II

(Informacije)

INFORMACIJE INSTITUCIJA, TIJELA, UREDA I AGENCIJA EUROPSKE UNIJE

EUROPSKA KOMISIJA

OBAVIJEST KOMISIJE

Smjernice o godišnjim revizorskim izvješćima koja se dostavljaju u skladu s člankom 15. stavkom 8. Direktive 2014/40/EU u kontekstu sustava sljedivosti za duhanske proizvode

(2020/C /)

(2020/C 167/01)

IZJAVA O OGRANIČENJU ODGOVORNOSTI: Svrha je ovog dokumenta dati smjernice ovlaštenom revizoru o opsegu revizije i postupku za podnošenje godišnjeg izvješća o reviziji. On nije pravno obvezujući, ali pruža općenite smjernice s preporukama i razmišljanja o primjerima najbolje prakse. Ovim se Smjernicama ne dovode u pitanje nacionalni propisi.

1. **Uvod**

Kao odgovor na problem nezakonite trgovine, člankom 15. Direktive 2014/40/EU Europskog parlamenta i Vijeća ([1]) propisana je uspostava sustava sljedivosti duhanskih proizvoda na razini EU-a. Sustav je operativan od 20. svibnja 2019.

Kao dio tog sustava, člankom 15. stavkom 8. Direktive 2014/40/EU utvrđeno je da države članice osiguravaju da proizvođači i uvoznici duhanskih proizvoda sklapaju ugovore o pohrani podataka s neovisnom trećom stranom („treća strana koja je pružatelj tih usluga") u svrhu uspostave sustava za pohranu podataka; u tim objektima pohranjuju se podaci o duhanskim proizvodima pojedinačnih proizvođača i uvoznika („primarni repozitorij").

Kako bi se zaštitio neovisan rad sustava sljedivosti, člankom 15. stavkom 8. Direktive 2014/40/EU utvrđeno je da aktivnosti primarnog repozitorija i treće strane koja je pružatelj tih usluga mora pratiti vanjski revizor. Tog revizora predlaže i plaća proizvođač duhanskih proizvoda, a odobrava Komisija. Vanjski revizor svoju ocjenu dostavlja nadležnim tijelima i Komisiji u godišnjem izvješću, u kojemu se posebno procjenjuju sve nepravilnosti u pogledu pristupa.

Svrha je ovog dokumenta dati smjernice ovlaštenom revizoru o opsegu revizije i postupku za podnošenje godišnjeg izvješća o reviziji. Trebalo bi ga čitati zajedno s Provedbenom uredbom Komisije (EU) 2018/574 ([2]), kojom su utvrđeni tehnički zahtjevi za uspostavu i rad sustava sljedivosti, uključujući za primarne repozitorije, i Delegiranom uredbom Komisije (EU) 2018/573 ([3]) u kojoj su definirani ključni elementi ugovora o pohrani podataka koji se sklapaju u okviru sustava sljedivosti duhanskih proizvoda.

([1]) Direktiva 2014/40/EU Europskog parlamenta i Vijeća od 3. travnja 2014. o usklađivanju zakona i drugih propisa država članica o proizvodnji, predstavljanju i prodaji duhanskih i srodnih proizvoda i o stavljanju izvan snage Direktive 2001/37/EZ (SL L 127, 29.4.2014., str. 1.).

([2]) Provedbena uredba Komisije (EU) 2018/574 od 15. prosinca 2017. o tehničkim standardima za uspostavu i rad sustava sljedivosti duhanskih proizvoda (SL L 96, 16.4.2018., str. 7.).

([3]) Delegirana uredba Komisije (EU) 2018/573 od 15. prosinca 2017. o ključnim elementima ugovora o pohrani podataka koji se sklapaju u okviru sustava sljedivosti duhanskih proizvoda (SL L 96, 16.4.2018., str. 1.).

