dun & bradstreet
WORLDWIDE NETWORK

Bisnode

Technické a organizačné opatrenia na ochranu údajov

V tejto prílohe nájdete viac podrobností o tom, ako zabezpečujeme dáta.

verzia 2012

Poštová adresa
Bisnode Slovensko, s. r. o.
Ľ. Stárka 2150/16
911 05 Trenčín

www.bisnode.sk
+421 32 746 26 40
info@bisnode.sk

Obsah

Rozsah použitia

Podľa nariadenia o ochrane osobných údajov (GDPR) je každý subjekt, ktorý zhromažďuje, spracováva alebo používa osobné údaje, povinný prijať také technická a organizačné opatrenia, ktoré sú potrebné na zabezpečenie splnenia pravidiel ochrany údajov.

Vstupná kontrola

Vstupná kontrola sa používa na zákazu neoprávneným osobám získať prístup k technickému zariadeniu, v ktorom sa spracovávajú alebo používajú osobné údaje.

Vstupná kontrola v našich prevádzkových priestoroch

Vstup do našich budov je regulovaný kontrolnými mechanizmami pri vstupe. Pre našich zamestnancov sú nimi predovšetkým elektronické kľúče, ktoré povoľujú vstup do prevádzkových priestorov podľa prístupových práv stanovených pre každý kľúč. Prístupové práva sú zladené s právomocami udelenými pracovníkom s ohľadom na miesto (podľa konkrétnych častí prevádzkových priestorov).

Pre návštevníkov je vstupná kontrola zabezpečovaná centrálnou recepciou alebo vrátnikom, ktorý zaznamenáva údaje o návštevníkoch a vydáva im preukazy návštevníka platné počas príslušnej návštevy.

Kontrola vstupu do nášho počítačového strediska

Naše IT systémy sú za nás prevádzkované rôznymi dátovými centrami. Dátové centrá sú navrhnuté ako uzatvorené bezpečnostné priestory. Je tu fyzická aj technická kontrola vstupu. Dátové strediská sú zabezpečené elektronicky a návštevníkom je povolený vstup len v doprovode. Návštevníci sa nemôžu v dátovom centre pohybovať bez dozoru. Potrebné vstupné karty sú vydávané len po predchádzajúcom vyrozumení a za prísnych podmienok. Použitie je evidované. Dátové strediská sú monitorované videom. Priestory a kritické vnútorné oblasti budovy sú zároveň 24 hodín pod dohľadom bezpečnostnej firmy.

Kontrola práva vstupu

Kontrola práva vstupu zahŕňa opatrenia, ktorými sa zabraňuje neoprávneným osobám použiť systémy spracovania dát (logická bezpečnosť).

Kontrola práva vstupu do našich prevádzkových priestorov

Administratívna práca vykonaná nami alebo prevádzkovateľom dátového strediska je vykonávaná určitými členmi personálu, ktorí podpísali zvláštnu dohodu o mlčanlivosti a pred prijatím do zamestnania boli preverení. Dohoda o mlčanlivosti obsahuje záväzok utajenia dát. Identifikácia užívateľskými menami a bezpečnými heslami je povinná. Naše IT systémy sú taktiež chránené pred vonkajším prostredím.

Kontrola práva vstupu u prevádzkovateľa dátového centra

Prevádzkovateľ dátového centra taktiež nainštaloval ďalšie pokročilé funkcie firewallu v rámci sieťovej vrstvy a produktov na právo vstupu.

Kontrola prístupu

Kontrola prístupu sú opatrenia prijaté na to, aby zabezpečili, že užívatelia majú prístup len k údajom, ku ktorým majú oprávnenie pristupovať, a že osobné údaje nie je možné bez oprávnenia čítať, skopírovať, zmeniť alebo zmazať v priebehu spracovávania alebo používania a potom, čo boli uložené.

Kontrola prístupu v našich prevádzkových priestoroch

Definovali a zdokumentovali sme vnútorné normy pre udeľovanie oprávnení. Podľa nich sa riadia práva, ktoré majú administrátori pri prevádzke zákazníckych systémov. Tieto normy stanovujú napríklad požiadavky na bezpečnosť hesiel.

Kontrola prístupu u prevádzkovateľa dátového centra

V prípadoch, keď uzavrieme zmluvu s prevádzkovateľom dátového centra, aby prevzal nastavenie užívateľov a autorizácií na aplikačnej vrstve, bude tento prevádzkovateľ viazaný rovnakými bezpečnostnými normami, ktoré platia pre naše vlastné prevádzkové priestory. Odchýlky sú povolené len vtedy, pokiaľ ich písomne nariadime. Stanovujeme aj formuláciu smerníc, pokiaľ ide o to, ako má prevádzkovateľ dátového centra koncipovať vnímanie autorizácie špecifickej pre danú aplikácii.

