Technická specifikace a časový harmonogram předmětu plnění veřejné zakázky s názvem:

„Dodávka služeb bezpečnostního dohledu nad informačními systémy ČZU a rozšířeného odborného GDPR poradenství“

Tato příloha slouží k vymezení minimálních technických a obsahových požadavků zadavatele, dle kterých bude zajištěna požadovaná dodávka licencí, implementace programového vybavení a služeb odborného poradenství.

1. PŘEDMĚT PLNĚNÍ

PŘEDMĚT VEŘEJNÉ ZAKÁZKY SE SKLÁDÁ Z NÁSLEDUJÍCÍCH ČÁSTÍ:

1.1. Dodávka licencí pro stávající platformu IBM SIEM a jejich implementace

- Doplnění o licence modulu ochrany databázového a souborového prostředí pro stávající platformu IBM SIEM
- Implementace modulu ochrany databázového a souborového prostředí pro stávající platformu IBM SIEM

1.2. Poskytování služeb technické a poradenské podpory platformy IBM SIEM

- Služby správy a údržby platformy IBM SIEM
- Služby kybernetické bezpečnosti na platformě IBM SIEM – vyhodnocování událostí, rizik a bezpečnostní monitoring z pohledu kybernetické bezpečnosti

1.3. Podpora a poradenství pro DPO, zajištění programového vybavení pro komplexní správu GDPR agendy v modelu SaaS (Software as a Service)

- Poskytování služeb a rozšířeného poradenství v oblasti GDPR agendy a podpora aktivit DPO
- Programové vybavení pro komplexní správu GDPR agendy v modelu SaaS (Software as a Service)

1.4. Speciální služby, rozšířená podpora

2. HARMONOGRAM DODÁVEK A POSKYTOVÁNÍ SLUŽEB

T = datum uveřejnění smlouvy v registru smluv

	Předmět plnění	Termín zahájení plnění	Termín ukončení plnění
Jednorázové dodávky a služby	Vypracování projektu Detailního návrhu řešení zabezpečení DB prostředí	T	T + 10 pracovních dnů
	Dodávka a instalace povýšení zdrojů SIEM serverů před implementací modulu na ochranu DB	T	T + 20 kalendářních dnů
	Dodávka licencí a instalace modulů pro ochranu DB a souborových dat a zahájení podpory (včetně 36 měsíců software podpory od výrobce)	T	T + 20 kalendářních dnů
	Implementace řešení na ochranu DB a ochrany souborových dat, včetně inicializace aplikace pro správu GDPR agendy	T	T + 30 kalendářních dnů
	Zpracování implementační dokumentace	T	T + 30 kalendářních dnů
	Zkušební provoz rozšířené platformy IBM SIEM o modul na ochranu DB a souborů, včetně aplikace na správu GDPR agendy	T + 1 měsíc	T + 2 měsíce

Kontinuelní služby	Poskytování služeb technické správy platformy IBM SIEM a bezpečnostního monitoringu událostí SIEM	T + 2 měsíce	T + 36 měsíců
	Poskytování služeb poradenské podpory v oblasti GDPR agendy a podpory DPO	T + 2 měsíce	T + 36 měsíců
	Poskytnutí programového vybavení pro komplexní správu GDPR agendy formou SaaS	T + 2 měsíce	T + 36 měsíců

3. PODROBNÁ TECHNICKÁ SPECIFIKACE A POPIS POŽADOVANÉHO ŘEŠENÍ

3.1. Dodávka licencí pro stávající platformu IBM SIEM - licence pro ochranu databázového prostředí a souborů

Poptávané řešení je součástí technických opatření zaváděných především v souvislosti s nařízení EU o ochraně osobních údajů tzv. GDPR. Povyšuje doposud provozovaný SIEM systém IBM QRADAR o důležitou komponentu z pohledu zlepšení celkové úrovně řízení informační bezpečnosti Zadavatele a eliminace rizik zcizení nebo zneužití dat, jejichž je Zadavatel správcem.

3.1.1 Doplnění o licence modulu ochrany databázového a souborového prostředí pro stávající platformu IBM SIEM

Popis fungování ochrany databázového prostředí:

Řešení ochrany databází musí umožňovat monitoring a logování databázových a souborových operací v reálném čase bez dopadu na rychlost zpracování požadavků jednotlivých aplikací. Součástí tohoto monitoringu musí být v reálném čase také bezpečnostní analýza zaznamenaných databázových a souborových operací s cílem detekce podezřelého chování nebo vzniku mimořádné události. Případná rizika jsou formou alertů zasílána pověřeným pracovníkům Zadavatele k dořešení, případně podle závažnosti dojde k okamžitému zablokování podezřelé operace tak, aby se zabránilo úniku dat. Všechny monitorovací výstupy, bezpečnostní aletry a další související informace jsou centrálně dostupné ve webové konzoli, která dále slouží i pro nastavování bezpečnostních politiky, tvorbu přehledových reportů, klasifikaci dat z pohledu jejich citlivosti apod.