Ovaj dokument ponuđen je kao alat za pomoć ovlaštenim revizorima; radi se o smjernicama koje nisu obvezujuće i ne stvaraju nikakve nove pravne obveze. U mjeri u kojoj bi se ovim smjernicama mogli tumačiti pravni akti, stajalištem Komisije ne dovodi se u pitanje bilo koje tumačenje Direktive 2014/40/EU koje bi mogao objaviti Sud Europske unije.

2. **Opći kontekst revizija**

Svaki primarni repozitorij o kojem je proizvođač sklopio ugovor podliježe godišnjem postupku revizije. Ako ista treća strana koja je pružatelj tih usluga vodi dva ili više primarnih repozitorija, za svaki od tih repozitorija trebala bi se provesti zasebna revizija i dostaviti zasebno izvješće o reviziji.

Trebalo bi provoditi revizije primarnog repozitorija i s njim povezanih usluga, što uključuje procjenu ispunjava li treća strana koja je pružatelj tih usluga (i, ako je primjenjivo, njegovi podizvođači) relevantne zahtjeve iz Direktive 2014/40/EU, Provedbene uredbe (EU) 2018/574 i Delegirane uredbe (EU) 2018/573.

Svaki proizvođač ili uvoznik mora obavijestiti Komisiju o revizoru kojega predlaže za reviziju svojeg primarnog repozitorija i odgovarajuće treće strane koja je pružatelj tih usluga. Svi predloženi revizori podliježu odobrenju Komisije.

3. **Opseg revizija**

Područje primjene i cilj

Izvješća o reviziji dostavljaju se kako bi se nadležna nacionalna tijela i Komisiju izvijestilo o nalazima revizora, posebno u pogledu svih nepravilnosti u pogledu pristupa podacima pohranjenima u primarnim repozitorijima.

U izvješću o reviziji svakom od šest područja navedenih u nastavku trebalo bi posvetiti posebno poglavlje. U svakom poglavlju trebale bi biti navedene točke provjere odgovarajuće domene, kako su navedene na kontrolnom popisu u Prilogu.

Revizije bi trebalo provoditi u skladu s tim kontrolnim popisom, kojim su utvrđene obvezne domene i točke provjere u skladu s normom ISO/IEC 27001:2013 o sustavima upravljanja informacijskom sigurnošću ([4]). U tu svrhu revizori bi trebali uzeti u obzir da se u članku 10. Delegirane uredbe Komisije (EU) 2018/573 upućuje na ISO/IEC 27001:2013 kao preferiranu normu za upravljanje informacijskom sigurnošću u kontekstu upravljanja primarnim repozitorijima.

Područje	Ciljevi
Organizacijska i fizička sigurnost	Uspostaviti okvir za upravljanje informacijskom sigurnošću unutar organizacije. Osigurati da zaposlenici i izvođači razumiju svoje odgovornosti i da su prikladni za uloge koje im se povjeravaju. Spriječiti neovlašten fizički pristup, nanošenje štete ili uplitanje u organizaciju, uključujući podatke i sredstva za obradu informacija. Spriječiti gubitke, oštećenja, krađe ili ugrožavanje imovine i prekide u radu organizacije.
Sigurnost operacija	Osigurati ispravan i siguran rad objekta za obradu podataka. Zaštititi od gubitka podataka. Bilježiti događaje i generirati dokaze. Osigurati integritet operativnih sustava. Spriječiti iskorištavanje tehničkih slabih točaka.
Kontrola pristupa (korisnici i aplikacije)	Ograničiti pristup informacijama i objektima za obradu podataka. Osigurati pristup ovlaštenom korisniku i spriječiti neovlašteni pristup sustavu i uslugama. Učiniti korisnike odgovornima za zaštitu vlastitih podataka za autentifikaciju. Spriječiti neovlašteni pristup sustavima i aplikacijama. Osigurati da je informacijska sigurnost osmišljena i da se provodi unutar razvojnog ciklusa informacijskih sustava.

