Grupacija Bisnode

Tehničke i organizacijske mjere za zaštitu podataka u skladu s Općom uredbom EU-a o zaštiti podataka – Bisnode TOM –

Hrvatska inačica
ožujak 2018.
ID dokumenta: 2018 03 12 Bisnode TOM FINAL.docx

SADRŽAJ

A. Područje primjene

Temeljem Opće uredbe EU-a o zaštiti podataka (GDPR), svatko tko samostalno prikuplja, obrađuje ili upotrebljava osobne podatke dužan je uvesti odgovarajuće tehničke i organizacijske mjere u skladu s člankom 32. koje su potrebne kako bi se osiguralo izvršenje zakonskih odredbi propisa o zaštiti podataka.

U ovom dokumentu opisuju se zaštitne mjere „sigurnosti obrade", kako su definirane člankom 32. Opće uredbe o zaštiti podataka, za djelatnosti društava u sklopu grupacije Bisnode (koja se u ovome dokumentu zajednički nazivaju „Bisnode").

B. Mjere povezane s POVJERLJIVOŠĆU (članak 32. stavak 1. Opće uredbe o zaštiti podataka)

I. NADZOR PRISTUPA PROSTORIMA

Svrha nadzora pristupa jest spriječiti neovlaštene osobe da ostvare pristup tehničkim sustavima kojima se obrađuju ili upotrebljavaju osobni podaci.

Nadzor pristupa u prostorima društva Bisnode

Pristup zgradama društva Bisnode regulira se nadzorom pristupa. Za djelatnike društva Bisnode taj se nadzor prvenstveno sastoji od elektroničkih ključeva koji omogućuju pristup poslovnim prostorima, pri čemu su svakom ključu dodijeljena odgovarajuća prava pristupa. Prava pristupa usklađena su s ovlaštenjima djelatnika prema vremenskim parametrima (dozvoljenoj upotrebi određene dane u tjednu i u određeno doba dana) i prostornim parametrima (određenim dijelovima poslovnog prostora). Nadzor pristupa posjetitelja osigurava središnja recepcija ili vratarska služba koja bilježi podatke posjetitelja i izdaje im propusnice koje vrijede tijekom njihova posjeta.

	Mjere
01.	Provodi se nadzor pristupa za pristup prostorima/zgradi.
02.	Provodi se učinkovit nadzor pristupa koji ostaje u funkciji čak i u slučaju kvara tehničke opreme (nestanak struje i sl.). (Npr. magnetska kartica / čip kartica, ključ, tvorničko osiguranje, oprema za nadzor, videonadzor, alarmni sustavi.)
03.	Postoji sustav za nadzor pristupa u kojem su navedeni ovlašteni djelatnici.
04.	Bilježe se zapisi o pristupu, čime se jamči da se može ući u trag neovlaštenim ulascima.
05.	Postoje pravila za osoblje trećih strana, čistače, posjetitelje, tehničare održavanja i rukovoditelje kojima se osigurava da ne može doći do neovlaštenog pristupa.
06.	Smjernicom je propisano da se posjetitelji zgradom smiju kretati uz pratnju.
07.	Pristup računalnom centru siguran je i redovito se provode revizije mjera. Računalni centar nositelj je certifikata ISO 27001.
08.	Poslužitelji su smješteni u ormarima koji se zaključavaju i zaštićeni su od neovlaštenog fizičkog pristupa.
09.	Prijenosnici se čuvaju pod ključem u sigurnim prostorijama.

10.	Sigurnosne kopije podataka (primjerice na vrpcama, CD-ima, DVD-ima) čuvaju se u sefovima i sigurnim prostorijama.
11.	Redovito se povlače ovlaštenja za pristup koja više nisu potrebna.
12.	Provodi se revizija prakse kako bi se osigurala učinkovitost poduzetih mjera.

