Príloha č. 6

Bezpečnostné opatrenia, notifikačné a iné povinnosti Dodávateľa v oblasti kybernetickej bezpečnosti

A. Základné dojednania

1. Objednávateľ je prevádzkovateľom základných služieb podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a súčasne tiež správcom informačných technológií verejnej správy podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
2. Služby poskytované Dodávateľom definované v Článku 2 Predmet zmluvy priamo súvisia s jednou lebo viacerými základnými službami prevádzkovanými Objednávateľom.
3. Na povinností týkajúce sa bezpečnostných opatrení a nahlasovania a riešenia kybernetický bezpečnostných incidentov neupravené v tejto Zmluve sa použijú ustanovenia Zákona o kybernetickej bezpečnosti, vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška NBÚ"), Zákona o informačných technológiách vo verejnej správe a právnymi predpismi vydanými na ich vykonanie.
4. Pojmy uvedené v tejto prílohe č. 6 k Zmluve, ktoré sú definované v Zákone o kybernetickej bezpečnosti, vyhláške NBÚ, Zákone o informačných technológiách vo verejnej správe a právnych predpismi vydaných na ich vykonanie sa budú vykladať tak, ako ich definujú tieto právne predpisy.

B. Bezpečnostné opatrenia a notifikačné povinnosti

Bezpečnostné politiky a bezpečnostná dokumentácia

1. Dodávateľ sa zaväzuje dodržiavať aktuálne a schválené bezpečnostné politiky, ako aj ďalšiu bezpečnostnú dokumentáciu koncového užívateľa, s ktorými bol oboznámený.
2. Objednávateľ preukázateľne zabezpečí sprístupnenie bezpečnostných politík a bezpečnostnej dokumentácie, ktoré je Dodávateľ povinný dodržiavať, ako aj každú ich aktualizáciu Dodávateľovi.
3. Dodávateľ podpisom zoznamu sprístupnených bezpečnostných politík a bezpečnostnej dokumentácie, ako aj ich aktualizácií, vyjadrí oboznámenie sa a súhlas s nimi.

Ochrana informácií

1. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením úloh podľa tejto Zmluvy vo vzťahu ku koncovému užívateľovi, najmä nevyužiť ani nesprístupniť tretím osobám žiadne skutočnosti, informácie, poznatky, podklady alebo iné záležitosti, o ktorých bol počas platnosti tejto Zmluvy informovaný, alebo o ktorých sa dozvedel počas plnenia tejto Zmluvy. Povinnosť zachovávať mlčanlivosť trvá aj po zániku tejto Zmluvy.
2. Dodávateľ je povinný písomne zaviazať všetky osoby, svojich zamestnancov, subdodávateľov a ich zamestnancov, ktoré sú zúčastnené na plnení tejto Zmluvy zachovávať mlčanlivosť v zmysle § 12 ods. 1 Zákona o kybernetickej bezpečnosti a predchádzajúceho bodu 1. Dodávateľ v plnej miere zodpovedá za dodržiavanie záväzku mlčanlivosti týmito osobami aj po zániku Zmluvy.
3. Výnimky z povinnosti mlčanlivosti sa riadia režimom Zákona o kybernetickej bezpečnosti.
4. Dodávateľ je povinný chrániť všetky informácie, ktoré mu boli poskytnuté Objednávateľom alebo koncovým užívateľom, a to najmä pred ich neoprávneným vymazaním, zmenou alebo pred ich poskytnutím neoprávnenej osobe.
5. Dodávateľ je oprávnený použiť informácie získané v súvislosti s realizáciou tejto Zmluvy a údaje nachádzajúce sa v informačných systémoch koncového užívateľa výhradne na účely súvisiace s plnením tejto Zmluvy.

Bezpečnostné opatrenia

1. Dodávateľ je povinný dodržiavať a bezodkladne prijímať bezpečnostné opatrenia v oblasti kybernetickej a informačnej bezpečnosti v rozsahu podľa Zákona o kybernetickej bezpečnosti a

vyhlášky NBÚ a vyhlasuje, že bezvýhradne súhlasí s rozsahom a špecifikáciou bezpečnostných opatrení, ktoré sú relevantné k vykonávaným činnostiam Dodávateľa podľa tejto Zmluvy.

