Polityka Ochrony Danych Osobowych

I. Wstęp

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora danych w Atest sp. z o.o w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO). Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

II. Inwentaryzacja danych

1. Dane osobowe wymagające ochrony administrator danych opracował w postaci papierowej, i zakresie sprzedaży obejmują:
• Dane wymagane ustawą o systemie oświaty
• Dane wymagane ustawą o rachunkowości
• Dane wymagające kontaktu – adres email
• Wszelkie inne dane ABI uznał za nadmiarowe i po ewentualnym wykorzystaniu dane są likwidowane w terminach i sposobami określonymi w polityce Bezpieczeństwa Informacji Teleinformacyjnej
2. W Spółce została opracowana Polityka Zarządzaniem Ryzykiem w przetwarzaniu danych osobowych, określająca zasady szacowania skali ryzyka i prawdopodobieństwa jego wystąpienia.
3. Administrator, w uzgodnieniu z Inspektorem Ochrony Danych, opracował karty zawierające analizę ryzyka dla poszczególnych operacji przetwarzania danych w zakresie aktywów biorących udział w przetwarzaniu danych.

III. Zapewnienie o przetwarzania danych osobowych zgodnie z prawem.

1. Administrator zapewnia, że:
1) dane osobowe są przetwarzane legalnie na podstawie art. 6 i 9 RODO;
2) zakres danych osobowych jest adekwatny do celów przetwarzania, z zachowaniem zasady minimalizacji danych;
3) Administrator przechowuje dane osobowe przez konkretnie określony czas, określony ustawami o systemie oświaty oraz ustawą o rachunkowości
4) wobec osób, których dane są przetwarzane wykonano obowiązek informacyjny (art. 12, 13, 14 RODO) wraz ze wskazaniem im: prawa dostępu do danych osobowych, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, „bycia zapomnianym”;
5) osoby, których dane osobowe są przetwarzane zostały poinformowane o funkcji IOD i przekazano dane kontaktowe;
6) zapewniono ochronę danych osobowych w przypadku powierzenia danych w postaci umów powierzenia z podmiotami przetwarzającymi (art. 28 RODO).

IV. Upoważnienia

1. Administrator odpowiada za nadawanie/anulowanie upoważnień do przetwarzania danych w zbiorach papierowych i systemach informatycznych.
2. Każda osoba upoważniona może przetwarzać dane wyłącznie na polecenie administratora

lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych.
4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia.

V. Postepowanie z incydentami

Katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz sposobów reagowania na ewentualne incydenty, sporządzono w celu minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń w przyszłości.
1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego lub Inspektora Ochrony Danych.
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności, napad obcej cywilizacji, wybuch pandemii);
2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);
3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator lub IOD) prowadzi postępowanie wyjaśniające w toku, którego:
1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
2) proponuje ewentualne działania dyscyplinarne;
3) proponuje działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu;
4) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

VI. Wykaz zabezpieczeń

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych.
2. W wykazie wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne, informatyczne i organizacyjne
3. Wykaz jest aktualizowany po każdej analizie ryzyka

VII. Szkolenia

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO.
2. Za przeprowadzenie szkolenia odpowiada Administrator danych.
3. Administrator dokonał szkolenia wszystkich pracowników szkoły w formie e-szkolenia.
4. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.
5. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.