([4]) ISO/IEC 27001:2013. Informacijska tehnologija – sigurnosne tehnike – sustavi upravljanja informacijskom sigurnošću – zahtjevi. Zahtjevi utvrđeni u normi ISO/IEC 27001:2013 općenite su prirode i osmišljeni su tako da budu upotrebljivi za sve organizacije, bez obzira na njihovu vrstu, veličinu ili prirodu.

Područje	Ciljevi
Sigurnost komunikacija	Osigurati ispravnu i djelotvornu upotrebu kriptografije za zaštitu povjerljivosti, autentičnosti i/ili cjelovitosti informacija. Osigurati zaštitu informacija u mrežama i pripadajućim pratećim objektima za obradu podataka. Održavati sigurnost informacija koje se prenose unutar organizacije i unutar vanjskih subjekata.
Kontinuitet poslovanja	Osigurati dosljedan i djelotvoran pristup upravljanju incidentima povezanima sa sigurnošću informacija, uključujući komunikaciju o sigurnosnim događajima i sigurnosnim slabostima. Kontinuitet informacijske sigurnosti trebao bi biti ugrađen u sustave upravljanja kontinuitetom poslovanja organizacije. Osigurati dostupnost objekata za obradu podataka. Izbjeći kršenje pravnih, zakonskih, regulatornih ili ugovornih obveza povezanih s informacijskom sigurnošću te neispunjavanje sigurnosnih zahtjeva.
Integritet imovine i podataka	Utvrditi imovinu organizacije i primjerenih odgovornosti za njezinu zaštitu. Osigurati odgovarajuću razinu zaštite podataka. Spriječiti neovlašteno otkrivanje, mijenjanje, uklanjanje ili uništavanje informacija pohranjenih na nosačima podataka.

Zaključci i preporuke

Treba navesti zaključke revizije za svaku točku provjere navedenu u kontrolnoj listi.

U izvješću o reviziji trebalo bi naglasiti i podrobno objasniti nalaze koji se odnose na nesukladnosti ili druge utvrđene rizike. Nalaze bi trebalo popratiti primjerenim preporukama u kojima se navode mjere potrebne da bi se eliminirali problemi i nedostaci utvrđeni tijekom revizije.

4. **Postupovni aspekti**

Učestalost

Revizori su dužni podnositi izvješća o reviziji na godišnjoj osnovi. Budući da je sustav sljedivosti postao operabilan 20. svibnja 2019., revizori se pozivaju da svoje prvo godišnje izvješće o reviziji koje obuhvaća prvu godinu primjene sustava sljedivosti (tj. od 20. svibnja 2019. do 19. svibnja 2020.) dostave do 30. studenoga 2020. Nakon toga revizori svoja godišnja izvješća za sljedeće godine primjene sustava trebaju podnositi do kraja listopada svake kalendarske godine.

Daljnje postupanje po reviziji

Ako se provodi daljnje postupanje kako bi se procijenilo je li treća strana koja je pružatelj usluga na odgovarajući način provela preporuke iz godišnjeg izvješća o reviziji, revizor se poziva da, ako je moguće, rezultate dostavi Komisiji i nacionalnim nadležnim tijelima u roku od tri mjeseca od podnošenja godišnjeg izvješća o reviziji.

5. **Postupovni aspekti izvješća o reviziji**

Informacije o revizorima

Imena revizora i, ako je to primjenjivo, povezanog revizorskog društva ili povezanih revizorskih društava, trebalo bi navesti u uvodu u izvješće o reviziji.

Oblik

Izvješće o reviziji treba dostaviti u elektroničkom obliku (pretraživ, nezaštićeni PDF).

Revizori se pozivaju da godišnja izvješća dostavljaju po mogućnosti na engleskom jeziku.

