Tehnični in organizacijski ukrepi za varstvo podatkov v skladu s Splošno uredbo o varstvu podatkov EU

– Bisnode TOM –

Februar 2020

VSEBINA

Obseg

V skladu s Splošno uredbo o varstvu podatkov EU (GDPR) je vsak, ki zbira, obdeluje ali uporablja osebne podatke, dolžan sprejeti ustrezne tehnične in organizacijske ukrepe (v skladu z 32. členom GDPR), ki so potrebni za zagotavljanje ustrezne ravni varstva osebnih podatkov.
Ta dokument opisuje zaščitne ukrepe za zagotavljanje »varnosti obdelave«, kot je opredeljeno v 32. členu GDPR, na območju Skupine Bisnode (v tem dokumentu imenovana Bisnode).

Ukrepi, ki se nanašajo na ZAUPNOST (32. člen (1) GDPR)

NADZOR NAD DOSTOPOM DO PROSTOROV

Namen nadzora dostopa je preprečiti, da bi nepooblaščene osebe pridobile dostop do tehničnih sistemov, ki se uporabljajo za obdelavo osebnih podatkov.

Nadzor nad dostopom do prostorov družbe Bisnode

Dostop do zgradb družbe Bisnode je urejen z nadzorom dostopa. Za uslužbence družbe Bisnode ta sestoji primarno iz elektronskih ključev, ki omogočajo dostop do poslovnih prostorov v obsegu pravic dostopa posameznega ključa. Pravice dostopa so časovno (dovoljena uporaba določene dni v tednu in ob določenih urah v dnevu) ter prostorsko (za določene dele poslovnih prostorov) prilagojene.

	Ukrepi
01	Izvajajo se ukrepi nadzora dostopa do prostorov/zgradbe.
02	V uporabi je učinkovit nadzor dostopa, ki deluje tudi v primeru okvare tehnične opreme (izpad električnega napajanja ali podobno): npr. magnetne kartice/kartice s čipom, ključi, video in alarmni sistemi.
03	V uporabi je sistem za nadzor dostopa, v katerem so opredeljeni pooblaščeni uslužbenci.
04	V uporabi je beleženje dostopov, kar zagotavlja sledljivost nepooblaščenih dostopov.
05	V uporabi so predpisi za osebje tretjih oseb, čistilno osebje, serviserje, ki zagotavljajo, da ne pride do nepooblaščenega dostopa.

06	Dostop do računalniškega središča je zaščiten in izvajajo se redni pregledi ukrepov. Računalniški center je certificiran s standardom ISO 27001.
07	Strežniki se nahajajo ločenem prostoru v prilagojeni omari za strežnike in so zaščiteni pred nepooblaščenim fizičnim dostopom.
08	Prenosniki se shranjujejo v zaklenjene zavarovane prostore.
09	Varnostne kopije podatkov (kasete, CD-ji, DVD-ji) so shranjene v sefih ali drugih zavarovanih prostorih.
10	Pooblastila za dostop, ki niso več potrebna, redno umikamo.
11	Izvajajo se redni pregledi za zagotavljanje učinkovitosti sprejetih ukrepov.

NADZOR DOSTOPA

Nadzor vstopa vključuje ukrepe za preprečevanje uporabe sistemov za obdelavo podatkov (logična varnost) s strani nepooblaščenih oseb.

Nadzor dostopa v poslovnih prostorih družbe Bisnode

Dostop do sistemov za obdelavo imajo le določeni zaposleni, ki so podpisali ustrezno izjavo o zaupnosti podatkov. Če se dejavnosti izvajajo prek zunanjega dostopa, so te t. i. povezave VPN šifrirane v skladu z najsodobnejšimi standardi, zahtevano pa je tudi dodatno preverjanje istovetnosti. Identifikacija z uporabniškim imenom in varnim geslom, samodejni zaklepni mehanizmi za računalnike in šifriranje nosilcev mobilnih podatkov so obvezni.

Poleg tega so IT-sistemi družbe Bisnode pred zunanjimi motnjami zaščiteni s tehnologijo požarnega zidu.

Požarni zid centralno upravlja in vzdržuje matično podjetje Bisnode AB, Solna (Švedska).

	Ukrepi
01	Ustrezni ukrepi za preprečevanje nepooblaščene uporabe IT-sistemov so opisani, se izvajajo in so predmet rednih pregledov. (npr. ID uporabnika, dodelitev gesla, samodejen zaklep zaslona z aktivacijo gesla).

