Polityka Ochrony Danych Osobowych

TecVantage Marek Growiec

z dnia 25.05.2018 r.

Uwzględniając obowiązki wynikające z art. 25 oraz art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1), celem zapewnienia, że Dane osobowe w TecVantage Marek Growiec są przetwarzane i zabezpieczone zgodnie z postanowieniami prawa poprzez wdrożenia odpowiednich środków technicznych i organizacyjnych zaprojektowanych w celu skutecznej realizacji zasad ochrony danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń; a TecVantage Marek Growiec zapewnia, że domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

§ 1 Przepisy ogólne

1.1. Polityka określa środki techniczne i organizacyjne stosowane przez Administratora Danych dla zapewnienia ochrony danych osobowych oraz tryb postępowania w przypadku stwierdzenia Naruszenia lub podejrzenia o Naruszeniu. Polityka stanowi zbiór oraz podstawę wdrażanych u Administratora, procedur oraz zasad ochrony danych osobowych. Polityka zawiera:

(i) opis zasad ochrony danych obowiązujących u Administratora;

(ii) zbiór procedur, instrukcji i regulacji szczegółowych dotyczących przetwarzania Danych osobowych u Administratora, dotyczących poszczególnych obszarów z zakresu ochrony danych osobowych; stanowiących załączniki do Polityki.

1.2. Polityka obowiązuje wszystkich Pracowników oraz współpracowników Administratora. Za przestrzeganie i utrzymanie postanowień Polityki odpowiedzialni są:

(i) Administrator;

(ii) Pracownicy.

1.3. Dla skutecznej realizacji Polityki, uwzględniając zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia Administrator zapewnia:

(i) wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność przetwarzania Danych osobowych z wymogami prawa oraz niezbędne zabezpieczenie przetwarzanych danych osobowych;

(ii) zabezpieczenie zasobów systemów informatycznych, infrastruktury technicznej, sprzętu i osprzętu przed zniszczeniem, uszkodzeniem lub kradzieżą;

(iii) uniemożliwienie dostępu do Danych osobowych zawartych w systemach informatycznych oraz przechowywanych w formie papierowej osobom do tego nieupoważnionym;

(iv) stałe monitorowanie zgodności przetwarzania Danych osobowych z wymogami prawa oraz poddawanie środków, o których mowa w ust. (i) wyżej ciągłym przeglądom oraz uaktualnianiu;

(v) kontrolę i nadzór nad przetwarzaniem Danych osobowych.

1.4. Nadzór nad przestrzeganiem zasad opisanych w niniejszej Polityce oraz przepisów ochrony danych osobowych pełni Marek Growiec.

1.5. Zobowiązuję się wszystkich Pracowników do zapoznania się z Polityką Ochrony Danych Osobowych oraz do bezwzględnego przestrzegania zawartych w Polityce zasad.

1.6. Polityka jest przechowywana i udostępniana w wersji papierowej oraz elektronicznej w siedzibie Administratora.

1.7. Politykę udostępnia się:

(i) obligatoryjnie wszystkim osobom upoważnionym do przetwarzania Danych osobowych u Administratora, celem zapewnienia osobom upoważnionym należytej wiedzy oraz informacji na temat zasad i wymogów dotyczących przetwarzania Danych Osobowych u Administratora;

(ii) osobom zainteresowanym, w szczególności osobom fizycznym, których dane dotyczą – na ich wniosek.

§ 2 Słownik pojęć

2.1. Ilekroć w niniejszej Polityce zostaną wykorzystane poniższe definicje lub zwroty, należy nadawać im następujące znaczenie:

(i) Administrator– oznacza TecVantage Marek Growiec, 40-514 Katowice, ul. Ceglana 4, NIP: PL 954-136-90-98, REGON: 242725247.

(ii) Bezpieczeństwo informacji – oznacza zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

(iii) Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, takie jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej; o których mowa w art. 4 pkt 1 RODO;

(iv) Dane szczególne oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;

(v) Dokumenty z danymi osobowymi – oznaczają wszelkie dokumenty, w których zawarte są dane osobowe, z wyjątkiem wizytówek, kalendarzy i notatników prowadzonych w formie papierowej lub elektronicznej;

(vi) Hasło – oznacza ciąg znaków alfanumerycznych, znany jedynie Użytkownikowi;

(vii) Identyfikator – rozumie się przez to, ciąg znaków literowych, jednoznacznie identyfikujący Osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

(viii) Incydent ochrony danych osobowych – zdarzenie albo seria niepożądanych lub niespodziewanych zdarzeń ochrony danych osobowych stwarzających znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrożenia ochrony danych osobowych.