Postupak podnošenja

Godišnje izvješće o reviziji i sva izvješća o daljnjim postupanjima nakon godišnjeg izvješća treba dostavljati elektroničkim putem e-porukom na adresu SANTE-TT-SW@ec.europa.eu sa sljedećim naslovom: „Izvješće o reviziji [daljnjem postupanju nakon izvješća o reviziji] za [godina] – [naziv proizvođača naručitelja] – [naziv treće strane koja je pružatelj usluga, nad kojom se vrši revizija]”

Transparentnost

U cilju promicanja opće transparentnosti i pouzdanosti sustava sljedivosti duhanskih proizvoda, Komisija poziva proizvođače duhanskih proizvoda da se na dobrovoljnoj bazi dogovore sa svojim revizorima o tome da se Komisiji dostavlja i javna verzija njihova izvješća o reviziji, bez osobnih i poslovno osjetljivih podataka.

Takve javne verzije izvješća o reviziji bit će objavljene na posebnoj internetskoj stranici Europske komisije.

PRILOG

Kontrolni popis za revizije primarnih repozitorija

Domena	Točke provjere ([1])	Regulatorne smjernice	Smjernice u pogledu dokazâ
Organizacijska i fizička sigurnost	**A.6. Organizacija informacijske sigurnosti** — A.6.1. Unutarnja organizacija — A.6.2. Mobilni uređaji i rad na daljinu **A.7. Sigurnost u pogledu zaposlenika** — A7.1. Prije zaposlenja — A7.2. Tijekom radnog odnosa — A7.3. Pri prestanku radnog odnosa i promjeni zaposlenja **A.11. Fizička sigurnost i sigurnost okruženja** — A.11.1. Sigurna područja — A.11.2. Oprema	U vezi s točkama A.6. i A.11.: Repozitorij se fizički mora nalaziti na području EU-a. Podaci se ne smiju pohranjivati u trećoj zemlji ni prenositi u treću zemlju. (članak 15. stavak 8. Direktive 2014/40/EU) Repozitorij mora biti zaštićen sigurnosnim postupcima i sustavima kojima se osigurava da se pristup repozitorijima odobrava samo nadležnim tijelima država članica, Komisiji i vanjskim revizorima. U vezi s točkom A.7.: Pružatelj usluga koji upravlja primarnim repozitorijem, kao i njegovi podizvođači, moraju biti neovisni i obavljati svoje funkcije nepristrano. Vrijede zahtjevi u pogledu pravne neovisnosti, financijske neovisnosti i nepostojanja sukoba interesa. (članak 35. Provedbene uredbe (EU) 2018/574)	Organigram organizacije, opisi poslova koje je potpisalo ključno osoblje, pohađani tečajevi važni za odgovarajuće uloge. Popis imenovanja (službenik za informacijsku sigurnost, engl. „Central Informatics Security Officer”, CISO, službenik za zaštitu podataka engl. „Data Protection Officer”, DPO) i opis odgovornosti i zadataka za uloge u području sigurnosti. Dokazi o sudjelovanju osoblja u osposobljavanjima (npr. prihvaćen poziv, datum i program osposobljavanja, potpisan popis sudionika tijekom informativne radionice itd.) Politike/postupci za sigurnost u pogledu zaposlenika redovito se preispituju i ažuriraju (evidencija o izvođenju postupaka). Osnovna provedba fizičkih mjera sigurnosti i nadzora okoline, primjerice brava na vratima i ormarima, protuprovalnog alarma, protupožarnog alarma, aparatâ za gašenje požara, nadzornih kamera itd. Popis osoblja koje ima ovlaštenje za pristup i autorizacijski podaci. Dokumentirana politika za fizičke sigurnosne mjere i nadzor okoline, uključujući opis relevantnih objekata i sustava. Detaljan inventar uključujući hardverske resurse koji se koriste u administrativne svrhe.
Sigurnost operacija	**A.12. Sigurnost operacija** — A.12.1. Operativni postupci i odgovornosti — A.12.3. Zaštitni mehanizmi — A.12.4. Evidencija i nadzor — A.12.5. Kontrola operativnog softvera — A.12.6. Upravljanje tehničkim slabim točkama	U vezi s točkom A.12.3.: Za sve sastavnice repozitorija i sve usluge moraju postojati dostatni zaštitni mehanizmi. (članak 25. stavak 1. točka (i) Provedbene uredbe (EU) 2018/574) U vezi s točkom A.12.4.: Repozitorij mora sadržavati cjelovitu evidenciju	Ispravno dokumentiran postupak za održavanje optimalne sigurnosti koji je odobrilo više rukovodstvo. Jasno definiran postupak održavanja minimalne sigurnosti. Popis svih ugovora s trećim stranama ([2]). Eksplicitni sigurnosni zahtjevi u ugovorima s trećim stranama koje isporučuju IT proizvode, IT usluge, obavljaju eksternalizirane poslovne procese, usluge službe za pomoć itd.

