OFERTA

RFI – GDPR

Analiza procesów dotycząca spełnienia wymagań nowych regulacji w zakresie ochrony danych osobowych wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływów takich danych oraz uchylenia dyrektywy 945/46/WE

Opracował:

Piotr Krajewski, Prezes Zarządu, Adwokat, Ekspert ds. bezpieczeństwa transakcji elektronicznych RBE ZBP

Usamah Afifi – konsultant

Portal Informacyjny Bezpieczny Bank Sp. z o. o.

1. Informacje wstępne.

1.1 Podstawa przygotowania oferty.

Niniejsza oferta Portal Informacyjny Bezpieczny Bank Sp. z o. o. dalej zwana **Spółką** lub **Zleceniobiorcą** dlaj **Klientem** lub **Zleceniodawcą.**

1.2 Streszczenie dla Kierownictwa.

1.2.1 ZAKRES OFEROWANYCH USŁUG.

W dniu 24 maja 2016 r. weszły w życie przepisy ogólnego Rozporządzenia Unii Europejskiej nr 2016/679 w sprawie ochrony danych osobowych (dalej RODO). Nowe przepisy zaczną obowiązywać z dniem 25 maja 2018 r. Konsekwencje niedostosowania się do przepisów RODO są Wymierne (min.przewidziano również bardzo wysokie kary pieniężne za nieprzestrzeganie przepisów Rozporządzenia). Już teraz jednak należy podjąć szereg działań mających na celu dostosowanie organizacji do nowych obowiązków. Zasadą jest bowiem, że do obecnie zbieranych danych osobowych stosować się będą nowe wymogi. Ich adresatami są zarówno administratorzy danych, processorzy jak i osoby bezpośrednio/pośrednio odpowiedzialne za bezpieczeństwo danych osobowych w organizacji czyli również osoby zarządcze.

Wprowadzone zmiany będą miały kluczowe znaczenie dla zarządzania kluczowymi procesami jak i systemami IT. Dotyczy to zarówno fazy projektowania (m.in. konstrukcje privacy by default oraz privacy by design), jak fazy korzystania z systemów (m.in. obowiązki w zakresie wdrożenia odpowiednich środków technicznych, procesowych i organizacyjnych).

Oferta Spółki zarówno obejmuję część prawną usługi, a więc odpowiedź na pytanie, co nowego w stosunku do dotychczasowego stanu prawnego wprowadzają nowe regulacje i jak to wpływa na bezpieczeństwo danych osobowych, oraz część operacyjną (procesowe, organizacyjne IT), wskazując które procesy wspierają kluczowe zagadnienia związane z wdrożeniem regulacji GDPR pod kątem odpowiedzialności i wdrożenia procesów pod kątem zmniejszenia ryzyka i wskazanie obszarów, na jakie wpływa RODO w TMPL.

Zakres prac będzie obejmował:

a) Analizę procesów biznesowych w celu identyfikacji tych, które przetwarzają dane osobowe w kontekście regulacji GDPR („Open Analysis”),

b) Ocenę procesów biznesowych przetwarzających dane osobowe pod kątem spełnienia wymagań regulacji GDPR zwana dalej („Gap Analysis”),

c) Rekomendacje zmian procesów biznesowych, które zapewnią spełnienie wymagań regulacji GDPR na poziomie najniższych kosztów („Low Cost Analysis”),

d) Rekomendacje w pełni usprawniające zarządzanie danymi osobowymi i procesami biznesowymi przetwarzającymi dane osobowe w świetle regulacji GDPR („Full Cost Analysis”).

e) Przeprowadzenie prac analitycznych w zakresie przeglądu infrastruktury IT TMPL oraz narzędzi informatycznych wspierających procesy biznesowe przetwarzające dane osobowe w celu:

- Identyfikacji magazynów danych pod kątem przechowywania danych spełniających kryteria danych osobowych w świetle regulacji GDPR oraz identyfikacja aplikacji korzystających z tych danych,

- Rekomendacji w zakresie zmian w sposobie przetwarzania danych (np. magazynowania i prezentacji) pod kątem spełnienia regulacji GDPR

Zakładamy, iż prace będą podzielone na 2 fazy:

Faza inicjalna, obejmie:

- Wstępne ustalenie zakresu wpływu GDPR na organizację
- Sesję Executive briefing z zarządem TMPL
- Warsztaty pogłębiające wiedzę z GDPR z przepisów i praktycznego wpływu na organizację

Faza wykonawcza, obejmie:

- Identyfikacja obszarów wpływu GDPR na organizację.
- Analiza luk i rekomendacje zmian w obszarach:
  - Organizacji
  - Procesów
  - Prawnym
  - Infrastrukturalnych
- Przegląd i benchmarking rozwiązań w zakresie ochrony danych wrażliwych i prezentacja best practice
- Pomoc przy budowie procedur kontrolnych i raportowych

Zakładamy, że prace projektowe będą wykonane:

Faza I – 20 MD od podpisania umowy.