Řešení musí podporovat korelaci data z většiny komerčně používaných databází a big data řešení, minimálně pak ze systémů Oracle, IBM DB2, Microsoft SQL Server, mySQL, IBM Informix, Teradata, NoSQL, MongoDB a Hadoop. Zadavatel požaduje výše uvedený výčet databázových platforem z důvodu ochrany investice pro možná budoucí řešení, založená na některých z těchto databází, byť je v současné době neprovozuje všechny.

Poptávané řešení bude fungovat tak, že do operačního systému, kde je provozována konkrétní databáze je nainstalovaná sonda, která monitoruje všechny operace nad konkrétní databází a tato data poté odesílá na další zpracování do systému IBM SIEM. Zadavatel požaduje tento způsob nasazení proto, aby bylo možné monitorovat aktivity privilegovaných uživatelů, kteří se mohou do databáze připojit přímo a nepřistupují k ní přes aplikaci nebo přes počítačovou síť.

Řešení musí umožnit plnou integraci do společné management konzole systému IBM QRADAR SIEM a podporovat propojení s dalšími LDAP databázemi, například pro účely provázání se stávajícími service-desk / ticketovacími/ systémy.

Podrobné vymezení řešení na ochranu databází a souborů:

Účastník vyplní v následujících kapitolách pouze všechny žlutě označené části.

Tato příloha slouží k uvedení názvu / typu konkrétního nabízeného řešení či zařízení a dále k vymezení minimálních technických požadavků zadavatele na řešení a osvědčení jejich splnění účastníkem. Požadavky zadavatele jsou uvedeny ve sloupci 1. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnuté zařízení a jeho technické parametry.

V níže uvedené tabulce (sloupci 1) jsou uvedeny veškeré povinné minimální parametry kladené na poptávané řešení ochrany DB prostředí a souborů. Nesplnění těchto požadavků je důvodem k vyřazení nabídky.

Dodavatel v níže uvedených tabulkách vyplní sloupce „Vyjádření ANO/NE“ a pokud je požadováno i „Popis jak bude požadavek splněn/řešen“.

Sloupec „Vyjádření ANO/NE“ může nabývat pouze hodnot ANO nebo NE, bude-li uvedeno něco jiného, je to rovněž důvod k vyřazení nabídky.

Sloupec „Technická specifikace nabízeného zařízení“ a „Popis jak bude požadavek splněn/řešen“ bude obsahovat podrobný popis, jak dodavatel požadavek naplní.

Nebude-li popis splnění/řešení požadavku odpovídat popisu požadavku, tato skutečnost může mít za následek i to, že bude konstatováno, že dodavatel nesplnil zadávací podmínky stanovené Zadavatelem.

Technická specifikace - Ochrana databází a souborů

Výrobce / název / typ zařízení: ……

	Minimální technické požadavky	**„Vyjádření ANO/NE“**	**„Technická specifikace nabízeného zařízení“, pokud je vyžadováno, pak i „Popis jak bude požadavek splněn/řešen“**
1	Řešení podporuje monitoring veškerých sezení (vzdálená nebo lokální).	……	……
2	Podporované databáze: Oracle, IBM DB2, Microsoft SQL Server, mySQL, IBM Informix, PostgreSQL, MongoDB.	……	……
3	Podpora platforem: Windows, UNIX, Linux.	……	……
4	Řešení identifikuje: časovou značku každé operace, celý příkaz operace, uživatelské jméno, odkazovaný objekt.	……	……

5	Řešení poskytuje nepřetržitý monitoring používání a toku citlivých dat.	.....	.....
6	Řešení musí podporovat monitoring šifrovaných spojení na Oracle, MSSQL a DB2.	.....	.....
7	Řešení musí analyzovat data v reálném čase.	.....	.....
8	Řešení umožňuje aktivní blokování dle: ip adresy zdroje a cíle, uživatelského jména, databáze, tabulky, sloupce nebo názvu souboru, typ database.	.....	.....
9	Řešení musí korelovat události dle nastavených prahů.	.....	.....
10	Řešení by se mělo být schopno učit odhalit anomálie, aby identifikovalo: neobvyklé nebo nové aktivity, neobvyklé nebo nové chyby, nové uživatele, nové typy objektů žádaných uživatelem, změnu chování v SQL struktuře, změnu chování v přístupovém čase.	.....	.....
11	Řešení musí umožňovat nativní zasílání poplachů a zakládání událostí, které identifikuje, do systému SIEM IBM QRADAR a dále samostatně pomocí: emailu, syslog události (konfigurovatelné pro integraci s nástroji třetích stran) a	.....	.....

