Bisnode Grupa

Tehničke i organizacione mere zaštite podataka u skladu s Opštom uredbom o zaštiti podataka EU – Bisnode TOM –

Verzija za Sloveniju
od marta 2018.
ID dokumenta: 2018 03 12 Bisnode TOM FINAL.docx

SADRŽAJ

A. Obim primene

Prema Opštoj uredbi o zaštiti podataka EU (GDPR), svako ko samostalno prikuplja, obrađuje ili koristi podatke o ličnosti u obavezi je da primeni odgovarajuće tehničke i organizacione mere u skladu sa članom 32. koje su neophodne kako bi se osiguralo sprovođenje pravnih odredbi propisa o zaštiti podataka.

U ovom dokumentu su opisane zaštitne mere za „bezbednost obrade" kako je definisano u članu 32. GDPR-a u oblasti grupe kompanija Bisnode (zajedno se u ovom dokumentu nazivaju „Bisnode").

B. Mere koje se odnose na POVERLJIVOST (član 32(1) GDPR-a)

I. KONTROLA PRISTUPA PROSTORIJAMA

Svrha kontrole pristupa je da se neovlašćenim osobama spreči pristup tehničkim sistemima u okviru kojih se obrađuju ili koriste podaci o ličnosti.

Kontrola pristupa prostorijama kompanije Bisnode

Pristup objektima kompanije Bisnode je uređen kontrolama pristupa. Za zaposlene u kompaniji Bisnode, one se sastoje primarno od elektronskih ključeva koji omogućavaju pristup poslovnim prostorijama, u obimu prava pristupa po ključu. Prava pristupa su prilagođena vremenski (na dozvoljenu upotrebu određenim danima u nedelji i u određenom trenutku tokom dana) i prostorno (određenim delovima poslovnih prostorija) dozvolama zaposlenih. Za posetioce, kontrola pristupa je osigurana centralnom recepcijom ili portirskom službom, gde se evidentiraju podaci o posetiocima i posetiocima se daju bedževi koji važe tokom trajanja posete.

	Mere
01	Kontrola pristupa za pristup prostorijama / objektu je primenjena
02	Postoji delotvorna kontrola pristupa koja ostaje operativna čak i u slučaju kvara tehničke opreme (nestanak struje ili slično). (na primer, magnetna kartica / kartica sa čipom, obezbeđenje u fabrici, oprema za nadzor, video, sistemi alarma).
03	Postoji sistem kontrole pristupa u kom su navedeni ovlašćeni zaposleni.
04	Postoji evidentiranje pristupa koje obezbeđuje praćenje neovlašćenih ulazaka.
05	Postoje propisi za osoblje treće strane, osoblje zaduženo za čišćenje, goste, tehničare za održavanje i izvršno osoblje koji osiguravaju da ne dolazi do neovlašćenog pristupa.
06	Praćenje posetilaca u objektu je uređeno smernicama.
07	Pristup (računarskom centru) je obezbeđen i mere se redovno revidiraju. Računarski centar je sertifikovan prema standardu ISO 27001.
08	Serveri su smešteni na police za servere koje se zaključavaju i zaštićeni su od neovlašćenog fizičkog pristupa.
09	Uskladištene beležnice su pod ključem u obezbeđenim prostorijama.

10	Rezervne kopija podataka (kao što su trake, CD, DVD) se skladište u sefovima i bezbednim prostorijama.
11	Ovlašćenja za pristup koja više nisu potrebna se redovno povlače.
12	Praktični pregled će biti sproveden da bi se osigurala delotvornost preduzetih mera.

II. KONTROLA PRIJEMA

Kontrola prijema obuhvata mere za sprečavanje upotrebe sistema za obradu (logička bezbednost) od strane neovlašćenih lica.

Kontrola prijema u prostorijama kompanije Bisnode
Administrativni rad od strane kompanije Bisnode ili drugog operatera centra podataka obavljaće samo određeni zaposleni koji su potpisali odvojeni ugovor o poverljivosti i koji su verifikovani pre zapošljavanja. Ako se administrativne aktivnosti obavljaju preko spoljnog pristupa, te tzv. VPN veze su enkriptovane u skladu sa najnovijim tehnologijama i neophodna je dodatna potvrda identiteta. Identifikacija korisničkim imenom i bezbednom lozinkom, mehanizmi automatskog zaključavanja za računare i šifrovanje operatera mobilnih podataka su obavezni.