Faza II – 116 MD od zakończenia Fazy I.

Lp.	Zadanie	Czas
1.	przygotowanie mapy procesów biznesowychTMPL, których wykonanie wymaga przetwarzania danych osobowych.	10 MD
2.	naniesienie na mapę procesów informacji, w jakim stopniu każdy z procesów przetwarzających dane osobowe spełnia wymagania regulacji GDPR. Oczekuje się, że całość oceny zostanie przeprowadzona względem jednej zaproponowanej skali spełniania wymagań oraz w każdym przypadku ocena zostanie poparta komentarzem uzasadniającym decyzję.	15 MD
3.	dostarczenie TMPL rekomendacji, które pozwolą na spełnienia wymagań regulacji GDPR na minimalnym rekomendownym poziomie.	3 MD
4.	przygotowanie kompleksowej listy zmian dotyczących zarówno procesów biznesowych ale również narzędzi i systemów informatycznych zwiększających efektyność zarządzania analizowanym obszarem.	20 MD
5.	przygotowanie mapy magazynów danych zawierających dane osobowe wraz z informacjami: a) Typ danych b) Lokalizacja w infrastrukturze TMPL, c) Wskazanie technologi przechowywania d) Identyfikacja systemów, aplikacji i użytkowników korzystających z magazynów e) Powiązanie mapy magazynów danych z mapą	63 MD

	procesów biznesowych	
6.	przedstawienie rekomendacji w odniesieniu do okresów retencji, środków bezpieczeństwa i zakresu przechowywanych danych.	15 MD

4. Szacujemy, iż koszt projektu jest możliwy po zapoznaniu się z potrzebami Klienta.

Opierając się na informacji o planowanym wdrożeniu/uruchomieniu RODO (GDPR) u Klienta, proponuję jako wiodący temat audytu bezpieczeństwa obrać JAKOŚĆ DANYCH. Wdrożenie RODO (GDPR) jest prawie zawsze zaczątkiem stosowania rozwiązań zwanych zazwyczaj Business Intelligence (analityka biznesowa, BI).

Na początek, tytułem wstępu, trochę informacji podstawowych. Jak wiadomo BI ma szerokie znaczenie, ale ogólnie można przedstawić je jako proces przekształcania danych w informacje, a informacji w wiedzę, która może być wykorzystana np. do zarządzania strategicznego i zwiększania konkurencyjności Klienta. Funkcjonuje maksyma „śmieci weszły, śmieci wyszły". Chodzi o to, że wyniki przetwarzania błędnych danych, będą błędne nawet wtedy, gdy procedura przetwarzania jest najzupełniej poprawna.

Nie chodzi więc tylko o to JAK się przetwarza, ale CO się przetwarza. Niska jakoś danych stanowi główną przyczynę niepowodzeń rozwiązań BI. Zespoły projektowe, które nie biorą pod uwagę zapewnienia jakości danych, zazwyczaj się przekonują, że ich rozwiązanie nie dostarcza wiarygodnych informacji, a niedociągnięcie nie polega na zastosowaniu błędnych algorytmów przetwarzania, lecz na niedostatecznej jakości przetwarzanych danych. Czyli właśnie „śmieci weszły, śmieci wyszły".

Czas i zasoby wydatkowane na wielokrotne poprawianie i przetwarzanie tych samych danych nie są przy tym najistotniejszym czynnikiem generującym potencjalne straty. Dane nieodpowiedniej jakości skutkują niedokładnym obrazem wyników działalności i mogą prowadzić do błędnych decyzji. Naraża to Klienta na utratę szans biznesowych i możliwości redukcji kosztów działalności oraz naraża na ryzyko nadużyć, wobec których nie można odpowiednio szybko reagować. Problem jest potęgowany przez fakt wykorzystywania danych przez różnych odbiorców (nie koniecznie końcowych). Otóż dla jednego odbiorcy, ten sam zestaw danych (być może wykorzystywanych selektywnie) może mieć zupełnie inną jakość niż dla innego. Dane, te same dane, użytkowane w jednym celu mogą być wystarczająco dobre, a w innym (nie koniecznie bardziej zaawansowanym) – nie dość precyzyjne. Czyli: te same dane mogą być jednocześnie dobrej i niedobrej jakości, w zależności od ich wykorzystywania od punktu odniesienia.