II. NADZOR PRISTUPA

Nadzor pristupa uključuje mjere kojima se sprječava da se neovlaštene osobe mogu koristiti sustavima za obradu podataka (logička sigurnost).

Nadzor pristupa u prostorima društva Bisnode
Administrativne zadatke društva Bisnode ili operatera podatkovnog centra izvršavaju samo određeni djelatnici koji su potpisali zaseban ugovor o povjerljivosti i za koje je prije zapošljavanja izvršena sigurnosna provjera. Ako se administrativni poslovi obavljaju putem vanjskog pristupa, šifriranje tih takozvanih VPN veza provodi se primjenom najsuvremenije tehnologije te je potrebna i dodatna provjera vjerodostojnosti. Obvezna je identifikacija korisničkim imenom i sigurnom zaporkom, mehanizmi automatskog zaključavanja računala i šifriranje prijenosnih podatkovnih medija.

Uz to, IT sustavi društva Bisnode od vanjskih su napada zaštićeni tehnologijom vatrozida. Vatrozidom upravlja i održava ga matično društvo Bisnode AB sa središnje lokacije u gradu Solna (Švedska).

	Mjere
01.	Opisane su i provode se odgovarajuće mjere za sprječavanje neovlaštene upotrebe IT sustava koje podliježu redovitim revizijama. (Npr. ID korisnika, dodjeljivanje zaporki, automatsko zaključavanje zaslona koje iziskuje zaporku za otključavanje.)
02.	Svaka ovlaštena osoba ima vlastitu zaporku s kojom je samo ona upoznata.
03.	Postoji smjernica za postavljanje, upravljanje, dodjelu i upotrebu zaporki.
04.	Prilikom pohrane potrebnih zaporki u kontekstu naručene obrade podataka uzimaju se u obzir mjerodavni sigurnosni standardi za koje se redovito provjerava jesu li ažurirani.
05.	Postoji kontrolirani postupak za obnavljanje zaboravljenih zaporki.
06.	Sve nužne aktivnosti povezane s naručenom obradom podataka automatski se zapisuju u IT sustavima kako bi se moglo ući u trag zlouporabi.
07.	Mogućnost daljinskog pristupa sustavima koji rade na naručenoj obradi podataka može biti ograničena na ovlašteno osoblje.
08.	Provode se mjere kojima se sprječava neovlaštena upotreba ovih objekata ili u najmanju ruku omogućuje analiza takve upotrebe. Učinkovitost ovih mjera dokazuje se redovitim provjerama. (Npr. VPN, funkcijska raspodjela korisničkih uređaja, bilježenje zapisa o upotrebi sustava te analiza zapisa.)
09.	Nove ranjivosti IT sustava otkrivaju se, prijavljuju, analiziraju i, po potrebi, otklanjaju kako bi se spriječio ulazak neovlaštenih trećih strana u IT sustave.
10.	Osim redovitog nadzora provode se i druge neovisne revizije učinkovitosti mjera kojima se sprječava ulazak neovlaštenih trećih strana (kao što je testiranje prodora).

11.	Postoje definirani organizacijski i tehnički postupci i metode za upravljanje incidentima (upravljanje sigurnosnim incidentima ili poremećajima, kvarovima itd. koji su otkriveni ili na koje se sumnja).

Nadzor pristupa pri operateru podatkovnog centra
Kako bi osigurao sustave kojima upravlja za društvo Bisnode, operater podatkovnog centra postavio je visokokvalitetne funkcije vatrozida između slojeva mreže i proizvoda koji omogućuju pristup.

III. NADZOR PRISTUPA – OVLAŠTENJE

Nadzor pristupa uključuje mjere kojima se osigurava da korisnici sustava za obradu podataka mogu pristupiti samo onim podacima za koje imaju prava pristupa te da se osobni podaci ne mogu bez dopuštenja čitati, umnožavati, mijenjati ili brisati tijekom obrade, upotrebe te nakon spremanja.

