**REPUBLIKA HRVATSKA**

**FOND ZA ZAŠTITU OKOLIŠA I ENERGETSKU UČINKOVITOST**

**10 000 ZAGREB, RADNIČKA CESTA 80**

**MBS: 1781286, OIB: 85828625994**

**broj telefona: 01/ 5391 800, broj telefaksa: 01/ 5391 810**

**PROJEKTNI ZADATAK**

**DOGRADNJA INFORMACIJSKOG SUSTAVA**

**FONDA ZA ZAŠTITU OKOLIŠA I ENERGETSKU UČINKOVITOST**

**- USKLAĐIVANJE S UREDBOM O ZAŠTITI OSOBNIH PODATAKA (GDPR)**

**Zagreb, travanj 2018.**

**SADRŽAJ**

1. **UVOD**
2. **CILJ PROJEKTA**
3. **TRENUTNO STANJE**
4. **OPSEG POSLOVA I ZADATAKA**
5. **TEHNIČKA I FUNKCIONALNA SPECIFIKACIJA**
6. **ROKOVI**
7. **NAČIN ISPORUKE I KONTROLA KVALITETE**
8. **IZVJEŠĆIVANJE**
9. **UVOD**

Fond za zaštitu okoliša i energetsku učinkovitost (u daljnjem tekstu Fond) osnovan je Zakonom o Fondu za zaštitu okoliša i energetsku učinkovitost ("Narodne novine" broj 107/03 i 144/12) kao izvanproračunski Fond te ima svojstvo pravne osobe s javnim ovlastima. Osnivač Fonda je Vlada Republike Hrvatske.

Prema odredbama Zakona o zaštiti okoliša („Narodne novine“, broj 80/2013, 153/13, 78/15) Fond je osnovan radi osiguranja dodatnih sredstava financiranja projekata, programa i sličnih aktivnosti u području očuvanja, održivog korištenja, zaštite i unapređenja okoliša.

Prema odredbama Zakona o održivom gospodarenju otpadom („Narodne novine“, broj 94/13) Fond organizira i osigurava provođenje sustava gospodarenja posebnim kategorijama otpada.

Fondom upravlja Upravni odbor koji ima predsjednika i šest članova koje imenuje i razrješuje Vlada Republike Hrvatske i direktor Fonda koji vodi poslovanje Fonda te obavlja druge poslove propisane Zakonom. Vlada Republike Hrvatske imenuje i razrješuje članove Upravnog odbora i direktora Fonda.

U svrhu obavljanja djelatnosti koje su propisane zakonodavnim aktima, u Fondu su ustrojenje slijedeće organizacijske jedinice:

Ured direktora

Tajništvo

Sektor zaštite okoliša

Sektor za energetsku učinkovitost

Sektor za fondove EU (Provedbeno tijelo)

Posredničko tijelo - Samostalna služba (za sufinanciranje projekata EU fondova)

Sektor za gospodarenje posebnim kategorijama otpada

Sektor za pravne poslove

Sektor za financijske poslove

Samostalna služba za nabavu

Samostalna služba za kontroling i poslovne procese

Samostalna služba za unutarnju reviziju

1. **CILJ PROJEKTA**

Cilj ovog projekta je dogradnja Informacijskog sustava Fonda za zaštitu okoliša i energetsku učinkovitost, u svrhu zaštite osobnih podataka, a sukladno Uredbi o zaštiti osobnih podataka (General Data Protection Regulation – GDPR), Uredba (EU) 2016/679 Europskog Parlamenta i Vijeća od 27.4.2016.

S obzirom na širinu i multidisciplinarnost poslova koji se u Fondu obavljaju, nužno je osigurati konzultantske usluge vezane uz implementaciju spomenute Uredbe i tehnološka rješenja za zaštitu podataka.

1. **TRENUTNO STANJE**

Aplikativna podrška poslovnim procesima Fonda sastoji se od poslovnog informacijskog sustava (ERP), uredskog poslovanja s upravljanjem dokumentima te aplikativnih rješenja za specifične djelatnosti Fonda.

Uz gotova aplikativna rješenja vanjskih dobavljača, Fond ima i vlastiti razvoj aplikacija.

Postojeće aplikacije izrađene su nad relacijskim bazama podataka – Firebird, SQL Server i Oracle (povremeno-arhivska rješenja) u Microsoft, Delphi i Oracle Forms (povremeno-provjera arhivskih rješenja) programskom okruženju, međutim velika se količina podataka nalazi u pojedinačnim Microsoft Office (većinom Excel tablicama) i PDF dokumentima.

S obzirom na djelatnosti Fonda, informacijski sustav uz podatke kadrovske evidencije, sadrži i velik broj osobnih podataka obveznika plaćanja naknada, korisnika sredstava Fonda i ostalih partnera.

Informatička infrastrukturna podrška ključnim poslovnim procesima Fonda sastoji se od tri (3) poslužitelja postavljenih u klaster, dedicirana za virtualizaciju, gdje se koristi VmWare ESX zajedno s poslužiteljem namijenjenim za sustav njihovog upravljanja (Virtual centar).

Osnovne karakteristike poslužitelja :

|  |
| --- |
| **Poslužitelji HP DL380G8** |
| CPU | Intel Xeon šesterojezgreni model E5-2667 |
| BROJ CPU | 2 šestojezgrena procesora |
| CACHE L2 | 1x15MB L3 priručne memorije po procesoru |
| RAM | 144 GB DDR (1333Mhz) Advanced ECC Fully Buffered DIMM's, proširivo do maksimalno 384 GB |

Ostali poslužitelji, stariji modeli HP Proliant serije, namijenjeni su za pojedinačne funkcije potrebne u sustavu Fonda kao što su: backup, samostalni odvojeni DC, telefonska centrala i sl.

Operativni sustavi koji se koriste su najvećim dijelom Microsoft bazirani OS, dok se Linux operativni sustavi koriste za specifične svrhe pojedinih poslužiteljskih, upravljačkih i nadzornih potreba i alata.

|  |  |
| --- | --- |
| **Sistemska software-ska platforma** | **Količina** |
| Microsoft Windows server 2012 R2  | 22 |
| Microsoft Windows server 2008 R2 | 4 |
| Microsoft Windows server 2003 | 1 |
| SuSe Linux server  | 2 |
| UBuntu Linux server NTS | 1 |
| Microsoft TMG | 1 |
| Microsoft Exchange | 2 |
| Microsoft SQL ENTERPRISE (2008 i 2016- odnosno najnoviji) | 3 |
| Firebird 257 | 1 |
| Vmware ESXi (3 poslužitelja) + vCenter (1 poslužitelj) | 4 |
| Veeam Backup & Replication | 1 |
| McAffee antivirusno rješenje | 2 |
| Microsoft Windows 7 i Microsoft 10 klijenti | 300 |

Klijenti u Fondu rade na Windows 7 PRO i Windows 10 PRO operativnim sustavima. Minimalna radna memorija radnih stanica iznosi 4 GB.

Fond koristi HP te novije IBM storage uređaje i trenutno ima raspoloživo 32 TB diskovnog prostora, čije je proširenje u tijeku. Koriste se SAS, SATA, SSD diskovi.

Interna mreža Fonda ima propusnost 1Gbit/s, a vanjska mreža 200/200 Mbit/s.