02	Vsaka pooblaščena oseba ima lastno geslo, ki ga pozna samo on/-a.
03	Sprejete so smernice za nastavitev, upravljanje, dodelitev in uporabo gesel.
04	Pri shranjevanju gesel, ki so zahtevana v kontekstu obdelave podatkov, se varnostni standardi upoštevajo in redno preverjajo.
05	V uporabi je nadzorovan proces za obnovitev pozabljenih gesel.
06	Vse ključne dejavnosti, povezane z obdelavo podatkov, se samodejno beležijo v IT-sisteme, tako da je zlorabe mogoče izslediti.
07	Potencialni oddaljeni dostop do sistemov za obdelavo podatkov mora biti omejen na pooblaščeno osebje.
08	Izvajajo se ukrepi, ki preprečujejo ali vsaj omogočajo zaznavanje nepooblaščene uporabe teh objektov. Učinkovitost teh ukrepov dokazujejo redni pregledi (npr. funkcionalna razporeditev uporabniških naprav, beleženje uporabe sistema in analiza dnevnika).
09	Nove ranljivosti v IT-sistemih so posredovane, se odkrivajo, analizirajo in po potrebi odpravijo z namenom preprečevanja vdora nepooblaščenih tretjih oseb v IT-sisteme.
10	Poleg rednih nadzorov se izvajajo tudi drugi neodvisni pregledi učinkovitosti ukrepov za preprečevanje vdora nepooblaščenih tretjih oseb (kot je preskus vdora).
11	Opredeljeni so organizacijski in tehnični postopki ter metode za upravljanje incidentov (upravljanje zaznanih ali domnevnih varnostnih incidentov, prekinitev, izpadov itd.).

Nadzor dostopa pri upravljavcu podatkovnega centra

Z namenom zaščite sistemov, ki se uporabljajo za družbo Bisnode, upravljavec podatkovnega centra izvaja visokokakovostne funkcije požarnega zidu znotraj omrežne plasti in tudi izdelkov za dostop.

NADZOR NAD DOSTOPOM – POOBLASTILO

Nadzor nad dostopom vključuje ukrepe za zagotavljanje, da lahko uporabniki sistemov za obdelavo podatkov dostopajo do podatkov, do katerih lahko dostopajo le glede na dodeljene pravice dostopa, in da se podatki med obdelavo, uporabo in po shranjevanju ne berejo, kopirajo, spreminjajo ali odstranjujejo nepooblaščeno.

Nadzor nad pooblastilom v prostorih družbe Bisnode

Družba Bisnode je opredelila in dokumentirala notranje standarde za ravnanje z dovoljenji.

Dovoljenje ustreza načelu »potrebno je vedeti«.

	Ukrepi
01	Obstaja dokumentirano upravljanje pooblastil, v katerem je opredeljeno, kako je za pooblastila mogoče zaprositi, jih razrešiti, odobriti in umakniti.
02	Obstaja funkcionalna/osebna ločitev odobritve pravic (organizacijska) in pooblastila (tehnična).
03	Med vsakim nosilcem podatkov in enim pooblaščenim uporabnikom (zlasti za omrežne naprave) obstaja jasna zadolžitev.
04	Obnavljanje podatkov iz varnostnih kopij (kdo sme naložiti podatke varnostnih kopij, na čigavo zahtevo in kdaj) ureja zavezujoč postopek.
05	Uporaba programa in datoteke je zabeležena in se vrednoti naključno.
06	Družba Bisnode je razvila ali vzdržuje aplikacije, ki se uporabljajo pri obdelavi podatkov.
07	Med razvojem programa se uporablja funkcionalno ločevanje (testno in produkcijsko okolje).

Nadzor dostopa pri upravljavcu podatkovnega centra

Do obsega, do katerega upravljavec podatkovnega centra v imenu družbe Bisnode prevzame nastavitev uporabnikov in privilegijev aplikativne ravni (aplikativna raven), je v osnovi zavezan istim varnostnim standardom, kot veljajo na območju družbe Bisnode.

Odstopanja so dovoljena samo na osnovi pisnih navodil družbe Bisnode. Družba Bisnode je odgovorna za določitev specifikacij, kako naj upravljavec podatkovnega centra oblikuje koncepte pooblastil za določene aplikacije.

NADZOR LOČEVANJA

Zahteva za ločevanje vključuje ukrepe za zagotavljanje, da se podatki, zbrani za različne namene, obdelujejo ločeno.