Pored toga, IT sistemi u kompaniji Bisnode su zaštićeni od spoljnih uticaja tehnologijama zaštitnog zida. Zaštitnim zidom centralno rukuje i upravlja matična korporacija Bisnode AB, Solna (Švedska).

	Mere
01	Odgovarajuće mere za sprečavanje neovlašćenog korišćenja IT sistema su opisane, sprovedene i podležu redovnom pregledu. (npr. ID korisnika, dodela lozinke, automatsko zaključavanje ekrana aktiviranjem lozinke)
02	Svako ovlašćeno lice ima sopstvenu lozinku koja je poznata samo njemu.
03	Postoji smernica za podešavanje, pokretanje, dodelu i korišćenje lozinke.
04	Kada se čuvaju lozinke koje su neophodne u kontekstu obrade podataka po nalogu, razmatraju se relevantni bezbednosni standardi i redovno se proverava da li su ažurirane.
05	Ovo je kontrolisani proces za oporavak zaboravljenih lozinki.
06	Sve osnovne aktivnosti koje se odnose na obradu podataka po nalogu se automatski evidentiraju u IT sistemima kako bi mogla da se prati zloupotreba.
07	Potencijalni pristup s udaljene tačke sistemima u kojim se obrađuju podaci po nalogu može biti ograničen na ovlašćeno osoblje.
08	Sprovedene su mere kojima se sprečava ili bar omogućava razumevanje neovlašćene upotrebe ovih postrojenja. Delotvornost ovih mera se dokazuje redovnim proverama. (npr. VPN, funkcionalna alokacija korisničkih uređaja, evidentiranje korišćenja sistema i analiza evidencije)
09	Nove ranjivosti u IT sistemima se prijavljuju, otkrivaju, analiziraju i, ako je potrebno, uklanjaju da bi se sprečio upad neovlašćenih trećih strana u te IT sisteme.

10	Pored redovnih kontrola, postoje nezavisni pregledi delotvornosti mera preduzetih protiv upada neovlašćenih trećih strana (kao što je simulacija hakerskog napada).
11	Postoje definisane organizacione i tehničke procedure i metode za upravljanje incidentima (upravljanje otkrivenim ili potencijalnim bezbednosnim incidentima ili prekidima, kvarovima itd.).

Kontrola pristupa kod operatera centra podataka
Da bi se osigurali sistemi kojima upravlja Bisnode, operater centra podataka je primenio visokokvalitetne funkcije zaštitnog zida u okviru sloja mreže kao i proizvoda kojima se pristupa.

III. KONTROLA PRISTUPA – AUTORIZACIJA

Kontrola pristupa obuhvata mere kojima se osigurava da korisnici sistema za obradu podataka mogu da pristupe samo podacima u vezi sa njihovim pravima pristupa i da se podaci o ličnosti ne mogu neovlašćeno čitati, kopirati, menjati ili brisati tokom obrade, korišćenja i nakon čuvanja.

Kontrola autorizacije u postrojenjima kompanije Bisnode
Bisnode ima definisane i dokumentovane interne standarde za rukovanje dozvolama. Njima se uređuje autorizacija administratora na upravljanim sistemima. Na primer, opisuju se zahtevi za bezbedne lozinke.

Dozvole odgovaraju načelu „samo ono što je potrebno da zna”. Ovi detalji su uređeni u Bisnode „konceptu uloge i autorizacije”.

	Mere
01	Postoji dokumentovano upravljanje autorizacijama gde je definisano kako se autorizacije zahtevaju, izdaju, odobravaju i povlače.
02	Postoji funkcionalno/lično odvajanje odobrenja prava (organizaciono) i autorizacija (tehničko).
03	Postoji jasna dodela između svakog nosača podataka i jednog ovlašćenog korisnika (posebno za mrežne uređaje).
04	Vraćanje podataka iz rezervnih kopija (kome je dozvoljeno da šalje rezervne kopije podataka, na čiji zahtev i kada) uređeno je obaveznom procedurom.
05	Korišćenje programa i datoteka se evidentira i ocenjuje na nasumičnoj osnovi.
06	Za obradu podataka po nalogu koriste se aplikacije koje je razvila ili koje održava kompanija Bisnode.
07	Tokom razvoja programa, koristi se funkcionalno razdvajanje (okruženje testiranja i produkcije).

