POLITYKA OCHRONY DANYCH OSOBOWYCH

KOENIG & BAUER CODING (PL) SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

§ 1.

Definicje

1. **[Dane osobowe]** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, wskazane w Polityce ochrony danych osobowych, przetwarzane w Spółce i objęte ochroną w oparciu o przepisy Ustaw.
2. **[Inspektor ochrony danych]** – Inspektor ochrony danych w rozumieniu RODO.
3. **[Instrukcja]** – instrukcja zarządzania systemem informatycznym służącym do przetwarzania Danych osobowych w Spółce, stanowiąca załącznik do Polityki ochrony danych osobowych.
4. **[Polityka ochrony danych osobowych]** – niniejszy dokument polityki ochrony danych osobowych, stanowiący politykę ochrony danych osobowych w Spółce w rozumieniu RODO.
5. **[Spółka]** – Koenig & Bauer CODING (PL) spółka z ograniczoną odpowiedzialnością z siedzibą w Dąbrowie (62-069), przy ul. Bukowskiej17A, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Poznań - Nowe Miasto i Wilda w Poznaniu VIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000610660, NIP 7773260882, kapitał zakładowy 310.500,00 zł.
6. **[RODO]** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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).
7. **[Ustawy]** – wszelkie akty prawne powszechnie obowiązujące na terenie Rzeczpospolitej Polskiej regulujące zasady przetwarzania i ochrony danych osobowych, w szczególności RODO i ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018, poz. 1000 ze zm.).
8. **[Użytkownik]** – osoba przetwarzająca Dane osobowe, w tym będąca użytkownikiem sprzętu komputerowego, za pośrednictwem którego można uzyskać dostęp do Danych osobowych.

§ 2.

Naczelne zasady ochrony Danych osobowych w Spółce

1. Spółka przetwarza Dane osobowe przestrzegając następujących naczelnych zasad:
   - **a)** zasada zgodności z prawem, rzetelności i przejrzystości – Dane osobowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą,
   - **b)** zasada ograniczenia celu – Dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,

c) zasada minimalizacji danych – Dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne dla celów, w których są przetwarzane,

d) zasada prawidłowości – Dane osobowe są prawidłowe i w razie potrzeby uaktualniane, a Spółka podejmuje wszelkie rozsądne działania, aby dane osobowe nieprawidłowe w świetle celów przetwarzania zostały niezwłocznie usunięte lub sprostowane,

e) zasada ograniczenia przechowywania – Dane osobowe są przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy niż jest to niezbędne dla celów przetwarzania,

f) zasada integralności i poufności – Dane osobowe są przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych,

g) zasada rozliczalności – Spółka jest odpowiedzialna za przestrzeganie zasad przetwarzania Danych osobowych i musi być w stanie wykazać ich przestrzeganie,

h) zasada *privacy by default* – Spółka wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te Dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania,

i) zasada *privacy by design* – 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 wynikające z przetwarzania, Spółka – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

2. Interpretacja i stosowanie niniejszej Polityki ochrony danych osobowych powinny być dokonywane z poszanowaniem i w celu realizacji wszystkich zasad wymienionych w ust. 1 powyżej.

§ 3.

Ogólne zasady przetwarzania Danych osobowych

1. Projektując rozwiązania oraz przetwarzając Dane osobowe, Spółka kieruje się założeniem konieczności poszanowania prywatności osób fizycznych.

2. Spółka respektuje prawa osoby, której Dane osobowe dotyczą, jednocześnie respektując prawa innych osób.

3. Spółka komunikuje się z osobą, której Dane osobowe dotyczą, językiem zrozumiałym, klarownym i przejrzystym.

4. Spółka podaje osobie, której Dane osobowe dotyczą, wszystkie informacje konieczne dla poszanowania jej praw, co najmniej w zakresie przewidzianym przepisami Ustaw.

5. Spółka realizuje prawo dostępu do Danych osobowych, prawo do sprostowania Danych osobowych, prawo do usunięcia Danych osobowych („prawo do bycia zapomnianym”) osoby, której Dane osobowe dotyczą, w sposób każdorazowo dopasowany do okoliczności, zgodny z przepisami Ustaw.
6. Na uprawnione żądanie osoby, której Dane osobowe dotyczą, Spółka dokonuje ograniczenia przetwarzania Danych osobowych, na zasadach przewidzianych w RODO.
7. Spółka bada każdy sprzeciw osoby, której Dane osobowe dotyczą, pod kątem jego zasadności i obowiązku jego uwzględnienia przez Spółkę, stosując zasady określone w RODO i niniejszej Polityce ochrony danych osobowych.
8. Jeżeli Spółka będzie przetwarzać Dane osobowe w sposób zautomatyzowany, to Spółka zapewni osobie, której Dane osobowe dotyczą, możliwość odwołania się do interwencji ludzkiej, do wyrażenia własnego stanowiska i do zakwestionowania ewentualnej decyzji podjętej w sposób zautomatyzowany.

§ 4.