(ix) Naruszenie ochrony danych osobowych - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

(x) Nośniki danych – oznaczają wszelkie nośniki, na których są zapisane informacje w postaci elektronicznej, w szczególności: dyski CD–ROM, DVD–ROM, BluRay, dyski, pamięć USB i inne pamięci przenośne, karty magnetyczne oraz dokumenty papierowe zawierające dane osobowe;

(xi) Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, z tym zastrzeżeniem, że organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego nie są uważane za Odbiorcę;

(xii) Osoba upoważniona – oznacza osobę upoważnioną przez Administratora do przetwarzania Danych osobowych w danym zakresie;

(xiii) Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

(xiv) Polityka – oznacza niniejszą Politykę Ochrony Danych Osobowych Grupy Inter-Optyk z dnia 25 maja 2018 r. wraz ze wszystkimi ewentualnymi Załącznikami;

(xv) Pracowni – oznacz zarówno osobę zatrudnioną u Administratora na podstawie stosunku pracy, jak również osoby fizyczne współpracujące z Administratorem na podstawie umowy cywilnoprawnej;

(xvi) Przetwarzanie – oznacza operację lub zestaw operacji wykonywanych na Danych osobowych lub zestawach Danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie, o których mowa w art. 4 pkt 2 RODO;

(xvii) RODO – oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1);

(xviii) System – oznacza System ochrony Danych osobowych u Administratora, o którym mowa w § 5 Polityki;

(xix) System informatyczny – oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania Danych osobowych;

(xx) Urządzenie mobilne – oznaczają komórkowe telefony przenośne, tablety oraz inne urządzenia przenośne, które za pomocą posiadanych właściwości przeznaczone są lub mogą służyć do Przetwarzania Danych osobowych;

(xxi) Uwierzytelnienie – oznacza działanie, którego celem jest weryfikacja deklarowanej tożsamości Użytkownika;

(xxii) Użytkownik – oznacza osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania Danych umieszczonych w systemach, oprogramowaniu, zasobach sieciowych, plikach i folderach zapisanych na komputerach, serwerach, Nośnikach danych i innych urządzeniach elektronicznych;

(xxiii) Zbiór danych – oznacza każdy uporządkowany zestaw Danych osobowych, dostępny według określonych kryteriów;

(xxiv) Obszar przetwarzania danych – rozumie się przez to budynki i pomieszczenia określone przez Administratora tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione;

(xxv) Osoba lub Podmiot danych - oznaczają osobę, której Dane osobowe dotyczą;

(xxvi) Postępowanie z ryzykiem – proces planowania i wdrażania działań wpływających na ryzyko; Ryzyko – niepewność osiągnięcia zamierzonych celów;

(xxvii) System informatyczny – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną Administratora ;

(xxviii) Zgoda - oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

§ 3 Dane osobowe

3.1. Administrator przetwarza Dane osobowe gromadzone w Zbiorach danych. Zbiory danych przetwarzane u Administratora określa Załącznik nr 1 do Polityki.

3.2. Uaktualnienie lub poszerzenie listy Zbiorów danych następuje po uprzednim przeprowadzeniu analizy skutków oraz ryzyka przetwarzania Danych osobowych dla praw i wolności osób fizycznych objętych zbiorem.

3.3. Administrator nie podejmuje czynności Przetwarzania, które mogłyby wiązać się z istotnym ryzykiem naruszenia praw i wolności osób, których Dane osobowe dotyczą. W przypadku planowania podjęcia czynności, o których mowa w zdaniu poprzedzającym Administrator obligatoryjnie przeprowadza uprzednią ocenę skutków przetwarzania, o których mowa w art. 35 RODO.

3.4. Dane osobowe domyślnie Przetwarzane są na Obszarze przetwarzania danych obejmującym:

(i) pomieszczenia znajdujące się w siedzibach podmiotów wchodzących w skład Administratora;

(ii) pomieszczenia do Administratora lub będące we władaniu Administratora;

(iii) dodatkowy obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne i inne Urządzenia mobilne oraz Nośniki danych znajdujące się poza obszarem wskazanym w zdaniu poprzedzającym.