	programovatelného API rozhraní.		
12	Řešení musí přístup ke kontrolovaným datům kontrolovat RBAC a to na dvou vrstvách: přístup k systémovým funkcionalitám, přístup k uloženým datům.	.....	.....
13	Analýza SQL proudu by měla pokrývat příchozí a odchozí provoz a generované chyby.	.....	.....
14	Řešení musí umět klasifikovat data pro identifikaci citlivých informací v databázích.	.....	.....
15	Řešení musí podporovat sady pravidel pro požadavky PCI-DSS, SOX a GDPR.	.....	.....
16	Řešení musí umožňovat vytváření vlastních klasifikačních pravidel dle: regulárních výrazů, porovnání se slovníkem, programovatelného API rozhraní.	.....	.....
17	Řešení musí umožňovat tvorbu reportů v tabulkové a grafické formě.	.....	.....
18	Řešení musí umožňovat vytváření automatizovaných reportů dle naplánovaného rozsahu.	.....	.....
19	Systém by měl umožnit definovat postup vytváření a distribuce	.....	.....

	automatických výstrah a zpráv.		
20	Řešení musí archivovaná data ukládat v šifrované podobě.	.....	.....
21	Řešení musí obsahovat modul pro zhodnocení zranitelností, který pokrývá: CVE identifikaci, konfigurační zranitelnosti a slabiny dle CSI a STIG standard, identifikace nadměrných oprávnění a překryv oprávnění.	.....	.....
22	Řešení musí být schopno monitorovat konfigurační nastavení a identifikovat změny na: databázové úrovni (SQL, skripty), na úrovni operačního systému (skripty, proměnné prostředí, registry).	.....	.....
23	Řešení musí poskytovat aktualizaci definic pro vyhodnocování nejméně každé čtvrtletí.	.....	.....
24	Řešení musí provádět vyhodnocování opakovaně a automaticky.	.....	.....
25	Řešení musí umožňovat zasílat výsledky vyhodnocení dle definovatelného postupu a přímo příjemcům.	.....	.....
26	Je požadována licence pro pokrytí **8 ks** fyzických databázových serverů, bez ohledu na počet	.....	.....

	provozovaných DB instancí v rámci jednoho serveru. Licence tzv. per node nebo per fyzická IP adresa serveru.		
27	Je požadována licence pro pokrytí **1 ks** souborového serveru. Licence tzv. per node nebo per fyzická IP adresa serveru.	.....	.....

3.1.2 Implementace modulu ochrany databázového a souborového prostředí pro stávající platformu IBM SIEM

V rámci implementační části plnění je požadováno:

- vypracování materiálu „Detailní návrh řešení ochrany databázových a souborových serverů“
- dodávka a instalace povýšení HW zdrojů (RAM, CPU, HDD) pro servery na kterých je provozována platforma IBM SIEM
- dodávka všech potřebných licencí části ochrana databázových a souborových serverů dle bodu 3.1.
- zprovoznění modulů ochrany databázových systému pro 8ks databázových serverů a 1ks souborového serveru, na operačním systému Windows Server.
- implementace 10 nejčastěji používaných use-case pro databázové servery (prototypů - vzorových řešení pro řešení incidentů na databázovém serveru)
    - vyhotovení implementační dokumentace
- zajištění zkušebního provozu pro modul ochrany databázových systémů po dobu 10 pracovních dnů v sídle Zadavatele

Významné informační systémy:

Mezi významné informační systémy zadavatel řadí všechny aplikace, které využívají nebo přímo zpracovávají osobní údaje a jsou provozovány na databázových technologiích MS SQL a Oracle DB. Do stejné skupiny významných informačních systémů zadavatele patří i systémy zajišťující souborové operace na platformě Microsoft Server.

Typicky se jedná o následující informační systémy, které budou primárně zařazeny do systému bezpečnostního monitoringu ICT prostředí zadavatele:

1. ekonomický systém MAGION
2. studijní systém UIS
3. systém spisové služby eSPIS
4. systém elektronické pošty MS Exchange
5. document management systém DMS

6. e-learningový systém Moodle
7. ISKaM……
8. systém provozních databází ČZU

3.2. Poskytování služeb technické a poradenské podpory platformy **I**BM SIEM

Poskytovatel bude poskytovat Zadavateli kontinuální i jednorázové služby spočívající v zajištění odborné správy platformy IBM SIEM, monitoringu bezpečnostních událostí a rizik včetně jejich vyhodnocování, nastavení a kontrole nápravných opatření v oblasti kybernetické bezpečnosti a také dodávkách konzultačních služeb v oblastech ISMS, GDPR a podpory činností DPO (dále jen „**Služby**“).