Kontrola pristupa kod operatera centra podataka
U obimu u kom operater centra podataka, u ime kompanije Bisnode, preduzima podešavanje korisnika i privilegija na sloju aplikacije (sloj aplikacije), u osnovi je posvećeno istim bezbednosnim standardima koji se primenjuju na samim Bisnode lokacijama. Odstupanja su dozvoljena isključivo pisanim uputstvima

kompanije Bisnode. Utvrđivanje specifikacija o tome kako treba programirati koncepte autorizacije za određenu aplikaciju od strane operatera centra podataka je odgovornost kompanije Bisnode.

IV. KONTROLA SEPARACIJE

Zahtev o separaciji obuhvata mere kojima se osigurava odvojena obrada podataka prikupljenih za različite svrhe.

Zahtev o separaciji u postrojenjima kompanije Bisnode
U odnosu na opštu obradu podataka u kompaniji Bisnode (podaci o zaposlenima, dobavljačima, glavni podaci o korisnicima), zahtev o separaciji se primenjuje, na primer, fizičkim odvajanjem i skladištenjem na odvojenim sistemima ili nosačima podataka, razdvajanjem okruženja produkcije, testiranja i razvoja za naše aplikacije i IT sisteme. Odgovarajući koncepti autorizacije, kao i prava za baze podataka. Pored toga, logička separacija klijenata se sprovodi sa strane softvera.

Kao deo obrade poslovnih podataka od strane kompanije Bisnode, posebno prijem i obezbeđivanje podataka o korisnicima u kontekstu Bisnode poslovanja u informacionim uslugama, separacija u smislu zaštite podataka se odigrava uglavnom na osnovu aplikacije. Svi isporučeni paketi podataka se obrađuju strogo odvojeno jedan od drugog, tako da se isključuje preklapanje podataka o korisnicima. Za te potrebe su preduzete neophodne mere predostrožnosti (hardver i softver).

	Mere
01	Podaci iz raznih zadataka za obradu podataka po nalogu klijenta međusobno i sa podacima drugih korisnika obrađuju se fizički i logički odvojeno u kompaniji Bisnode.
02	Postoji koncept autorizacije koji uzima u obzir odvojenu obradu naručenih podataka podacima drugih korisnika/klijenata.

Zahtev o separaciji kod operatera centra podataka
Operater centra podataka odvaja sve podatke fizički ili logički, najmanje na nivou korisnika. Ako se slojevi kompanije Bisnode poveravaju operateru centra podataka, uglavnom postoje dodatni nivoi odvajanja na osnovu sistema ili baze podataka.

V. PSEUDONIMIZACIJA

Pseudonimizacija se koristi u statističkoj analizi, ocenama učestalosti i uporedivim evaluacijama gde poznavanje osobe koja je stvarno pogođena nije neophodno.

C. Mere koje se odnose na INTEGRITET (član 32(1) GDRP-a)

VI. STALNA KONTROLA PRENOSA

Kontrola prenosa obuhvata mere kojima se osigurava da se podaci o ličnosti ne mogu čitati, kopirati, menjati ili brisati tokom elektronskog prenosa ili tokom transporta ili skladištenja na nosačima podataka, kao i da je moguće proveriti i utvrditi u koja mesta su podaci o ličnosti preneti sredstvima prenosa podataka.

Kontrola prolaska u postrojenjima kompanije Bisnode
Što se tiče opšte obrade podataka u kompaniji Bisnode (podaci o zaposlenima, dobavljačima, glavni podaci o korisnicima), kontrola prenosa (kontrola prenosa, transporta) osigurava se odgovarajućim tehničkim merama. To podrazumeva zaštitne zidove, zaštitu od virusa, VPN tunele, šifrovanje podataka, zaštitu pojedinačnih dokumenata lozinkama. Za elektronski prenos poverljivih podataka koriste se samo medijumi za skladištenje koji omogućavaju šifrovanje podataka. Za logistički transport podataka koriste se samo odgovarajući pružaoci usluga.