§ 4 Podstawy ochrony Danych osobowych u Administratora

4.1. Administrator zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych. Ochrona danych osobowych u Administratora realizowana jest poprzez wdrożenie odpowiednich środków oraz zabezpieczeń technicznych i organizacyjnych, takich jak:

(i) zabezpieczenia fizyczne,

(ii) procedury oraz rozwiązania organizacyjne;

(iii) oprogramowanie;

(iv) logiczne środki techniczne.

4.2. Administrator zapewnia, aby dostęp do Danych Osobowych miały wyłącznie osoby posiadające stosowne upoważnienie do ich przetwarzania. Wzór Upoważnienia stanowi Załącznik nr 2 do Polityki»

4.3. Osoby upoważnione oraz wszystkie inne osoby, którym udostępnia się Dane osobowe Przetwarzane u Administratora zobowiązane są do Przetwarzania Danych osobowych zgodnie z wymogami prawa oraz zgodnie z postanowieniami Polityki, jak również innych wewnętrznych aktów prawnych Administratora lub procedur wewnętrznych związanych z Przetwarzaniem Danych Osobowych.

4.4. Administrator zapewnia, aby Dane osobowe Przetwarzane u Administratora były:

(i) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;

(ii) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

(iii) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

(iv) prawidłowe i w razie potrzeby uaktualniane; Administrator zapewnia podejmowanie działań, mających na celu usuwanie lub sprostowanie Danych osobowych, które są nieprawidłowe w świetle celów ich przetwarzania ("prawidłowość");

(v) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;

(vi) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo Danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

4.5. Przy zapewnieniu Przetwarzania Danych osobowych zgodnie z zasadami wskazanymi w ust. 4.1 wyżej Administrator opiera Przetwarzanie na następujących podstawach:

(i) Legalność – Administrator dba o ochronę prywatności i przetwarza Dane osobowe zgodnie z wymogami prawa;

(ii) Bezpieczeństwo − Administrator zapewnia odpowiedni poziom bezpieczeństwa Danych osobowych podejmując stale działania w tym zakresie;

(iii) Prawa Jednostki − Administrator umożliwia osobom, których Dane osobowe są przetwarzane, wykonywanie swoich praw i prawa te realizuje;

(iv) Rozliczalność – Administrator zapewnia należyte udokumentowanie sposobu spełniania obowiązków w zakresie ochrony Danych osobowych.

4.6. Realizację powyższych zamierzeń powinny zagwarantować następujące założenia:

(i) wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych;

(ii) przeszkolenie Użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych.

(iii) przypisanie Użytkownikom określonych atrybutów pozwalających na ich identyfikację, takich jak hasła i identyfikatory;

(iv) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,

(v) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.

§ 5 System ochrony danych osobowych

5.1. Administrator zobowiązuje wszystkie osoby, które w obrębie wykonywania obowiązków służbowych, uzyskają w jakimkolwiek zakresie dostęp do Danych osobowych przetwarzanych przez Administratora do zapoznania się przed przystąpieniem do pracy z obowiązującymi zasadami ochrony Danych osobowych określonymi w Polityce. Wzór zobowiązania stanowi Załącznik nr 3 do Polityki.

5.2. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia Administrator wdraża środki techniczne i organizacyjne zapewniające należyty stopień ochrony Danych osobowych, odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Administratora.

5.3. Administratora przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa Danych osobowych. W tym celu Administrator:

(i) kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;

(ii) przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Administrator analizuje możliwe sytuacje i scenariusze naruszenia ochrony Danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia;

5.4. Administrator wdraża środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

5.5. Administrator zapewnia zgodność Przetwarzania Danych osobowych z wymogami prawa również poprzez zaprojektowanie, wprowadzenie i utrzymywanie Systemu. Na System składają się środki organizacyjne oraz środki techniczne ochrony, adekwatne do poziomu ryzyka zidentyfikowanego dla poszczególnych Zbiorów danych oraz kategorii danych. Na System składają się w szczególności następujące środki:

(i) zapewnienie, że każda osoba działająca z upoważnienia Administratora i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenie Administratora.