Nadzor ovlaštenja u objektima društva Bisnode
Društvo Bisnode definiralo je i dokumentiralo interne standarde za upravljanje odobrenjima. Njima se propisuje ovlašćivanje administratora sustava koji se upotrebljavaju. Primjerice, opisuju se zahtjevi za sigurne zaporke.

Ovlaštenja su u skladu s načelom otkrivanja podataka onima koji trebaju imati uvid u te podatke. Pojedinosti su definirane u „konceptu uloga i ovlaštenja" društva Bisnode.

	Mjere
01.	Postoji dokumentirano upravljanje ovlaštenjima u sklopu kojega se definiraju obvezujuća pravila za traženje, izdavanje, odobravanje i povlačenje ovlaštenja.
02.	Odobravanje prava (organizacijskih) i dodjela ovlaštenja (tehničkih) odvojeni su prema funkcijama/osobama.
03.	Postoji jasna dodjela svakog podatkovnog medija jednom ovlaštenom korisniku (to se posebice odnosi na mrežne uređaje).
04.	Obvezujućim je postupkom propisan način vraćanja podataka iz sigurnosnih kopija (kome je dozvoljeno učitavanje podataka sigurnosnih kopija, na čiji zahtjev i kada).
05.	Bilježe se zapisi o upotrebi programa i datoteka i ti se zapisi nasumično analiziraju.
06.	Za naručenu obradu podataka upotrebljavaju se aplikacije koje je društvo Bisnode razvilo ili ih održava.
07.	Tijekom razvoja programa primjenjuje se odvajanje funkcija (testna i proizvodna okolina).

Nadzor pristupa pri operateru podatkovnog centra
Kada operater podatkovnog centra provodi postavljanje korisnika i ovlaštenja na razini aplikacije u ime društva Bisnode, obvezuju ga isti sigurnosni standardi koji se primjenjuju za objekte društva Bisnode. Odstupanja su dopuštena samo uz pisanu uputu društva Bisnode. Društvo Bisnode dužno je odrediti pojedinosti o tome kako operater podatkovnog centra treba osmisliti posebne koncepte ovlaštenja za aplikaciju.

IV. NADZOR ODVAJANJA

Zahtjev o odvajanju uključuje mjere kojima se osigurava da se podaci koji su prikupljeni u različite svrhe mogu obrađivati odvojeno.

Zahtjev o odvajanju u objektima društva Bisnode
Po pitanju opće obrade podataka u društvu Bisnode (podataka o djelatnicima, podataka o dobavljačima, glavnih podataka o klijentima), zahtjev o odvajanju provodi se, primjerice, fizičkim odvajanjem i pohranom u različitim sustavima ili na različitim podatkovnim medijima; odvajanjem proizvodne, testne i razvojne okoline za naše aplikacije i IT sustave; odgovarajućim konceptima odobrenja; kao i pravima za bazu podataka. Osim toga, sa softverske se strane provodi logičko odvajanje klijenata.

U sklopu poslovne obrade podataka koju provodi društvo Bisnode, a posebice primanja i pružanja podataka klijenata u kontekstu djelatnosti pružanja informacijskih usluga društva Bisnode, odvajanje u smislu zaštite podataka uglavnom se provodi na temelju aplikacija. Svi dostavljeni paketi podataka obrađuju se potpuno odvojeno jedan od drugoga i time se onemogućuje preklapanje podataka klijenata. U tu se svrhu poduzimaju potrebne mjere opreza (hardverske i softverske).

	Mjere
01.	Društvo Bisnode obrađuje podatke za različite zadatke klijentove naručene obrade podataka fizički ili logički odvojeno od ostalih zadataka tog klijenta te fizički ili logički odvojeno od podataka drugih klijenata.
02.	Postoji koncept ovlaštenja koji obuhvaća odvojenu obradu naručenih podataka od podataka drugih klijenata.