Prostorije Fonda smještene su na jednoj lokaciji, u dvije spojene zgrade na adresi Naručitelja, povezane optičkim kabelom, s najvećim međusobnim udaljenostima oko 150 metara. Mrežni preklopnici su HP i Cisco.

Fond raspolaže sustavima za besprekidno napajanje kako za centralni sustav (do 3 sata rada) tako i za klijente i lokacijske preklopnike (do 30 min rada).

Fond ima razrađen sustav spremanja podataka (backup) koji obuhvaća spremanje podataka na matičnoj lokaciji i udaljeni DR (Disaster Recovery Site) koji je u mogućnosti preuzeti poslovanje u kritičnim situacijama.

1. **OPSEG POSLOVA I ZADATAKA**

Projekt „Dogradnja Informacijskog sustava Fonda za zaštitu okoliša i energetsku učinkovitost – usklađivanje s Uredbom o zaštiti osobnih podataka (GDPR) obuhvaća analizu stanja, konzultativne usluge, aplikativna rješenja i podatkovne strukture s pripadajućom dokumentacijom, izobrazbom zaposlenika - korisnika sustava, svim potrebnim licencama, te održavanjem u jamstvenom roku koji se određuje kao prvih šest (6) mjeseci po puštanju sustava u rad.

Od Ponuditelja se očekuje dobro poznavanje i stalno praćenje zakonodavstva vezanog uz predmet nabave, kako bi mogao promptno reagirati na sve izmjene u zakonodavstvu u smislu prilagodbe i nadogradnje aplikativnih rješenja te davati konstruktivne savjete i prijedloge kako za vrijeme trajanja projekta dogradnje sustava, tako i kasnije u fazi produkcije.

U sklopu ovog projekta treba napraviti:

1. Analizu osobnih podataka i poslovnih procesa u svrhu usklađivanja istih s Uredbom o zaštiti osobnih podataka
2. Sigurnosnu reviziju informacijskog sustava Fonda vezanu uz upravljanje i zaštitu osobnih podataka
3. Analizu pravnog aspekta vezanog za usklađivanje s Uredbom o zaštiti osobnih podataka
4. Savjetovanje u provedbi organizacijskih i pravnih mjera usklađenja
5. Nabaviti i implementirati sustav za pretraživanje repozitorija, praćenja tijeka osobnih podataka i sprječavanja kompromitiranja, neovlaštene upotrebe i prijenosa osobnih podataka zajedno s pratećim uslugama
6. Nabaviti i implementirati sustav za klasifikaciju podataka zajedno s pratećim uslugama
7. Nabaviti i implementirati sustav za upravljanje informacijskom imovinom, rizicima, bazom znanja, evidencijama osobnih podataka, zahtjevima i privolama ispitanika zajedno s pratećim uslugama

U sklopu održavanja u jamstvenom roku (najmanje 6 mjeseci po puštanju sustava u rad) traži se da:

1. odabrani Ponuditelj organizira 24 satnu tehničku podršku, 7 dana u tjednu,
2. intervencije obavlja u najkraćem mogućem roku,
3. očekuje se stabilan rad sustava u dužem razdoblju.

Vezano za održavanje sustava u ponuđenom garantnom roku (najmanje 6 mjeseci po puštanju sustava u rad), očekuje se poduzimanje slijedećih aktivnosti:

* Preventivne aktivnosti

Preventivne aktivnosti podrazumijevaju periodičnu provjeru i kontrolu rada sustava čime se osigurava ispravan rad sustava i pravovremena reakcija u slučaju potrebe. Provjera i kontrola obuhvaćaju pregled trenutnog stanja podatkovnih struktura, aplikativnih poslužitelja i aplikacija sustava, te pregled datoteka sa zabilješkama o radu sustava (logova) direktno s lokacije Ponuditelja u svrhu identifikacije mogućih budućih problema u radu sustava. U slučaju otkrivanja naznaka mogućih problema, Ponuditelj će poduzeti sve potrebne zahvate nad podatkovnim strukturama i aplikativnim rješenjima da spriječi moguće zastoje u radu sustava.

Jednom mjesečno Naručitelju se podnosi izvještaj o stanju podatkovnih struktura i aplikacijskog sustava uz prijedlog za eventualne promjene konfiguracije kako bi se osigurala pouzdanost i funkcionalnost sustava.

* Korektivne aktivnosti

Korektivne aktivnosti uključuju otklanjanje uzroka zastoja, odnosno nepravilnosti u radu ili analize u slučaju sumnje na neispravnost. Izvršitelj ih obavlja po pisanoj prijavi zastoja, sumnje na grešku ili neispravnosti u radu, zaprimljenoj fax-om, poštom ili elektroničkim putem od ovlaštenog predstavnika Naručitelja. Obveza je Ponuditelja promptno reagiranje i dijagnosticiranje problema, bez obzira na razlog greške i uzročnika, te dovođenje sustava u funkcionalno stanje.

Do otklanjanja će doći ukoliko se utvrdi neusuglašenost između funkcioniranja software-a i software-ske dokumentacije, a ta se nepodudarnost može pripisati programu ili dokumentaciji. Nepodudarnost će biti otklonjena ukoliko se može reproducirati i/ili dokumentirati. Izvršitelj će dati predvidivi rok otklanjanja nepodudarnosti. U nepodudarnosti ne spadaju problemi vezani uz nepravilno funkcioniranje opreme (hardware) i osnovnog i/ili operacijskog software-a.

* Adaptivne aktivnosti

Adaptivne aktivnosti obuhvaćaju aplikativne izmjene postojećeg sustava inicirane promjenama u software-skoj okolini (novi sistemski software, novi hardware, povezivanje s novim aplikacijama u sustavu itd.) ili promjenama u zakonskoj regulativi koje zahtijevaju usklađivanje postojećih funkcionalnosti aplikacijskog sustava, poboljšanje performansi sustava zbog povećanog broja korisnika, unaprjeđenje korisničkog sučelja radi jednostavnijeg i bržeg obavljanja aktivnosti.

Izmjene se obavljaju prema pisanom zahtjevu Naručitelja.

U opsegu ugovora koji proizlazi iz ove nabave za adaptivne aktivnosti ulazi angažman do 40 ing/h stručnog osoblja Ponuditelja. U slučaju prekoračenja 40 ing/h i potrebe za većim angažmanom, takav angažman se dodatno naručuje i ugovara.

Za vrijeme trajanja garantnog roka, Ponuditelj je dužan osigurati raspoloživost stručnog osoblja za obavljanje Perfektivnih aktivnosti kako je specificirano u nastavku, ali obavljanje usluga Perfektivnih aktivnosti nije u opsegu ugovora koji proizlazi iz ove nabave i takve se usluge dodatno naručuju i ugovaraju.

* Perfektivne aktivnosti

Perfektivne aktivnosti uključuju sve aplikativne izmjene koje nisu otklanjanje grešaka u radu sustava i koje ne spadaju u adaptivne aktivnosti, a imaju za cilj unapređenje postojećih mogućnosti sustava u skladu s novonastalim ili modificiranim potrebama Naručitelja. Pod aplikativnim izmjenama podrazumijeva se funkcionalno proširenje sustava uslijed promjene zakonske regulative, primjene novih propisa ili ispunjenja novih obveza prema institucijama Republike Hrvatske i međunarodnim institucijama, odnosno uslijed drugih potreba promjena opsega projekta.