(ii) zapewnienie, że każdy z Pracowników powinien zachować szczególną ostrożność przy przenoszeniu danych;

(iii) ograniczenie dostępu do pomieszczeń, w których przetwarzane są Dane osobowe, jedynie do Osób upoważnionych oraz zapewnienie, że inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do Przetwarzania Danych osobowych wyłącznie w towarzystwie Osoby upoważnionej;

(iv) zamykanie pomieszczeń tworzących Obszar przetwarzania danych na czas nieobecności Pracowników, w sposób uniemożliwiający dostęp do nich osobom trzecim;

(v) zapewnienie zabezpieczenia obszaru, o którym mowa w ust. 3.4 Polityki przed czynnikami losowymi, takimi jak pożar lub powódź;

(vi) wdrożenie Polityki czystego biurka, która stanowi Załącznik nr 4 do Polityki;

(vii) wdrożenie zasad zarządzania systemem informatycznym służącym do przetwarzania Danych osobowych;

(viii) zapewnienie, że:

(a) dostęp do komputerów, na których są przetwarzane Dane osobowe mają tylko Osoby upoważnione,

(b) monitory komputerów, na których przetwarzane są Dane osobowe są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane,

(c) w wypadku potrzeby wyniesienia komputera przenośnego zawierającego Dane osobowe, lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane,

(d) Osoby upoważnione nie udostępniają osobom nieupoważnionym tych komputerów;

(ix) wdrożenie zasad dotyczących tworzenia kopii zapasowych;

(x) wdrożenie zasad przechowywania i archiwizowania gromadzonej dokumentacji zawierającymi Dane osobowe;

(xi) wdrożenie zasad przekazywania i obiegu Danych osobowych w obrębie Administratora;

(xii) zapewnienie skutecznego usuwania lub niszczenia dokumentów zawierających Dane osobowe, w sposób uniemożliwiający ich późniejsze odtworzenie;

(xiii) zapewnienie bezpieczeństwa sprzętowego i informatycznego, obejmującego:

(a) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz,

(b) zapewnienie aktualności stosowanego oprogramowania,

(c) zabezpieczenie sprzętu komputerowego wykorzystywanego u Administratora przed złośliwym oprogramowaniem,

(d) zapewnienie stałego i częstotliwego sporządzania kopii zapasowych danych przechowywanych na komputerach, serwerze oraz w sieci Administratora,

(xiv) przeprowadzanie analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

(xv) realizację standardów weryfikacji i doboru Podmiotów przetwarzających, jak również warunków powierzenia Przetwarzania danych na rzecz poszczególnych Podmiotów przetwarzających;

(xvi) monitorowanie zmian w zakresie procesów Przetwarzania Danych osobowych w Administratora oraz na bieżąco zarządzanie zmianami mającymi wpływ na ochronę Danych osobowych u Administratora.

§ 6 Naruszenie danych osobowych

6.1. Za naruszenie ochrony danych osobowych uważa się w szczególności:

(i) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują

(ii) naruszenie lub próby naruszenia integralności danych rozumiane jako wszelkie modyfikacje, zniszczenia lub próby ich dokonania przez osoby nieuprawnione lub

uprawnione działające w złej wierze lub jako błąd w działaniu osoby uprawnionej (np. zmianę zawartości danych, utratę całości lub części danych),

(iii) naruszenie lub próby naruszenia integralności systemu

(iv) zmianę lub utratę danych zapisanych na kopiach zapasowych,

(v) naruszenie lub próby naruszenia poufności danych,

(vi) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),

(vii) udostępnienie osobom nieupoważnionym danych osobowych

(viii) zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w system informatyczny zmierzające do zakłócenia jego działania bądź pozyskania w sposób niedozwolony lub w celach niezgodnych z przeznaczeniem danych zawartych w systemie,

(ix) inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy.

6.2. Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

6.3. W przypadku stwierdzenia naruszenia:

(i) zabezpieczenia systemu informatycznego;

(ii) technicznego stanu urządzeń;

(iii) zawartości zbioru danych osobowych;

(iv) ujawnienia metody pracy lub sposobu działania programu;

(v) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych;

(vi) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.);

- każda osoba zatrudniona przy przetwarzaniu danych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora. Powiadomienie, o którym mowa w zdaniu poprzedzającym składane jest na ręce Marka Growca.

6.4. W przypadku stwierdzenia Naruszenia ochrony Danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych oraz szacuje skalę ryzyka.