Wg istniejących już opracowań: „Dane są wysokiej jakości, jeżeli nadają się do użycia zgodnie z przeznaczeniem w zakresie działania, podejmowania decyzji i planowania. Dane nadają się do użycia zgodnie z przeznaczeniem, jeżeli nie zawierają defektów i posiadają pożądane cechy". Jest to sygnał do tego, by podejść do zagadnienia jakości danych jako do problemu wielowymiarowego. Na etapie projektowym, podstawowym problemem jest ustalenie z jakimi danymi /rodzaj i jakość/ i z jakim sposobem wprowadzania danych do systemu mamy do czynienia. Stąd propozycja Audytu Bezpieczeństwa.

1.2.2 Szczegółowy zakres usług obejmuje:

1.2.2.1 Zakres projektu:

Ważne aby podkreślić, że na etapie projektowym, podstawowym problemem jest ustalenie z jakimi rozwiązaniami w zakresie umieszczania danych w SI mamy do czynienia. Stąd właśnie propozycja Audytu Bezpieczeństwa w RODO (GDPR), który powinien objąć następujące, podstawowe etapy:

(0) Zapoznanie się z głównymi dokumentami regulującymi wprowadzanie danych do SI. Ich ilość, rodzaj, jakość i objętość jest nieznana, tym niemniej - z praktyki - etap ten, obejmujący również przygotowanie wstępnych pytań. Po dostarczeniu dokumentacji, etap taki składa się jedynie z analizy. Zajmie około 15 dni roboczych

(1) Kompletowanie dokumentów źródłowych. Etap obejmujący gromadzenie danych związanych z zaistniałymi FAKTAMI oraz wiedzą specjalistyczną zbierających je pracowników/agentów. Etap obejmuje też wstępną weryfikację spójności zapisów roboczych oraz ich ew. potwierdzanie. Ocenić należy przede wszystkim sposoby gromadzenia danych w dokumentacji roboczej (szkice, notatki, dokumentacja

fotograficzna, korespondencja itp.), przed wprowadzeniem do SI Klienta. W grę wchodzi dokumentacja papierowa, dokumentacja fotograficzna i elektroniczna. Zbierana dokumentacja, w pewnym momencie jest uznawana za wystarczającą, aby wprowadzać ją do SI "pod numerem" szkody, nadawanym zapewne na samym początku (np. jako numer zgłoszenia). Chodzi o kryteria oceny, czy zebrane dane mogą już stanowić podstawę do dalszego ich procesowania. Czy są podpisywane, potwierdzane, kto to robi, czy w grę wchodzi skanowanie itp. Konieczna faza fieldworku i analizy.

Obejmuje około 15 dni roboczych.

(2) Wprowadzanie danych do systemu. Etap obejmujący procedury przenoszenia danych z zapisów roboczych/podręcznych (szkice, notatki, korespondencja, dokumentacja fotograficzna, itp.) do właściwego SI. Kto to robi, czy dysponuje pełną wiedzą o szkodzie czy tylko "wklepuje" dane. Czy możliwa jest modyfikacja danych (np. użyte sformułowania, "oczywiste" pomyłki w tekstach). Uwaga: etap ten może okazać się jednym procesem z Etapem (I), nie jest to błąd ale konieczne jest istnienie adekwatnych mechanizmów kontrolnych. Konieczna faza fieldworku i analizy. Obejmuje około 5 dni roboczych.

(3) Weryfikacja zapisów. Etap obejmujący kontrolne porównanie danych w systemie (przed ich przekazaniem do przetwarzania!) z zapisami źródłowymi. Weryfikacja może być realizowana w sposób permanentny lub na próbie. Etap ten obejmuje też metody poprawiania danych. Kto to robi, czy są ponownie weryfikowane, czy są prowadzone statystyki błędów. Konieczna faza fieldworku i analizy. Obejmuje około 5 dni roboczych.

(4) Archiwizacja. Etap obejmujący przenoszenie do bezpiecznego przechowywania danych źródłowych. Czy Klient ma archiwum, czy outsourcuje to zadanie, czasy dostępu, bezpieczeństwo fizyczne. Może wystarczyć sama faza fieldworku.

Obejmuje około 5 dni roboczych.

(5) Analiza, wnioski i propozycje usprawnień. Etap obejmujący sporządzenie raportu z audytu i przygotowanie propozycji w zakresie dokumentacji, polityki bezpieczeństwa ew. szkice regulaminów i instrukcji w zakresie zlecenia.

Obejmuje około 15 dni roboczych.

(6) Opracowanie polityki, regulaminów, instrukcji. Uwzględniając potrzebę sporządzenia odpowiedniej jakości materiałów, Obejmuje około 14 dni roboczych.

(7) Całość budżetuję wstępnie na około 52 dni robocze.

