POLITYKA BEZPIECZEŃSTWA
w zakresie ochrony danych osobowych
P.Z. Catzy of Poland Jan Blom

1. Polityka bezpieczeństwa przetwarzania danych osobowych w P.Z. Catzy of Poland Jan Blom, zwana dalej „Polityką”, została opracowana zgodnie z wymogami S 4 rozporządzenia 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. Nr 100,poz. 1024).

2. Polityka ma zastosowanie wobec wszystkich jednostek organizacyjnych.

3. Celem Polityki jest ochrona przetwarzanych danych osobowych przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.

4. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów.

5. Polityka dotyczy wszystkich danych osobowych, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.

Definicje

Użyte w Polityce określenia i skróty oznaczają:
Ustawa – przez to określenie należy rozumieć Ustawę z dnia 29.08.1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.),

Rozporządzenie – rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 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. Nr 100, poz. 1024),

Administrator Danych Osobowych – P.Z. Catzy of Poland Jan Blom, zwana dalej Administratorem

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba możliwa do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiające określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działania.

Dane wrażliwe — szczególna kategoria danych osobowych, których przetwarzanie jest zabronione za wyjątkiem przypadków ściśle określonych Ustawą. Ustawodawca zaliczył do tej kategorii dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniowa, partyjna lub związkowa, jak równie dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatach karnych, a także innych orzeczeń wydanych w postępowaniu sadowym lub administracyjnym.

Zbiór danych osobowych – to każdy posiadający strukturę zestaw danych osobowych, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Przetwarzanie danych osobowych – to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Upoważnienie - to dokument sporządzony na papierze, na podstawie którego Administrator dopuszcza osoby do przetwarzania danych osobowych.

Osoba upoważniona — zwana dalej użytkownikiem — osoba posiadająca upoważnienie nadane przez Administratora lub osobę przez niego wskazana, uprawnioną do przetwarzania danych osobowych w zakresie przewidzianym w upoważnieniu.

Zasady bezpiecznego przetwarzania danych osobowych

Dane osobowe w P.Z. Catzy of Poland Jan Blom są przetwarzane w celu realizacji zadań określonych przepisami prawa.

1. Cel, o którym mowa w ust. 1, należy osiągać przez zachowanie szczególnej staranności w realizacji przedsięwzięć dotyczących ochrony interesów osób, których dane dotyczą oraz przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych, uwzględniając:

a. przepisy prawa,
b. zasady udostępniania danych osobowych,
c. zachowanie obowiązku informacyjnego,
d. procedury ochrony danych osobowych,
e. dotrzymanie okresu przechowywania danych identyfikujących osobę.

2. Celem przetwarzania przez firmę danych osobowych pracowników jest w szczególności:

a. zidentyfikowanie tożsamości,
b. uzyskanie miejsca zameldowania i adresu, na który można kierować korespondencje,
c. uzyskanie informacji charakteryzujących pracownika od strony przydatności zawodowej, takich jak: wykształcenie, kursy, przebieg pracy zawodowej (doświadczenie zawodowe),
d. realizacja szczególnych uprawnień przewidzianych w prawie pracy i wewnętrznych regulaminach Spółki, w tym celu przetwarzane są także, pozyskane od pracownika na mocy art. 221 Kodeksu Pracy, dane osobowe osób bliskich pracownika.

3. Dane osobowe pracowników pozostają w dyspozycji i na użytek jedynie Administratora Danych, którym jest pracodawca, a w jego imieniu osób mających na podstawie przepisów wewnętrznych oraz niniejszego Zarządzenia, prawo dostępu do danych osobowych pracownika firmy oraz osób bliskich.
4. Przetwarzanie danych osobowych pracowników, jest dopuszczalne jedynie w zakresie niezbędnym do wypełniania jego usprawiedliwionych celów związanych z zatrudnieniem, ale nie może ono naruszać praw i wolności osoby, której dane dotyczą.
5. Zakres informacji, niezbędnych pracodawcy do nawiązania z pracownikiem stosunku pracy, określa rozporządzenie MPiPS z dnia 28.05.1996 r., w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. z 1996 r. nr 62 poz.286) a także art. 221 Kodeksu Pracy.
6. Przetwarzanie przez pracodawcę innych danych osobowych pracowników jest zabronione. W szczególności zabronione jest przetwarzanie danych wrażliwych za wyjątkiem wystąpienia przesłanek z art. 27 ust 2. ustawy.
7. Przetwarzanie pozyskanych od pracownika na mocy art. 221 Kodeksu Pracy, danych osobowych osób bliskich pracownika jest dopuszczalne wyłącznie w ramach Prawa Pracy.