6.5. W przypadku naruszenia ochrony Danych Osobowych, Administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Wzór zawiadomienia, o którym mowa w zdaniu poprzedzającym, stanowi Załącznik nr 5 do Polityki.

6.6. Jeżeli ryzyko naruszenia praw i wolności osoby, której Dane osobowe dotyczą jest wysokie, Administrator zawiadamia o incydencie także osobę, której danej dotyczą, chyba że:

(i) Administrator wdroży odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

(ii) Administrator zastosuje następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; lub

(iii) wymagałoby to niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

6.7. Niezależnie od obowiązków wskazanych w ust. 16.2-16.4 wyżej, Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Wzór rejestru naruszeń danych osobowych stanowi Załącznik nr 6 do Polityki.

6.8. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

§ 7 Prawa podmiotów danych.

7.1. Każdej osobie, której dane osobowe są przetwarzane przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:

(i) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych;

(ii) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;

(iii) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;

(iv) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;

(v) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;

(vi) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów prawa albo są już zbędne do realizacji celu, dla którego zostały zebrane.

7.2. Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, i inne) oraz

rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności, takich jak zgłoszenie sprzeciwu lub ograniczenie przetwarzania.

7.3. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których Dane osobowe przetwarza.

7.4. Administrator publikuje na stronie internetowej Administratora oraz pozostawia do wglądu w siedzibie Administratora:

(i) Informację o prawach osób, których dane dotyczą;

(ii) Informację o zakresie przetwarzanych danych osobowych w poszczególnych celach;

(iii) Metodach kontaktu z Administratorem w zakresie Danych osobowych;

7.5. W celu realizacji praw osoby, której Dane osobowe dotyczą Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Administratora, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.

7.6. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób, informując osobę, której dane dotyczą o:

(i) przetwarzaniu jej Danych osobowych, przy pozyskiwaniu danych od tej osoby.

(ii) przetwarzaniu jej Danych osobowych, przy pozyskiwaniu danych o tej osobie nie bezpośrednio od niej;

(iii) planowanej zmianie celu przetwarzania danych;

(iv) uchyleniu ograniczenia przetwarzania Danych osobowych przed uchyleniem ograniczenia przetwarzania;

(v) sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe;

(vi) uprawnieniu do złożenia sprzeciwu względem przetwarzania Danych osobowych najpóźniej przy pierwszym kontakcie z tą osobą.

7.7. Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony Danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

7.8. Niezależnie od postanowień ust. 7.5 wyżej, Administrator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe.

7.9. Na żądanie osoby dotyczące dostępu do jej danych, Administrator informuje osobę, czy przetwarza jej Dane osobowe oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych.

7.10. Administrator wydaje osobie, której Dane osobowe dotyczą kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

7.11. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której Dane osobowe dotyczą. Administrator ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się

domaga. W przypadku sprostowania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.12. Administrator uzupełnia i aktualizuje dane na żądanie osoby, której Dane osobowe dotyczą. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administratora procedur lub prawa albo zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

7.13. Z uwzględnieniem ust. 7.13 niżej, na żądanie osoby, Administrator usuwa dane, gdy:

(i) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,

(ii) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

(iii) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

(iv) dane były przetwarzane niezgodnie z prawem,

(v) konieczność usunięcia wynika z obowiązku prawnego,

(vi) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

7.14. Administrator przy usuwaniu Danych osobowych uwzględnia, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

7.15. Jeżeli dane podlegające usunięciu zostały upublicznione przez Administrator, wówczas Administrator podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.16. Administrator dokonuje ograniczenia Przetwarzania danych na żądanie osoby, gdy:

(i) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

(ii) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu Danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

(iii) Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

(iv) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

7.17. W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.18. Na żądanie osoby Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Administratora.

7.19. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, o którym mowa w art. 21 RODO, a dane przetwarzane są przez Administratora w oparciu o uzasadniony interes Administratora lub o powierzone Administratorowi zadanie w interesie publicznym, Administrator zobowiązuje się uwzględnić sprzeciw, o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

7.20. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administratora na potrzeby marketingu bezpośredniego, Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

§ 8 Powierzenie przetwarzania

8.1. Administrator może powierzyć Przetwarzanie Danych osobowych Podmiotowi przetwarzającemu wyłącznie w drodze umowy zawartej w formie pisemnej lub innego instrumentu prawnego (np. Regulaminu lub ogólnych Zasad powierzania Danych osobowych) zgodnie z wymogami wskazanymi w art. 28 ust. 3 RODO.