Zahteva za ločevanje družbe Bisnode

V zvezi s splošno obdelavo podatkov v družbi Bisnode (podatkov o uslužbencih, podatkov o dobavitelju, podatkov o strankah) se zahteva za ločevanje izvaja, na primer, s fizično ločitvijo in shranjevanjem na ločenih sistemih ali nosilcih podatkov ter z ločitvijo proizvodnega, testnega in razvojnega okolja naših aplikacij in IT-sistemov. Ustrezni koncepti pooblastil, kot tudi pravice do baze podatkov. Poleg tega se v programski opremi izvaja logična ločitev strank.

V okviru obdelave podatkov v družbi Bisnode, zlasti prejema in zagotavljanja podatkov strank v kontekstu poslovanja družbe Bisnode, ločitev v smislu varstva podatkov pretežno poteka na osnovi uporabe. Za ta namen so sprejeti potrebni previdnostni ukrepi (strojna in programska oprema).

	Ukrepi
01	Podatki različnih nalog obdelave podatkov po naročilu stranke med seboj in s podatki drugih strank so v družbi Bisnode na fizičen ali logičen način obdelani ločeno.
02	Obstaja koncept pooblastila, ki upošteva ločeno obdelavo naročenih podatkov s podatki drugih strank.

Zahteva za ločevanje pri upravljavcu podatkovnega centra
Upravljavec podatkovnega centra vse podatke loči fizično ali logično vsaj na ravni strank. Če so plasti družbe Bisnode izkoriščene za upravljavca podatkovnega centra, običajno obstajajo dodatne ravni ločevanja na osnovi sistema ali podatkovne baze.

PSEVDONIMIZACIJA

Psevdonimizacija se uporablja pri statističnih analizah, ocenah pogostosti in primerljivih vrednotenjih, kadar poznavanje zadevne osebe dejansko ni potrebno.

Ukrepi, ki se nanašajo na INTEGRITETO (32. člen (1) GDPR)

NEPREKINJEN NADZOR PRENOSA

Nadzor prenosa vključuje ukrepe za zagotavljanje, da osebnih podatkov ni mogoče brati, kopirati, spreminjati ali odstraniti med elektronskim prenašanjem oziroma med transportom ali shranjevanjem na nosilce podatkov, ter da je mogoče preveriti in določiti, na katera mesta poteka oddaja prenosa podatkov s pomočjo naprav za oddajanje podatkov.

Nadzor prenosa v družbi Bisnode
V zvezi s splošno obdelavo podatkov v družbi Bisnode (podatkov o uslužbencih, podatkov o dobavitelju, podatkov o strankah) je nadzor prenosa (nadzor oddaje, nadzor transporta) zagotovljen z ustreznimi tehničnimi ukrepi. Slednji vključujejo požarne zidove, virusno zaščito, tunele VPN, šifriranje podatkov, zaščito posameznih dokumentov z geslom. Za elektronski prenos zaupnih podatkov se uporabljajo samo mediji za shranjevanje, ki omogočajo šifriranje podatkov. Za logističen transport podatkov se uporabljajo samo ustrezni ponudniki storitev.

V okviru poslovne obdelave podatkov s strani družbe Bisnode, zlasti prejema in zagotavljanja podatkov svojih strank kot del informacijskih storitev družbe Bisnode, je nadaljnji nadzor nad obdelavo zagotovljen z beleženjem vseh korakov obdelave podatkov. Podatki strank, ki jih družba Bisnode obdeluje za stranke na osnovi njihovega naročila, so predani tretjim osebam v skladu s pravnimi predpisi za naročilo obdelave podatkov (28. člen GDPR) šele po pisnih navodilih stranke.

	Ukrepi
01	Podatke bo družba Bisnode poslala le strankam ali tretjim osebam oz. bo pogodbena stranka zadevnim tretjim osebam dovolila dostop do podatkov strank, če je to nujno potrebno za

	izpolnitev pogodbe. V teh primerih družba Bisnode zagotavlja, da tretje osebe ohranjajo vsaj enako raven varstva podatkov – glejte seznam podizvajalcev.

Nadzor prenosa pri upravljavcu podatkovnega centra

Upravljavec podatkovnega centra je predmet enakih zahtev glede nadzora prenosa kot sama družba Bisnode. Za poslovno kritične kopije (varnostno kopijo), zlasti v kontekstu zahtevanih varnostnih kopij, se uporabljajo samo standardizirani in dokumentirani postopki. Priprava vsake varnostne kopije je zabeležena.