Domena	Točke provjere ([1])	Regulatorne smjernice	Smjernice u pogledu dokazâ
		(„revizijski trag”) o svim radnjama povezanima s pohranjenim podacima korisnika koji su te radnje izvršili, uključujući vrstu izvršenih radnji i povijest pristupa korisnika. (članak 25. stavak 1. točka (m) Provedbene uredbe (EU) 2018/574) Smjernice o dokazima u vezi s događajima i evidentiranjem: — pokušaji prijave i odjave (i uspješni i neuspješni pokušaji) — ponovna pokretanja poslužitelja baze podataka — naredbe korisnikâ s ovlastima administratora sustava — pokušaji povrede integriteta podataka (ako izmijenjeni ili uneseni podaci ne odgovaraju ograničenju vrijednosti, ograničenju jedinstvenosti ili referencijalnom ograničenju.) — operacije odabira, unosa, ažuriranja i brisanja — pohranjena izvođenja postupaka — neuspješni pokušaji pristupa bazi podataka ili tablici (neuspješne autorizacije) — izmjene u tablicama kataloga sustava	Dokumentirana sigurnosna politika za ugovore s trećim stranama Dokumentirani komentari ili evidencija izmjenâ politike. Uspostavljeni su i provode se politika i/ili postupak upravljanja rizikom/procjene rizika povezanog s prodavateljem. Dokumentirana izmjena odnosa s trećim stranama ili prestanak takvih odnosa. Izvješća o povezanim aktivnostima informiranja i osposobljavanja. Sustavi, alati i postupci za otkrivanje i analizu incidenata. Dokumentirana politika otkrivanja i analize incidenata koja obuhvaća pitanja svrhe, opsega, uloga i odgovornosti te koordinacije među svim povezanim subjektima, uključujući klijente. Postojanje izvješća o otkrivanju i eskalaciji prošlih sigurnosnih incidenata. Ažurirana dokumentacija o politici otkrivanja incidenata i s tim povezanim postupcima i sustavima. Inventar otkrivenih i eskaliranih velikih prošlih incidenata, uključujući s tim povezane informacije (uzrok, posljedice, redoslijed poduzetih mjera). Dokazi o provedenim kibervježbama uključujući datume njihove provedbe.
Kontrola pristupa (korisnici i aplikacije)	**A.9. Kontrola pristupa** — A.9.1. Poslovni zahtjevi u pogledu kontrole pristupa — A.9.2. Upravljanje pristupom korisnikâ — A.9.3. Odgovornosti korisnika	U vezi s točkom A.9.: Pristup sustavima za pohranu podataka i podacima koji su u njima pohranjeni mora biti ograničen na države članice, Europsku komisiju i ovlaštene vanjske revizore. (članak 15. stavak 8. Direktive 2014/40/EU; članak 25. stavak 1. točka (j) Provedbene uredbe (EU) 2018/574)	Politika kontrole pristupa uključujući opis uloga, skupinâ, pravâ pristupa, postupaka za dodjelu i oduzimanje prava pristupa informacijskim sustavima. Definicija pravila za brisanje korisničkih računa koji se više ne koriste nakon kratkog razdoblja.