8.2. Administrator korzysta wyłącznie z usług takich Podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których Dane osobowe dotyczą. W celu weryfikacji spełnienia obowiązku, o którym mowa w zdaniu poprzedzającym, Administrator przed powierzeniem przetwarzania potencjalnemu Podmiotowi przetwarzającemu w miarę możliwości uzyskuje informacje o zasadach ochrony Danych osobowych stosowanych przez potencjalny Podmiot przetwarzający oraz o praktykach tego podmiotu dotyczących zabezpieczenia Danych osobowych.

8.3. Szczegóły i zasady powierzenia Danych osobowych określa właściwa umowa lub instrument prawny.

§ 9 Przekazywanie Danych osobowych w obrębie Administratora

9.1. Dokumentacja zawierająca Dane osobowe przekazywana jest pomiędzy poszczególnymi jednostkami organizacyjnymi oraz Pracownikami z uwzględnieniem zasad ochrony Danych osobowych wskazanych w niniejszej Polityce.

9.2. W przypadku braku upoważnienia Pracownika odbierającego dokument do przetwarzania Danych osobowych, przekazywany jest on w sposób uniemożliwiający naruszenie Danych osobowych przy zastosowaniu wystarczających środków technicznych i organizacyjnych:

(i) wiadomości e-mail przesyłane są do innego Pracownika nieupoważnionego do przetwarzania Danych po wcześniejszym usunięciu Danych osobowych ze stopek maila oraz jego treści lub zaszyfrowaniu Danych w sposób uniemożliwiający identyfikację osoby, której Dane dotyczą;

(ii) dokumenty papierowe i elektroniczne przekazywane do innego Pracownika nieupoważnionego do przetwarzania Danych osobowych podlegają anonimizacji lub szyfrowaniu w zakresie Danych;

(iii) dokumenty w formie papierowej przekazywane do osoby, której Dane osobowe dotyczą za pośrednictwem innego Pracownika nieupoważnionego do przetwarzania Danych, wkładane są do kopert lub nieprzezroczystych teczek opisanych w sposób uniemożliwiający identyfikację adresata.

9.3. Dokumenty papierowe przekazywane do osoby, której Dane osobowe dotyczą za pośrednictwem innego Pracownika, przechowywane są i transportowane do czasu ich wydania adresatowi w sposób uniemożliwiający naruszenie Danych osobowych.

§ 10 Przekazywanie danych do Państwa trzeciego

10.1. Administrator nie przekazuje Danych osobowych do państwa trzeciego położonego poza terytorium Unii Europejskiej lub Europejskiego Obszaru Gospodarczego, poza sytuacjami, w których następuje to na wniosek osoby, której Dane osobowe dotyczą.

10.2. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych, Administrator okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

§ 11 Postanowienia końcowe

11.1. Polityka wchodzi w życie z dniem ogłoszenia.

11.2. W sprawach nieuregulowanych w Polityce odpowiednie zastosowanie znajdują postanowienia RODO oraz powszechnie obowiązujące przepisy prawa polskiego i europejskiego.

11.3. Wszelkie zmiany lub uzupełnienia do Polityki wymagają dla swej skuteczności formy pisemnej pod rygorem nieważności. Zmiany lub uzupełnienia do Polityki wchodzą w życie nie wcześniej niż w terminie 7 dni od dnia ich ogłoszenia.

11.4. Do Polityki dołączono następujące Załączniki, stanowiące integralną część Polityki:

(i) Załącznik nr 1 – Lista Zbiorów danych u Administratora;

(ii) Załącznik nr 2 – Wzór Upoważnienia do przetwarzania danych osobowych;

(iii) Załącznik nr 3 – Wzór Zobowiązania do zachowania poufności;

(iv) Załącznik nr 4 – Polityka czystego biurka;

(v) Załącznik nr 5 – Wzór zgłoszenia naruszenia ochrony Danych osobowych;

(vi) Załącznik nr 6 – Rejestr naruszeń danych osobowych;

11.5. Użytkownicy i Pracownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych postanowień zawartych w niniejszej Polityce. W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących u Administratora Danych, użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony informacji.