2. Wykonanie zlecenia.

Wykonanie zlecenia przez Zleceniobiorcę jest uzależnione od otrzymania informacji i kopii dokumentów wskazanych przez Zleceniobiorcę, jako niezbędne. Z czasu wykonania zlecenia należy wyłączyć czas, kiedy Zleceniobiorca nie będzie mógł podejmować czynności z przyczyn od niego niezależnych, w szczególności w czasie oczekiwania na informacje i materiały oraz w czasie oczekiwania na akceptację wstępnego projektu materiałów. Czas wykonania zlecenia nie obejmuje formułowania pytań i analizy otrzymanych materiałów (regulacji wewnętrznych Klienta), które konkretyzują w poszczególnych obszarach ogólne zasady Polityki Zgodności. Z powyższych przyczyn oraz w przypadku konieczności zmian we wstępnym projekcie materiałów, czas wykonania zlecenia może ulec przedłużeniu.

Zleceniobiorca może zlecić wykonanie części zlecenia innej osobie, ponosząc jednak za jej działania odpowiedzialność, jak za działania i zaniechania własne. Zleceniobiorca nie ponosi odpowiedzialności za nienależyte wykonanie zlecenia spowodowane przyczynami niezawinionymi przez Zleceniobiorcę, w szczególności wynikające z nie przekazania przez Zleceniodawcę informacji lub nie udostępnienia dokumentów, istotnych dla realizacji zlecenia, działania siły wyższej i osób trzecich (np. awarie serwera, łączy

telekomunikacyjnych, katastrofy itp.) Zleceniodawca pokrywa koszty, poniesione przez Zleceniobiorcę w trakcie wykonywania zlecenia, zgodnie z przedstawioną przez Zleceniobiorcę kalkulacją kosztów, w przypadku odstąpienia/wypowiedzenia przez Zleceniodawcę od realizacji zlecenia w trakcie trwania umowy.

3. Harmonogram

Harmonogram prac do uzgodnienia. Zakładamy, że wykonanie powyższych prac u Klienta oraz przygotowanie raportu potrwa do 52 dni (analiza przez ekspertów zebranych informacji, dokumentów i regulacji) oraz rozmów z osobami odpowiedzialnymi u Klienta za poszczególne podobszary.

4. Wymiana informacji.

Dokumenty zostaną dostarczone w formie elektronicznej w formacie MS Office na nośniku CD lub DVD. Wymiana informacji istotnych dla wykonania zlecenia następować będzie wyłączenie w formie pisemnej. Za formę pisemną uznaje się również formę fax`u i e-mail`a podanych w umowie. W celu zapewnienia prawidłowego wykonania zlecenia wyznacza się osoby odpowiedzialne po stronie Zleceniodawcy i Zleceniobiorcy za koordynację działań związanych z jego przebiegiem.

5. Osoby upoważnione do kontaktów ze strony Spółki.

Usmah Afifi - Konsultant Tel: +48 664 056 060 e-mail: usamah.afifi@bezpieczny-bank.eu
Stefan Cieśla – Radca prany Tel. +48 667 490 911 e-mail: stefan.ciesla@bezpieczny-bank.eu
Mariusz Podolski – Starszy audytor Tel. +48 663 431 744 e-mail : mariusz.podolski@bezpieczny-bank.eu
Jarosław Samonek – Dyrektor Zarządzajcy Tel. +48 501 173 999 e-mail: jaroslaw.samonek@bezpieczny-bank.eu
Piotr Krajewski – Prezes Zarządu – Adwokat – Ekspert ds. bezpieczeństwa transakcji elektronicznych Rady Bankowości Eleltronicznej Związku Banków Polskich Tel: +48 605610623 e-mail: piotr.krajewski@bezpieczny-bank.eu

6. Nazwa i siedziba oferenta.

Piotr Krajewski - Prezes Zarządu

e - mail: piotr.krajewski@bezpieczny-bank.eu

tel. kom./mobile +48605610623

Portal Informacyjny Bezpieczny Bank Sp. z o. o.