Podrobnější popis a katalogový list služeb technické a poradenské podpory:

3.2.1 **Služby správy platformy SIEM (kontinuální služba na měsíční bázi)**

- poskytování služby údržby a servisní podpory platformy IBM SIEM
- poskytování nových verzí IBM SIEM a opravných patchů dle aktuální technologické úrovně
- poskytování služeb on-line monitoringu platformy IBM SIEM (monitoring dostupnosti HW/SW platformy)
- průběžná aktualizace implementační a provozní dokumentace
- SLA parametry:
  - služby údržby a servisní podpory v režimu 8/5/365 tj. tj. v pracovní dny od 8-16 hodin
  - služeby on-line monitoringu platformy IBM SIEM v režimu 24/7/365

3.2.2 **Služby podpory Security Operation Centre (SOC) – vyhodnocování událostí a bezpečnostního monitoringu (kontinuální služba na měsíční bázi)**

- poskytování poradenských služeb prostřednictvím HotLine/Helpdesk při řešení běžných provozních problémů správců informačních systémů. Služba bude dostupná 8/5/365 tj. tj. v pracovní dny od 8:00 – 16:00 hodin.
- poskytování služeb bezpečnostního monitoringu (sběr a detekce bezpečnostních událostí). Služba zajišťuje detekci událostí, investigaci, správu zranitelností, reporting, doporučení v oblasti nápravných opatření a odborných konzultací, a to vše prostřednictvím vyhodnocovacího centra pro řešení incidentů.
- SLA parametry:
  - služba vyhodnocovacího centra bude dostupná 8/5/365 tj. v pracovní dny od 8-16 hodin
  - bezpečnostní monitoring (sběr událostí) bude zaručen v režimu 24/7/365

3.2.3 **Katalogový list služeb**

Katalogový list slouží jako detailní specifikace obsahu a rozsahu požadovaných služeb.

Správa a údržba platformy IBM SIEM a Služby kybernetické bezpečnosti SOC	
VYMEZENÍ SLUŽBY	
Prostředí	Produkční HW appliance IBM QRADAR SIEM, modul Vulnerability management, modulu na ochranu databází a souborových služeb, který je předmětem dodávky v rámci této zakázky.
Cílová skupina	Interní zaměstnanci, externí subjekty, studenti, veřejnost
Zkrácený popis služby	Proaktivní dohled nad zabezpečením infrastruktury pomocí nástroje IBM SIEM a doplňkových modulů
Předpokládaný minimální rozsah hodin za jeden kalendářní měsíc	48 hodin
ROZSAH POŽADOVANÝCH ČINNOSTÍ	
Telefonická podpora 8x5 v českém jazyce, jednotné kontaktní místo pro hlášení problémů, incidentů a poruch. **Správa zařízení IBM SIEM (HW/SW)** <u>1. Provoz zařízení IBM SIEM</u> • Profylaktické činnosti, kontrola služeb (na týdenní bázi), • Kontrola provozních logů zařízení (na týdenní bázi), • Návrh případných opatření s cílem předejít možným výpadkům a omezením poskytovaných služeb zařízením SIEM, • Odborná technická podpora a odstraňování závad v předmětné oblasti, • Správa licenčních pravidel. <u>2. Správa zařízení IBM SIEM</u> • Kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobce (na měsíční bázi), • Údržba a zajištění dostupnosti služby IBM SIEM, • Analýza vhodnosti a potřebnosti implementace opravného balíku, • Návrh opatření a postupu implementace opravného balíku ke schválení Zadavateli, • Implementace schválených požadavků na změnu konfigurace služby SIEM.	

Pravidelné činnosti – analytická činnost IBM SIEM, služby SOC

Služby 1. úroveň – Podpora, dohled a analýzy

- Analýza bezpečnostních incidentů v systému IBM SIEM
    - Posouzení incidentu z hlediska false-possitives bezpečnostních incidentů
    - Vyhodnocení příčin vzniku bezpečnostních incidentů
    - Vyhodnocení dopadu bezpečnostních incidentů (změny v systémech / infrastruktuře, uniklá data, atd.)
    - Návrh a konzultace nápravných a preventivních opatření
- SIEM – Security Information & Event Management
    - Vzdálená kontrola bezpečnostních událostí – incidentů 8x5 (investigace pro jejich klasifikaci)
    - Eskalace a informování pověřených osob dle kompetenční a komunikační matice.
        - Eskalace významných událostí ze sítě na CESNET-CERTS bezpečnostní tým nebo národními CERT® týmy a CSIRT týmy.
- Konfigurace log zdrojů napojených na SIEM
    - Vytváření DSM modulu pro neznámé zdroje v SIEM, aby bylo možné kategorizovat informace obsažené v logu.
    - Kontrola správné funkce infrastruktury a případná náprava nežádoucího stavu
    - Přidávání Logsources
- Vulnerability management
    - Aktivní kontrola zranitelnosti infrastruktury
    - Vyhodnocení bezpečnostního incidentu na základě známé zranitelnosti v infrastruktuře
    - Reporting zranitelností (1 x měsíčně)
- Strukturovaný reporting