Dorade i izmjene se obavljaju prema pisanom zahtjevu Naručitelja koji sadržava popis i opis potrebnih funkcionalnosti na temelju kojih Izvršitelj daje financijsku procjenu i procjenu potrebnog vremena.

Perfektivne aktivnosti razvoja i nadogradnje će se dokumentirati, a vrijednost perfektivne aktivnosti se mora prije usuglasiti s Naručiteljem. Perfektivne aktivnosti razvoja i nadogradnje se dokumentiraju projektnom dokumentacijom.

Svi potencijalni rizici i način upravljanja promjenama, kao i detaljna strukturna raščlamba poslova, uloge i odgovornosti, detaljni terminski plan, način komunikacije i svi ostali ključni detalji bit će definirani najkasnije 30 dana od početka radova tj. potpisivanja ugovora, realizacijom prvog tehničkog dokumenta: Izjavom o opsegu aktivnosti (Activity/Project Scope Statement) te ažuriranjem istog tijekom provedbe.

1. **TEHNIČKA I FUNKCIONALNA SPECIFIKACIJA**

Ponuditelj mora isporučiti programska rješenja (softver) s originalnim licencama i usluge stručnjaka kako je traženom ovim predmetom nabave. Ponuđena programska rješenja moraju minimalno zadovoljiti sve funkcionalne i tehničke zahtjeve iz Tablica 1., 2. i 3. Funkcionalnih i tehničkih zahtjeva u Projektnom zadatku. Ponuditelj u svojoj ponudi prilaže Obrasce 3., 4. i 5. *Tehnička specifikacija* za tražene sustave. Ponuditelj je za svaki zahtjev iz tablica iz Projektnog zadatka, dužan u Obrascima *Tehničke specifikacije* ponuditi adekvatan odgovor i navesti dokaz podržane funkcionalnosti ili tehničke karakteristike na način da u stupcu " *Bilješke, napomene, reference na tehničku dokumentaciju*" upiše poveznicu sa stranicom u tehničkoj dokumentaciji u ponudi gdje se nalazi opisana zahtijevana karakteristika. Ponuditelj je dužan u okviru ponude za tražena programska rješenja dostaviti tehničku dokumentaciju proizvođača iz koje je vidljivo da ponuđeno programsko rješenje ispunjava tražene zahtjeve. Tehnička dokumentacija proizvođača ponuđenog rješenja može biti na hrvatskom ili engleskom jeziku.

Ponuda mora uključivati originalno jamstvo proizvođača (eng. maintenance) na sve ponuđene licence iz ovog predmeta nabave u trajanju od minimalno 1 godine od trenutka izdavanja licenci. Jamstvo mora uključivati pravo na nove verzije softvera, otklanjanje grešaka u softveru te pravo na tehničku podršku proizvođača putem otvaranja servisnih prijava u sustavu proizvođača.

Naručitelj osigurava hardversku infrastrukturu, VMware virtualnu okolinu i licence i Microsoft licence za operativne sustave i MS SQL bazu podataka.

**5.1. Analiza osobnih podataka i poslovnih procesa u svrhu usklađivanja istih s Uredbom o zaštiti osobnih podataka**

5.1.1. Pregled i analiza svih tipova i zbirki osobnih podataka koji se obrađuju u sklopu poslovanja organizacije, uzimajući u obzir proširenu definiciju osobnih podataka sukladno GDPR

5.1.2. Pregled i analiza procesa nastanka, upravljanja i toka podataka u organizaciji, unutar kojih se obrađuju osobni podaci

5.1.3. Pregled i analiza postojeće dokumentacije vezane uz zaštitu osobnih podataka. Analiza utjecaja novih prava vlasnika podataka na poslovne procese

**5.2. Sigurnosna revizija informacijskog sustava Fonda vezana uz upravljanje i zaštitu osobnih podataka**

5.2.1. Snimka IT servisa vezanih uz poslovne procese

5.2.2. Snimka postojećih mjera zaštite podataka i specijaliziranih sigurnosnih rješenja

5.2.3. Procjena rizika naspram zaštite osobnih podataka

**5.3. Analiza pravnog aspekta vezanog za usklađivanje s Uredbom o zaštiti osobnih podataka**

5.3.1. Identifikacija svih primjenjivih zakonskih i strukovnih propisa spram zaštite osobnih podataka te analiza mogućnosti izmjene i dopune istih u smislu usklađivanja s Uredbom o zaštiti osobnih podataka

5.3.2. Pregled i analiza postojećih poslovnih odnosa FZOEU s trećim stranama vezano uz obradu i čuvanje osobnih podataka

5.3.3. Definicija pravnog statusa u odnosu na treće strane (*Data Controller* i/ili *Processor)*

5.3.4. Analiza tipičnih ugovora između FZOEU i njegovih poslovnih partnera s aspekta obrade osobnih podataka

**5.4. Izrada Objedinjenog izviješća**

Nakon izvršenih navedenih usluga, Ponuditelj je dužan isporučiti dokumentaciju (objedinjeni izvještaj) za sva tri segmenta vezano uz savjetodavne usluge sukladno zahtjevima navedenim u točkama 5.1, 5.2 i 5.3. Dokumentacija mora biti usuglašena s FZOEU te obostrano potpisan primopredajni zapisnik od strana ovlaštenih osoba oba pravna subjekta.

Objedinjeni izvještaj treba sadržavati:

5.4.1. Specifikaciju zatečenog stanja, identifikaciju procesa s aspekta upotrebe osobnih podataka te prijedloge za poboljšanje i ostvarivanje sukladnosti s Uredbom

5.4.2. Izradu metodologije za procjenu i preporuka za tretiranje rizika vezano uz zaštitu podataka, koju bi FZOEU koristio i nakon završetka projekta

5.4.3. Detaljnu evidenciju zatečenog sigurnosnog stanja

5.4.4. Detaljnu analiza tehničke ICT infrastrukture i prijedlog za realizaciju tehnoloških rješenja za identificirane poslovne zahtjeve

5.4.5. Evidenciju zatečenog stanja propisa referentnih za poslovanje Fonda

5.4.6. Prijedlog izmjena i dopuna legislativnih akata kojima će FZOEU zaštititi interese vezano uz primjenu Uredbe, prijedlog metodologije za upravljanje ugovorima i prijedlog za uspostavu pravnog okvira za prekograničniprijenos podataka

**5.5. Projektni plan, projektni timovi i edukacija**

Po provedenoj snimci stanja i prihvaćenom Objedinjenom Izviješću od strane ovlaštenih predstavnika Naručitelja, Ponuditelj će u suradnji s Fondom:

5.5.1. Izraditi detaljan Projektni plan

5.5.2. Formirati Projektne timove

5.5.3. Održati najmanje jednu radionicu za definiranje poslovnih potreba (Business Requirements Workshop)

5.5.4. Održati jednu informativnu radionicu za ključne ljude unutar FZOEU vezano uz implementaciju sukladnosti s Uredbom

5.5.5. Izraditi plan i sadržaj edukacije zaposlenika Fonda s ciljem unapređenja svijesti potrebe zaštite osobnih podataka

**5.6. Savjetovanje u provedbi organizacijskih i pravnih mjera usklađenja**

U ovoj fazi treba se pružiti savjetodavna podrška Naručitelju u usklađivanju postojećih internih akata te pripremi novih u svrhu potpunog usklađivanja s Uredbom. To podrazumijeva pripremu potrebnih internih akata za reguliranje svih obveza Naručitelja koje proizlaze iz Uredbe po pitanju zaštite osobnih podataka koje obrađuje, uključujući zaštitu njihove povjerljivosti, integriteta i raspoloživosti te mogućnost adekvatnog upravljanje incidentima koji mogu ugroziti osobne podatke.