ul. Portowa 22A, 30 - 709 Kraków,

tel. +48 12 294 25 80, fax. +48 12 294 25 81,

www.bezpieczny-bank.eu

NIP: 6751482480, REGON: 122691188, KRS 0000438113

Sąd Rejonowy dla Krakowa –Śródmieścia w Krakowie,

XI Wydział Gospodarczy

7. Zarządzający projektem.

7.1 Piotr Krajewski *– adwokat, radca prawny, Prezes zarządu*

jest absolwentem Uniwersytetu Jagiellońskiego w Krakowie, byłym pracownikiem Prokuratury Rejonowej Kraków - Śródmieście w Krakowie oraz kilku instytucji finansowych. Pracował jako prawnik w Krakowskim Domu Maklerskim S.C. Ekspert Instytutu Copernicus. Jest Ekspertem Związku Banków Polskich w zakresie bezpieczeństwa bankowości elektronicznej. Był Prezesem Stowarzyszenia Biegłych ds. Przeciwdziałania Nadużyciom Gospodarczym ACFE Polska, która jest oddziałem ACFE USA. Posiada wieloletnie doświadczenie w zakresie prowadzenia dochodzeń w sprawach gospodarczych, obsługi prawnej instytucji rynku finansowego i pozafinansowego. Ma ponad 10 letnie doświadczenie oraz wiedzę z zakresu bezpieczeństwa instytucji finansowych, spółek prawa handlowego, Compliance, rynku kapitałowego i zagadnień IT. Przez wiele lat pełnił funkcje Dyrektora Operacyjnego oraz Zastępcy Dyrektora w Departamencie Bezpieczeństwa Banku w Banku BPH S.A. w Krakowie oraz funkcje Dyrektora Operacyjnego w Banku Pekao SA., nadzorując zespoły odpowiedzialne za przeciwdziałanie praniu pieniędzy, bezpieczeństwa informatycznego, zapobieganiu nadużyciom oraz prowadzeniu postępowań wyjaśniających (investigation). Specjalizuje się m.in. w następujących obszarach:

- *prawo karne, ze szczególnym uwzględnieniem problematyki przestępczości w obrocie gospodarczym oraz przestępstw finansowych w podmiotach gospodarczych,*
- *prowadzenie postępowań wyjaśniających i audytów dochodzeniowych w podmiotach gospodarczych,*
- *przeciwdziałanie wprowadzeniu do obrotu wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł (pranie pieniędzy),*
- *bezpieczeństwo prowadzenia biznesu - projektowanie i opiniowanie rozwiązań ograniczających straty finansowe,*
- *ryzyko utraty reputacji oraz ryzyko strat powstałych w wyniku działań nieuczciwych klientów i pracowników,*
- *zagadnienia związane z bezpieczeństwem systemów teleinformatycznych, procedury, rozwiązania, standardy, postępowania wyjaśniające, audyt bezpieczeństwa,*
- *prawo gospodarcze, ze szczególnym uwzględnieniem prawa bankowego i publicznego obrotu papierami wartościowymi,*
- *zarządzanie ciągłością prowadzenia biznesu, Business Continuity Management,*
- *zagadnienia związane z Compliance w zakresie informacji poufnych i zgodności przestrzegania przepisów w podmiotach gospodarczych.*

7.2 Usamah Afifi - konsultant

Ponad 19 lat doświadczenia w zarządzaniu projektami, doradztwie biznesowym, usługach transformacji biznesowej i integracji złożonych projektów
Międzynarodowe doświadczenie: Niemcy, Francja, Rosja, Portugalia, Rumunia, Czechy, Polska, Holandia, Emiraty Arabskie i in.
Usługi doradcze dla kierownictwa wyższego szczebla (po stronie i w imieniu klienta)
Doświadczenie w kierowaniu złożonymi projektami oraz dużymi zespołami.
Wiedza specjalistyczna, zarządzanie operacyjne, doradztwo biznesowe (Strategia, procesy biznesowe, IT, Vendor Selection), Rozwiązania Informatyczne (integracja, Billing, ERP, CRM, BPMS, Analityka-Big Data, fraud, Bezpieczeństwo, SCADA, OSS).
Szeroka wiedza rynkowa – w telekomunikacji, przemyśle (Chemical & Petroleum, Automotive, Energetyka), rynku publicznym.
Wizjoner silnie zorientowany na ludzi i osiąganie mierzalnych rezultatów

7.3. Dariusz Głogowski Ekspert ds. Bezpieczeństwa Systemów Teleinformatycznych

Specjalizuje się w zakresie testów bezpieczeństwa konfiguracji systemów operacyjnych oraz aplikacji webowych.

*Systemy operacyjne – Doświadczenie w administrowaniu oraz zabezpieczaniu systemów Unix, Linux (Red Hat, Debian, Slackware), *BSD, Windows NT/2000/2003/XP, Vista (aktualne testy),*
Bazy Danych - PostgreSQL, MySQL, Oracle
Servery Web – Apache, IIS, Websphere
Sieci - LAN, WLAN (Wi-Fi)
- IP, TCP, UDP, ICMP
- HTTP, SMTP, DNS, DHCP, NFS,
Inne - Lotus Notes, audyty i bezpieczeństwo sieci i systemów Linux/Unix/Windows, analiza powłamaniowa Linux/Unix i Windows, konfiguracja i administracja systemem IDS (ISS) oraz urządzeń firewall, monitorowanie informacji związanych z zagrożeniami antywirusowymi oraz potencjalnymi atakami na sieci i systemy operacyjne, audyt aplikacji Web oraz bezpieczeństwo wykonywania transakcji elektronicznych, debugging aplikacji, fuzzing aplikacji, reverse engineering, tworzenie procedur i polityki bezpieczeństwa sieci i systemów teleinformatycznych, tworzenie scenariusza ataków i testów bezpieczeństwa aplikacji i systemów, bezpieczeństwo transakcji elektronicznych, oraz bankowości elektronicznej, Doświadczenie w używaniu aplikacji komercyjnych do audytu bezpieczeństwa takich jak: Nessus, GFI Lan Guard Scanner, ISS Internet Scanner, Accunetix Vulnerability Web Scanner, Appdetective Scanner for Oracle, Security Expressions, oraz open-source hping, Nmap, Flawfinder, Webscarab, SPIKE, i inne)