NADZOR VNOSA

Nadzor vnosa vključuje ukrepe za zagotavljanje možnosti naknadnega preverjanja in ugotavljanja, ali so bili osebni podatki vneseni, spremenjeni ali odstranjeni in kdo jih je vnesel, spremenil ali odstranil iz računalniških sistemov.

Vnos lahko izvedejo le uslužbenci, ki imajo dostop do podatkov (glejte tudi opis v III. poglavju, ki se nanaša na nadzor nad dostopom).

	Ukrepi
01	V uporabi je koncept, ki opredeljuje uporabniški privilegij za vnos (profili) in zagotavlja, da je dostop do podatkov omejen glede na potreben obseg (načelo »potrebno je vedeti«).
02	Uporabniška dovoljenja se razlikujejo glede na naslednje kriterije: preberi, spremeni, izbriši, delni dostop do podatkov ali funkcij.
03	V tehnični aplikaciji obstaja dnevnik o tem, kdo je kaj vnesel in kdaj, tako da je mogoče izslediti zlorabo.
04	Obstaja dnevnik dejavnosti (oblikovanje uporabnikov, spreminjanje uporabniških pravic), tako da je mogoče izslediti zlorabe.

Ukrepi, ki se nanašajo na RAZPOLOŽLJIVOST in DOPUSTNOST (32. člen (1) GDPR)

NADZOR RAZPOLOŽLJIVOSTI

Nadzor razpoložljivosti vključuje ukrepe, ki zagotavljajo, da so osebni podatki zaščiteni pred nenamernim uničenjem ali izgubo.

Osnova za nadzor razpoložljivosti je izkoriščanje delovanja zmogljivosti IT-sistemov s strani podatkovnih centrov z visokimi varnostnimi standardi upravljavca podatkovnega centra. Upravljavec ima zlasti dodatne sisteme napajanja z neprekinjeno dobavo električne energije, kot tudi zasilni sistem napajanja z električno energijo.

Podatkovni center je z neposredno povezavo na srednjenapetostni ravni prek lastne transformatorske postaje ali enakovredne povezave povezan z zgradbami družbe Bisnode. Podatkovni centri uporabljajo tudi sisteme za zgodnje zaznavanje požarov, ki samodejno sprožijo proces gašenja.

Poleg tega je razpoložljivost podatkov, zlasti zaščita pred izgubo podatkov zaradi tehnične okvare ali nenamernega brisanja, zagotovljena z rednim varnostnim kopiranjem in varnostnimi kopijami relevantnih podatkovnih baz in sistemov, tako da jih je v primeru okvare mogoče ponovno vzpostaviti na dnevni ravni.

	Ukrepi
01	Opisani so ukrepi za zagotavljanje zaupnosti, integritete in razpoložljivosti osebnih podatkov in nosilcev podatkov v primeru katastrofe.
02	Na voljo je priročnik za nujne primere z načrti za krizna stanja, predstavitvijo organizacije v nujnih primerih ter jasno ureditvijo odgovornosti v nujnih primerih.
03	Na voljo so rezervni podatkovni centri (delujoči sistemi v pripravljenosti ali sistemi v pripravljenosti).
04	Na voljo je sistem UPS (brezprekinitveni napajalnik).
05	Nepooblaščeni uporabniki so zavrnjeni (npr. pri poskusih preplavljanja).
06	Ustrezni varnostni sistemi (programska oprema/strojna oprema) ščitijo družbo Bisnode pred preobremenitvijo (DDoS), program za iskanje virusov, požarni zidovi, filter neželene pošte,

	programi za šifriranje.
07	Obstaja sistem za upravljanje zmogljivosti, ki redno prepoznava obstoječe napake na enem samem mestu, jih analizira in jih obravnava z ustreznimi ukrepi.
08	Na voljo so redno pregledani predpisi, ki zmanjšujejo tveganje za napake in zlorabo vzdrževalnih del v podatkovnem centru (na primer načelo štirih oči).

Ukrepi za redni PREGLED, OCENO in VREDNOTENJE (25. člen (1) GDPR)

UPRAVLJANJE VARSTVA PODATKOV

Upravljanje varstva podatkov opisuje interne ukrepe za posebne zahteve varstva podatkov.