Također, Naručitelju se treba pružiti i pravna podrška u usklađivanju ugovora koje Naručitelj ima sa svojim dobavljačima i općenito izvršiteljima obrade.

Isporuka ovog segmenta treba biti u obliku izrađenih internih akata kojima se regulira način zadovoljenja zahtjeva Uredbe.

**5.7. Sustav za pretraživanje repozitorija, praćenja tijeka osobnih podataka i sprječavanja kompromitiranja, neovlaštene upotrebe i prijenosa osobnih podataka**

Ponuditelj mora isporučiti sustav za pretraživanje repozitorija, praćenja tijeka osobnih podataka i sprječavanja kompromitiranja, neovlaštene upotrebe i prijenosa osobnih podataka u obliku programskog rješenja (softvera) zajedno sa originalnim licencama i uslugama implementacije. Sustav i njegova isporuka moraju zadovoljavati sve funkcionalne i tehničke zahtjeve kako je navedeno u Tablici 1.

|  |
| --- |
| **Tablica 1. Sustav za pretraživanje repozitorija, praćenja tijeka osobnih podataka i sprječavanja kompromitiranja, neovlaštene upotrebe i prijenosa osobnih podataka** |
| **Puni naziv ponuđenog sustava:** |
| **Proizvođač ponuđenog sustava:** |
| **Količina i originalni naziv ponuđenih licenci sa kataloškim brojem (P/N – product number):** |
| **Trajanje uključenog proizvođačkog jamstva na ponuđene licence:** |