Zahtjev o odvajanju pri operateru podatkovnog centra
Operater podatkovnog centra fizički ili logički odvaja sve podatke, barem na razini pojedinog klijenta. Kada se operater podatkovnog centra angažira kao vanjski suradnik na razini društva Bisnode, uglavnom postoje dodatne razine odvajanja ovisno o sustavu ili bazi podataka.

V. PSEUDONIMIZACIJA

Pseudonimizacija se primjenjuje za statističke analize, procjene učestalosti i slične procjene kada nije potrebno znati identitet osobe na koju se podaci odnose.

C. Mjere povezane s CJELOVITOŠĆU (članak 32. stavak 1. Opće uredbe o zaštiti podataka)

VI. NEPREKIDAN NADZOR PRIJENOSA

Nadzor prijenosa uključuje mjere kojima se osigurava da se osobni podaci ne mogu čitati, umnožavati, mijenjati ili uklanjati tijekom elektroničkog prijenosa odnosno prijenosa ili pohrane na podatkovnom mediju te da je moguće provjeriti i utvrditi gdje se osobni podaci prenose opremom za prijenos podataka.

Nadzor prijenosa u objektima društva Bisnode
Po pitanju opće obrade podataka u društvu Bisnode (podataka o osoblju, podataka o dobavljačima, glavnih podataka o klijentima), nadzor prijenosa (nadzor prijenosa, nadzor prijevoza) osigurava se odgovarajućim tehničkim mjerama. Te mjere uključuju vatrozide, antivirusnu zaštitu, VPN tunele, šifriranje podataka, zaštitu pojedinačnih dokumenata zaporkom. Za elektronički prijenos povjerljivih podataka upotrebljavaju se samo oni mediji za pohranu koji omogućuju šifriranje podataka. Za logistički prijevoz podataka angažiraju se samo odgovarajući pružatelji usluga.

U sklopu poslovne obrade podataka koju provodi društvo Bisnode, a posebice primanja i pružanja podataka klijenata u sklopu djelatnosti pružanja informacijskih usluga društva Bisnode, nadzor daljnje obrade osigurava se bilježenjem zapisa o svim koracima obrade podataka. U slučajevima u kojima je tako dogovoreno s klijentom, podaci za koje je određeno da su izuzetno povjerljivi štite se dodatnim šifriranjem tijekom prijenosa javnim mrežama. Podaci klijenata koje društvo Bisnode obrađuje po narudžbi klijenta mogu se prenijeti trećim stranama u skladu sa zakonskim odredbama o naručenoj obradi podataka (članak 28. Opće uredbe o zaštiti podataka) samo nakon što klijent o tome izda pisanu uputu.

	Mjere
01.	Društvo Bisnode slat će podatke samo klijentu ili trećim stranama. Tim će trećim stranama biti dopušteno da pristupe klijentovim podacima samo kao podizvođači, ako to bude posve nužno za izvršenje ugovora. U tim slučajevima društvo Bisnode osigurava da treće strane održavaju najmanje istu razinu zaštite podataka – vidjeti popis podizvođača.
02.	Primjenjuje se samo na one načine otkrivanja definirane pojedinom naručenom obradom podataka ili tehničkim i organizacijskim mjerama društva Bisnode za naručene obrade podataka. Sigurnost mogućnosti prijenosa redovito se provjerava.

Nadzor prijenosa pri operateru podatkovnog centra
Operater podatkovnog centra podliježe istim obvezama nadzora prijenosa kao i društvo Bisnode. Za izradu kopija koje su nužne za rad (sigurnosnih kopija), posebice u kontekstu obveznih sigurnosnih kopija, primjenjuju se samo standardizirani i dokumentirani postupci. Bilježe se zapisi o izradi svih sigurnosnih kopija.

VII. NADZOR UNOSA

Nadzor unosa uključuje mjere kojima se osigurava da će kasnije biti moguće provjeriti i utvrditi jesu li osobni podaci uneseni u računalne sustave, jesu li izmijenjeni u njima ili uklonjeni iz njih te tko je izvršio te radnje.