Požadujeme vytváření kvartálního reportu o stavu událostí na síti ČZU a o všech provedených konfiguračních změnách poskytovatelem. Součástí pravidelného reportingu bude mj.:

- Reporting zjištěných bezpečnostních incidentů a TOP 10 opakujících se hlášení bezpečnostního monitoringu
- Reporting zjištěných zranitelností a rizik v infrastruktuře - SWOT
- Reporting anomálií v infrastruktuře a nekorektního chování infrastruktury nebo jejich částí
- Reporting zjištěných zranitelností v databázovém a souborovém prostředí
- Konzultace nad reporty, navrhovaná nápravná opatření

- Informace o množství přidaných Logsources
- Informace o zjištěných zranitelnostech a identifikovaných útocích na infrastrukturu,
- Informace o přijatých opatřeních

- Provoz manažerského rozhraní (Dashboard)
  - Přehled o aktuální bezpečnostní situaci v informačním systému
  - Přehled o správě detekovaných událostí a průběhu analytických činností
  - Přehled o kvalitě služeb bezpečnostní infrastruktury
- Škálování konfigurace na specifické prostředí zákazníka
- Podpora služby v provozním režimu 5x8 s možností telefonní nebo e-mail komunikace přímo se SOC operátorem. V případě významných incidentů i specificky domluveným způsobem.

Součinnost v rámci procesů „Projektového řízení" souvisejících s návrhem změn v infrastruktuře (společně s dodavateli technologií).

- Správa a aktualizace provozní dokumentace v rozsahu:
  - Postupy pro provoz a správu služby,
  - Postupy pro obnovu služby ze záloh jednotlivých systémů,
- Správa a aktualizace technické dokumentace v rozsahu (konzole systému):
  - Aktuální přehled infrastruktur jednotlivých systémů/aplikací služby IBM SIEM,
  - Aktuální přehled parametrů jednotlivých aplikací IBM SIEM,
  - Správa konfigurací předmětných služeb IBM SIEM.

SERVICE LEVEL AGREEMENT (SLA)

Vyhodnocovací období	1 kalendářní měsíc

SLA PARAMETRY	**Jednotka**	**Hodnota**
Dostupnost	[%/měs]	98
Monitoring dostupnosti platformy SIEM	[hod-hod]	00-00 (24x7)
Sběr dat platformy SIEM	[hod-hod]	00-00 (24x7)
Provozní doba zaručená	[hod-hod]	08–16 (8x5)
Max. doba výpadku	[hod]	4
Max. doba nedostupnosti dat	[hod]	4
Max. doba servisní odezvy	[min]	30
Odstranění výpadku – A	[hod]	4

Odstranění výpadku – B	[dny]	1	
Odstranění výpadku – C	[dny]	2	

Upřesnění kategorií incidentů a závad (zpřesnění globálních definic daných smlouvou)	
Kategorie A	Nedostupnost služby IBM SIEM, zejména: Nedochází ke sběru událostí, neběží monitoring v reálném čase.
Kategorie B	Závada nebo výpadek části služby IBM SIEM, které způsobí sníženou dostupnost služby, avšak nezpůsobí celkovou nedostupnost služby IBM SIEM. Např. nelze spravovat zdroje IBM SIEM, systém nemá funkční analýzu útoků.
Kategorie C	Ostatní závady nespadající do kategorie A nebo B, např. nefungují reporty.
PODMÍNKY A OMEZENÍ SLUŽBY	
Měrná jednotka provozu služby	Počet EPS, tzv. Events Per Second (událostí za vteřinu) a počet zařízení napojených do IBM SIEM Počet DEVICES, tzn. počet zařízení napojených na VULNERABILITY MANAGER Počet chráněných Databázových a souborových serverů Hodinový fond na řešení související problematiky
Limit objemu služby	2000 EPS, 1280 VM SCAN ASSETS, 8 Databází, 48 hodin za měsíc
Omezení	Do doby na odstranění výpadku se nezapočítává čas potřebný k odstranění HW závady nebo závady spočívající ve vývoji mikro kódu SW 10 detekovaných, popsaných a zadavateli předaných incidentů týdně z toho 5 prošetřených a zadavateli předaných návrhů na nápravná opatření