Bezpieczeństwo Danych osobowych

1. Spółka analizuje ryzyka wynikające z przetwarzania Danych osobowych, prawdopodobieństwo ich zaistnienia oraz wagę zagrożenia w celu wdrażania w miarę potrzeb adekwatnych środków bezpieczeństwa Danych osobowych. W szczególności Spółka analizuje ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania Danych osobowych.
2. Spółka przeprowadza ocenę skutków planowanych operacji przetwarzania dla ochrony Danych osobowych wszędzie tam, gdzie dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
3. Jeżeli jest to celowe lub – z uwagi na ryzyko naruszenia praw lub wolności osób fizycznych lub inne zagrożenia – konieczne, Spółka wdraża odpowiednie środki techniczne lub organizacyjne, w szczególności takie jak:
   a) pseudonimizacja i szyfrowanie Danych osobowych,
   b) środki do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
   c) środki do szybkiego przywrócenia dostępności Danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
   d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
4. Spółka wdraża procedury pozwalające Spółce zgłosić właściwemu organowi nadzorczemu ewentualne naruszenia ochrony Danych osobowych bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin.
5. Spółka stosuje instrumenty prawne mające zapewnić, że podmioty, którym Spółka powierza przetwarzanie Danych osobowych, będą przestrzegały zasad przetwarzania danych osobowych wynikających z Ustaw.

§ 5.

Szczegółowe zasady przetwarzania Danych osobowych

1. Spółka zapewnia ważną podstawę prawną dla każdego przypadku przetwarzania Danych osobowych.

2. Spółka wdraża odpowiednie środki techniczne i organizacyjne, aby Dane osobowe przetwarzane były w niezbędnym zakresie i przez niezbędny okres wobec celu ich przetwarzania.

3. Spółka przetwarza Dane osobowe:

   a) potencjalnych klientów Spółki będących osobami fizycznymi,

   b) klientów Spółki będących osobami fizycznymi,

   c) osób fizycznych reprezentujących kontrahentów Spółki,

   d) kontrahentów (w tym dostawców) Spółki będących osobami fizycznymi,

   e) potencjalnych pracowników i współpracowników Spółki,

   f) pracowników i współpracowników Spółki.

   Spółka może ubocznie przetwarzać inne Dane osobowe niż określone powyżej.

4. Dane osobowe przetwarzane są:

   a) w biurze Spółki pod adresem: ul. Bukowska 17A, 62-069 Dąbrowa (w tym na komputerach przenośnych, tabletach oraz telefonach komórkowych) oraz na serwerach w wydzielonych serwerowniach poza biurem Spółki,

   b) z wykorzystaniem programów komputerowych, a w szczególności: pakietu Microsoft Office, programu do obsługi poczty elektronicznej, oprogramowania Google Workspace, oprogramowania do zarządzania przedsiębiorstwem (tak zwany system informatyczny ERP), przeglądarek internetowych, czytników plików PDF, programów do zarządzania relacjami z klientami, programów kadrowych.

5. Przepływ Danych osobowych pomiędzy systemami informatycznymi odbywa się z wykorzystaniem:

   a) środków komunikacji elektronicznej, sieci LAN oraz WAN,

   b) poszczególnych funkcjonalności oprogramowania wykorzystywanego do przetwarzania Danych osobowych, a także

   c) zewnętrznych nośników danych (pendrive, płyty CD/DVD, dyski zewnętrzne).

6. Podczas przetwarzania Danych osobowych Spółka wykorzystuje następujące środki techniczne i organizacyjne niezbędne dla zapewnienia realizacji zasad, o których mowa w § 2:

   a) Dane osobowe przechowywane są w zabezpieczonych pomieszczeniach, w tym zabezpieczonych drzwiami z zamkiem,

   b) biuro posiada zbiorczą ochronę budynku, w tym system alarmowy,

c) dostęp do niektórych pomieszczeń, w których przetwarzane są Dane osobowe nadzorowany jest przez pracowników lub współpracowników Spółki,

d) dostęp do niektórych pomieszczeń, w których przetwarzane są Dane osobowe jest przez całą dobę (także w czasie nieobecności zatrudnionych tam pracowników lub współpracowników) nadzorowany przez służbę ochrony (system alarmowy),

e) budynki lub pomieszczenia biura, w którym przetwarzane są Dane osobowe, zabezpieczone są każdorazowo po zakończeniu pracy przez osoby uprawnione w sposób uniemożliwiający dostęp do nich osób trzecich, w szczególności poprzez zamknięcie budynków/pomieszczeń na klucz lub kod,

f) przebywanie w obszarze przetwarzania i przechowywania Danych osobowych osób nieuprawnionych do dostępu do Danych osobowych może nastąpić tylko w obecności osoby uprawnionej do dostępu do zbioru Danych osobowych lub za zgodą Spółki bądź Inspektora ochrony danych (w przypadku jego wyznaczenia),

g) każda z osób biorących udział w procesie przetwarzania Danych osobowych zostaje zaznajomiona z przepisami dotyczącymi ochrony danych osobowych oraz z wszelkimi instrukcjami i procedurami obowiązującymi w tym zakresie w Spółce,

h) pomieszczenia, w których przetwarzane są Dane osobowe zabezpieczone są przed skutkami pożaru, w szczególności za pomocą systemu przeciwpożarowego lub wolnostojącej gaśnicy,

i) dokumenty zawierające Dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów lub profesjonalnej firmy utylizującej dokumenty,

j) zastosowano urządzenia typu UPS,

k) osoby przetwarzające Dane osobowe obowiązane zostały do zachowania ich w tajemnicy,

l) zastosowano dodatkowe środki techniczne i organizacyjne, wskazane w pozostałych postanowienia Polityki ochrony danych osobowych oraz załączników do niej, w tym w Instrukcji.