7.4. Mariusz Podoslki - Starszy Audytor

Audyt wszystkich obszarów działalności, zwłaszcza związanych z Zarządzaniem Ryzykiem, Operacjami; Bezpieczeństwem, Compliance oraz usługami wewnętrznymi i zarządzaniem projektami; Postępowania wyjaśniające, zwłaszcza w zakresie głównej odpowiedzialności; Tworzenie i rozwój metodologii oceny ryzyka oraz doradztwo w zakresie zarządzania ryzykiem; Sporządzanie analiz ryzyka oraz wieloletnich planów działania (około 40 tematów z cz. 1-3 lata); Odpowiedzialność za sporządzenie planów rocznych, szczegółowych i wytycznych;Kontrole jakości i efektywności procesów i procedur oraz konsultacje w tym zakresie; Kontrole zakresie ryzyka zgodności; Audyt kooperantów w zakresie bezpieczeństwa danych i bezpieczeństwa ciągłości działania; Postępowania wyjaśniające w sprawach związanych z zakresem głównej odpowiedzialności; Udział w licznych projektach (w tym międzynarodowych, Bazylea II, SOX, ryzyko operacyjne i inne); Sporządzanie raportów i analiz w powyższych tematach;
- Współpraca międzynarodowa z BACA (Austria), HVB (Niemcy), UCI (Włochy), GE (global).

7.5 Stefan Cieśla – radca prawny

radca prawny, menadżer, promotor koncepcji chmury obliczeniowej. Ukończył Wydział Prawa i Administracji na Uniwersytecie Wrocławskim i rozpoczął pracę jako asystent w Zakładzie Prawa Finansowego tego samego uniwersytetu. Na początku lat 90. był dyrektorem departamentu prawnego Ministerstwa Łączności, miedzy innymi reformował rynek usług telekomunikacyjnych. W 1992 przeniósł się do branży bankowej.

specjalizuje się obecnie w zagadnieniach prawnych związanych z chmurą obliczeniową. Jest współautorem pierwszego polskiego raportu na ten temat, który współtworzył z dr. Thomasem Helbingiem i firmą informatyczną Asseco. Angażuje się również w liczne konferencje i inicjatywy edukacyjne związane z tym trendem informatycznym.

W latach 1992-94 wniósł znaczący wkład w tworzenie Polskiego Banku Rozwoju, zaś w 1994 roku jako specjalny wysłannik NBP został przewodniczącym Zarządu Komisarycznego w Banku Posnania, który upadł w związku z machinacjami finansowymi jego właścicieli, związanych z Elektromisem i Mariuszem Świtalskim.

Był również odpowiedzialny za inną głośną likwidację w sektorze bankowym: w 1999 roku został przewodniczącym Zarządu Komisarycznego w Banku Staropolskim, doprowadzonym do bankructwa przez biznesmena Piotra Bykowskiego. Według raportu "Polityki" z maja 2000 roku, występował tam jako zaufany współpracownik Zygmunta Solorza.

W następnych latach zasiadał w zarządach i radach nadzorczych kilku innych instytucji (m.in. Invest-Bank S.A. oraz TUŻ Polisa Życie S.A.), a zarazem rozpoczął prowadzenie kancelarii prawnej. Zarówno w swojej praktyce menadżerskiej, jak i prawniczej, specjalizuje się m.in. w zagadnieniach związanych z informatyką – w początkach lat 2000 uznawany był wręcz za pioniera innowacyjnych rozwiązań w sektorze finansowym. W latach 2004–2011 związany z Grupą Polsat jako doradca prezesa zarządu.

Od końcówki lat 90. zaangażowany jest w prace nad reformami w służbie zdrowia. Współtworzył Kasy Chorych, zaś w 2004 roku był głównym doradcą prawnym zespołu prof. Religi, pracującego nad obywatelskim projektem reformy NFZ.