8. Podstawową zasadą przetwarzania danych osobowych w P.Z. Catzy of Poland jest zachowanie w tajemnicy wszelkich informacji dotyczących przetwarzania oraz sposobów zabezpieczania danych przez osoby mające do nich dostęp.
9. Możliwość wystąpienia zagrożeń danych przetwarzanych w systemach lub kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych nakłada na użytkowników i ich przełożonych obowiązek wykonywania czynności kontrolnych.
10. Kopiowanie danych osobowych oraz wykonywanie wydruków jest zabronione, chyba że konieczność ich sporządzania wnika z nałożonych na użytkownika obowiązków (np. kopie bezpieczeństwa) i dozwolona jest przepisami prawa.
11. Kopie zawierające dane osobowe można przekazywać wyłącznie osobom upoważnionym lub podmiotom do tego uprawnionym z zachowaniem zapisu art. 36 Ustawy.
12. Kopie, o których mowa w ust. 7, mogą być wykorzystywane tylko w celach do jakich zostały sporządzone. Niepotrzebne kopie należy niszczyć w sposób uniemożliwiający ich odtworzenie, zgodnie z obowiązującymi przepisami.
13. Przetwarzanie danych osobowych może być wykonywane wyłącznie przez osoby
14. Przełożeni użytkowników w miarę możliwości technicznych i organizacyjnych są zobowiązani nie dopuszczać do wchodzenia osób nieupoważnionych do pomieszczeń w których są przetwarzane i przechowywane zbiory danych osobowych po zakończeniu pracy w tych pomieszczeniach (w szczególności dotyczy to personelu sprzątającego). Wszędzie, gdzie jest to możliwe organizacyjnie, należy organizować prace personelu sprzątającego w wymienionych pomieszczeniach w ciągu dnia pracy pod nadzorem upoważnionego pracownika. Jeżeli nie jest możliwe zorganizowania sprzątania wymienionych pomieszczeń w ciągu dnia pracy, wszystkie dane osobowe w formie papierowej lub te na przenośnych elektronicznych nośnikach danych bezwzględnie należy przechowywać w zamykanych na zamek wielozapadkowy w szafach, sejfach i innych urządzeniach zapewniających, że dane nie będą bezprawnie ujawnione. Procedurę zabezpieczania klucza od tych urządzeń określa przełożony użytkowników. Dostęp do systemu informatycznego na wszystkich jednostkach komputerów w tych pomieszczeniach musi zawierać procedurę logowania za pomocą niepowtarzalnego identyfikatora i hasła.

Szkolenia w zakresie ochrony danych osobowych

1. Każda osoba przed rozpoczęciem przetwarzania danych osobowych ma obowiązek zapoznania się z przepisami dotyczącymi bezpieczeństwa przetwarzania i ochrony danych osobowych.

2. Przełożony zobowiązany jest umożliwiać użytkownikom zapoznanie się z przepisami dotyczącymi ochrony danych osobowych a w szczególności z Ustawą, Rozporządzeniem i aktami wewnętrznego zarządzania dotyczącymi tej problematyki w tym z niniejszą Polityką Bezpieczeństwa.

Obowiązki osób upoważnionych przez Administratora

1. Administrator wykonuje zadania z zakresu przetwarzania i ochrony danych zgodnie z przepisami prawa.
2. Do obowiązków użytkowników należy:
    a. przetwarzanie danych osobowych, w tym z użyciem systemu informatycznego, wyłącznie w sposób zgodny z zakresem upoważnienia,
    b. zachowanie bezpieczeństwa danych osobowych, w tym przetwarzanych w systemie informatycznym oraz bezpieczne przechowywanie zbiorów niestanowiących systemu informatycznego, nośników danych i wydruków komputerowych,
    c. przestrzeganie procedury określającej sposób postępowania w sytuacji naruszenia,
    d. dopilnowanie, aby przed oddaniem sprzętu informatycznego do naprawy serwisowej zostały usunięte dane osobowe zapisane na nośnikach w komputerze lub uzyskane zostało zezwolenie Administratora na ich pozostawienie, zgodnie z zasadami określonymi w Polityce Bezpieczeństwa,
    e. dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnienie, aby dane te były:
        i. przetwarzane zgodnie z prawem,
        ii. zbierane tylko dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
        iii. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.
    f. stosowanie się do niżej wymienionych zasad:
        i. zasada czystego biurka - w celu zapobieżenia nadużyciom, kradzieżom dokumentów, nośników elektronicznych i innych zasobów, po zakończeniu pracy należy uporządkować swoje stanowisko pracy, zabezpieczając dokumenty i nośniki elektroniczne z danymi osobowymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
        ii. Zasada czystego komputera - należy bezwzględnie przestrzegać zasady, aby w komputerze nie przechowywać zbędnych kopii zbiorów danych osobowych oraz aby w komputerze było zainstalowane wyłącznie oprogramowanie posiadające stosowne licencje, a sprzęt komputerowy był używany wyłącznie do celów służbowych.
        iii. Zasada czystego ekranu - ekrany monitorów powinny być umieszczone na stanowiskach pracy w taki sposób, aby uniemożliwić podgląd osobom nieupoważnionym. Dotyczy to zwłaszcza stanowisk, na których dostęp do danych osobowych jest niezbędny do obsługi

