ZALEWSKI
ARCHITECTURE GROUP

POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

wersja 1.0 – maj 2018 r.

UL. KOŚCIUSZKI 30I9, 44-100 GLIWICE
WWW.ZALEWSKIAG.COM
NIP 631 167 94 97 I REGON 240096327

TEL I FAX 32 230 21 31
OFFICE@ZALEWSKIAG.COM
NR KONTA 93 1140 2004 0000 3902 3844 8110

1. [definicje]
    a. Administrator Danych – Krzysztof ZALEWSKI, prowadzący działalność gospodarczą pod nazwą ZALEWSKI ARCHITECTURE GROUP, Gliwice, ul. Kościuszki 30/9
    b. Dane osobowe - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego 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.
    c. Przetwarzanie - operacja 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.
    d. RODO - Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.
    e. Osoba upoważniona – osoba upoważniona przez Administratora do przetwarzania danych osobowych. Upoważnienie określa rodzaj danych, do których Osoba upoważniona ma dostęp oraz zawiera deklarację Osoby upoważnionej, co do nieograniczonego w czasie zachowania w poufności danych osobowych do których ma i miała dostęp. Upoważnienie ma formę pisemną i jest udzielane przez reprezentantów Administratora, którzy mogą

upoważnić do udzielenia upoważnienia kierowników działów. Administrator prowadzi ewidencję upoważnień.

f. Identyfikator użytkownika – ciąg znaków identyfikujący Osobę upoważnioną do przetwarzania danych w systemie informatycznym.
g. Hasło – ciąg znaków umożliwiający zalogowanie się Osoby upoważnionej w systemie informatycznym.

2. [miejsce przetwarzania danych]
    a. Dane są przetwarzane w siedzibie Administratora.
    b. Przetwarzanie danych poza siedzibą Administratora jest dopuszczalne jedynie w razie zapewnienia środków bezpieczeństwa danych osobowych w stopniu analogicznym do Polityki Bezpieczeństwa.

3. [podstawowe zasady]
    a. Dane są udostępnianie jedynie w niezbędnym zakresie wymaganym dla wykonywania czynności przez Osoby upoważnione.
    b. Administrator oraz Osoby upoważnione w możliwe najszerszy i najpełniejszy sposób zapewniają:
        - poufność i integralność – tj, iż dane będą przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, a także zapewniające, że dane te nie będą ujawnione osobom nieuprawnionym,
        - dostępność – tj. iż dane są dostępne na żądanie upoważnionego podmiotu lub Upoważnionej osoby,
        - rozliczalność – tj. takie postępowanie, aby możliwe było wykazanie przestrzegania przepisów RODO.
    c. Przekazywane danych Procesorowi wymaga zawarcia umowy, której minimalne standardy określa RODO.

d. Załącznikami do Polityki bezpieczeństwa są:
    - rejestr czynności przetwarzania danych,
    - wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

4. [zakres obowiązywania]

Polityka bezpieczeństwa obowiązuje wszystkich pracowników Administratora oraz osoby i podmioty z nim współpracujące bez względu na prawną podstawę współpracy.

5. [osoby mające dostęp do danych osobowych przetwarzanych]

a. Do danych osobowych przetwarzanych w formie papierowej oraz w systemach informatycznych mają dostęp osoby upoważnione:
    - pracownicy Administratora – na podstawie imiennego upoważnienia określającego zakres dostępnych danych,
    - pełnomocnicy Administratora – na podstawie imiennego upoważnienia określającego zakres dostępnych danych lub odpowiedniej umowy,
    - eksperci i doradcy Administratora – na podstawie imiennego upoważnienia określającego zakres dostępnych danych lub odpowiedniej umowy,
    - osoby działające na zlecenie władz państwowych lub sądu działające na podstawie przepisów prawa.

b. Każda osoba posiadająca upoważnienie do przetwarzania danych osobowych w systemach informatycznych posiada swój identyfikator oraz hasło, pozwalające na zalogowanie się do systemu informatycznego, w którym przetwarzane są dane osobowe. W razie prowadzenia czynności serwisowych zdalnych przez firmy informatyczne wgląd w dane osobowe powinien być niemożliwy lub maksymalnie ograniczony. Jeżeli wgląd taki jest

technologicznie niezbędny firma informatyczna winna niezwłocznie po wykorzystaniu zniszczyć skopiowane dane.

c. Jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym dokonywane w siedzibie firmy w obszarze przetwarzania danych osobowych, powinny odbywać się w obecności Administratora lub w sytuacji wyjątkowej – osoby przez niego wyznaczonej.

6. [bezpieczeństwo fizyczne]
   a. Pomieszczenia w których przechowywane są nośniki zawierające dane osobowe (np. akta osobowe, umowy z osobami fizycznymi, księga akcjonariuszy, systemy informatyczne, serwerownie) nie są dostępne dla interesantów i osób postronnych,
   b. W pomieszczeniach w których przechowywane są nośniki zawierające dane osobowe obowiązuje zakaz używania rejestrujących obraz lub dźwięk,
   c. Pomieszczenia, w których przechowywane są nośniki zawierające dane osobowe są poza godzinami pracy zamykane na klucz.
   d. Pomieszczenia, w których przechowywane są nośniki zawierające dane osobowe nie mogą pozostawać otwarte bez dozoru,
   e. Interesanci mają dostęp jedynie do sekretariatu i pokoju konferencyjnego, w których to pomieszczeniach nie są przechowywane jakiekolwiek dane osobowe lub są przechowywane w szafach zamykanych na klucz.