| **Minimalne zahtijevane funkcionalne i tehničke specifikacije**  |
| --- |
|  |
| Rješenje mora biti u obliku visoko specijalizirane programske podrške (softvera) za pretraživanje repozitorija, praćenja tijeka osobnih podataka i sprječavanja kompromitiranja, neovlaštene upotrebe i prijenosa osobnih podataka u korporativnom okruženju (u daljnjem tekstu DLP - eng. Data Loss Prevention) |
| Rješenje mora uključivati licence za 330 računala i 330 korisnika |
| Rješenje mora biti sveobuhvatno i namijenjeno korporativnim okruženjima te detektirati i kontrolirati podatke u tri različita stanja/oblika:* Data-in-use, DLP na računalu (DLP Endpoint)
* Data-in-motion, DLP na mreži (DLP Prevent for E-mail, DLP Prevent for Web)
* Data-at-rest, DLP discovery funkcionalnosti pretraživanja mrežnih repozitorija i baza podataka (DLP Discover)
 |
| Rješenje mora uključivati zaštitu podataka na radnim stanicama putem DLP Endpoint agenata i kontrolu korištenja odljeva podataka svim potencijalnim kanalima na radnim stanicama. Arhitektura mora podrazumijevati da se na štićena računala implementiraju DLP Endpoint agenti kojima se potpuno upravlja iz centraliziranog administrativnog sučelja. |
| Rješenje mora uključivati komponentu u obliku virtualnog mrežnog uređaja na VMware platformi za kontrolu i zaštitu e-mail poruka (DLP Prevent for E-mail) putem SMTP protokola koristeći dodavanje X header oznaka u e-mail poruke na temelju koje podržano MTA rješenje može poduzeti odgovarajuću sigurnosnu radnju.Komponentom se mora upravljati iz centraliziranog administrativnog sučelja. |
| Rješenje mora uključivati komponentu u obliku virtualnog mrežnog uređaja na VMware platformi za kontrolu i zaštitu web prometa (DLP Prevent for Web) na način da se integrira sa ICAP kompatibilnim web gateway uređajem i na taj način pregledava odlazne mrežne pakete.Komponentom se mora upravljati iz centraliziranog administrativnog sučelja. |
| Rješenje mora uključivati komponentu za pretraživanje mrežnih repozitorija i baza podataka (DLP Discover) sa podrškom za pretraživanje minimalno:* Common Internet file system/ server message block (CIFS)
* Network file system (NFS)
* Baze podataka: Microsoft SQL, IBM DB2, MySQL Enterprise, Oracle
* Microsoft Sharepoint
 |
| Rješenje mora imati mogućnosti analitike podataka otkrivenih pretraživanjem putem DLP Discover komponente koristeći Online Analytical Processing (OLAP) tehnologiju. |
| Agent na štićenim računalima mora biti potpuno funkcionalan i kada računala nisu spojena na mrežu (off-line mod). |
| Rješenje mora imati podršku za rad i zaštitu minimalno slijedećih operativnih sustava:- Windows 7 SP1 i noviji- Windows Server 2008 R2 i noviji - Mac OS 10.10 i noviji |
| Rješenje mora imati podršku sa minimalno slijedećih Internet preglednicima:- Internet Explorer- Mozilla Firefox- Google Chrome |
| Agent na računalu mora imati podršku za rad sa FastUserSwitching (FUS) u Windows OS okolini sa više korisnika. |
| Rješenje mora podržavati integraciju sa MS Active Directory imeničkim servisom. |
| Rješenje mora omogućiti učinkovitu zaštitu od odjeljiva podataka putem svih od slijedećih kanala: prijenosni mediji, email, web, printing, clipboard, screen capture / print screen, kopiranje na mrežne diskove i vanjske diskove, WiFi, Bluetooth, IM - instant messaging, slanje u cloud servise. |
| Rješenje mora funkcionirati po principu dubinskog pregleda sadržaja digitalnih podataka (eng. Content-based ili content-aware). |
| Rješenje mora imati ugrađenu mogućnost klasifikacije podataka minimalno slijedećim metodama:- rječnici (eng. dictionary)- validacijski algoritmi- registracija dokumenata- ručno tagiranje (digitalno označavanje datoteka)- automatsko tagiranje- whitelisting- podrška za prepoznavanje metadata oznaka specijaliziranih rješenja drugih proizvođača (TITUS i Boldon James) |
| Rješenje mora imati mogućnost izrade i primjene sigurnosnih politika minimalno prema slijedećim kategorijama zaštite pri pokušaju:- slanja e-maila- slanja na web- slanjem putem mreže- slanja na print- kopiranja na prijenosni medij- kopiranja na mrežni disk- kopiranja (clipboard)- screen capture / print screen |
| Rješenje mora imati mogućnost minimalno slijedećih reakcija u slučaju detekcije određene radnje sa osjetljivim podatkom:- bez reakcije- blokiraj- premjesti datoteku- zatraži opravdanje- primijeni RM - rights management politiku- quarantine- tagiraj / označi- otvori DLP incident - prikaži u centralnoj konzoli- obavijesti korisnika- spremi originalnu datoteku - sačuvaj dokaz |
| Rješenje mora imati mogućnosti da zatraži od korisnika da unese opravdanja za iznošenje/slanje podataka (eng. justification). |
| Rješenje mora imati mogućnosti prilagodbe notifikacija za korisnike. |
| Rješenje mora imati mogućnosti privremene deaktivacije agenta. |
| Rješenje mora imati ugrađenu mogućnosti za digitalno označavanje datoteka (eng. content fingerprinting) automatski s obzirom na to koja je aplikacija proizvela datoteka. Na temelju oznake moraju se moći primjenjivati DLP sigurnosne politike. |
| Rješenje mora imati ugrađenu mogućnosti za digitalno označavanje datoteka (eng. content fingerprinting) automatski s obzirom na to sa koje je web aplikacije skinuta datoteka. Na temelju oznake moraju se moći primjenjivati DLP sigurnosne politike. |
| Rješenje mora imati ugrađenu mogućnosti za digitalno označavanje datoteka (eng. content fingerprinting) automatski s obzirom na to sa koje je mrežne lokacije skinuta datoteka. Na temelju oznake moraju se moći primjenjivati DLP sigurnosne politike. |
| Rješenje mora imati ugrađenu mogućnosti za nasljeđivanje digitalne oznake datoteke (eng. content fingerprinting) prilikom kopiranja ili premještanja osjetljivog sadržaja u drugu datoteku na način da se prilikom te radnje parsira sadržaj koji se replicira ili premješta te, u slučaju prepoznavanja, automatski dodjeljuje oznaka (eng. fingerprint). Na temelju oznake moraju se moći primjenjivati DLP sigurnosne politike. |
| Rješenje mora imati ugrađenu mogućnosti učinkovitog upravljanja sigurnosnim politikama putem pravila za zaštitu podataka. Pravila se moraju moći grupirati i dodjeljivati prema objektima u MS Active Directory imeničkom servisu. |
| Rješenje mora imati ugrađenu podršku za skeniranje, analizu i pronalaženje podataka (eng. Discovery scan) na korisničkim računalima koje po pronalasku mora imati minimalnu mogućnosti slijedećih radnji:- prijavi incident u središnjoj DLP konzoli- prikupi dokaz što podrazumijeva kopiranje pronađene datoteke na lokaciju za prikupljanje dokaza radi daljnjeg pregleda i obrade |
| Rješenje mora imati funkcionalnu mogućnost za podizanje svijesti korisnike te kroz poruke i upozorenja na računalu korisnika uključiti ga u proces medijacije. |
| Rješenje mora imati mogućnost standardne integracije sa postojećim rješenjem za enkripciju podataka koje Naručitelj ima na raspolaganju (McAfee Encryption) ili mora uključivati funkcionalnost i licence za enkripciju datoteka, mapa i prijenosnih medija. |
| Rješenje mora imati ugrađenu mogućnosti upravljanja sigurnosnim politikama za prijenosne medije (eng. Device Control ili Removable Media Control) koje raspolaže minimalno sa slijedećim mogućnostima:- filtriraj- nadgledaj (monitor)- blokiraj prijenos osjetljivih sadržaja na prijenosne medije |
| Upravljanje politikama za prijenosne medije mora uključivati mogućnost primjene odabirom minimalno slijedećih kriterija:- korisnik i grupa korisnika- računalo- product ID- ID proizvođača- serijski broj- klasa uređaja- naziv uređaja |
| Upravljanje politikama za prijenosne medije mora uključivati mogućnost primjene prema redu. |
| Rješenje mora imati ugrađenu mogućnost da učini određeni prijenosni mediji blokiranim ili read-only. |
| Rješenje mora imati mogućnost integracije sa rješenjima za enkripciju datoteka i mapa. |
| Rješenje mora imati mogućnost integracije sa DRM (Digital Rights Management) rješenjima i to minimalno MS AD RMS. |
| Rješenje mora imati mogućnost integracije sa specijaliziranim rješenjima za klasifikaciju i označavanje podataka koja rade na principu da datotekama dodaju meta podatke (eng. metadata). DLP rješenje mora biti u mogućnosti detektirati takav podatak prema prepoznatim meta podacima te automatski primijeniti određenu sigurnosnu politiku. |
| Rješenje mora imati mogućnost blokiranja pristupa podacima kod mapiranih uređaja na tankim klijentima i to minimalno:- lokalnim diskovima- prijenosnim medijima- printerima- CD/DVD- clipboard |
| Rješenjem se mora upravljati putem centralizirane upravljačke konzole u obliku web aplikacije. |
| Centralna upravljačka konzola mora biti prilagodljiva korisničkim zahtjevima (eng. customizable). |
| Centralna upravljačka konzola mora imati mogućnosti da se sučelje prilagođeno za jednog korisnika može jednostavno primijeniti i na druge korisnike. |
| Centralna upravljačka konzola mora imati mogućnosti izrade naprednih izvještaja i mogućnost da se izvještaji prikažu u obliku dashboarda u konzoli. Izvještaji se moraju moći izvesti (eng. export) ili automatski poslati e-mailom. |
| Rješenje mora imati mogućnosti podešavanja automatiziranih dnevnih aktivnosti. |
| Centralna upravljačka konzola mora podržavati granulirano upravljanje korisničkim pravima putem uloga (RBAC – Roled Based Access Control). |
| Rješenje mora imati mogućnost naknadne integracije sa rješenjem za zaštitu od naprednih prijetnji (eng. APT - Advanced Persistent Threats). |
| Rješenje mora imati mogućnosti iz centralne upravljačke konzole udaljeno implementirati agente na računala i kasnije njima upravljati. |
| Povezani incidenti moraju se moći grupirati u slučaj "case" koji se zatim može delegirati nadležnom korisniku na daljnju obradu. |
| Rješenje mora podržavati mogućnost da se definiraju korisnici sa posebnim pravima nad pojedinim elementima u sustavu (eng. stakeholders) koji bivaju automatski notificirani kada se dogodi određena vrsta incidenta ili koji imaju posebne privilegije u sustavu. |
| Rješenje mora imati dostupno API sučelje. |
| Rješenje mora omogućiti iz centralne upravljačke konzole izradu detaljnih izvještaja koji pokazuju auditorima, upravi i ostalim interesnim stranama informacije vezane uz interne i regulatorne sigurnosne sukladnosti. |

Uz sve gore navedeno, Ponuda mora uključivati stručne usluge Ponuditelja kako slijedi:

**Implementacija**

**Analiza**

* izrada upitnika za implementaciju sustava
* snimka postojećih poslovnih procesa i njihovih prioriteta, pravilnika i infrastrukture neophodnih za implementaciju sustava
* organiziranje Data Governance radionica za prikupljanje informacija od korisnika koje točno poslovne informacije je potrebno štititi i na koji način - definiranje politika;
* definiranje elemenata infrastrukture na kojima će se raditi zaštita podataka:

**Dizajn rješenja**

* dizajn arhitekture rješenja;
* definiranje sigurnosnih politika i postavki:
* definiranje rasporeda skeniranja i repozitorija koji će se skenirati;
* izrada dokumenta prijedloga rješenja.