pracowników lub interesantów. W czasie opuszczania stanowiska pracy z wyjściem z pomieszczenia, bezwzględnie należy wylogować się z systemu komputerowego. Ponadto należy stosować wygaszacze ekranu zabezpieczone hasłem.

iv. Zasada czystego dostępu - osoba upoważniona powinna korzystać z dostępu wyłącznie do tych zbiorów danych osobowych, w tym przetwarzanych w systemach informatycznych, do których dostęp ten wynika z powierzonych jej przez przełożonego obowiązków służbowych oraz z zakresu upoważnienia.

v. Właściwe zabezpieczenie haseł do systemu — zabrania się zapisywania haseł do systemu komputerowego i umieszczania ich w formie pisemnej w pobliżu stanowiska komputerowego.

Postępowanie w sytuacji naruszenia ochrony danych osobowych P.Z. Catzy of Poland Jan Blom

1. Każda osoba upoważniona i każdy pracownik, który uzyskał informacje lub sam stwierdził naruszenie ochrony danych osobowych jest zobowiązany do niezwłocznego powiadomienia Administratora.
2. Osoby upoważnione do przetwarzania danych osobowych oraz wszyscy pracownicy, powinni niezwłocznie podjąć działania, których celem będzie, miedzy innymi, odpowiednie zabezpieczenie danych osobowych w sytuacjach stwierdzenia:
    a. wystąpienia zdarzeń losowych w strefach przetwarzania danych takich jak pożary, powódź, katastrofa budowlana, zalanie pomieszczenia itp. W takich przypadkach należy niezwłocznie podjąć działania które będą miały na celu ograniczenie rozmiarów zdarzenia. Należy zawsze pamiętać, że podstawową wartością która należy chronić w pierwszej kolejności jest zdrowie i życie ludzkie a w następnej kolejności posiadane zbiory danych osobowych i sprzęt służący do ich przetwarzania,
    b. awarii sprzętu lub oprogramowania, stwierdzenia działania złośliwego oprogramowania, podjęcia informacji pochodzącej z infrastruktury sieci informatycznej wskazującej na zdalny dostęp do niej osoby nieupoważnionej (hacking). Należy wtedy przerwać prace, wyłączyć urządzenia (jeżeli wcześniej były włączone),
    c. stwierdzenia bezprawnego naruszenia strefy przetwarzania danych czego skutkiem jest kradzież, modyfikacja, nieuprawnione kopiowanie lub zniszczenie zbioru danych, lub też kradzież lub zniszczenie sprzętu komputerowego.

Zasady transportowania danych osobowych poza obszarem przetwarzania

1. Dane osobowe w postaci zbiorów lub wydruków mogą być przekazywane poza obszar przetwarzania po uzyskaniu zgody Administratora.

2. W przypadku przekazywania droga elektroniczną danych osobowych podmiotom zewnętrznym na mocy obowiązującego prawa, należy stosować wymagana ochronę kryptograficzna przesyłanych danych.

3. Przekazywanie danych osobowych za pomocą sieci komputerowych odbywać się może tylko wtedy, gdy oprogramowanie i sprzęt sieci zawiera środki zabezpieczające dostęp lub przechwycenie tych danych, przez niepowołane osoby lub instytucje.

4. Przekazywanie danych osobowych na nośnikach papierowych, magnetycznych lub poprzez siec teleinformatyczna a także w innej formie poza systemami, może odbywać się wyłącznie pomiędzy osobami fizycznymi, które posiadają upoważnienie do przetwarzaniu danych osobowych pod warunkiem odpowiedniego ich zabezpieczenia.

Archiwizacja danych osobowych

1. Dokumentacje zawierające dane osobowe archiwizuje się zgodnie z wymogami szczególnych ustaw i rozporządzeń określających wymogi odnośnie okresu i warunków przechowywania tych danych. Szczególne wymagania w tym zakresie dotyczą dokumentacji związanej z zatrudnieniem i wynagradzaniem pracowników.