§ 6.

Udostępnienie Polityki ochrony danych osobowych oraz jej zmiany. Załączniki.

1. Dopuszcza się możliwość dokonywania zmian w treści Polityki ochrony danych osobowych.
2. Tekst Polityki ochrony danych osobowych zostanie udostępniony w taki sposób, aby Użytkownicy mogli zapoznać się z jego treścią przed uzyskaniem pierwszego dostępu do Danych osobowych, a także w każdym czasie podczas posiadania uprawnień dostępu do Danych osobowych.
3. W przypadku zmian w Polityce ochrony danych osobowych Spółka po ich ogłoszeniu określi czas niezbędny do wejścia w życie Polityki ochrony danych osobowych w zmienionym kształcie.

4. Załączniki do Polityki ochrony danych osobowych stanowią jej integralną część.
5. Wszelkie definicje określone w Polityce ochrony danych osobowych mają także zastosowanie do załączników do Polityki ochrony danych osobowych, chyba że w treści załącznika postanowiono inaczej lub określono inne definicje.

Za Spółkę:

_____

Tomasz Ratajczak – Prezes Zarządu

ZAŁĄCZNIK NR 1

DO POLITYKI OCHRONY DANYCH OSOBOWYCH

KOENIG & BAUER CODING (PL) SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 1.
Cel, przedmiot i zakres Instrukcji

1. Celem Instrukcji jest zapewnienie ochrony Danych osobowych przetwarzanych w Spółce (w szczególności przetwarzanych w systemach informatycznych Spółki), w tym odpowiedniego bezpieczeństwa tych Danych osobowych.
2. Przedmiotem niniejszej Instrukcji jest określenie zasad organizacyjnych (w tym zasad nadawania uprawnień do przetwarzania Danych osobowych w Spółce) w celu zapewnienia następujących właściwości Danych osobowych:
   a) poufność (ujawnianie Danych osobowych uprawnionym Użytkownikom w określonych przypadkach i w dozwolony sposób),
   b) integralność (zapewnienie kompletności i dokładności Danych osobowych oraz zapobieganie ich nieautoryzowanej zmianie lub zniszczeniu),
   c) rozliczalność (możliwość jednoznacznej weryfikacji podmiotu wykonującego operacje na Danych osobowych),
   d) zgodność z prawem, rzetelność, przejrzystość,
   e) zgodność z naczelnymi zasadami ochrony Danych osobowych zawartymi w § 2 Polityki ochrony danych osobowych.
3. Zakres Instrukcji obejmuje wszystkie osoby biorące bezpośredni lub pośredni udział w procesie przetwarzania Danych osobowych, zwłaszcza w systemach informatycznych. Odniesienia do słów „system informatyczny” w liczbie pojedynczej obejmują również liczbę mnogą i odwrotnie.
4. Postanowienia Instrukcji mają także zastosowanie do Danych osobowych przetwarzanych poza systemem informatycznym, chyba, że dane postanowienia – ze względu na swój charakter – dotyczą tylko systemu informatycznego lub Danych osobowych w nim przetwarzanych.

I.
PODMIOTY UCZESTNICZĄCE W PRZETWARZANIU DANYCH OSOBOWYCH

§ 2.
Procedury nadawania i odbierania uprawnień do przetwarzania Danych osobowych

1. Każdy Użytkownik musi posiadać upoważnienie nadane przez Spółkę oraz być uwzględniony w ewidencji osób upoważnionych do przetwarzania Danych osobowych prowadzonej w Spółce.
2. Spółka może powierzyć Inspektorowi ochrony danych (w przypadku jego wyznaczenia) lub innej osobie wykonywanie czynności technicznych związanych z nadawaniem (a także zmianą zakresu oraz odbieraniem) upoważnień do przetwarzania Danych osobowych w imieniu Spółki lub z prowadzeniem ewidencji, o której w § 2 ust. 1 powyżej. W przypadku takiego powierzenia, o nadaniu / zmianie zakresu / odebraniu upoważnienia do przetwarzania Danych osobowych decyduje każdorazowo Spółka.
3. Użytkownikowi przyznany zostaje unikatowy identyfikator w systemie informatycznym wraz z poufnym hasłem dostępu, które powinno być zmieniane nie rzadziej niż co 90 dni. Hasło składa się z co najmniej ośmiu znaków, w tym małych i wielkich liter oraz cyfr lub znaków specjalnych.
4. Identyfikator wraz z prawidłowym hasłem umożliwia Użytkownikowi dostęp do systemu informatycznego, w którym przetwarzane są Dane osobowe, z wykorzystaniem sprzętu, z którego korzysta Użytkownik.
5. Każdy Użytkownik przed nadaniem upoważnienia do przetwarzania Danych osobowych oraz identyfikatora wraz z poufnym hasłem zostaje zapoznany z:
   a) Instrukcją i Polityką bezpieczeństwa,
   b) pozostałymi, wdrożonymi w Spółce, instrukcjami i procedurami określającymi zasady przetwarzania Danych osobowych,
   c) przepisami prawa dotyczącymi ochrony danych osobowych,