3.3. Podpora a rozšířené poradenství pro DPO, zajištění programového vybavení pro komplexní správu GDPR agendy v modelu SaaS (Software as a Service)

3.3.1 **Poskytování služeb a rozšířeného poradenství v oblasti GDPR agendy a podpora aktivit DPO**

Služby rozšířeného poradenství a podpory GDPR a činností DPO (kombinace kontinuálních a jednorázových služeb)

- služby poradenství pro interní roli DPO s důrazem na operativní řešení požadavků plynoucích z GDPR při zajištění výkonu činnosti Zadavatele
- realizace pravidelných „status meetingů“ k agendě GDPR
- realizace kvartálních informačních školení v rozsahu řešené problematiky
- provádění průběžné GAP analýzy s ročním výstupem
- publikace informační bulletin (newsletter) o aktualitách v rozsahu řešení problematiky na měsíční bázi
- ad-hoc poskytování konzultačních služeb – rolí – odborných specialistů v oblasti kybernetické bezpečnosti a GDPR
- právní konzultace – v oblasti práva na ochranu osobních údajů

- konzultací v oblasti kybernetické ochrany
- konzultace v oblasti ISMS
- konzultace v oblasti systémů řízení kvality (ISO)
- konzultací v oblasti GDPR – DPO a metodiky
- metodická podpora implementace náprávných opatření spojených s GDPR
- podpora a shromažďování argumentace při jednání s ÚOOÚ

3.3.2 **Katalogový list služeb**

Katalogový list slouží jako detailní specifikace obsahu a rozsahu požadovaných služeb

Rozšířené poradenství v oblasti GDPR agendy a podpora aktivit DPO	
VYMEZENÍ SLUŽBY	
Prostředí	Informační systémy a další aplikace ČZU
Cílová skupina	DPO, GDPR team, zaměstnanci
Zkrácený popis služby	Poradenství v oblasti GDPR agendy a podpory DPO
Předpokládaný minimální rozsah hodin za jeden kalendářní měsíc	**3 člověkodny (MD)** služeb specialistů **Jednorázové služby** na základě objednávky zadavatele
ROZSAH POŽADOVANÝCH ČINNOSTÍ	
- První fáze poskytování služby Podpory DPO - První fáze bude realizována v rámci implementace programové vybavení pro komplexní správu GDPR agendy v modelu SaaS (Software as a Service) , bod 3.3.3 - - Vytvoření kontaktního místa pro subjekty údajů a dozorový orgán. - Vytvoření registru operací zpracování osobních údajů v dodané aplikaci podpory GDPR. - Vytvoření právního registru týkajícího se ochrany osobních údajů a nařízením GDPR. - Vytvoření doplňkových registrů v aplikaci na správu GDPR agendy: - Registr souhlasů ke zpracování osobních údajů; - Registr oprávněných zájmů; - Evidence žádostí o výkon práv subjektu údajů; - Evidence a řízení porušení zabezpečení osobních údajů (incidentů); - Evidence posouzení vlivu na ochranu osobních údajů. - Příprava na provedení školení klíčových zaměstnanců organizace. - Druhá fáze poskytování rozšířené podpory DPO je orientována na rutinní provoz nařízením vyžadovaných procesů. - Služba rozšířené podpory DPO v této fázi zajistí zadavateli poradenské služby, vyšší odborné znalosti a zkušenosti o právech a postupech v oblasti ochrany osobních údajů a bezpečnosti tak, aby organizace byla schopna zajistit plnění požadavků nařízení GDPR a příslušných zákonů a předpisů o ochraně osobních údajů. -	