Kao deo obrade poslovnih podataka u kompaniji Bisnode, naročito prijem i obezbeđivanje podataka o korisnicima u okviru Bisnode poslovanja u informacionim uslugama, dodatna kontrola obrade se osigurava evidentiranjem svih koraka u obradi podataka. Ako je tako dogovoreno sa korisnikom, podaci klasifikovani kao posebno poverljivi biće dodatno šifrovani tokom prenosa preko javnih mreža. Podaci korisnika koje Bisnode obrađuje za korisnika prema njihovom nalogu prenose se trećim stranama u skladu sa pravnim propisima za poverenu obradu podataka (član 28. GDPR-a) samo nakon pisanog naloga korisnika.

	Mere
01	Podaci iz kompanije Bisnode će se slati samo klijentu ili trećim stranama i te treće strane će moći da pristupaju podacima klijenta preko ugovarača samo ako je to apsolutno neophodno za izvršenje ugovora. U tim slučajevima, Bisnode osigurava da treće strane zadrže najmanje isti nivo zaštite podataka – videti spisak podizvođača.
02	Koristiće se samo u obradi podataka po nalogu ili na načine otkrivanja koji su navedeni u Bisnode TOM-u za obradu podataka. Bezbednost opcija prenosa se redovno proverava.

Kontrola prenosa kod operatera centra podataka
Operater centra podataka ima iste obaveze u pogledu prenosa podataka kao i kompanije Bisnode. Za kopije koje su od suštinskog značaja za poslovanje (rezervne kopije), posebno u kontekstu neophodnih rezervnih kopija, koriste se isključivo standardizovane i dokumentovane procedure. Priprema svake rezervne kopije se evidentira.

VII. KONTROLA UNOSA

Kontrola unosa obuhvata mere kojima se osigurava da se naknadno može potvrditi i verifikovati da li je i ko je u računarske sistem uneo, izmenio ili izbrisao podatke o ličnosti.

Unos mogu da obavljaju samo zaposleni koji imaju pristup podacima (videti i opise za kontrolu pristupa pod III).

Pored toga, na sistemima se automatski kreiraju evidencije „specifičnih akcija" procesa. Protokoli „specifične akcije" se odnose na procese koji služe da održavaju rad sistema, svrhe naplate i ispunjavanje zakonskih zahteva u pogledu skladištenja.

	Mere
01	Postoji koncept koji definiše privilegiju korisnika za unos (profili) i osigurava da je pristup korisnika podacima ograničen u neophodnoj meri (načelo „samo ono što je potrebno da zna").
02	Korisničke dozvole se razlikuju prema sledećim kriterijumima. Čitaj, Izmeni, Izbriši Delimičan pristup podacima ili funkcijama
03	Postoji evidentiranje toga ko je uneo šta i kada u tehničku aplikaciju kako bi se pratila zloupotreba.
04	Postoji evidentiranje aktivnosti administratora (kreiranje korisnika, promena prava korisnika) kako bi se pratila zloupotreba.
05	Navedeni su periodi skladištenja/brisanja specifični za kompaniju ili predviđeni zakonom. Ovom politikom je takođe uređeno zadržavanje evidencija o unosu i administraciji.

D. Mere koje se odnose na DOSTUPNOST i TOLERABILNOST (čl. 32(1) GDPR-a)

VIII. KONTROLA DOSTUPNOSTI

Kontrola dostupnosti obuhvata mere kojima se osigurava zaštita podataka o ličnosti od slučajnog uništenja ili gubitka.

Osnova za kontrolu dostupnosti je poveravanje rada IT sistema visokobezbednom centru podataka operatera centra podataka. On poseduje naročito redundantne sisteme snabdevanja sa neprekidnim napajanjem kao i sistemom za pokretanje u hitnim slučajevima (na primer, veliki agregati na dizel). Centar podataka je povezan sa Bisnode lokacijama direktnom vezom srednjeg napona putem sopstvene trafo stanice ili jednake veze. Centri podataka takođe koriste sisteme za ranu detekciju požara koji automatski aktiviraju proces gašenja.