   a także – w przypadkach wymaganych przez Spółkę – podpisuje umowę o zachowaniu poufności lub inną umowę podobnego rodzaju.
6. Nadanie Użytkownikowi identyfikatora wraz z poufnym hasłem, umożliwiających dostęp do systemu informatycznego, w którym przetwarzane są Dane osobowe, jest możliwe wyłącznie po nadaniu temu Użytkownikowi upoważnienia do przetwarzania Danych osobowych w zakresie umożliwiającym ich przetwarzanie w systemie informatycznym lub równocześnie z nadaniem takiego upoważnienia.
7. Spółce oraz Inspektorowi ochrony danych (w przypadku jego wyznaczenia) przysługuje prawo zablokowania dostępu Użytkownika do Danych osobowych w każdym czasie. O każdym przypadku blokady dostępu dokonanej przez Inspektora ochrony danych (w przypadku jego wyznaczenia) informuje on Spółkę, z podaniem przyczyny blokady.
8. Blokada dostępu Użytkownika do Danych osobowych może być dokonana w szczególności w przypadku stwierdzenia naruszenia (lub powzięcia uzasadnionego podejrzenia naruszenia) przez Użytkownika wdrożonych w Spółce:
   a) instrukcji lub procedur określających zasady przetwarzania Danych osobowych,
   b) zabezpieczeń dotyczących ochrony Danych osobowych,
   c) procedur bezpieczeństwa,

lub przepisów powszechnie obowiązującego prawa dotyczących ochrony danych osobowych.

9. Spółka dokonuje zmian zakresu upoważnienia Użytkownika do przetwarzania Danych osobowych lub odbiera upoważnienie na wniosek przełożonego Użytkownika lub z własnej inicjatywy. Jeśli odebranie upoważnienia lub zmiana jego zakresu wymaga zmiany lub odebrania uprawnień dostępu do systemu informatycznego służącego do przetwarzania Danych osobowych albo usunięcia lub zmiany parametrów konta Użytkownika w tym systemie, Spółka podejmuje równocześnie odpowiednie działania dotyczące uprawnień dostępu lub określenia parametrów konta.

§ 3.

Konta Użytkowników korzystających ze sprzętu komputerowego

1. Każdemu Użytkownikowi korzystającemu ze sprzętu komputerowego, za pośrednictwem którego można uzyskać dostęp do Danych osobowych, Spółka lub Inspektor ochrony danych (w przypadku jego wyznaczenia; także na wniosek przełożonego Użytkownika), zakłada konto lub założenie konta zleca osobie trzeciej (firmie zapewniającej wsparcie IT, w szczególności dostarczającej Spółce system informatyczny) i przyznaje uprawnienia dostępu do Danych osobowych (przyznaje unikalny identyfikator wraz z poufnym hasłem dostępu).
2. Każdy Użytkownik, któremu przyznano hasło, zobowiązany jest do jego zapamiętania. Zapisywanie hasła jest zabronione.
3. Z zastrzeżeniem zdania drugiego, identyfikator i hasło przyznane jednemu Użytkownikowi nie mogą być powtórnie użyte. W przypadku niektórych systemów informatycznych hasło jest powtarzalne i tymczasowo przyznawane Użytkownikom przy tworzeniu nowych kont – Użytkownik jest zobowiązany do niezwłocznej zmiany hasła przy pierwszym logowaniu.
4. Konta Użytkowników usuwa Spółka z inicjatywy własnej bądź na wniosek przełożonego Użytkownika. Postanowienie niniejszego § 3 ust. 4 dotyczy także zmiany parametrów kont Użytkowników.
5. Inspektor ochrony danych (w przypadku jego wyznaczenia) lub Spółka może zablokować konto Użytkownika lub zablokowanie konta Użytkownika zlecić osobie trzeciej (firmę zapewniającą wsparcie IT, w szczególności dostarczającej Spółce system informatyczny) w każdym czasie, w tym w przypadkach opisanych w § 2 ust. 8 powyżej. O każdym przypadku blokady konta dokonanej przez Inspektora ochrony danych (w przypadku jego wyznaczenia) powiadamia on Spółkę, z podaniem przyczyny blokady.
6. W odniesieniu do czynności opisanych w niniejszym paragrafie, wykonujący te czynności przedstawiciel Spółki (w tym Inspektor ochrony danych – w przypadku jego wyznaczenia) może korzystać w wymaganym zakresie z pomocy firmy zapewniającej wsparcie IT dla Spółki.