**Instalacija i konfiguracija rješenja**

* Instalacija i inicijalna konfiguracija
* Integracija u postojeću infrastrukturu
* Izrada i konfiguracija sigurnosnih politika i postavki:
* Implementacija rješenja na pilot grupi računala (do 20 računala)
* Prikupljanje i analiza povratnih informacija od korisnika;
* Dorada, ispravljanje i fino podešavanje sigurnosnih politika;
* Priprema za produkciju

**Obuka**

Usluge obuke osoblja Naručitelja. Obuka će se sastojati od teoretskog i praktičnog dijela u trajanju od ukupno 2 dana tako da pruži neophodna znanja za administratore i operatere sustava te službeniku za zaštitu osobnih podataka. Obuku provodi Ponuditelj.

**Izrada dokumentacije**

Izvedbena dokumentacija za implementirani sustav sa detaljno opisanim rješenjem i pojedinačnim komponentama;

**5.8. Sustav za klasifikaciju podataka**

Ponuditelj mora isporučiti sustav za klasifikaciju podataka u obliku programskog rješenja (softvera) zajedno sa originalnim licencama i uslugama implementacije. Sustav i njegova isporuka moraju zadovoljavati sve funkcionalne i tehničke zahtjeve kako je navedeno u Tablici 2.

|  |
| --- |
| **Tablica 2. Sustav za klasifikaciju podataka** |
| **Puni naziv ponuđenog sustava:** |
| **Proizvođač ponuđenog sustava:** |
| **Količina i originalni naziv ponuđenih licenci sa kataloškim brojem (P/N – product number):** |
| **Trajanje uključenog proizvođačkog jamstva na ponuđene licence:** |

| **Minimalne zahtijevane funkcionalne i tehničke specifikacije**  |
| --- |
| Specijalizirano industrijski prepoznato programsko rješenje (softver) za klasifikaciju i označavanje digitalnih podataka (eng. labelling tool) koje uključuje minimalno module za klasifikaciju:* MS Office dokumenata
* E-mail poruka u MS Outlook konzoli
* Bilo kakvih tipova podataka na MS Windows OS-u
 |
| Rješenje mora uključivati licence za 330 računala i 330 korisnika koji na njima rade. |
| Arhitektura rješenja mora podrazumijevati da se na štićena računala implementiraju agenti kojima se upravlja iz centralne upravljačke konzole pokretane na poslužitelju. |
| Rješenjem se mora upravljati putem centralizirane upravljačke konzole u obliku web aplikacije. |
| Agent na štićenim računalima mora biti potpuno funkcionalan i kada računala nisu spojena na mrežu (off-line mod). |
| Rješenje mora imati podršku za rad i zaštitu minimalno slijedećih operativnih sustava:* Windows 7 SP1 i noviji
 |
| Rješenje mora funkcionirati kao proširenje standardnih MS Office alata na način da se u alatnu traku ugrade dodatne funkcionalnosti – meni za odabir klasifikacije i to minimalno za alate:* MS Word
* MS Excel
* MS PowerPoint
* MS Outlook
 |
| Rješenje mora omogućiti korisnicima da odabirom klasifikacije podataka rješenje automatski doda vizualne oznake na dokument i “persistent metadata” oznaka u svojstva dokumenta. |
| Rješenje mora imati mogućnosti klasifikacije bilo koje datoteke na MS Windows operativnom sustavu na način da se korisniku omogući da desnim klikom dođe do izbornika gdje odabire prethodno definirane razine klasifikacije i time klasificira/označi datoteku |
| Rješenje mora omogućavati dodavanje vizualnih oznaka MS Office dokumentima i Outlook e-mail porukama. |
| Rješenje mora podržavati da MS Office dokumenti proizašli iz prethodnih verzija dokumenta nasljeđuju klasifikaciju. |
| Rješenje mora imat mogućnost prilagodbe razina klasifikacije i vizuala za dokumente. |
| Korisnici moraju biti u mogućnosti odabrati razinu klasifikacije dokumenata u izborniku. |
| Rješenje mora omogućiti vlastite razine klasifikacije koje odredi Naručitelj. |
| Rješenje mora omogućavati nametanje obavezne klasifikacije kod spremanja datoteka. |
| Rješenje mora podržavati punu integraciju sa MS AD imeničkim servisom na temelju kojeg se dodjeljuju sigurnosne politike. |
| Rješenje mora podržavati integraciju sa MS AD Rights Management Service (RMS) rješenjem na način da je moguće automatski primijeniti RMS politiku na klasificiranu datoteku. |
| Rješenje mora omogućiti evidenciju korisničkih aktivnosti i izvještavanje. |

Uz sve gore navedeno, Ponuda mora uključivati stručne usluge Ponuditelja kako slijedi:

**Implementacija**

**Analiza**

* izrada upitnika za implementaciju sustava
* snimka postojećih poslovnih procesa i njihovih prioriteta, pravilnika i infrastrukture neophodnih za implementaciju sustava
* organiziranje Data Governance radionica za prikupljanje informacija od korisnika koje točno poslovne informacije je potrebno štititi i na koji način - definiranje politika;
* definiranje elemenata infrastrukture na kojima će se raditi zaštita podataka:

**Dizajn rješenja**

* dizajn arhitekture rješenja;
* definiranje sigurnosnih politika i postavki:
* definiranje rasporeda skeniranja i repozitorija koji će se skenirati;
* izrada dokumenta prijedloga rješenja.

**Instalacija i konfiguracija rješenja**

* Instalacija i inicijalna konfiguracija
* Integracija u postojeću infrastrukturu
* Izrada i konfiguracija sigurnosnih politika i postavki:
* Implementacija rješenja na pilot grupi računala (do 20 računala)
* Prikupljanje i analiza povratnih informacija od korisnika;
* Dorada, ispravljanje i fino podešavanje sigurnosnih politika;
* Priprema za produkciju

**Obuka**

Usluge obuke osoblja Naručitelja. Obuka će se sastojati od teoretskog i praktičnog dijela u trajanju od ukupno 2 dana tako da pruži neophodna znanja za administratore i operatere sustava te službeniku za zaštitu osobnih podataka. Obuku provodi Ponuditelj.

**Izrada dokumentacije**

Izvedbena dokumentacija za implementirani sustav sa detaljno opisanim rješenjem i pojedinačnim komponentama;

**5.9. Sustav za upravljanje informacijskom imovinom, rizicima, bazom znanja, evidencijama osobnih podataka, zahtjevima i privolama ispitanika**

Ponuditelj mora isporučiti sustav za upravljanje informacijskom imovinom, rizicima, bazom znanja, evidencijama osobnih podataka, zahtjevima i privolama ispitanika u obliku programskog rješenja (softvera) zajedno sa originalnim licencama i uslugama implementacije. Sustav i njegova isporuka moraju zadovoljavati sve funkcionalne i tehničke zahtjeve kako je navedeno u Tablici 3.