Pored toga, dostupnost podataka, posebno zaštita od gubitka podataka zbog tehničkog kvara ili slučajnog brisanja, obezbeđuje se redovnim pravljenjem rezervnih kopija svih relevantnih baza podataka i sistema kako bi mogli da se ponovo uspostave na nivou dana u slučaju kvara.

	Mere
01	Postoje opisane mere za obezbeđivanje poverljivosti, integriteta i dostupnosti podataka o ličnosti i nosača podataka uz slučaju katastrofe.
02	Postoji priručnik za hitne slučajeve sa planovima za nepredviđene slučajeve, prezentacija organizacije za hitne slučajeve i jasno uređene odgovornosti za hitne slučajeve.
03	Postoje dostupni centri podataka za rezervne kopije (vruća i hladna rezerva).
04	Postoji dostupan UPS sistem (neprekidno napajanje).
05	Neovlašćeni korisnici (npr. pri pokušaju zatrpavanja) se odbijaju.
06	Odgovarajući bezbednosni sistemi (softver/hardver) štite kompaniju Bisnode od napada preopterećenjem (DDoS), Skener za viruse zaštitni zidovi Filter za bezvredan sadržaj programi za enkripciju
07	Postoji sistem za upravljanje kapacitetom koji redovno identifikuje postojeće jedinične tačke kvara, analizira ih i tretira odgovarajućim merama.
08	Postoje propisi koji se redovno revidiraju i pomoću kojih se rizik od grešaka i zloupotrebe održavanja centra podataka svodi na minimum (na primer, načelo duple kontrole).

E. Mere za redovnu INSPEKCIJU, PROCENU i EVALUACIJU (Član 25(1) GDPR-a)

IX. UPRAVLJANJE ZAŠTITOM PODATAKA

Upravljanje zaštitom podataka opisuje interne mere za posebne zahteve zaštite podataka.

	Mere
01	U kompaniji Bisnode je imenovan službenik za zaštitu podataka u kompaniji.
02	U kompaniji Bisnode postoji službenik za IT/bezbednost informacija.
03	Za rukovaoca podataka (odgovoran za primenjenu IT infrastrukturu ugovarača) u kompaniji Bisnode postoje propisi o predstavljanju.
04	Službenici za IT/bezbednost informacija i službenici za zaštitu podataka u kompaniji Bisnode su adekvatno obučeni i poseduju odgovarajuće praktične veštine i lične osobine.
05	Službenici za IT/bezbednost informacija i za zaštitu podataka ugovarača su na odgovarajući način uključeni u organizacionu strukturu (kao jedinica osoblja za upravljanje ili neka uporediva nezavisna funkcija).
06	Održavaju se redovne osnovne obuke za zaposlene o bezbednosti informacija i zaštiti podataka.
07	Postoje procesi za redovnu procenu i ažuriranje ponude obuka za neophodni nivo i za izmene u zahtevima ili okvirnim uslovima (izmene zakona, novi zakoni i propisi).
08	Zaposleni koji se bave podacima o ličnosti će biti upućeni ili posvećeni privatnosti i ovlašćenim praksama.
09	Postoji sveobuhvatna politika privatnosti.
10	Postoji sveobuhvatna politika za IT bezbednost.
11	Ove smernice se čuvaju centralno i mogu im pristupiti svi zaposleni.
12	Zahtevi ovih smernica se poštuju u uputstvima za rad i sličnim dokumentima.
13	Postoje dokumentovani procesi za identifikaciju, analizu, ocenu i uzimanje u obzir izmena u zahtevima (npr. zakoni o privatnosti) kao i IT procesima i procedurama (procena uticaja zaštite podataka, nove aplikacije, novi IT sistemi itd.).
14	Postoje dokumentovani procesi za identifikaciju, analizu, ocenu incidenata sa zaštitom podataka u vezi sa izmenama kao i izvođenje mera za sprečavanje ponovne pojave (veza između upravljanja promenama i upravljanja incidentima).