7.6 Jarosław Samonek – Dyrektor Zarządzający

***j**est doświadczonym specjalistą w zakresie budowania strategii biznesowej przedsiębiorstwa, wzmacniania świadomości marki, zarządzania projektami, a także tworzenia i rozbudowy kanałów partnerskich. Jako dyrektor generalny Symantec Polska tworzył kompleksową strategię wprowadzenia firmy na rynek polski, a następnie przez wiele lat zarządzał nią z sukcesem. Jest absolwentem Instytutu Organizacji Zarządzania, Wydziału Mechanicznego Technologii i Automatyzacji Politechniki Warszawskiej oraz University of Minessota, programu MBA Szkoły Głównej Handlowej. Prywatnie lubi podróże z dala od utartych szlaków oraz górskie wędrówki. Zachowuje je na długo w pamięci dzięki swojej pasji, jaką jest fotografia.*

8. Wynagrodzenie.

Proponowane wynagrodzenie za przeprowadzenie projektu wynosi, od 5000,00 zł (słownie: pięć tysięcy zł 00/100) do 500 000,00 zł (słownie: pięciuset tysięcy złoty 00/100) netto. Kwota zostanie indywidualnie ustalona z Klientem w zaleznosci od jego potrzeb

Przy założeniu, że nakład pracy będzie obejmował standardowy zakres prac, a ilość godzin nie przekroczy ilość godzin pomnożonych przez zaproponowane stawki poniżej.

Powyższe wynagrodzenie zastało skalkulowane w oparciu o stawki Spółki zawarte w poniższej tabeli. (Po przekroczeniu ilości godzin wynikających z zaproponowanego wynagrodzenia stosuje się stawki o 10% wyższe).

Stanowisko	**Stawka netto (za godzinę)/(za dzień)**
Prezes/Dyrektor Zarządzajacy/Dyrektor/Konsultant	450,00 zł/3000,00 zł
Menedżer/Radca prawny/Adwokat/	300,00 zł/2000,00 zł
Ekspert	250,00 zł/1600,00 zł

9. Płatności.

Platne w 50 % w dniu podpisania umowy zlecenia oraz 50 % 30 dni po zakończeniu projektu i jego wdrożeniu na podstawie faktury + podatek VAT zgodnie z obowiązującymi przepisami stawkami. Zleceniodawca upoważni Zleceniobiorcę do wystawiania faktur VAT bez jego podpisu. Wynagrodzenie będzie powiększane o wysokość kosztów bezpośrednich, niezbędnych do wykonania zlecenia, w szczególności udokumentowanych kosztów tłumaczeń, dojazdów i noclegów, delegacji, na które zgodę wyrazi Zleceniodawca.

Wynagrodzenie obejmuje przygotowanie projektu i przeprowadzenie projektu zgodnie z zamowieniem

Oferta ważna jest 30 dni.

10. Klauzula o poufności oferty.

Niniejszy dokument stanowi tajemnicę handlową Spółki i podlega następującym zastrzeżeniom:

- jest przeznaczony wyłącznie dla Klienta do wiadomości osób zaangażowanych w zagadnienia objęte niniejszą ofertą;

- udostępnianie go w jakiejkolwiek formie innym osobom bez Spółki jest zabronione.

11. Uwagi. Bezpieczeństwo Informacji.

Wykorzystanie w biznesie nowoczesnych technologii niesie za sobą oczywiste korzyści. Warto jednak zdawać sobie sprawę również z potencjalnych zagrożeń związanych z bezpieczeństwem informacji, takich jak włamania, kradzież danych, utrata danych, nieuprawniona modyfikacja czy też ataki z wykorzystaniem złośliwego oprogramowania. Świadome zarządzanie przedsiębiorstwem to między innymi zapewnienie ochrony newralgicznych danych, których utrata , nieuprawniona modyfikacja, bądź wyciek mogą mieć dla firmy negatywne skutki.

Nasz Dział Audytu Bezpieczeństwa Informacji to grupa ekspertów - specjalistów z wieloletnim doświadczeniem w zakresie bezpieczeństwa informacji. Nasze doświadczenie, zdobyte

w różnorodnych projektach i pracach konsultingowych pozwala nam na podjęcie współpracy niezależnie od skali przedsięwzięcia.

Obszary, w których się specjalizujemy to:

Zgodność z przepisami i regulacjami.

Bezpieczeństwo urządzeń występujących w środowisku użytkownika końcowego.

Bezpieczeństwo rozwiązań sieciowych.

Bezpieczeństwo usług serwerowych.

Bezpieczeństwo aplikacji .

Bezpieczeństwo Informacji i Ochrona Danych

Metodyka, którą opracowaliśmy gwarantuje rozsądny dobór zakresu usług i rozwiązań opartych na sprawdzonych standardach. Potrafimy oszacować ryzyko związane z utratą danych, co pozwala naszym Klientom uniknąć znaczących kosztów oraz umożliwia zaplanowanie wydatków na bezpieczeństwo zgodnie ze stanem faktycznym oraz realnymi potrzebami.

Nasza oferta w zakresie bezpieczeństwa informacji obejmuje między innymi:

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI/ISMS) zgodnie

z normą PN-ISO/IEC 27001.