§ 4.

Obowiązki i odpowiedzialność Użytkownika korzystającego ze sprzętu komputerowego

1. Użytkownik korzystający ze sprzętu komputerowego, za pośrednictwem którego można uzyskać dostęp do Danych osobowych, ponosi odpowiedzialność za:
   a) bezpieczeństwo informacji przechowywanych w komputerze,
   b) sporządzanie kopii bezpieczeństwa i kopii archiwalnych danych podlegających przetwarzaniu na komputerze na stanowisku pracy, w tym w razie konieczności także Danych osobowych – w zakresie w jakim Spółka lub Inspektor ochrony danych (w przypadku jego wyznaczenia) polecili Użytkownikowi sprzętu komputerowego sporządzanie tych kopii.
2. Użytkownik korzystający ze sprzętu komputerowego, za pośrednictwem którego można uzyskać dostęp do Danych osobowych, zobowiązany jest:
   a) eksploatować sprzęt i oprogramowanie zgodnie z instrukcjami obsługi oraz wyłącznie w celu służbowym,
   b) zachować szczególną ostrożność podczas transportu, przechowywania i użytkowania sprzętu,
   c) używać wyłącznie oprogramowania i podzespołów zatwierdzonych do użytku przez Inspektora ochrony danych (w przypadku jego wyznaczenia) lub Spółkę,
   d) nie dokonywać samodzielnej zmiany konfiguracji systemu operacyjnego oraz instalacji nowych i aktualizacji starych wersji oprogramowania, chyba że obowiązek wykonania tych czynności wynika bezpośrednio z polecenia Inspektora ochrony danych (w przypadku jego wyznaczenia) lub Spółki,
   e) zachować użytkowany sprzęt komputerowy w stanie sprawnym i czystym,
   f) nie udostępniać identyfikatora i hasła dostępu innym osobom,
   g) logować się w systemie informatycznym wyłącznie z użyciem nadanego temu Użytkownikowi identyfikatora i hasła dostępu; praca w systemie informatycznym przy użyciu identyfikatora i hasła innego Użytkownika jest zabroniona,
   h) dokonać skutecznego wylogowania się z systemu, uśpić komputer lub aktywować ekran blokady za każdym razem, gdy zamierza opuścić stanowisko komputerowe, niezależnie od tego na jak długo opuszcza to stanowisko; wylogowanie następuje poprzez wyłączenie sprzętu komputerowego, wybranie opcji systemu „wyloguj”, „uśpij” lub zablokowanie wyświetlanych treści na ekranie w sposób, który uniemożliwia odblokowanie go bez znajomości hasła,
   i) odnotowywać oraz niezwłocznie zgłaszać awarie i niesprawności sprzętu lub oprogramowania Inspektorowi ochrony danych (w przypadku jego wyznaczenia), Spółce lub firmie zapewniającej obsługę IT Spółki, w tym z podaniem (o ile jest to wymagane): nazwy i typu urządzenia lub programu, numeru ewidencyjnego, numeru fabrycznego urządzenia lub numeru licencyjnego programu, daty instalacji, opisu niewłaściwego działania, daty i nazwiska zgłaszającego.

3. W przypadku nieprzewidzianych sytuacji, zagrażających bezpieczeństwu Danych osobowych, każdy Użytkownik posiadający wiedzę o takim fakcie zobowiązany jest niezwłocznie zawiadomić Inspektora ochrony danych (w przypadku jego wyznaczenia) lub Spółkę.
4. Każdy Użytkownik zobowiązany jest ponadto do zachowania szczególnej staranności przy przetwarzaniu Danych osobowych w celu ochrony interesu osób, których dane dotyczą.

§ 5.

Obowiązki i odpowiedzialność Inspektora ochrony danych

1. Spółka może wyznaczyć Inspektora ochrony danych. Inspektor ochrony danych jest powoływany i odwoływany przez Spółkę.
2. W zakresie wykonywania swych zadań Inspektor ochrony danych może korzystać w wymaganym zakresie z pomocy firmy zapewniającej wsparcie IT dla Spółki.
3. Inspektor ochrony danych zobowiązany jest do nadzoru nad przestrzeganiem zasad ochrony Danych osobowych oraz zapewniania przestrzegania przepisów o ochronie danych osobowych, w tym do podejmowania czynności określonych w Polityce ochrony danych osobowych, Instrukcji oraz Ustawach (w tym w RODO), a w szczególności do wykonywania następujących zadań:
   a) informowanie administratora, podmiotu przetwarzającego, pracowników oraz współpracowników, którzy przetwarzają Dane osobowe, o obowiązkach spoczywających na nich na mocy Ustaw oraz przepisów Unii Europejskiej lub państw członkowskich Unii Europejskiej o ochronie danych i doradzanie im w tej sprawie;
   b) monitorowanie przestrzegania Ustaw oraz przepisów Unii Europejskiej lub państw członkowskich Unii Europejskiej oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
   d) współpraca z organem nadzorczym;
   e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

II.