|  |
| --- |
| **Tablica 3. Sustav za upravljanje informacijskom imovinom, rizicima, bazom znanja, evidencijama osobnih podataka, zahtjevima i privolama ispitanika** |
| **Puni naziv ponuđenog sustava:** |
| **Proizvođač ponuđenog sustava:** |
| **Količina i originalni naziv ponuđenih licenci sa kataloškim brojem (P/N – product number):** |
| **Trajanje uključenog proizvođačkog jamstva na ponuđene licence:** |

| **Minimalne zahtijevane funkcionalne i tehničke specifikacije**  |
| --- |
| **Opći zahtjevi i arhitektura sustava** |
| Specijalizirano industrijski prepoznato programsko rješenje (softver) za upravljanje informacijskom imovinom, rizicima, bazom znanja, evidencijama osobnih podataka i privolama ispitanika |
| Rješenje mora uključivati licence za 1 sustav bez ograničenja na broj analitičara, korisnika, IT servisa, rizika niti drugih ograničenja |
| Informatičko/aplikativno programsko rješenje u obliku dvoslojne aplikacije: * Web aplikativni dio
* Podatkovni dio / baza podataka
 |
| MS SQL baza podataka (osigurava Naručitelj) |
| Podržani različiti web preglednici (Internet Explorer, Chrome, Firefox, Opera). |
| API sučelje |
| Podrška za različite korisničke uloge u sustavu. |
| Mogućnost da korisnici sami mijenjaju svoje zaporke. |
| Mogućnost postavljanja politike zaporki. |
| Sučelje lokalizirano na hrvatski jezik |
| Način rada jedinstven kroz cijeli sustav. |
| Podaci na svim ekranima su pretraživi po više kriterija (jednako, sadrži, počinje s, veće od, manje od, između i sl.) |
| Pojedine prikaze u sustavu je moguće ispisati u više poznatih formata (PDF, Word, Excel, slike). |
| **Upravljanje informacijskom imovinom i procjena rizika** |
| Kreiranje popisa informacijske imovine i vrednovanje. |
| Organizacija procjene rizika po projektima. |
| Praćenje povijesti vrednovanja rizika. |
| Automatsko kreiranje rizika iz baze znanja. |
| Automatski izračun rizika na temelju statusa implementiranih kontrola. |
| Grupno izračunavanje rizika.  |
| Kreiranje plana implementacije kontrola. |
| Definiranje odgovornosti za obradu rizika. |
| Veza sa sustavom unutarnjih kontrola. |
| Odabir kontrola iz baze znanja. |
| Izvještavanje o rizicima po procesima. |
| Mogućnost brzog vrednovanja rizika u „data sheet“ modu (ažuriranje kao u Excel tablici). |
| Distribucija procjene rizika na više korisnika. Korisnici mogu sami procjenjivati rizike za koje su odgovorni. |
| Podržan uvoz informacijske imovine iz Excela, CSV-a |
| **Baza znanja** |
| Baza znanja kontrola i njihovih veza s poznatim standardima (ISO 27001:2013, ISO 27002:2013, ISO 22301:2012, CobiT, NIST, GDPR). |
| Popis prijetnji i grupa imovine. Gotovi katalozi prijetnji i grupa imovine. |
| Mogućnost kreiranja vlastitih grupa i veza između prijetnji, imovine i kontrola. |
| Prijavom kao administrator moguće je sve pripremljene kataloge izmijeniti po vlastitoj želji. |
| Izmjena kataloga vjerojatnosti, utjecaja, veličine rizika, statusa i tipova entiteta i sl. |
| Uvoz podataka iz vanjskih izvora za gotovo sve kataloge putem web formi. |
| Automatsko kreiranje SoA izvješća (Statement of Applicability). |
| **Katalog IS servisa i procesa te procjena usklađenosti** |
| Izrada kataloga IT servisa. |
| Izrada kataloga poslovnih procesa. |
| Set podataka potreban za izradu analize utjecaja na poslovanje (engl. BIA – Business Impact Analysis). |
| Automatsko generiranje plana oporavka IT servisa na temelju unesenih podataka  |
| Povijesno praćenje statusa revizija kontrola. |
| Upravljanje nalazima/ranjivostima. |
| **Izrada izvještaja** |
| Sve ekrane je moguće ispisati u više poznatih formata (PDF, Word, Excel, slike). |
| Set osnovnih izvješća poput popisa imovine i prijetnji, popisa rizika, statusa usklađenosti po raznim standardima (ISO 27001:2013, ISO 27002:2013, ISO 22301:2012, CobiT, NIST, GDPR). |
| Dio izvješća je moguće prikazati i u grafičkom formatu („dashboard“ stranica s više grafova). |
| Jednostavno sortiranje i filtriranje sadržaja izvještaja po gotovo svim parametrima. |
| Logo korisnika u izvješćima. |
| **Upravljanje evidencijama osobnih podataka** |
| Sve ekrane je moguće ispisati u više poznatih formata (PDF, Word, Excel, slike). |
| Set osnovnih izvješća poput popisa imovine i prijetnji, popisa rizika, statusa usklađenosti po raznim standardima (ISO 27001:2013, ISO 27002:2013, ISO 22301:2012, CobiT, NIST, GDPR). |
| Dio izvješća je moguće prikazati i u grafičkom formatu („dashboard“ stranica s više grafova). |
| Jednostavno sortiranje i filtriranje sadržaja izvještaja po gotovo svim parametrima. |
| Logo korisnika u izvješćima. |
| Vođenje registra evidencijama obrada osobnih podataka koji uključuje unos, promjenu, brisanje pojedinih evidencija osobnih podataka. |
| Mogućnost provođenja DPIA analize nad evidencijama obrada osobnih podataka |
| Pregledno sučelje za vizualni prikaz i obradu svih evidencija obrada osobnih podataka zajedno sa njihovim parametrima (informacijama o obradama). |
| Registar evidencija obrada osobnih podataka mora uključivati minimalno slijedeće informacije:* Tip evidencije i osobnih podataka
* Svrha
* Izvori prikupljanja osobnih podataka
* Osobe čiji podaci se prikupljaju
* Pravna osnova temeljem koje se podaci prikupljaju
* Kada se osobni podaci prikupljaju i ažuriraju
* Kome osobni podaci smiju biti otkriveni
* Mjesto i period čuvanja evidencije i osnova po kojoj se čuva
* Veza prema drugim aplikacijama, uvoz i izvoz osobnih podataka
* Mogućnost nadzora aktivnosti u aplikaciji putem evidencije pristupa
* Mogućnost osiguranja raspoloživosti evidencije
 |
| **Upravljanje zahtjevima i privolama** |
| Mogućnost unosa i obrade korisničkih zahtjeva i privola od strane ispitanika. |
| Mogućnost unosa i obrade korisničkih zahtjeva i privola od strane DPO u ime ispitanika. |
| Mogućnost unosa i obrade svrhe prikupljanja osobnih podataka |
| Mogućnost promjene svrhe prikupljanja osobnih podataka |
| Obrada zahtjeva i privola ispitanika. Ispitanik mora imati mogućnost povlačenja privole, uvida u osobne podatke, brisanje osobnih podataka i promjenom privole. Na osnovi tog zahtjeva DPO mora moći odrediti tko je odgovoran za njegovu obradu. Sve aktivnosti koje se obavljaju prilikom obrade ovog zahtjeva se bilježe na zahtjev te ispitanik ima uvid u tijek obrade zahtjeva. |
| Prijava incidenta ugroze podataka. Sustav mora omogućiti prijavu incidenta od strane ispitanika ili DPO. DPO mora imati mogućnost upisa svih aktivnosti koje se radi tijekom obrade incidenta. |
| Prijava zahtjeva ili incidenta od strane ispitanika ili DPO-a. Mora se moći odabrati na što se odnosi incident. |
| Mogućnost obrade incidenta koja omogućuje unos aktivnosti koje su poduzete prilikom obrade incidenta. |
| Mogućnost izrade fleksibilnih izvještaja sa različitim kombinacijama parametara o zahtjevima i privolama. |
| Prikaz povijesti privola ispitanika za određenu svrhu prikupljanja podataka. |
| Davanje privole ispitanika na pojedinačne tipove osobnih podataka. |
| Upravljanje povlačenjem privole na pojedine svrhe prikupljanja osobnih podataka ili za pojedine osobne podatke. |

Uz sve navedeno, Ponuda mora uključivati stručne usluge Ponuditelja kako slijedi:

**Implementacija**

**Analiza**

* izrada upitnika za implementaciju sustava
* snimka postojećih poslovnih procesa i njihovih prioriteta, pravilnika i infrastrukture neophodnih za implementaciju sustava
* organiziranje Information Governance radionica za prikupljanje informacija

**Dizajn rješenja**

* dizajn arhitekture rješenja i modela u sustavu;
* definiranje sigurnosnih politika i postavki:
* izrada dokumenta prijedloga rješenja.

