Príloha č.1
OBSAHOVÁ ŠPECIFIKÁCIA PREDMETU ZMLUVY

1. BEZPEČNOSTNÝ PROJEKT :

A) bezpečnostný zámer

- základné bezpečnostné ciele
- technické, organizačné a personálne opatrenia na zabezpečenie ochrany OÚ v informačných systémoch prevádzkovateľa
- vymedzenie okolia IS v súvislosti s možným narušením ochrany OÚ v informačných systémoch prevádzkovateľa

B) analýza bezpečnosti

- identifikácia všetkých IS, v ktorých sa spracúvajú osobné údaje dotknutých osôb u prevádzkovateľa
- identifikácia prostredia prevádzkovaných informačných systémov (fyzický priestor, technické prostriedky spracúvania, ostatné technické prostriedky)
- vytvorenie zoznamu aktív, zraniteľností, hrozieb a ich ohodnotenie
- identifikácia a kvalitatívna analýza relevantných rizík a ich ohodnotenie
- návrh ochranných opatrení na elimináciu identifikovaných rizík

C) bezpečnostné smernice

- smernica na zabezpečenie prevádzky informačných systémov
- pravidlá manipulácie s citlivými dátami
- smernica na ochranu osobných údajov
- plány na riešenie havarijných stavov informačných systémov

Normy, z ktorých sa vychádza pri spracovaní dokumentácie:

Pre vypracovanie bezpečnostnej dokumentácie na ochranu osobných údajov zhotoviteľ vychádza z požiadaviek národnej legislatívy, teda v čase tvorby ponuky platného zákona na ochranu osobných údajov č. 122/2013. Ďalej je východiskom súbor medzinárodných štandardov pre systémy riadenia informačnej bezpečnosti ISO 27001 a súvisiacich predpisov a z požiadaviek výnosu MF č.312/2010 pre bezpečnosť ISVS §28 až. §42.

Spôsob získavania informácií k spracovaniu príslušnej dokumentácie:

Pri vypracovaní bezpečnostnej dokumentácie na ochranu OÚ je najdôležitejšou podmienkou správna a jednoznačná identifikácia všetkých informačných systémov, v ktorých prevádzkovateľ spracúva OÚ. Ďalej nasleduje podrobný popis jednotlivých informačných systémov . Táto fáza tvorby projektu je analytickou fázou, ktorá spočíva v získavaní požadovaných informácií prostredníctvom vopred pripravených dotazníkov zhotoviteľa. Poverený zástupca prevádzkovateľa obdrží od audítora súbor otázok ku konkrétnym skutočnostiam v elektronickej forme, ktoré v spolupráci s poverenými oprávnenými osobami vyplní podľa pokynov na dotazníku. Následne pokračuje analytická časť osobnými konzultáciami audítora s oprávnenými osobami poskytujúcimi informácie na ich detailizácii

tak, aby sa spresnili jednotlivé odpovede a odstránili prípadne nejasnosti. Po absolvovaní rozhovorov dostanú jednotlivé oprávnené osoby, ktoré poskytli informácie, dotazníky na ich verifikáciu, kde svojim podpisom potvrdzujú správnosť poskytnutých informácií. (Jeden rovnopis zostáva zamestnancovi, jeden rovnopis získa prevádzkovateľ ako súčasť projektovej dokumentácie a jeden rovnopis je pre zhotoviteľa)

Rozsah dotazníkov k analytickej časti projektu :

Identifikácia informačných systémov. V tejto časti sa zisťujú podrobné informácie o informačných systémoch, v ktorých prevádzkovateľ spracúva OÚ. Dotazník okrem iných obsahuje nasledovné údaje: Názov informačného systému, Zoznam spracúvaných osobných údajov, Zoznam spracúvaných kópii osobných dokladov, Spôsob získavania OÚ, Právny základ IS, Oprávnené osoby, Okruh dotknutých osôb, Sprístupňovanie OÚ z IS, Poskytovanie OÚ z IS, Zverejňovanie OÚ z IS, Prenos OÚ do tretích krajín, Sprostredkovatelia pre spracovanie OÚ z IS, Automatizované prostriedky spracúvania, Neautomatizované prostriedky spracúvania, Umiestnenie IS Automatizovaná forma, Umiestnenie IS neautomatizovaná forma, Logický prístup k automatizovanej forme spracovania.

Každý popis k identifikovanému informačnému systému obsahuje fyzické umiestnenie dát z informačného systému, pričom je zachované individuálne členenie na automatizované dáta a neautomatizované dáta. Z týchto informácií sa generuje zoznam fyzických miest s umiestnením dát z jednotlivých IS. Pre každé fyzické miesto uloženia dát sa vytvára dotazník získavajúci informácie o tomto konkrétnom umiestnení. (Popis fyzického prostredia , použité technické prostriedky na spracovanie v tomto mieste, prijate bezpečnostné opatrenia....). Ďalej popis IS obsahuje informáciu o logickom prístupe k dátam jednotlivých IS. Z tejto informácie vzniká zoznam miest logického prístupu. Každý logický prístup generuje dotazník s informáciami obsahujúcimi popis jednotlivého miesta. Získavajú sa nasledovné informácie: Popis fyzického prostredia, použité technické prostriedky, spôsob autorizácie oprávnených osôb, prijate ochranné opatrenia.