Unos mogu obavljati samo oni djelatnici koji imaju pristup podacima (vidjeti opise za nadzor pristupa u III. odjeljku).

Uz to, u sustavima se automatski bilježe zapisi „posebnih radnji" u sklopu postupaka. Protokoli „posebnih radnji" odnose se na postupke koji služe za održavanje rada sustava, fakturiranje te zadovoljavanje zakonskih zahtjeva o pohrani.

	Mjere
01.	Postoji koncept kojim se definiraju korisnička ovlaštenja za unos (profili) i osigurava da korisnički pristup podacima bude ograničen do one mjere do koje je to potrebno (načelo otkrivanja podataka onima koji trebaju imati uvid u te podatke).
02.	Ovlaštenja korisnika razlikuju se prema sljedećim kriterijima: čitanje, izmjena, brisanje; djelomičan pristup podacima ili funkcijama.
03.	U tehničkoj aplikaciji bilježe se zapisi o tome tko je što i kada unio kako bi se moglo ući u trag zlouporabi.
04.	Bilježe se zapisi aktivnosti administratora (izrada korisničkih računa, promjena korisničkih prava) kako bi se moglo ući u trag zlouporabi.
05.	Definirana su razdoblja za pohranu/brisanje koja su propisana zakonom ili koja određuje društvo. Ovom se politikom propisuje i zadržavanje zapisa o unosu i administraciji.

D. Mjere o DOSTUPNOSTI i OTPORNOSTI (članak 32. stavak 1. Opće uredbe o zaštiti podataka)

VIII. NADZOR DOSTUPNOSTI

Nadzor dostupnosti uključuje mjere kojima se osigurava da osobni podaci budu zaštićeni od slučajnog uništenja ili gubitka.

Temelj nadzora dostupnosti jest angažiranje operatera podatkovnog centra kao vanjskog suradnika i upotreba IT sustava u njegovom podatkovnom centru s visokom razinom sigurnosti. Posebno je važno da potonji bude opremljen višestrukim sustavima napajanja koji omogućuju neprekidno napajanje električnom energijom te da bude opremljen sustavom napajanja za slučaj nužde (primjerice višestrukim dizelskim generatorima). Podatkovni centar povezan je s objektima društva Bisnode putem vlastite transformatorske postaje izravnom vezom na srednjonaponskoj razini ili istovrsnom vezom. Podatkovni centri opremljeni su i sustavima za rano otkrivanje požara koji automatski pokreću postupak gašenja.

Osim toga, dostupnost podataka, a posebice zaštita od gubitka podataka uslijed tehničkog kvara ili slučajnog brisanja, osigurava se redovitom izradom sigurnosnih kopija i izradom sigurnosnih kopija svih relevantnih baza podataka i sustava kako bi se u slučaju kvara mogli vratiti u prethodno stanje za koje se sigurnosna kopija izrađuje jednom dnevno.

	Mjere
01.	Postoje mjere kojima se osigurava povjerljivost, cjelovitost i dostupnost osobnih podataka i opisanih podatkovnih medija u slučaju katastrofe.
02.	Postoji priručnik za slučaj nužde koji sadrži planove, organizaciju rada i jasnu raspodjelu dužnosti u slučaju nužde.
03.	Dostupni su pričuvni podatkovni centri (aktivno ili pasivno stanje pripravnosti).
04.	Dostupan je sustav neprekidnog napajanja električnom energijom.
05.	Odbijaju se neovlašteni korisnici (npr. u pokušajima preplavljivanja).
06.	Odgovarajući sigurnosni sustavi (softverski/hardverski) štite društvo Bisnode od napada uskraćivanjem usluge (DDoS): alat za pretraživanje virusa, vatrozidi, filtar za neželjenu e-poštu, programi za šifriranje.
07.	Postoji sustav upravljanja kapacitetima koji redovito utvrđuje postojeće jedinstvene točke kvara, analizira ih i na njih primjenjuje odgovarajuće mjere.
08.	Postoje pravila koja se redovito revidiraju i koja rizik od pogrešaka ili zlouporabe rada na održavanju podatkovnog centra svode na najmanju moguću mjeru (npr. načelo „četiri oka”).