2. Pre oblasť technických zraniteľností systémov a zariadení sa Dodávateľ zaväzuje realizovať opatrenia podľa § 9 vyhlášky NBÚ, najmä identifikovať technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní Služieb v mene Objednávateľa prostredníctvom opatrení definovaných v nasledovných bodoch:
   a) zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
   b) zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,
   c) využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.
3. Pre oblasť riadenia bezpečnosti sietí a informačných systémov sa Dodávateľ zaväzuje realizovať opatrenia podľa § 10 vyhlášky NBÚ, prostredníctvom opatrení definovaných v nasledovných bodoch:
   a) riadenie prístupov používateľov k sieťam a informačným systémom v súlade s § 12 vyhlášky NBÚ,
   b) riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami koncového užívateľa, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom,
   c) povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií,
   d) zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov,
   e) sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete,
   f) spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov,
   g) servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu,
   h) udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave,
   i) zavedenie a prevádzka automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou,
   j) blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje,
   k) neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty,
   l) zavedenie a prevádzka systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete,
   m) implementácia systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky,
   n) smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu,
   o) vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,
   p) vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.
4. Pre oblasť riadenia prístupov sa Dodávateľ zaväzuje realizovať opatrenia podľa § 12 vyhlášky NBÚ, prostredníctvom opatrení definovaných v nasledovných bodoch:

a) riadenie prístupov osôb k sieti a informačnému systému, musia byť založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa,
b) riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb koncového užívateľa, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou,
c) riadenie prístupov osôb k sieti a informačnému systému, ktoré zahŕňa najmenej (i) vypracovanie zásad riadenia prístupu k informáciám, (ii) riadenia prístupu používateľov, (iii) zodpovednosti používateľov, (iv) riadenia prístupu k sieťam, (v) prístupu k operačnému systému a jeho službám, (vi) prístupu k aplikáciám, (vii) monitorovania prístupu a používania informačného systému a riadenia vzdialeného prístupu,
d) pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému,
e) zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov,
f) využitie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy),
g) výkon kontroly prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov v pravidelných intervaloch,
h) určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej bezpečnostnej politiky.

5. Pre oblasť riešenia kybernetických bezpečnostných incidentov realizuje Dodávateľ opatrenia podľa § 14 vyhlášky NBÚ, najmä deteguje a rieši kybernetické bezpečnostné incidenty, ktoré môžu mať dopad na poskytovanie Služieb, čo zahŕňa najmä prijatie opatrení definovaných v nasledovných bodoch:
   a) oboznámenie sa so štandardmi a postupmi koncového užívateľa pri riešení kybernetických bezpečnostných incidentov a spracovanie interných postupov riešenia kybernetických bezpečnostných incidentov, ktoré zahŕňajú najmä minimálne postupy hlásenia kybernetických bezpečnostných incidentov voči Objednávateľovi v súlade so Zákonom o kybernetickej bezpečnosti a vyhláškou NBÚ tak, aby mal koncový užívateľ primeraný čas na splnenie si svojich práv a povinností plynúcich mu z právnych predpisov,
   b) monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie Služieb,
   c) detegovanie kybernetických bezpečnostných incidentov, najmä prostredníctvom nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát,
   d) zber relevantných informácií o kybernetických bezpečnostných incidentoch (najmä, avšak nie len: lokalita, hostname, MAC adresy, IP adresy, identifikačné údaje všetkých zariadení a zúčastnených osôb a dátum, čas manipulácie s údajmi a vymedzenie miesta ich uloženia) a vyhodnocovanie kybernetických bezpečnostných incidentov, najmä prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje (i) zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch, (ii) vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetický bezpečnostným incidentom, (iii) vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov, (iv) revíziu konfigurácie a monitorovacích

pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch,

e) riešenie zistených kybernetických bezpečnostných incidentov a zníženie následkov zistených kybernetických bezpečnostných incidentov podľa pokynov Objednávateľa alebo koncového užívateľa,

f) vyhodnocovanie spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov v súčinnosti s Objednávateľom.

6. Pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov sa Dodávateľ zaväzuje realizovať opatrenia podľa § 15 vyhlášky NBÚ, najmä implementovať centrálny nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov najmenej pre všetky informačné systémy a sieťové prvky, ktoré sú využívané pri poskytovaní Služieb, ktorý spĺňa všetky požiadavky ustanovené vo vyhláške NBÚ, a to najmä požiadavky na zabezpečenie bezpečnostného dohľadu nad sieťami a informačnými systémami a jeho funkčnosť.
7. Dodávateľ je povinný postupovať v súlade so schválenými normami upravujúcimi oblasť informačnej bezpečnosti, a to najmä podľa STN ISO/IEC 27002:2013 (Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti).

Zoznam osôb

1. Dodávateľ je povinný Objednávateľovi doručiť menný zoznam osôb a pracovných rolí Dodávateľa, ktoré majú prístup k informáciám a údajom koncového užívateľa. Každú zmenu v personálnom obsadení pracovných rolí podľa prechádzajúcej vety je Dodávateľ povinný Objednávateľovi najneskôr 7 dní pred plánovaným začatím výkonu činnosti touto osobou písomne oznámiť.
2. Dodávateľ je povinný zabezpečiť, aby sa osoby evidované v zozname podľa prvej vety zaviazali pred začatím výkonu činnosti dodržiavať mlčanlivosť o skutočnostiach v rozsahu uvedenom v časti B „Ochrana informácií“ tejto prílohy č. 6 k Zmluve, o ktorých sa v súvislosti s výkonom činnosti dozvedeli podľa tejto Zmluvy.

Hlásenie kybernetických bezpečnostných incidentov

1. Dodávateľ je povinný bezodkladne informovať Objednávateľa a koncového užívateľa o každom podozrení na kybernetický bezpečnostný incident ako aj o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej a informačnej bezpečnosti.
2. Hlásenie podozrenia o kybernetickom bezpečnostnom incidente musí obsahovať najmä informácie:
   a) o tom, kto hlási kybernetický bezpečnostný incident, a to:
      1. identifikačné údaje a
      2. kontaktné údaje,
   b) o kybernetickom bezpečnostnom incidente, a to:
      1. časové údaje priebehu kybernetického bezpečnostného incidentu,
      2. opis priebehu kybernetického bezpečnostného incidentu a
      3. rozsah vzniknutých škôd z dôvodu kybernetického bezpečnostného incidentu,
   c) o Službe zasiahnutej kybernetickým bezpečnostným incidentom, a to:
      1. konkrétny popis všetkých zasiahnutých aktív a
      2. vplyv kybernetického bezpečnostného incidentu na poskytovanú Službu,
   d) o riešení kybernetického bezpečnostného incidentu, a to:
      1. stav riešenia kybernetického bezpečnostného incidentu,
      2. vykonané nápravné opatrenia a
      3. popis následkov kybernetického bezpečnostného incidentu.
3. Pri riešení kybernetického bezpečnostného incidentu je Dodávateľ povinný spolupracovať s Objednávateľom, koncovým užívateľom, Ministerstvom investícií, regionálneho rozvoja a informatizácie Slovenskej republiky, Národným bezpečnostným úradom a na tento účel im poskytnúť všetku potrebnú súčinnosť a všetky informácie získane z vlastnej činnosti, ktoré by mohli byť dôležité pre riešenie kybernetického bezpečnostného incidentu.

4. Dodávateľ je povinný v čase kybernetického bezpečnostného incidentu zabezpečiť všetky dôkazy, ktoré budú slúžiť na objasnenie príčin jeho vzniku a napomôžu riešeniu kybernetického bezpečnostného incidentu.

