystkie komputery zawierające zbiory danych w firmie KIKGEL Sp. z o.o. zaopatrzone są w indywidualne licencjonowane programy do przetwarzania danych oraz programy

antywirusowe, które gwarantują bezpieczeństwo danych znajdujące się na dyskach twardych komputerów przed dostępem do nich osób nieupoważnionych.
Kopie danych zawartych w systemie tworzy się każdorazowo po zakończeniu dnia pracy. przechowywana jest na zdalnym serwerze, do którego dostęp ma wyłącznie ADO. Każda następna kopia zapisywana jest w miejsce poprzedniej. Celem takiego działania jest zabezpieczenie baz danych przed zniszczeniem, skopiowaniem i przekazem ich do wiadomości osób nieupoważnionych.
Bazy danych znajdujące się w biurze firmy tj: dane personalne znajdujące się w teczkach osobowych pracowników umieszczone są w szafie zamykanej na klucz, który znajduje się w posiadaniu ADO. Pliki zawierające dane osobowe (np. skany wyników badań) nie mogą być przechowywane na wymienialnych nośnikach tj. płyty cd, pendrive, dyski zewnętrzne.

Dostęp do danych osobowych „na papierze" oraz w rejestrze elektronicznym firmy ma ADO oraz pracownicy biurowi.
Pracownicy ci w sposób pisemny obowiązani są do zachowania tajemnicy i ochrony danych osobowych.
Użytkownicy systemu są odpowiedzialni za nieudostępnianie stanowisk pracy osobom postronnym.

Dane osobowe przetwarzane zgodnie z art. 27 ust. 2 pkt 7 ustawy mogą być wydane jedynie na pisemny wniosek osoby, której dotyczą lub pisemny wniosek osoby upoważnionej na piśmie przez zainteresowanego. W firmie KIKGEL Sp. z o.o. każdorazowe przekazywanie danych personalnych i ich przetwarzanie podlega kontroli przez ADO w ten sposób dane zastrzeżone czy dane poufne nie mogą trafić do odbiorcy nieupoważnionego.

§ 6

Procedura postępowania w sytuacji naruszenia polityki bezpieczeństwa

Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczenia danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym ADO lub inną upoważnioną osobę.

ADO (lub upoważniona osoba) po otrzymaniu powiadomienia:

- sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,

- sprawdza sposób działania programów (w tym obecność wirusów komputerowych),

- sprawdza jakość komunikacji w sieci telekomunikacyjnej,

- sprawdza zawartość zbioru danych osobowych,

- poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.

W przypadku stwierdzenia naruszenia zabezpieczeń danych administrator:
- podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych itp.),

- w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej podejmuje odpowiednie kroki poprzez: fizyczne odłączenie urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do bazy danych osoby nieupoważnionej, wylogowanie użytkownika podejrzewanego o naruszenie zabezpieczenia ochrony danych, zmianę hasła na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,

- zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,

- niezwłocznie przywraca prawidłowy stan działania systemu,

- dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,

- sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.

ADO podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:
- jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,

- jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza się dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje do administratora danych osobowych o wyciągnięcie konsekwencji przewidzianych prawem,

- jeżeli przyczyną zdarzenia jest sprzeczny z prawem czyn lub zachodzi takie podejrzenie, zawiadamia organy ścigania.