	Ukrepi
01	V družbi Bisnode je bila imenovana pooblaščena oseba za varstvo podatkov.
02	V družbi Bisnode obstajajo predpisi o zastopanju za upravljavca podatkov (odgovoren za uporabljeno IT-infrastrukturo pogodbenika).
03	Pooblaščena oseba za varstvo podatkov v družbi Bisnode je ustrezno usposobljena in ima ustrezno strokovno znanje ter osebno primernost za izvajanje nalog.
04	Izvaja se redno osnovno usposabljanje za zaposlene na področju informacijske varnosti in varstva podatkov.
05	Obstajajo postopki za redno ocenjevanje in posodabljanje ponudbe usposabljanja za zahtevano raven in za spremembe na področju zahtev ali okvirnih pogojev (dopolnitev zakonov, novih zakonov in predpisov).
06	Zaposleni, ki se obdelujejo in imajo vpogled v osebne podatke in druge zaupne informacije so ustrezno poučeni o ravnanju skladnemu z dobrimi praksami.
07	Sprejet je Pravilnik o varstvu osebnih podatkov

08	Sprejet je pravilnik o zagotavljanju informacijske varnosti.
09	Obstajajo dokumentirani postopki za prepoznavanje, analiziranje, vrednotenje in upoštevanje sprememb v zahtevah (npr. zakonih o zasebnosti), kot tudi v IT-procesih in postopkih (ocena vpliva varstva podatkov, nove aplikacije, novi IT-sistemi itd.).
10	Obstajajo dokumentirani procesi za prepoznavanje, analizo in vrednotenje incidentov varstva podatkov glede sprememb, kot tudi izpeljevanja ukrepov za preprečevanje ponovnega pojava (povezava upravljanja sprememb z upravljanjem incidentov).

UPRAVLJANJE ODZIVANJA NA INCIDENTE

Družba Bisnode se zaveda zakonskih obveznosti glede poročanja in je svoje uslužbence opozorila in usposobila za prepoznavanje kršitev, o katerih je treba poročati. Opredeljen je ustrezen postopek poročanja. Naslovniki sporočila (služba za stranke) in uslužbenci vedo, na koga se morajo obrniti v primeru kršitev. Po prejemu sporočila se izvaja postopek za hitro obdelavo poročila. Določeni so člani »krizne ekipe« in zagotovljena je ocena incidenta ter po potrebi obveščanje.

PREFERENCE, NAKLONJENE ZASEBNOSTI

Za izvajanje 25. člena (2) GDPR je družba Bisnode oblikovala »vgrajeno zasebnost družbe«. Družba Bisnode proaktivno vgrajuje varstvo podatkov v vsa področja. Ustrezna skladnost vključuje tudi upoštevanje ustreznih tehničnih in varnostnih ukrepov za zaščito osebnih podatkov.

NADZOR NAROČILA

Nadzor naročila vključuje ukrepe za zagotavljanje, da je osebne podatke, ki se obdelujejo v imenu stranke, mogoče obdelati le v skladu z navodili stranke.

Če družba Bisnode obdeluje osebne podatke v imenu pogodbenice, se vedno sklene pisna pogodba o obdelavi pogodbenih podatkov, ki vsebuje zakonsko zahtevano vsebino, ki se nanaša na 28. člen GDPR. Za ta primer ima družba Bisnode lastne modele pogodb. Pogodbene obveznosti zagotavljajo, da družba Bisnode obdeluje podatke samo v skladu z njenimi navodili, prav tako je zagotovljena zaupnost podatkov, zlasti pa je pomembno, da brez eksplicitnega pogodbenega navodila stranke ne pride do prenosa podatkov v podatkovne baze družbe Bisnode. Poleg tega je opis tehničnih in organizacijskih zaščitnih ukrepov v družbi Bisnode del vsake pogodbe o obdelavi podatkov z družbo Bisnode, saj je ta dokument priloga k pogodbi.

	Ukrepi
01	Zaposleni v družbi Bisnode so zavezani k varovanju zaupnosti podatkov.
02	Družba Bisnode sodeluje s podizvajalci (vključno z neodvisnimi hčerinskimi podjetji), ki izvajajo naročeno obdelavo (vključno z vzdrževanjem IT-sistemov). Glejte seznam podizvajalcev.
03	Pogodbe o obdelavi pogodbenih podatkov so bili sklenjeni z vsemi podizvajalci.
04	Pogodbe družbe Bisnode s podizvajalcem odražajo zahteve naročnika do izvajalca.
05	Zagotovljena je ustrezna raven varstva podatkov, na primer s standardnimi pogodbenimi klavzulami EU, posameznimi pogodbami z odobritvijo nadzornih organov oziroma gre za tretje države z vzpostavljeno ustrezno ravnjo varstva podatkov, ki jo je določila Evropska komisija.