Kontrolná činnosť a audit

1. Dodávateľ poskytne Objednávateľovi všetku potrebnú súčinnosť v prípade, ak koncový užívateľ požaduje od Objednávateľa umožniť vykonať u Dodávateľa audit alebo kontrolu, zameranú na overenie plnenia povinností Dodávateľa podľa tejto Zmluvy majúcich vplyv na povinnosti koncového užívateľa ako prevádzkovateľa základnej služby alebo Dodávateľa digitálnej služby.
2. Dodávateľ je povinný poskytnúť Objednávateľovi súčinnosť v potrebnom rozsahu aj v prípade, ak je Objednávateľ povinný umožniť vykonať audit prijatých bezpečnostných opatrení alebo kontrolu zo strany Národného bezpečnostného úradu, Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky, či iného ústredného orgánu podľa Zákona o kybernetickej bezpečnosti, Národného centra kybernetickej bezpečnosti SK-CERT, vládnej jednotky CSIRT alebo nimi poverenej osoby.
3. Dodávateľ je povinný poskytnúť na žiadosť Objednávateľa osobe vykonávajúcej audit alebo kontrolu všetky informácie, ktoré má k dispozícii a ktoré sú potrebné na preukázanie splnenia povinností Dodávateľa, Objednávateľa alebo koncového užívateľa v oblasti kybernetickej bezpečnosti.
4. Dodávateľ je tiež povinný na žiadosť Objednávateľa pri audite alebo kontrole spolupracovať s osobou vykonávajúcou predmetnú činnosť a sprístupniť všetky svoje priestory, ako aj všetku dokumentáciu a programové, technické a technologické vybavenie, ktoré slúžia na plnenie povinností podľa tejto Zmluvy v oblasti kybernetickej bezpečnosti.
5. Objednávateľ je povinný informovať Dodávateľa o termíne začiatku vykonania auditu alebo kontroly u Dodávateľa oznámením zaslaným elektronickou poštou, a to najmenej 7 dní pred začatím vykonaním auditu alebo kontroly. Dodávateľ je povinný najneskôr do druhého pracovného dňa od žiadosti Objednávateľa umožniť audítorovi prístup k ním spravovaným aktívam v zmysle Zmluvy, pričom sa však predpokladá, že termíny vykonania auditu budú dohodnuté na základe vzájomnej dohody Objednávateľa a Dodávateľa.
6. Prípadné nedostatky zistené auditom alebo kontrolou je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 70 kalendárnych dní odo dňa oznámenia nedostatku. O audite ako aj o kontrole bude spísaná zápisnica, ktorej obsah bude potvrdený podpisom Dodávateľa, Objednávateľa a osoby vykonávajúcej predmetnú činnosť, resp. povereným zamestnancom za tú ktorú stranu.
7. Náklady, ktoré v súvislosti s auditom alebo kontrolou vzniknú znáša každá strana samostatne. Dodávateľ poskytuje súčinnosť pri výkone auditu a kontroly bezodplatne, resp. prípadné náklady znáša bez nároku na ich náhradu.

Subdodávatelia

1. Ak Dodávateľ využíva pri plnení tejto Zmluvy subdodávateľov, je Dodávateľ povinný subdodávateľa oboznámiť s touto prílohou č. 6 k Zmluve a zabezpečiť jej dodržiavanie zo strany subdodávateľa.
2. Dodávateľ je zodpovedný za akékoľvek konanie, porušenie, opomenutie a/alebo zanedbanie ktoréhokoľvek Subdodávateľa, jeho zamestnancov a/alebo osôb ním poverených, akoby to bolo konanie, porušenie, opomenutie a/alebo zanedbanie Dodávateľa.
3. Dodávateľ je zodpovedný za akúkoľvek škodu spôsobenú subdodávateľom pri plnení povinností ustanovených touto prílohou č. 6 k Zmluve Objednávateľovi alebo koncovému užívateľovi a/alebo iným osobám.

Komunikácia

1. Zmluvné strany sa dohodli, že komunikácia vo veciach podľa tejto prílohy č. 6 k Zmluve realizovaná e-mailom musí byť zasielaná
   a) pre oblasť hlásenia výhradne na adresy oznámené na tento účel Objednávateľom alebo koncovým užívateľom, ak boli oznámené,

b) zasielaná v chránenej forme (napr. chránená heslom, chránená šifrovaním), v závislosti od dohody komunikujúcich strán a citlivosti informácií, ktoré sú obsahom komunikácie.

2. Dodávateľ je povinný bezodkladne oznámiť Objednávateľovi s ohľadom na prijaté bezpečnostné a notifikačné opatrenia všetky potrebné informácie súvisiace s plnením tejto Zmluvy, ktoré majú vplyv na povinnosti koncového užívateľa ako prevádzkovateľa základnej služby.