Domena	Točke provjere ([1])	Regulatorne smjernice	Smjernice u pogledu dokazâ
	— A.9.4. Kontrola pristupa sustavu i aplikaciji **A.14. Nabava, razvoj i održavanje sustava** — A.14.2. Sigurnost u postupcima razvoja i podrške		Matrice za kontrolu pristupa (npr. kontrolna matrica za razdvajanje dužnosti, kontrolu pristupa na daljinu itd.). Odjeljak o pravu pristupa u politici/postupcima kontrole pristupa. Politika kontrole pristupa uključuje registar mapiranja prava pristupa relevantnim resursima i/ili postupcima. Prilagođeni i dokumentirani administratorski računi s posebnim pravima pristupa za odgovarajuće osoblje. Dokumentirani postupak upravljanja administratorskim računima. Raspoloživa evidencija aktivnosti na administratorskom računu. Administrativni informacijski sustavi izolirani i odvojeni od ostatka infrastrukture u cilju veće otpornosti. Formalno dokumentirani zahtjevi za softver u cilju osiguravanja kompatibilnosti.
Sigurnost komunikacije	**A.10. Kriptografija** — A.10.1. Kontrola kriptografije **A.13. Sigurnost komunikacije** — A.13.1. Upravljanje sigurnošću mreže — A.13.2. Prijenos informacija	U vezi s točkom A.13.: Razmjena podataka između primarnih repozitorija i sekundarnog repozitorija i usmjerivača mora se odvijati u skladu s tehničkim specifikacijama koje je utvrdio pružatelj koji upravlja sekundarnim repozitorijem. (članak 28. stavak 1. Provedbene uredbe (EU) 2018/574) Sva elektronička komunikacija mora se odvijati upotrebom sigurnih sredstava. Primjenjivi sigurnosni protokoli i pravila o povezivosti moraju se temeljiti na javnim otvorenim standardima. (članak 36. stavak 1. Provedbene uredbe (EU) 2018/574)	Odgovarajući kriptografski postupci postoje. Zaštitne mjere kojima se štiti tajnost privatnih ključeva su uspostavljene. Politika i/ili postupak konfiguracije sustava uspostavljeni su i provode se. Tablice konfiguracije sustava. Vremenski raspored i plan ciklusâ pregleda konfiguracije sustava. Dokumentirane prethodne vježbe/testiranja kritičnih informacijskih sustava. Vremenski raspored i plan pregledâ sigurnosne konfiguracije.