E. Mjere za redovite INSPEKCIJE, PROCJENE i VREDNOVANJA (članak 25. stavak 1. Opće uredbe o zaštiti podataka)

IX. UPRAVLJANJE ZAŠTITOM PODATAKA

Upravljanje zaštitom podataka opisuje interne mjere za posebne zahtjeve zaštite podataka.

	Mjere
01.	U društvu Bisnode imenovan je službenik za zaštitu podataka.
02.	U društvu Bisnode postoji službenik za IT/informacijsku sigurnost.
03.	U društvu Bisnode postoje pravila o zastupanju za voditelja obrade podataka (koji je odgovoran za IT infrastrukturu podizvođača).
04.	Službenik za IT/informacijsku sigurnost i službenik za zaštitu podataka u društvu Bisnode odgovarajuće su osposobljeni, posjeduju odgovarajuće stručno znanje i iskustvo te svojom osobnošću odgovaraju zahtjevima radnog mjesta.
05.	Podizvođačevi službenici za IT/informacijsku sigurnost i zaštitu podataka na odgovarajući način sudjeluju u organizacijskoj strukturi (kao jedinica djelatnika pod vodstvom uprave ili na sličnom neovisnom položaju).
06.	Provodi se redovito osnovno osposobljavanje djelatnika o informacijskoj sigurnosti i zaštiti podataka.
07.	Postoje postupci za redovito procjenjivanje i dopunjavanje ponude osposobljavanja kako bi odgovarala potrebnoj razini i obuhvaćala promjene okvirnih uvjeta (izmjene i dopune zakona, nove zakone i propise).
08.	Djelatnici koji rade s osobnim podacima upućuju se ili obvezuju na zaštitu privatnosti i odobrenu praksu.
09.	Postoje opća pravila o privatnosti.
10.	Postoje opća pravila o IT sigurnosti.
11.	Ove smjernice pohranjene su na središnjoj lokaciji i dostupne su svim djelatnicima.
12.	Upute o radu i slični dokumenti usklađeni su sa zahtjevima navedenim u ovim smjernicama.
13.	Postoje dokumentirani postupci za utvrđivanje, analiziranje, vrednovanje i uzimanje u obzir promjena zahtjeva (npr. zakona o privatnosti) te IT procesa i postupaka (procjena učinka na zaštitu podataka, novih aplikacija, novih IT sustava itd.).
14.	Postoje dokumentirani postupci za utvrđivanje, analiziranje i vrednovanje incidenata u području zaštite podataka koji se tiču promjena te postupci za izradu mjera kojima će se spriječiti ponavljanje incidenata (povezanost upravljanja promjenama i upravljanja incidentima).

X. UPRAVLJANJE ODGOVOROM NA INCIDENT

Društvo Bisnode svjesno je zakonskih obveza izvještavanja te je osvijestilo i osposobilo svoje djelatnike za prepoznavanje bilo kakvih povreda o kojima su dužni izvijestiti. Definiran je odgovarajući postupak izvještavanja. Primatelji poruke (služba za korisnike) i djelatnici znaju kome se moraju obratiti u slučaju povrede privatnosti. Nadalje, nakon primitka izvješća provodi se postupak pravodobne obrade izvješća. Definirani su članovi „kriznog tima" te je zajamčena procjena incidenta i, po potrebi, pokretanje izvještavanja.

Upravljanje odgovorom na incident za incidente u području zaštite podataka povezano je s upravljanjem IT incidentima, upravljanjem sigurnosnim incidentima i kriznim upravljanjem društva Bisnode AB.