C. Vylúčené zariadenia

Obmedzenie používania produktu, procesu, služby alebo tretej strany

Ak Národný bezpečnostný úrad rozhodnutím podľa § 27a zakáže alebo obmedzí používanie konkrétneho produktu, procesu, služby alebo tretej strany (ďalej len „Produkt“) a tieto sú používané v rámci Služieb u koncového užívateľa, prijmú sa nasledovné opatrenia:

1. Dodávateľ písomne oznámi Objednávateľovi
   a) identifikáciu takýchto Produktov,
   b) lehotu, v ktorej je najskôr možné Produkt prestať používať v rámci poskytovania Služieb, alebo obmedziť jeho používanie v súlade s rozhodnutím Národného bezpečnostného úradu,
   c) odôvodnenie lehoty podľa písmena b), s uvedením informácií, na základe ktorých Dodávateľ k dĺžke lehoty dospel,
   d) návrh bezpečnostných opatrení na riadenie rizík do času, kým sa Produkt prestane používať, alebo kým dôjde k obmedzeniu jeho používania v rámci poskytovania Služieb,
2. na základe oznámenia podľa prvého bodu sa Objednávateľ a Dodávateľ písomne dohodnú na lehote a časovom harmonograme realizácie vyradenia Produktu z používania, alebo obmedzenia používania Produktu a realizácie bezpečnostných opatrení na riadenie rizík,
3. v súlade s dohodou podľa druhého bodu Objednávateľ režimom Objednávky podľa tejto Zmluvy zadá Dodávateľovi nahradiť Produkty, alebo vykonať činnosti potrebné na obmedzenie jeho používania a vykonať bezpečnostné opatrenia na riadenie rizík.

Certifikát kybernetickej bezpečnosti

Ak Dodávateľ v rámci poskytovania Služieb používa produkty, služby alebo procesy, ktoré majú vydané certifikáty kybernetickej bezpečnosti alebo európske certifikáty kybernetickej bezpečnosti (ďalej len „Certifikáty“) a tieto Certifikáty sú odňaté, prijmú sa nasledovné opatrenia:

1. Dodávateľ písomne oznámi Objednávateľovi
   a) identifikáciu takýchto produktov, služieb alebo procesov,
   b) odporúčanie, či takéto produkty, služby alebo procesy prestať používať, alebo pokračovať v ich používaní po prijatí primeraných opatrení,
   c) lehotu, v ktorej je najskôr možné produkty, služby alebo procesy prestať používať v rámci poskytovania Služieb, alebo prijať primerané opatrenia
   d) odôvodnenie odporúčania podľa písmena b) a lehoty podľa písmena c), s uvedením informácií, na základe ktorých Dodávateľ k záverom dospel,
   e) návrh bezpečnostných opatrení na riadenie rizík do času, kým sa produkt, služba alebo proces prestanú používať, alebo kým dôjde k prijatiu opatrení podľa písmena b),
2. na základe oznámenia podľa prvého bodu sa Objednávateľ a Dodávateľ písomne dohodnú na lehote a časovom harmonograme realizácie vyradenia produktov, služieb alebo procesov z používania, alebo prijatia opatrení podľa písmena b) a realizácie bezpečnostných opatrení na riadenie rizík,
3. v súlade s dohodou podľa druhého bodu Objednávateľ režimom Objednávky podľa tejto Zmluvy zadá Dodávateľovi nahradiť produkty, služby alebo procesy, alebo prijať opatrenia podľa písmena b) a vykonať bezpečnostné opatrenia na riadenie rizík.

ENISA a členské štáty

1. Ak ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) niektorým z oficiálnych dokumentov vydaných a zverejnených pri plnení jej úloh podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 v platnom znení označí produkt, proces, službu alebo tretiu stranu za rizikovú z pohľadu kybernetickej bezpečnosti a Objednávateľ tento dokument doručí Dodávateľovi a požiada ho o to, Dodávateľ vypracuje písomné oznámenie ako pri odňatí certifikátu

kybernetickej bezpečnosti. Zmluvné strany následne postupujú rovnako, ako pri odňatí certifikátu kybernetickej bezpečnosti.

2. Ak iný členský štát Európskej únie postupom podľa svojho právneho poriadku vydá rozhodnutie, ktoré je povahou účinkov obdobné rozhodnutiu Národného bezpečnostného úradu podľa § 27a Zákona o kybernetickej bezpečnosti a Objednávateľ toto rozhodnutie doručí Dodávateľovi a požiada ho o to, Dodávateľ vypracuje písomné oznámenie ako pri zákaze alebo obmedzení používania Produktu. Zmluvné strany následne postupujú rovnako, ako pri zákaze alebo obmedzení Produktu s tým, že okrem nahradenia alebo obmedzenia používania sa môžu dohodnúť aj na prijatí primeraných opatrení na predchádzanie rizík.