Domena	Točke provjere ([i])	Regulatorne smjernice	Smjernice u pogledu dokazâ
			Dokumentacija o provedbi odvajanja mreže i sustava te podataka. Izvješća o praćenju kritičnih mrežnih i informacijskih sustava. Dokumentirana politika postupaka praćenja, uključujući minimalne zahtjeve u pogledu praćenja. Dokaz o postojećim alatima za sustave praćenja.
Kontinuitet poslovanja	**A.16. Upravljanje incidentima povezanima s informacijskom sigurnošću** — A.16.1. Upravljanje incidentima povezanima s informacijskom sigurnošću i poboljšanja **A.17. Aspekti upravljanja kontinuitetom poslovanja koji se odnose na informacijsku sigurnost** — A.17. Aspekti upravljanja kontinuitetom poslovanja koji se odnose na informacijsku sigurnost — A.17.1. Kontinuitet informacijske sigurnosti — A.17.2. Redundantnost **A.18. Sukladnost** — A.18.1. Sukladnost sa zakonskim i ugovornim obvezama	U vezi s točkom A.17.: Mjesečna dostupnost svih sastavnica i usluga repozitorija mora iznositi najmanje 99,5 %. (članak 25. stavak 1. točka (i) Provedbene uredbe (EU) 2018/574) Prenosivost podataka mora biti osigurana u skladu s važećim zajedničkim podatkovnim rječnikom. (članak 36. stavak 2. Provedbene uredbe (EU) 2018/574) Pružatelj usluga mora uspostaviti primjenjiv izlazni plan. (članak 19. Delegirane uredbe (EU) 2018/573) U vezi s točkom A.18.1.: Aktivnosti obrade podataka moraju biti u skladu s Uredbom (EU) 2016/679 (Opća uredba o zaštiti podataka) i s ugovorom o obradi podataka sklopljenim između pružatelja usluga primarnog repozitorija i pružatelja usluga sekundarnog repozitorija.	Formalno dokumentirana strategija za kontinuitet pružanja usluga, uključujući ciljno vrijeme oporavka za ključne usluge i procese. Planovi za izvanredne okolnosti za ključne sustave, uključujući jasne korake i postupke za uobičajene prijetnje, pokretače aktivacije, korake i ciljno vrijeme oporavka. Evidencija o pojedinačnim aktivnostima osposobljavanja te izvješća nakon njihove provedbe. Mjere koje su na snazi za suočavanje s katastrofama (npr. potres, poplava, požar), kao što su pričuvni objekti u drugim regijama, sigurnosne kopije ključnih podataka koje moraju biti pohranjene na udaljenoj lokaciji (geografski različitoj od lokacije na kojoj se podaci prikupljaju i obrađuju), na dovoljnoj udaljenosti da se izbjegne svaka šteta od katastrofe na glavnoj lokaciji itd. Formalno dokumentirana politika/postupci za aktivaciju sposobnosti oporavka od katastrofa, uključujući popis prirodnih i/ili velikih katastrofa koje bi mogle utjecati na pružanje usluga te popis sposobnosti oporavka od katastrofa (sposobnosti dostupne interno ili one koje pružaju treće strane). Evidencija pojedinačnih aktivnosti osposobljavanja za osoblje uključeno u operacije oporavka od katastrofa.

Domena	Točke provjere ([1])	Regulatorne smjernice	Smjernice u pogledu dokazâ
Imovina i integritet podataka	**A.8. Upravljanje imovinom** — A.8.1. Odgovornost za imovinu — A.8.2. Klasifikacija informacija — A.8.3. Rukovanje nosačima podataka	U vezi s točkom A.8.1.: Odnosi se na imovinu povezanu s bazama podataka i repozitorijima (tj. sustav upravljanja bazom podataka, objekti iz baze podataka, poslužitelj za bazu podataka). U vezi s točkom A.8.2.: Visoka osjetljivost. Podaci sadržavaju osjetljive poslovne informacije. Podaci se upotrebljavaju za istrage koje provode nacionalna tijela i tijela EU-a.	Dokumentirana politika/postupci za upravljanje imovinom, uključujući uloge, odgovornosti, imovinu i konfiguracije na koje se politika odnosi. Popis ključne imovine kojom se upravlja centralizirano i ključnih konfiguracija sustava kojima se upravlja i koje se održavaju. Upravljanje softverskom/hardverskom imovinom formalno dokumentirano funkcionira. Ažurirana politika/postupci upravljanja imovinom, komentari na temelju pregledâ i/ili evidencija izmjena.

([1]) Redni brojevi točaka provjere odgovaraju rednim brojevima u normi ISO/IEC 27001:2013. U slučaju odstupanja, upućivati na redni broj koji je upotrijebljen u ovom dokumentu.
([2]) Treća strana neovisni je subjekt uključen u funkcioniranje usluge (ali ne glavni) i ima manji interes u pružanju usluge (npr. u ranijoj fazi (dobavljač, prodavatelj) ili u kasnijoj fazi (distributer, preprodavatelj).