§ 6.

Sposoby zabezpieczenia dostępu do Danych osobowych

1. System informatyczny Spółki, służący do przetwarzania Danych osobowych posiada zabezpieczenia o charakterze programistycznym mające na celu ochronę systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego. W celu zabezpieczenia dostępu do Danych osobowych przetwarzanych w systemie informatycznym przewidziane są w szczególności następujące środki bezpieczeństwa:
   a) wobec Danych osobowych przetwarzanych przy użyciu komputerów stosuje się w niezbędnym zakresie środki ochrony kryptograficznej, w szczególności stosowane są szyfrowane połączenia (SSL),
   b) identyfikator i hasło dostępu do systemu informatycznego Użytkownika sprzętu komputerowego są niedostępne dla osób nieupoważnionych,
   c) dostęp do systemu operacyjnego komputera oraz systemu informatycznego, w których przetwarzane są Dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora Użytkownika oraz hasła,
   d) zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii Danych osobowych przetwarzanych przy użyciu systemu informatycznego,
   e) zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie,
   f) użyto system firewall do ochrony dostępu do sieci komputerowej (w tym serwerów).
2. Inspektor ochrony danych (w przypadku jego wyznaczenia) lub Spółka dokonują okresowych kontroli poprawnego działania zabezpieczeń.

§ 7.

Profilaktyka antywirusowa. Przeglądy i konserwacja sprzętu oraz systemu informatycznego

W zakresie ochrony Danych osobowych przed zagrożeniami wirusowymi oraz wadami i awariami systemu informatycznego przewiduje się następujący tryb postępowania:

a) sprzęt komputerowy (w tym komputery przenośne, tablety, telefony komórkowe oraz nośniki danych) powinny mieć zainstalowane programy antywirusowe,
b) zgodnie z harmonogramem zaleconym przez firmę zapewniającą wsparcie IT dla Spółki wykonywane jest antywirusowe skanowanie zasobów komputera,
c) w przypadku znalezienia wirusa należy go usunąć przy pomocy programu antywirusowego, wyłączyć i włączyć ponownie komputer i przeprowadzić ponowne skanowanie. Jeśli wirusa nie da się usunąć, należy wyłączyć komputer, a następnie zgłosić problem Inspektorowi danych osobowych (w przypadku jego wyznaczenia) lub Spółce.

d) przegląd sprzętu komputerowego (w tym komputerów przenośnych, tabletów, telefonów komórkowych oraz nośników danych) oraz skanowanie systemu informatycznego służących przetwarzaniu Danych osobowych przeprowadzane są co najmniej raz na kwartał. Czynności tych dokonuje Użytkownik.

e) w przypadku stwierdzenia wady technicznej sprzętu lub wirusa w systemie, Użytkownik jest zobowiązany poinformować o tym Spółkę w celu niezwłocznego ich usunięcia. Użytkownik jest zobowiązany w każdym przypadku zabezpieczyć Dane osobowe przed dostępem osób nieupoważnionych.

§ 8.

Sporządzanie kopii bezpieczeństwa i kopii archiwalnych

W celu zabezpieczenia Danych osobowych przed utratą podejmowane są następujące działania:

a) sporządzanie kopii bezpieczeństwa danych (w tym Danych osobowych zgromadzonych na dysku twardym komputera) w celu chwilowego ich przechowania, przed wykonaniem na sprzęcie działań mogących uszkodzić lub usunąć przechowywane na nim dane (np. rekonfiguracja, aktualizacja lub nowa wersja systemu operacyjnego lub aplikacji).

b) periodyczne sporządzanie kopii archiwalnych danych (w tym Danych osobowych) według strategii przyjętej dla każdego systemu informatycznego przez Spółkę (kopia archiwalna służy do odtworzenia stanu systemu, aplikacji i baz danych służących do przetwarzania Danych osobowych, w przypadku awarii polegającej na uszkodzeniu dysków twardych, przypadkowego usunięcia lub modyfikacji danych, skutków działania wirusów itp.).

c) wykonywane są kopie zapasowe (kopie bezpieczeństwa i kopie archiwalne).

§ 9.

Przechowywanie kopii zapasowych i nośników z Danymi osobowymi oraz ich niszczenie

1. Dane osobowe, które nie są umieszczone na nośnikach umieszczonych wewnątrz sprzętu, za pomocą którego można uzyskać dostęp do Danych osobowych, są przechowywane na nośnikach danych takich jak dyski zewnętrzne zabezpieczone poprzez umieszczenie ich w kopercie w sejfie lub szafie pancernej lub też innym miejscu o równoważnym poziomie zabezpieczeń, do którego dostęp ma wyłącznie Spółka, Inspektor ochrony danych (w przypadku jego wyznaczenia) oraz Użytkownik upoważniony do przetwarzania tych Danych osobowych.
2. Kopie zapasowe, o których mowa w § 8 oraz nośniki wskazane w § 9 ust. 1 są przechowywane przez okres przydatności dla Spółki zawartości kopii zapasowej lub nośnika, w tym przez okres dozwolonego prawem przetwarzania Danych osobowych zawartych w tych kopiach i nośnikach. Kopie zapasowe i nośniki wskazane w § 9 ust. 1

(lub ich zawartość) są niezwłocznie niszczone po ustaniu przydatności zawartości tych kopii lub nośników.