X. UPRAVLJANJE ODGOVORIMA NA INCIDENT

Kompanija Bisnode svesna zakonskih obaveza o izveštavanju i obučila je svoje zaposlene da prepoznaju sve prekršaje koje treba prijaviti. Definisan je odgovarajući proces izveštavanja. Primaoci poruka

(korisnička služba) i zaposleni znaju kome da se obrate u slučaju povrede privatnosti. Dalje, sproveden je proces za brzu obradu izveštaja nakon prijema. Članovi „kriznog tima" su definisani i garantovana je procena incidenta i, ako je potrebno, aktiviranje izveštaja.

Upravljanje odgovorima na incident za incidente sa zaštitom podataka je povezano sa upravljanjem IT incidentima, upravljanjem bezbednosnim incidentima i upravljanjem krizom u kompaniji Bisnode AB.

XI. PODEŠAVANJA KOJA POŠTUJU PRIVATNOST

Da bi sprovela član 25(2) GDPR-a, kompanija Bisnode je kreirala „Smernicu za privatnost u grupi prema dizajnu i podrazumevanim postavkama". Njome je određeno da kompanija Bisnode integriše zaštitu podataka proaktivno i nereaktivno u sve oblasti i zaštita podataka se uzima u obzir već u fazi dizajna ponuda. Usaglašenost prema dizajnu u pogledu privatnosti nije samo pitanje korisničkog iskustva za kompaniju Bisnode. Odgovarajuća usaglašenost takođe podrazumeva preduzimanje odgovarajućih tehničkih i bezbednosnih mera za zaštitu podataka o korisnicima i podataka o ličnosti.

Dodatno, kompanija Bisnode je kreirala „Politiku zadržavanja u grupi". Ovo je osnovni dokument koji se primenjuje zasebno na svakom tržištu sa lokalnim odstupanjima. U tom cilju, kompanija Bisnode je sprovela odgovarajući koncept brisanja za podatke o ličnosti u Nemačkoj.

XII. KONTROLA NALOGA

Kontrola naloga podrazumeva mere kojima se osigurava da se podaci o ličnosti obrađuju u ime korisnika samo u skladu sa uputstvima korisnika.

Ako Bisnode obrađuje podatke o ličnosti u ime ugovora, pisani ugovor o obradi podataka o ugovoru sa zakonski neophodnim sadržajem prema članu 28. GDPR-a je već zaključen. Bisnode takođe ima svoje modele ugovora za ovaj slučaj, koje klijent može da koristi za puštanje u rad. Ugovornim obavezama je osigurano da Bisnode obrađuje podatke o klijentu isključivo prema njegovim uputstvima, garantovana je poverljivost podataka, a posebno bez izričito suprotnog uputstva korisnika ne dolazi do prenosa podataka o korisniku u inventar opštih podataka Bisnode-a. Pored toga, opisi tehničkih i organizacionih mera zaštite u Bisnode-u deo su svakog ugovora o obradi podataka sa kompanijom Bisnode, pošto je ovaj dokument dogovoren kao prilog ugovoru o poverenoj obradi podataka.

	Mere
01	Zaposleni u kompaniji Bisnode su posvećeni tajnosti podataka.
02	Kompanija Bisnode je angažovala podizvođače (uključujući nezavisna povezana društva) da obave obradu naloga (uključujući održavanje IT sistema) – videti spisak podizvođača.
03	Sa svim podizvođačima su sklopljeni ugovori o obradi podataka ili zaštiti podataka. Član 28. je sproveden.
04	Ugovori kompanije Bisnode sa podizvođačem oslikavaju zahteve ugovaračkog tela za ugovarača (videti okvirni ugovor i aneks obradi podataka po nalogu).
05	Postoje neki podizvođači koji se nalaze izvan Evropskog ekonomskog prostora (EEP) – videti spisak podizvođača.

06	Osiguran je odgovarajući nivo zaštite podataka, na primer preko standardnih EU ugovornih klauzula, pojedinačnih ugovora sa odobrenjem nadzornih organa, ili su u pitanju treće zemlje sa odgovarajućim nivoom zaštite podataka koji je utvrdila EU komisija.

XIII. INFORMACIJE O BEZBEDNOSTI INFORMACIJA

CANCOM Pironet AG & Co. KG	sertifikovan prema ISMS 27001
D&B UK	sertifikovan prema ISMS 27001
D&B International	informativni list za ISMS

dpo@bisnode.com