Všetky informácie z analytickej časti tvorby bezpečnostnej dokumentácie sú nevyhnutným predpokladom na spracovanie správnej a konkrétnej analýzy bezpečnosti informačných systémov u prevádzkovateľa. V súvislosti so spracovávaním dotazníkov k analytickej časti projektu sa zhotoviteľ zaväzuje rešpektovať a dodržiavať pokyny zodpovedného zamestnanca Odboru obrany, bezpečnosti a ochrany objednávateľa v súlade s vyhláškou NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení neskorších predpisov tak, aby žiadnym spôsobom nedošlo k narušeniu, resp. ohrozeniu bezpečnosti osôb ani objektov objednávateľa.

Predpokladaný zoznam dokumentov:

Dotazníková štruktúra analytickej časti vyzerá nasledovne:

Dokument obsahujúci zoznam informačných systémov

- Dokumenty obsahujúce informácie o IS 1 až IS X

Dokument obsahujúci zoznam fyzického umiestnenia dát IS

- Dokument obsahujúci popis miesta 1 až X

Dokument obsahujúci zoznam logických prístupov k dátam jednotlivých IS

- Dokument obsahujúci informácie o logickom prístupe 1 až X

Dokument obsahujúci zoznam areálov, v ktorých sa nachádzajú dáta jednotlivých IS.

Dokument obsahujúci zoznam budov v jednotlivých areáloch, v ktorých sa nachádzajú dáta jednotlivých IS.

Z vyššie uvedených dotazníkov analytickej časti, bude vypracovaná bezpečnostná dokumentácia, ktorá bude obsahovať nasledovné dokumenty:

1. Bezpečnostný zámer
2. Analýza bezpečnosti
3. Bezpečnostné smernice
4. Zoznam oprávnených osôb
5. Zoznam zodpovedných osôb
6. Zoznam sprostredkovateľov
7. Vzor poučenia oprávnených osôb.
8. Vzor poverenia zodpovednej osoby.
9. Vzor súhlasu so spracúvaním OÚ.
10. Vzor súhlasu so spracúvaním OD.(osobného dokladu)
11. Evidenčné listy jednotlivých IS. (Prípadne registračné listy ak sa pre daný IS vyžaduje registrácia, alebo osobitná registrácia)
12. Zoznam dôležitých procesov súvisiacich zo spracúvaním OÚ.

Školenie pre oprávnené osoby :

súčasťou implementácie bezpečnostnej dokumentácie bude aj školenie pre oprávnené osoby prevádzkovateľa, ktoré sa bude konať vo vybraných priestoroch prevádzkovateľa.

Rozsah školenia , cca 8 hodín:

1. Legislatívne požiadavky na ochranu osobných údajov v podmienkach SR vrátane súhrnu hlavných zmien v novej legislatívnej úprave a časové lehoty na zosúladenie s požiadavkami novej legislatívnej úpravy.
2. Definície základných pojmov ochrany OÚ, povinnosti prevádzkovateľa, povinnosti zodpovednej osoby, atď .
3. Bezpečnostný projekt a smernice na ochranu osobných údajov v rozsahu :

3a, informačné systémy, v ktorých SP spracúva osobné údaje dotknutých osôb, dôkladné vysvetlenie všetkých informačných systémov

3b, Právny základ spracúvania OÚ., vedenie evidencie IS a ich registrácia

3c, rozsah bezpečnostnej dokumentácie

4. Práva dotknutých osôb.
5. Požiadavky na systém ochrany OÚ (bezpečnostné smernice, bezpečnostný projekt, ochranné opatrenia)
6. Úrad na ochranu OÚ – postavenie, kontrolná a metodická činnosť
7. Informačná bezpečnosť v systéme riadenia ochrany osobných údajov
8. Nástroje na automatizovanú správu dokumentácie zjednodušujúce dohľad nad ochranou OÚ u prevádzkovateľa

2. Systém automatizovanej správy bezpečnostnej dokumentácie :

Licenčné podmienky pre softvérovú aplikáciu na zjednodušenie a sprehľadnenie implementácie systému riadenia ochrany osobných údajov

Zhotoviteľ je autorom softvérovej aplikácie ISSR – integrovaná správa systémov riadenia, ktorá sa skladá z viacerých modulov, pričom jej primárnym cieľom je automatizovaná správa bezpečnostnej dokumentácie, s riadeným prístupom nielen k dokumentácii, ale aj k aktívam spoločnosti – osobným údajom prevádzkovateľa.

Nový zákon č. 122/2013 ukladá prevádzkovateľom mimo iných povinností takisto riadiť manažment bezpečnostných incidentov, vykonávať interné audity za účelom riadenia ochrany osobných údajov,

viesť aktualizovanú databázu oprávnených osôb k jednotlivým informačným systémom, viesť aktualizovanú bezpečnostnú dokumentáciu a udržiavať v organizácii bezpečnostné povedomie pre oprávnené osoby prevádzkovateľa, všetko ako súbor účinných organizačných, personálnych a technických opatrení na zabezpečenie dostupnosti, dôvernosti a integrity spracúvaných osobných údajov. Mnoho z týchto pravidelných činností umožňuje pohodlne vykonávať práve softvérová aplikácia ISSR ako pre zodpovednú osobu, tak aj pre oprávnené osoby.

Implementácia aplikácie prebehne v užívateľskom prostredí kancelárie NRSR.

Súčasťou prác na úspešnej implementácii aplikácie je naplnenie databáz dátami z Bezpečnostného projektu v zmysle tejto ponuky.

Aplikácia funguje v prostredí operačného systému Windows XP a vyšší. Aplikácia je naprogramovaná vo Visual studiu 2010, v prostredí net Framework 4.0, dáta sú uložené v databázovom formáte MS Access.

Aplikácia ISSR garantuje riadený prístup užívateľov k jednotlivým modulom aplikácie.