3. Nośniki informatyczne przeznaczone do likwidacji, naprawy lub przekazania podmiotowi nieuprawnionemu do przetwarzania danych na nich zawartych, a zawierające Dane osobowe, zostają przed likwidacją, naprawą lub przekazaniem pozbawione zapisu danych w taki sposób, aby ich odczytanie bądź odzyskanie nie było możliwe.
4. Zniszczenie kopii zapasowych oraz nośników informatycznych zawierających Dane osobowe (lub zawartości tych kopii bądź nośników) jeżeli wymagają tego okoliczności, potwierdza się protokołem zniszczenia.

III.
POZOSTAŁE POSTANOWIENIA

§ 10.

Udostępnienie Instrukcji oraz jej zmiany

1. Dopuszcza się możliwość dokonywania zmian w treści Instrukcji.
2. Tekst Instrukcji zostanie udostępniony w taki sposób, aby Użytkownicy mogli zapoznać się z jego treścią przed uzyskaniem pierwszego dostępu do Danych osobowych zgromadzonych w systemie informatycznym, a także w każdym czasie podczas posiadania uprawnień dostępu do Danych osobowych w systemie informatycznym.
3. W przypadku zmian w Instrukcji, Spółka, po ich ogłoszeniu, określi czas niezbędny do wejścia w życie Instrukcji w zmienionym kształcie.

Za Spółkę:

_____

Tomasz Ratajczak – Prezes Zarządu

ZAŁĄCZNIK NR 2

DO POLITYKI OCHRONY DANYCH OSOBOWYCH

KOENIG & BAUER CODING (PL) SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

INSTRUKCJA POSTĘPOWANIA W RAZIE NARUSZENIA OCHRONY PRZETWARZANYCH DANYCH OSOBOWYCH

§ 1.

Cel, przedmiot i zakres instrukcji

1. Celem niniejszej instrukcji jest zapewnienie ochrony Danych osobowych przetwarzanych w Spółce w przypadku naruszenia lub uzasadnionego podejrzenia naruszenia wdrożonych w Spółce:
   a) instrukcji lub procedur określających zasady przetwarzania Danych osobowych,
   b) zabezpieczeń dotyczących ochrony Danych osobowych (w tym zabezpieczeń systemu informatycznego lub programu komputerowego, za pomocą których Dane osobowe są przetwarzane),
   c) procedur bezpieczeństwa,

   lub przepisów powszechnie obowiązującego prawa dotyczących ochrony danych osobowych (zwanych dalej łącznie: „**Zabezpieczeniami**"), poprzez określenie zasad postępowania w sytuacji, gdy stwierdzono naruszenie Zabezpieczeń lub powzięto uzasadnione podejrzenie, że takie naruszenie nastąpiło.
2. Zakres instrukcji obejmuje wszystkie osoby upoważnione do przetwarzania Danych osobowych w Spółce, biorące bezpośredni lub pośredni udział w procesie przetwarzania Danych osobowych, w tym ich przetwarzania w systemie informatycznym zgodnie z Ustawami. Każda z tych osób przed zaangażowaniem jej w przetwarzanie Danych osobowych, zostanie zaznajomiona z niniejszą instrukcją oraz z pozostałymi, wdrożonymi w Spółce, instrukcjami i procedurami określającymi zasady przetwarzania Danych osobowych, a także z przepisami powszechnie obowiązującego prawa dotyczącymi ochrony danych osobowych.

§ 2.

Tryb postępowania

Postępowanie rozpoznawcze

1. W przypadku stwierdzenia naruszenia stosowanych w Spółce zabezpieczeń lub powzięcia uzasadnionego podejrzenia, że takie naruszenie nastąpiło, osoba stwierdzająca takie naruszenie lub podejrzewająca naruszenie jest zobowiązana niezwłocznie zawiadomić o tym Spółkę lub Inspektora ochrony danych (w przypadku jego wyznaczenia), a także osobę pełniącą funkcję administratora systemu informatycznego w Spółce.