7. [zasada czystego biurka]

   Podczas obsługi interesanta monitory powinny być ustawione tak, aby uniemożliwić podgląd osobom postronnym, a dokumenty zawierające dany osobowe osoby innej, niż interesant nie mogą znajdować się w zasięgu wzroku interesanta.

8. [bezpieczeństwo urządzeń systemu informatycznego]

   Administrator jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie systemu informatycznego służącego do tego celu. Do obowiązków Administratora należy także kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej i systemu informatycznego. Obowiązkiem Administratora jest również zabezpieczenie sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.

9. [hasła i dostęp zdalny]

   a. Każda Osoba upoważniona posiada właściwy tylko dla siebie Identyfikator użytkownika.
   b. Logowanie do systemu odbywa się przy użyciu hasła.
   c. Hasło składa się, z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne;
   d. Użytkownik jest zobowiązany do zabezpieczenia swojego hasła przed nieuprawnionym dostępem osób trzecich.
   e. W sposób wskazany wyżej odbywa się logowanie także do systemu operacyjnego komputera na którym są przechowywane dane osobowe (np. umowy z osobami fizycznymi, korespondencja mailowa)
   f. Osoby upoważnione mogą w uzasadnionych przypadkach uzyskać zdalny dostęp do systemu informatycznego. W takim przypadku dane są szyfrowane, a dostęp wymaga środków bezpieczeństwa analogicznych do wskazanych w pkt. a – f.
   g. w przypadku wygaśnięcia upoważnienia Administrator zobowiązany jest do dopełnienia czynności uniemożliwiających ponowne wykorzystanie identyfikatora użytkownika, którego uprawnienia wygasły.

10. [zabezpieczenie systemu informatycznego]
    a. System informatyczny zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu poprzez stosowanie specjalistycznego oprogramowania (oprogramowaniem antywirusowym stosowanym w jednostce organizacyjnej jest: Norton Security)
    b. W systemie informatycznym stosowane jest oprogramowanie firewall zapewniające kontrolę przepływu informacji oraz działań inicjowanych z zewnątrz i od wewnątrz systemu;
    c. Użytkownikom nie wolno otwierać na komputerach, na których odbywa się przetwarzanie danych osobowych, plików pochodzących z niewiadomego źródła

11. [zasada czystego ekranu]
    a. System jest skonfigurowany w taki sposób, aby po okresie 30 minut bezczynności uruchamiany był wygaszacz ekranu. Do ponownego wznowienia pracy konieczne jest ponowne zalogowanie się przy użyciu identyfikatora i hasła.
    b. Po zakończeniu pracy użytkownik jest zobowiązany do wylogowania się, a następnie do wyłączenia komputera.
    c. W razie pracy z dokumentem lub innym plikiem w obecności innej osoby, w szczególności osoby, której dane dotyczą należy zadbać, aby nie był możliwy podgląd innych dokumentów lub plików.

12. [poczta elektroniczna]
    a. Poczta elektroniczna obsługiwana jest przez serwer home.pl.
    b. Operator poczty elektronicznej zapewnia bezpieczeństwo danych, w tym korespondencji mailowej, w szczególności zabezpieczenia dostęp do plików poczty przez osoby nieuprawnione.

c. Przesyłając korespondencję mailową należy zadbać o nieujawnianie adresów mailowych osób innych niż adresat, chyba, że korespondujące osoby ujawniły wobec siebie swoje adresy mailowe.

13. [kopie zapasowe]
    a. Raz w miesiącu Administrator wykonuje kopie pełne baz danych (backupy baz) do katalogu na serwerze baz danych, który znajduje się w szafie, do której dostęp ma jedynie Administrator oraz, w sytuacjach wyjątkowych, osoba przez niego wyznaczona;
    b. Wykonane kopie zapasowe przechowywane są również na serwerze kopii, który znajduje się w zamykanej szafie poza pomieszczeniem, w którym znajduje się serwer.

14. [przegląd bezpieczeństwa danych]
    a. Administrator raz na 12 miesięcy wykonuje generalny przegląd systemu informatycznego, polegający na ustaleniu poprawności działania tych jego elementów, które są niezbędne do zapewnienia realizacji funkcji wynikających z niniejszej Polityki.
    b. W przypadku stwierdzenia przez Administrator nieprawidłowości w działaniu elementów systemu opisanych podejmuje on niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania.
    c. Administrator wykonuje również przeglądu zasad bezpieczeństwa danych innych niż gromadzone w systemie informatycznym.

15. [naruszenia zasad ochrony danych osobowych]
    a. naruszenie danych osobowych podlega zgłoszeniu szczegółowo opisanemu w art. 33 RODO.
    b. Zgłoszenie powinno nastąpić organowi nadzorczemu nie później, niż w terminie 72 godzin po stwierdzeniu naruszenia,

c. W przypadku naruszenia ochrony danych osobowych, zgłoszenie go organowi nadzorczemu powinno:
d. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
e. zawierać imię i nazwisko oraz dane kontaktowe osoby, od którego możnej uzyskać więcej informacji;
f. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
g. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
h. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
i. Naruszenie ochrony danych osobowych powoduje każdorazowo przegląd procedur ochrony danych osobowych, w celu uniknięcia podobnej sytuacji w przyszłości,
j. Jeżeli naruszenie ochrony danych osobowych może spowodować wysokie naruszenia praw lub wolności osób fizycznych Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu (zgodnie z art. 34 RODO)

16. [postanowienia końcowe]

Administrator nie przeprowadził oceny skutków przetwarzania dla ochrony danych, gdyż charakter, zakres, kontekst i cele przetwarzania danych osobowych nie wskazują na duże prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.