XI. POSTAVKE PRILAGOĐENE ZA PRIVATNOST

Društvo Bisnode izradilo je „Smjernice grupacije o tehničkoj i integriranoj zaštiti privatnosti" radi provedbe članka 25. stavka 2. Opće uredbe o zaštiti podataka. Smjernicama je propisano da društvo Bisnode proaktivno i bez dodatnih poticaja integrira zaštitu podataka u sva područja te da se zaštita podataka uzima u obzir već u fazi izrade ponude. Sukladnost s odredbama o tehničkoj zaštiti privatnosti više je od pukog pitanja korisničkog iskustva za društvo Bisnode. Odgovarajuća sukladnost uključuje i poduzimanje odgovarajućih tehničkih i sigurnosnih mjera za zaštitu korisničkih i osobnih podataka.

Uz to, društvo Bisnode izradilo je „Pravila grupacije o zadržavanju podataka". To je osnovni dokument koji se provodi zasebno na svakom tržištu, uz odstupanja prilagođena lokalnim uvjetima. U tu je svrhu društvo Bisnode uvelo odgovarajući koncept brisanja osobnih podataka u Njemačkoj.

XII. NADZOR NARUDŽBI

Nadzor narudžbi uključuje mjere kojima se osigurava da se osobni podaci koji se obrađuju u ime klijenta mogu obrađivati isključivo u skladu s klijentovim uputama.

Ako društvo Bisnode obrađuje osobne podatke temeljem ugovora, uvijek se zaključuje pisani ugovor o obradi ugovornih podataka koji sadrži zakonom propisan sadržaj u skladu s člankom 28. Opće uredbe o zaštiti podataka. Za te je potrebe društvo Bisnode izradilo vlastite predloške ugovora kojima se klijent može koristiti za naručivanje usluga. Ugovornim se obvezama osigurava da društvo Bisnode obrađuje klijentove podatke isključivo u skladu s klijentovim uputama, jamči se povjerljivost podataka te je posebno napomenuto da se klijentovi podaci ne prenose u opći podatkovni inventar društva Bisnode ako klijent nije dao izričitu uputu za taj prijenos. Uz to, opisi tehničkih i organizacijskih zaštitnih mjera u društvu Bisnode sastavni su dio svakog ugovora s društvom Bisnode o naručenoj obradi podataka s obzirom na to da ovaj dokument čini dogovoreni dodatak ugovoru o naručenoj obradi podataka.

	Mjere
01.	Djelatnici društva Bisnode predani su očuvanju tajnosti podataka.
02.	Društvo Bisnode angažira podizvođače (uključujući neovisna pridružena društva) za obradu narudžbi (što uključuje održavanje IT sustava) – vidjeti popis podizvođača.
03.	Sa svim podizvođačima sklopljeni su ugovori o ugovornoj obradi podataka ili ugovori o zaštiti podataka koji su usklađeni s člankom 28.

04.	Ugovori između društva Bisnode i podizvođača odražavaju zahtjeve koje tijelo nadležno za ugovaranje postavlja podizvođaču (vidjeti okvirni ugovor i dodatak ugovoru o naručenoj obradi podataka).
05.	Neki od podizvođača nalaze se izvan Europskog gospodarskog prostora (EGP-a) – vidjeti popis podizvođača.
06.	Osigurava se odgovarajuća razina zaštite podataka, na primjer primjenom standardnih ugovornih odredbi EU-a, pojedinačnih ugovora koje su odobrila nadzorna tijela ili kada je riječ o trećim zemljama za koje je Europska komisija utvrdila da pružaju odgovarajuću razinu zaštite podataka.

XIII. INFORMACIJE O SIGURNOSTI PODATAKA

CANCOM Pironet AG & Co. KG	Nositelj certifikata ISMS 27001
D&B UK	Nositelj certifikata ISMS 27001
D&B International	Informativni list o ISMS-u

dpo@bisnode.com