**Instalacija i konfiguracija rješenja**

* Instalacija i inicijalna konfiguracija
* Integracija u postojeću infrastrukturu
* Izrada i konfiguracija sigurnosnih politika i postavki:
* Prikupljanje i analiza povratnih informacija od korisnika;
* Dorada, ispravljanje i fino podešavanje
* Priprema za produkciju

**Obuka**

Usluge obuke osoblja Naručitelja. Obuka će se sastojati od teoretskog i praktičnog dijela u trajanju od ukupno 2 dana tako da pruži neophodna znanja za administratore i operatere sustava te službeniku za zaštitu osobnih podataka. Obuku provodi Ponuditelj.

**Izrada dokumentacije**

* Izvedbena dokumentacija za implementirani sustav sa detaljno opisanim rješenjem i pojedinačnim komponentama;

Po uspostavi cjelokupnog sustava Ponuditelj treba isporučiti završno izviješće koje će uz pregled učinjenog, osvrt na tijek implementacije i uočene potencijalne buduće probleme, sadržavati i plan godišnjeg održavanja i prijedloge dogradnji sustava.

Ponuditelj treba izvršiti i završnu prezentaciju projekta.

1. **ROKOVI**

Odabrani ponuditelj je dužan realizaciju predmeta nabave početi izvršavati odmah po potpisu Ugovora.

Od Ponuditelja se traži da izradi detaljan terminski plan uvođenja pojedinih software-skih komponenti kao i plan uvođenja licenci i njihovo adekvatno dimenzioniranje. U skladu s terminskim planom uvođenja pojedinih aplikativnih modula, od Ponuditelja se traži da izradi i detaljan terminski plan izobrazbe djelatnika Fonda.

Rok za isporuku savjetodavnih usluga, instalaciju sustava i pripremu sustava za puštanje u rad je 6 mjeseci od potpisa ugovora.

Jamstveni rok traje 6 mjeseci i počinje teći nakon implementacije sustava što se potvrđuje obostrano potpisanim primopredajnim zapisnikom.

Ugovor se sklapa na razdoblje od 1 godinu (6 mjeseci za isporuku savjetodavnih usluga i implementaciju sustava + 6 mjeseci jamstveni rok).

**7. NAČIN ISPORUKE I KONTROLA KVALITETE**

7.1. Odabrani Ponuditelj je dužan implementirati ponuđene sustave prije roka za implementaciju, te izvršiti predviđenu izobrazbu djelatnika Fonda i omogućiti testiranje od strane djelatnika Fonda nad testnim podacima. Odabrani Ponuditelj je obvezan otkloniti sve uočene nedostatke aplikativnih rješenja do krajnjeg roka implementacije. Kontrola kvalitete odvija se u dva nivoa testiranja.

Verifikacijski tim Naručitelja provodi testiranje u oba nivoa, na razvojnom okruženju Ponuditelja, te na produkcijskom okruženju Naručitelja, ali nad testnim podacima, koje za svrhe testiranja posebno priređuje Ponuditelj.

|  |  |  |  |
| --- | --- | --- | --- |
| **Naziv testiranja** | **Aktivnosti** | **Relevantna dokumentacija** | **Odgovoran za izvršenje i verifikaciju** |
| SAT – Site Acceptance Test | Završno testiranje faze razvoja projekta na testnom okruženju, na lokaciji Ponuditelja. Provodi se po završetku korekcije sustava uslijed prijavljenih zahtjeva | ATD – Acceptance Test DocumentNavedenu dokumentaciju nije nužno potrebno isporučiti Naručitelju | Tim za upravljanje kvalitetom delegiran od strane Ponuditelja, tim za implementaciju Ponuditelja, verifikatorski tim Naručitelja |
| FA – Final Acceptance Test | Završno testiranje cjelokupnog projekta na produkcijskom okruženju Naručitelja | Izvješće o ispravku prijavljenih pogreški | Tim za implementaciju Ponuditelja, verifikatorski tim Naručitelja |

Odabrani Ponuditelj obvezan je isporučiti usluge i implementirati sustave sukladno terminskom planu razrađenom u točki 6. ovog Projektnog zadatka.

Odabrani Ponuditelj je obvezan otkloniti sve uočene nedostatke aplikativnih rješenja.

Nakon implementacije traženih radnih paketa potpisuje se primopredajni zapisnik.

7.2. Odabrani ponuditelj je dužan isporučiti traženu dokumentaciju na mediju za pohranu podataka (CD, DVD, USB).

7.3. Odabrani Ponuditelj je dužan osigurati predviđenu izobrazbu za svaki radni paket iz točke 5. ovog projektnog zadatka. Odabrani Ponuditelj je obvezan najmanje 24 sata prije početka edukacije dostaviti svu potrebnu dokumentaciju (korisničke priručnike, tehničku i drugu dokumentaciju) u formatu koji omogućava ispis.

Predmet nabave smatrat će se izvršenim tek po dokazivanju pune ugovorene funkcionalnosti čitavog podsustava i isporuke iz podtočaka 7.1, 7.2 i 7.3. ove točke, o čemu će ugovorne strane potpisati Objedinjeni Zapisnik o primopredaji.

Potpisivanju objedinjenog primopredajnog zapisnika prethodit će dvadesetodnevno testiranje pune ugovorene funkcionalnosti cjelovitog podsustava od strane zaposlenika Fonda.

Naručitelj i odabrani Ponuditelj imenuju ovlaštene osobe koje su dužne pratiti realizaciju ugovornih obveza.

U slučaju ne isporučenja potpuno funkcionalnog ugovorenog predmeta nabave u ugovorenom roku, Naručitelj može raskinuti ugovor s odabranim Ponuditeljem.

**8. IZVJEŠĆIVANJE**

Odabrani Ponuditelj je obvezan dostaviti izviješće za svaki radni paket najkasnije 20 dana po završetku implementacije istog, te završno izviješće najkasnije 30 dana po završetku projekta. Izviješća se dostavljaju na hrvatskom jeziku, pisana latiničnim pismom, u pisanom i elektroničkom obliku (tekst: MS Word, font Arial; tablice i grafovi: MS Excel, font Arial na odgovarajućem mediju za pohranu podataka – CD, DVD, USB).