- Služba podpory DPO je požadována jako doplnění kapacity interního pracovníka zadavatele na pozici DPO (Pověřence ochrany osobních údajů) a pro plnění rozšířených úkolů vycházející z požadavků GDPR.
-
- V rámci služby rozšířené podpora DPO bude možné, na základě pokynu zadavatele, konzultovat nebo zajišťovat následující činnosti:
-
- Monitorování souladu s Obecným nařízením o ochraně osobních údajů (GDPR) a právními normami ČR k problematice zpracování a ochrany osobních údajů a podávat o tomto zprávy vedení organizace.
- Realizace úkolů spojených s prováděním Posouzení vlivu na ochranu osobních údajů, a to zejména vydání posudku:
- zda je nebo není nutné provést posouzení vlivu,
- jakou metodiku při zpracování posouzení vlivu použít,
- zda posouzení vlivu zpracovat vlastními silami nebo jeho zpracování zadat externě,
- jaká ochranná opatření (včetně technických a organizačních) uplatnit pro zmírnění rizik vůči právům a zájmům subjektů údajů,
- zda posouzení vlivu bylo zpracováno správně a zda jeho závěry (ať už vedou či ne k pokračování zpracovatelské operace a bez ohledu na to, jaká ochranná opatření určují uplatnit) jsou v souladu s GDPR;
- Spolupracovat s dozorovým úřadem [ÚOOÚ] a být styčným bodem pro tento úřad v otázkách souvisejících se zpracováním osobních údajů a v případě potřeby konzultovat s dozorovým orgánem veškeré další osobní údaje a data.
- Prosazovat přístup založený na riziku, a to zejména stanovovat priority pro zajištění ochrany zpracování osobních údajů s vysokým rizikem pro práva a svobody subjektů údajů.
- Zdokumentovat a dále udržovat přehledy operací zpracování na základě informací od různých oddělení jejich organizace, zodpovědných za zpracování osobních údajů, a to včetně vedení jejich registru (evidence).
- Upozorňovat pověřené osoby na straně organizace na rizikové faktory pro řádné zabezpečení osobních údajů, jakož i na jakékoliv zjištěné nedostatky či rozpory s legislativou k GDPR.
- Průběžné monitorování a hodnocení souladu spolehlivosti, přiměřenosti a uplatňování bezpečnostních a dalších zásad pro ochranu a zpracování osobních údajů a obecně procesů týkajících se ochrany a zpracování osobních údajů s legislativou k GDPR, vč. analýzy, auditů a kontroly shody vnitřní praxe s legislativou k GDPR.
- Testování zásad a případné navržení dalších postupů a pravidel, které mohou být zavedeny zejména k řádné ochraně, zpracování osobních údajů a zachování důvěrnosti, integrity a dostupnosti osobních údajů.
- Poskytování poradenství v souvislosti se zpracovatelskými smlouvami, souhlasy subjektů údajů se zpracováním osobních údajů, plněním informační povinnosti apod.
- Poskytování informací a poradenství k problematice zpracovávání osobních údajů organizací.
- Poskytování informací o rozvoji, sjednocení výkladu a udržování všech zásad, postupů a procesů ochrany osobních údajů, pokud jde o zpracování, ochranu a bezpečnost osobních údajů.
- Zajištění školení a rozšiřování povědomí, aby byli všichni zaměstnanci, kteří se zabývají operacemi zpracování osobních údajů, seznámeni s povinnostmi a požadavky plynoucími z legislativy k GDPR.
- Návrh odpovědností za ochranu a zpracování osobních údajů či jejich zabezpečení organizací.

- Zjišťování, do jaké míry jsou osobní údaje shromažďovány, uchovávány a/nebo používány organizací a zda jsou řádně kontrolovány a chráněny před ztrátou důvěrnosti, integrity nebo dostupnosti z jakékoli příčiny.
- Zdokumentování a následně udržování přehledů operací zpracování na základě informací od organizace, a to včetně vedení jejich registru (evidence), jakož i vedení dalších registrů a evidencí.
- Poradenství k prosazování přístupu založeného na odpovědnosti a riziku, zejména stanovování priorit pro zajištění ochrany zpracování osobních údajů s vysokým rizikem pro práva a svobody subjektů údajů a konzultace při stanovení rizik pro práva a svobody subjektů údajů.
- Realizace úkolů spojených s prováděním posouzení vlivu na ochranu osobních údajů (zejména jeho kontrola, poskytování poradenství, zajištění vyhotovení posudku, monitorování uplatňování posouzení vlivu apod.).
- Spolupráce při posuzování bezpečnostních incidentů a stanovení dalšího postupu při jejich vzniku.
- Komunikace se subjekty údajů, poskytování poradenství v souvislosti s vyřizováním uplatněných práv subjektů údajů.
- Spolupráce s dozorovým úřadem (ÚOOÚ) včetně výkonu činnosti kontaktní osoby v otázkách souvisejících se zpracováním osobních údajů, konzultace s dozorovým orgánem (v případě potřeby) a dalších skutečnostech týkajících se zpracování osobních údajů.

Reporting (1 x měsíčně) :

- Počet hlášení událostí ve vztahu ke GDPR
- TOP10 incidentů Compliance Data report GDPR

Součástí služby je i Informační bulletin - Pravidelné sledování dodržování právních předpisů Evropské unie (zejm. GDPR) a národních právních předpisů o ochraně osobních údajů a doprovodné rozhodovací praxe či metodik a výkladů příslušných vnitrostátních i evropských autorit (dále jen „legislativa k GDPR“).

PODMÍNKY A OMEZENÍ SLUŽBY	
Měrná jednotka provozu služby	Počet MD nebo hodin
Omezení	Dodavatel obdrží přiměřenou součinnost DPO na straně zadavatele při plnění výše uvedených úkolů. Jednorázové služby rozšířeného poradenství pro DPO budou čerpány na základě objednávky zadavatele.