Opracowanie polityki bezpieczeństwa lub wybranych procedur.

Audyt zarządzania bezpieczeństwem informacji.

Audyt planów ciągłości działania.

Audyt zgodności z obowiązującymi regulacjami np. z Ustawą o ochronie danych osobowych.

Audyt bezpieczeństwa systemów informatycznych.

Audyt bezpieczeństwa aplikacji.

Audyt powdrożeniowy.

Audyt licencji oprogramowania.

Testy penetracyjne.

Ocena i dobór rozwiązań infrastrukturalnych.

Warsztaty i szkolenia.

Doradztwo w zakresie ochrony danych podlegających ochronie.

Doradztwo i wdrożenia w zakresie systemów backupu danych.

Doradztwo w zakresie szyfrowania wrażliwych danych.

Odtwarzanie poawaryjne danych i systemów.

Wykrywanie i zapobieganie inwigilacji elektronicznej

Wszystkie nasze działania oparte są na oficjalnych metodologiach i zaleceniach :

Norm ISO/IEC 27001: 2005 i ISO/IEC 17799:2005.

Ustawy o ochronie danych osobowych.

Ustawy o ochronie informacji niejawnych.

Ustawy o ochronie baz danych.

Rozporządzenia Rady Ministrów o wymogach systemów IT przetwarzających dane podlegające ochronie.

Rozporządzenia MSWiA o bezpieczeństwie danych osobowych.

Innych obowiązujących dobrych praktykach dotyczących bezpieczeństwa informacji.

Z poważaniem

Piotr Krajewski – Prezes Zarządu

Warszawa, dnia 22 stycznia 2018 r.

Referencje.

1. ASCOMP S. A. z Krakowa (Marta Szymowska).
2. NTT system S. A. z Warszawy (Tadeusz Kurek).
3. IGEPA Polska Sp. z o. o. z Krakowa (Dorota Gajdzińska).
4. FCA Sp. z o. o. z Krakowa (Andrzej Szymowski).
5. PHU „LOBOS" Sp. z o. o. z Krakowa (Marcin Łobos).
6. PH „LOBOS" Sp. J. z Krakowa (Adam Łobos).
7. SUPO CERBER Sp. z o. o. z Krakowa (Józef Seweryn).
8. ZIKO Spółka z ograniczoną odpowiedzialnością z Krakowa (Marzena Karcz).
9. EC Sybil Tech Sp. z o. o. (Marek Oliszewski).
10. FEV Motorentechnik GmbH, Aachen, Germany (Michael Voβ).
11. FEV Polska Sp. z o. o. z Krakowa (Filip Chełmiński, Hermana Ecker).
12. SPACECOM Ltd, Ramat Gan, Izrael (David Pollack).
13. Krakowski Dom Maklerski IDM SA z Krakowa.
14. Comp S. A. z Warszawy (Radosław Frydrych).
15. LEX – Kancelaria Odszkodowawcza Beata Jarzyna Sp. K. z Krakowa (Krzysztof Jarzyna).
16. Bank DnB Nord S. A. z Warszawy (Adam Grześkiewicz) .
17. Fundusz Pożyczkowy Województwa Świętokrzyskiego Sp. z o. o. z Kielc (Krzysztof Kobryń).
18. UPM – KYMMENE Sp. z o. o. z Warszawy (Heikki Taskinen, Andre Faust).
19. Korporacja Budowlana DORACO Sp. z o. o. z Gdańska (Karol Zduńczyk).
20. Kompania Piwowarska S. A. z Poznania (Bartłomiej Stachowiak).
21. Deloitte Advisory Sp. z o. o. z Warszawy (Romuald Paprzycki).
22. R.R. Donnelley Europe Sp. z o. o, z Krakowa (Jan Przepiór).
23. TUiR/TUnŻ Warta SA z Warszawy (Piotr Piasecki).
24. Alior Bank S.A. z Warszawy (Wojciech Sobieraj).
25. Bank BPH S.A. z Warszawy (Paweł Bandurski).
26. Bank Gospodarstwa Krajowego w Warszawie (Karol Pik).
27. Bank Pekao SA (Grzegorz Piwowar).
28 mBank (Dariusz Nalepa)
29. E&Y (Mariusz Witalis)
30. Bank BPS (Joanna Ciarczyńska)
31. Bank Spółdzielczy Limanowa(Adam Dudek)
32. Bank Spółdzielczy Lubaczów (Paweł Kapel)
33. CBB(Piotr Jarosz)
34. GBS BANK z Barlinka (Zbigniew Wielgosz)
35. Santander Consumer Bank (Piotr Żabski)
36. Bank Spółdzielczy w Kielcach (Przemysław Sporek)
37. BGZ PARIBAS S.A. (Ryszard Górny)