2. Inspektor ochrony danych (w przypadku jego wyznaczenia) lub Spółka, bądź osoba wyznaczona przez Inspektora ochrony danych (w przypadku jego wyznaczenia) lub Spółkę („**Osoba Wyznaczona**"), w razie stwierdzenia naruszenia lub uzyskania informacji o podejrzeniu naruszenia Zabezpieczenia, podejmuje niezwłocznie wymagane czynności, w szczególności:

   a) ustala okoliczności naruszenia Zabezpieczenia, to jest moment naruszenia, ewentualnego sprawcę i sposób dokonania naruszenia,

   b) określa stan systemu informatycznego lub programu komputerowego wykorzystywanego do przetwarzania Danych osobowych, w tym skutki dokonanego naruszenia i poprawność działania systemu operacyjnego,

   c) dokonuje sprawdzenia zasobów zawierających przetwarzane Dane osobowe, w tym zasobów systemu informatycznego i zawartości dokumentów lub plików zawierających Dane osobowe,

   d) w razie stwierdzenia naruszenia – dokonuje w wymaganym zakresie zmiany haseł dostępu umożliwiających dostęp do przetwarzanych Danych osobowych (w tym haseł dostępu do systemu informatycznego lub programu komputerowego), a także weryfikuje zakres pozostałych uprawnień dostępowych do przetwarzanych Danych osobowych i zmienia te uprawnienia w wymaganym zakresie, biorąc pod uwagę okoliczności naruszenia Zabezpieczenia,

   e) określa zakres niezbędnych zmian w Instrukcji albo w Polityce ochrony danych osobowych wdrożonych w Spółce,

   f) w razie uszkodzenia lub zniszczenia zbiorów zawierających Dane osobowe, odtwarza te dane z kopii bezpieczeństwa lub kopii archiwalnej,

   g) sporządza dokumentowy protokół z dokonanych czynności zaznaczając wszystkie informacje określone powyżej oraz godzinę rozpoczęcia i zakończenia czynności.

3. Na każdym etapie postępowania rozpoznawczego Spółka bądź Inspektor ochrony danych (w przypadku jego wyznaczenia) może podjąć decyzję o natychmiastowym przerwaniu połączeń mogących umożliwić nieuprawniony dostęp do systemu informatycznego lub programu komputerowego, za pomocą których Dane osobowe są przetwarzane.

Podjęcie przetwarzania danych

4. Po zakończeniu postępowania rozpoznawczego lub po przerwaniu połączenia na podstawie § 2 ust. 3 niniejszej instrukcji, ponowne rozpoczęcie przetwarzania Danych osobowych lub nawiązanie połączenia następuje po wyeliminowaniu wszystkich stwierdzonych błędów i zagrożeń, mogących spowodować powtórne naruszenie Zabezpieczeń.

5. W uzasadnionym przypadku, odpowiednio do ustalonych przyczyn naruszenia, Spółka (także na wniosek Inspektora ochrony danych – w przypadku jego wyznaczenia) może dokonać zmiany zasad postępowania w przedmiocie ochrony Danych osobowych i

zarządzania systemem informatycznym w takim zakresie, jaki uzna za niezbędny dla zminimalizowania wystąpienia w przyszłości ryzyka naruszenia Zabezpieczeń.

§ 3.

Zawiadomienie o naruszeniu

1. W przypadku naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, Spółka zgłasza to naruszenie do właściwego organu nadzorczego, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2. Zgłoszenie powinno w miarę możliwości nastąpić w terminie 72 godzin od ustalenia naruszenia. Jeżeli nastąpi w terminie późniejszym, do zgłoszenia Spółka dołącza wyjaśnienie przyczyn opóźnienia.
3. Zgłoszenie musi co najmniej:
   a) 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;
   b) zawierać imię i nazwisko oraz dane kontaktowe Inspektora ochrony danych (w przypadku jego wyznaczenia) lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) opisywać możliwe konsekwencje naruszenia ochrony Danych osobowych;
   d) 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.
4. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, Spółka udzieli je sukcesywnie bez zbędnej zwłoki.
5. Spółka prowadzi dokumentację naruszenia obejmującą okoliczności naruszenia ochrony Danych osobowych, jego skutki oraz podjęte działania zaradcze.
6. Jeżeli naruszenie ochrony Danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Spółka bez zbędnej zwłoki zawiadamia osobę, której Dane osobowe dotyczą, o takim naruszeniu, chyba że:
   a) Spółka wdrożyła odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do Danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych Danych osobowych;

b) Spółka zastosowała następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;

c) wymagałoby ono 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.

7. Zawiadomienie, o którym mowa w ust. 6 powyżej, jasnym i prostym językiem opisuje charakter naruszenia ochrony Danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w ust. 3 b), c) i d) powyżej.

§ 4.

Udostępnienie instrukcji oraz jej zmiany

1. Dopuszcza się możliwość dokonywania zmian w treści niniejszego dokumentu.
2. Tekst niniejszej instrukcji zostanie udostępniony w taki sposób, aby osoby upoważnione do przetwarzania Danych osobowych w Spółce mogły zapoznać się z jego treścią przed uzyskaniem pierwszego dostępu do Danych osobowych, a także w każdym czasie podczas posiadania uprawnień dostępu do Danych osobowych.
3. W przypadku zmian w niniejszej instrukcji Spółka po ich ogłoszeniu określi czas niezbędny do wejścia w życie instrukcji w zmienionym kształcie.

Za Spółkę:

_____

Tomasz Ratajczak – Prezes Zarządu