3.3.3 **Programové vybavení pro komplexní správu GDPR agendy v modelu SaaS (Software as a Service)**

Předmětem této služby je poskytnutí uživatelských licencí pro software na správu GDPR agendy. Zadavatel předpokládá neomezené využívání software pro všechny svoje zaměstnance a organizační celky.

Požadovaná funkcionalita pro zajištění komplexní správy GDPR agendy:

- požadujeme dodání platformy – webové portálové služby – jenž umožní efektivní, centralizovanou správu pro pověřence GDPR směrem k jeho organizacím
- požadujeme webový nástroj pro práci jednoho pověřence/správce osobních údajů (OÚ)nad GDPR procesy ve skupině organizací
- požadujeme webový nástroj umožňující kdykoliv zobrazit stav nápravných opatření za organizace ve skupině
- vytvoření šablon agendy a jejich distribuce organizacím zadavatele
- on-line stav a přehled o žádostech subjektů za organizace ve skupině
- vytvoření jednotných metodik, technických, organizačních opatření a jejich elektronická distribuce organizacím zřizovatele
- rychlá aplikace legislativních/procesních změn do všech organizací ve skupině
- on-line reporting stavu nápravných opatření a sdílení úkolů v rámci skupiny organizací
- systém šablon musí umožňovat zadavateli provést analýzu GDPR pro typovou organizaci a pak ji elektronicky distribuovat do svých organizací. Koncová organizace pak provádí pouze krok rozdílové analýzy a přejímá systém/metodiku organizačních a technických opatření.
- aplikace obsahuje šablony pro jednotlivá zpracování (personální a mzdová agenda)
- praktický dotazníkový průvodce náležitostmi zpracování včetně posouzení vlivu
- shromáždění všech informací o evidenci osobních údajů na jednom místě

Systém musí nabízet řešení pro evidenci následujících informací:

- co zpracovávám a ukládám
- jak osobní data zpracovávám
- proč konkrétní osobní údaje zpracovávám
- kde údaje ukládám
- kdy a na jak dlouho
- kdo má k osobním údajům (OÚ) přístup
- od koho data přijímám, zda od subjektu nebo třetí strany
- aktuální informace ke GDPR (Judikáty, WP29, praxe…)
- stav realizace nápravných opatření
- aktuální míra rizika porušení ochrany OÚ

Nástroj bude sloužit jako/pro:

- podpora práce Pověřence (DPO) a správce OÚ
- nástroj pro evidenci a řešení žádostí
- řešení incidentů a událostí – vyhodnocení konfliktu a dopadu na OÚ
- evidence konzultací s ÚOOÚ
- nástroj pro zastřešení procesů realizace nápravných opatření
- řešení realizace opatření
- nástroj pro posouzení účinnosti NO
- poskytovatel informačního servisu
- shromaždiště aktuálních dat z oblasti GDPR na jednom místě
- nástroj pro sledování novelizací zákonů a nařízení
- využití vodítek WP29
- možnost importu již zpracovaných dat a následného řízeného postupu zpracování
- automaticky generované dokumenty přímo z aplikace
- generování dokumentů Záznamů o činnostech zpracování
- generování dokumentů za účelem naplnění informačních povinností směrem k různým kategoriím subjektů osobních údajů
- posouzení vlivu na ochranu osobních údajů

Dodavatel ponese veškeré náklady na implementaci a aktualizaci programového vybavení (aplikace):

- aplikace bude poskytnuta v režimu služby (Software as a service)
- žádné další náklady na implementaci a provoz (Cloudová služba)
- vždy aktuální verze SW a plná kompatibilita mezi jednotlivými verzemi
- podpora a rozvoj aplikace s využitím zkušeností s používáním
- možnost správy GDPR pro skupinu organizací v rámci jednoho pověřence
- možnost správy dat více subjektů patřících jednomu zadavateli

3.4. Speciální služby, rozšířená podpora

- školení dle požadavků Objednatele nad sjednaný rozsah
- jednorázové poskytnutí rozšířené konzultační podpory v rozsahu dle potřeb zadavatele
- součinnost při řešení systémových problémů a při implementaci systémů třetích stran
- spolupráce při tvorbě koncepce či implementaci dalších bezpečnostních systémů
- úpravy a funkční doplnění IBM SIEM dle požadavků zadavatele
- forenzní analýza a penetrační testování
- služby podpory při pravidelných auditech

Servisní podpora výrobce musí být poskytována v České republice a v českém jazyce. Součástí nabídky musí být potvrzení od lokálního zastoupení výrobce řešení pro ochranu databázových systémů a souborových služeb o tom, že nabízené zboží/licence je určeno pro český (EU) trh a bude plně podporováno servisním střediskem v ČR.