Kontrola prenosu

Kontrola prenosu zahŕňa opatrenia, ktoré zabezpečujú, aby počas elektronického prenosu nebolo bez povolenia možné osobné dáta prečítať, zmeniť alebo vymazať, zatiaľ čo sú prenášané alebo ukladané na dátové média, a aby bolo možné overiť a preukázať, ako sa majú osobné dáta prenášať pomocou zariadení dátovej komunikácie.

Kontrola prenosu v našich prevádzkových priestoroch

S ohľadom na všeobecné spracovanie dát (údaje o zamestnancoch, údaje o dodávateľoch, údaje o klientskej základni) je kontrola prenosu (kontrola prenosu, kontrola komunikácie) zabezpečená pomocou náležitých technických opatrení. Tie zahŕňajú firewall, antivírusovú ochranu, tunel VPN, šifrovanie dát a ochranu heslom pre jednotlivé dokumenty. Pre logistickú prepravu dát sú zamestnávaní len vhodní poskytovatelia služieb. Pokiaľ ide o komerčné spracovanie údajov, príjem a poskytovanie údajov klientom v priebehu nášho informačného podnikania, je kontrola prenosu zabezpečovaná evidovaným všetkých štádií spracovania údajov. Pokiaľ je dohodnuté s klientom zaradenie dát do kategórie „obzvlášť dôverné“ sú dáta ďalej šifrované na účely prenosu prostredníctvom verejných sietí.

Kontrola prenosu u prevádzkovateľa dátového centra

Prevádzkovateľ dátového centra je viazaný rovnakými povinnosťami ohľadom kontroly prenosu, ako sme my. Pre prevádzky zásadná kópia (záloha), hlavne v súvislosti so zabezpečením veľmi dôležitých údajov, sa používajú len štandardizované a zdokumentované postupy. Vytváranie všetkých záloh je evidované.

Kontrola vkladania dát

Vstupná kontrola zahŕňa opatrenie zabezpečujúce, aby bolo možné následne overiť a preukázať, či došlo k vloženiu, zmene alebo vymazaniu osobných údajov do systémov spracovania dát a kým. Vložiť údaje môžu len pracovníci, ktorí majú prístup k dátam. Taktiež sa v systémoch automaticky vytvárajú protokoly „určitých procesných krokov“. Protokolovanie „určitých procesných krokov“ sa vzťahuje na procesy, ktoré slúžia na zabezpečenie kontinuity podnikania, ktoré slúžia na účtovnícke účely a splnenie zákonných požiadaviek na uchovanie údajov.

Kontrola dostupnosti

Kontrola dostupnosti zabezpečuje, že sú osobné údaje chránené pred náhodnou (neúmyselnou) stratou alebo zničením.

Základom kontroly dostupnosti je subdodávateľské zadanie spracovania IT zariadení maximálne strážanému dátovému centru prevádzkovateľa dátového strediska. Dátové centrá majú záložné napájacie zariadenia s neprerušiteľným zdrojom napájania a generátorovú jednotku pre prípad núdze (využívajúcu napríklad záložné dieselové generátory). Dostupnosť dát, predovšetkým ochrana pred stratou dát kvôli technickému zlyhaniu alebo náhodnému

vymazaniu, sa tiež zabezpečuje pomocou pravidelných bezpečnostných opatrení a záloh dát všetkých relevantných databáz a systémov, aby v prípade poruchy bolo možné dáta obnoviť aspoň na mesačnej báze.

Separačné pravidlo

Separačné pravidlo zabezpečuje možnosť, aby dáta zhromaždené na rôzne účely boli spracované oddelene.

Separační pravidlo v našich prevádzkových priestoroch

S ohľadom na všeobecné spracovanie údajov (údaje o zamestnancoch, údaje o dodávateľoch, údaje o klientskej základni) sa separačné pravidlo realizuje napríklad fyzickým oddelením a uložením do oddelených zariadení alebo dátových médií, oddelením výrobného, testovacieho a vývojového prostredia pre naše aplikácie a IT systémy, vhodnými autorizačnými koncepciami a zároveň databázovými právami. Naviac je na strane softwaru zavedený systém logistického oddelenia klientov.

Separačné pravidlo u prevádzkovateľa dátového centra

Prevádzkovateľ dátového centra oddeľuje všetky dáta ako fyzicky, tak logicky aspoň na úrovni klienta. V prípade dát, ktoré sú subdodávateľsky zadané prevádzkovateľovi dátového centra sú k dispozícii ďalšie oddelené rozhrania na úrovni systému alebo databázy.