dun & bradstreet
WORLDWIDE NETWORK

Bisnode

Technická a organizační opatření pro ochranu údajů

V této příloze najdete více podrobností o tom, jak zabezpečujeme data.

verze 1810

Adresa
Bisnode Česká republika, a. s.
Siemensova 2717/4
155 00 Praha 5

www.bisnode.cz
+420 274 000 000
info@bisnode.cz

Obsah

Rozsah použití

Dle nařízení o ochraně údajů (GDPR) je každý subjekt, který shromažďuje, zpracovává nebo používá osobní údaje, povinen přijmout taková technická a organizační opatření, která jsou nezbytná k zajištění splnění pravidel ochrany údajů.

Vstupní kontrola

Vstupní kontrola se používá k zákazu neoprávněným osobám získat přístup k technickému zařízení, v němž se zpracovávají nebo používají osobní údaje.

Vstupní kontrola v našich provozních areálech

Vstup do našich budov je regulován kontrolními mechanismy při vstupu. Pro naše zaměstnance jsou jimi především elektronické klíče, které povolují vstup do provozních areálů dle přístupových práv stanovených pro každý klíč. Přístupová práva jsou sladěna s pravomocemi udělenými pracovníkům s ohledem na místo (dle konkrétních částí provozních areálů).

Pro návštěvníky je vstupní kontrola zajišťována centrální recepcí nebo vrátným, který zaznamenává údaje o návštěvnících a vydává jim průkazy návštěvníka platné po dobu příslušné návštěvy.

Kontrola vstupu do našeho počítačového střediska

Naše IT systémy jsou za nás provozovány různými datovými centry. Datová centra jsou navržena jako uzavřené bezpečnostní prostory. Je zde fyzická i technická kontrola vstupu. Datová střediska jsou zabezpečena elektronicky a návštěvníkům je povolen vstup pouze v doprovodu. Návštěvníci se nemohou v datovém centru pohybovat bez dozoru. Nezbytné vstupní karty jsou vydávány pouze po předchozím vyrozumění a za přísných podmínek. Použití je evidováno. Datová střediska jsou monitorována videem. Prostory a kritické vnitřní oblasti budovy jsou zároveň 24 hodin pod dohledem bezpečnostní firmy.

Kontrola práva vstupu

Kontrola práva vstupu zahrnuje opatření, kterými se zabraňuje neoprávněným osobám použít systémy zpracování dat (logická bezpečnost).

Kontrola práva vstupu do našich provozních areálů

Administrativní práce provedená námi nebo provozovatelem datového střediska je vykonávána určitými členy personálu, kteří podepsali zvláštní dohodu o mlčenlivosti a před přijetím do zaměstnání byli prověřeni. Dohoda o mlčenlivosti obsahuje závazek utajení dat. Identifikace uživatelskými jmény a bezpečnými hesly je povinná. Naše IT systémy jsou také chráněny před vnějším prostředím.

Kontrola práva vstupu u provozovatele datového střediska

Provozovatel datového centra rovněž nainstaloval další pokročilé funkce firewallu v rámci síťové vrstvy a produktů pro právo vstupu.

Kontrola přístupu

Kontrola přístupu jsou opatření přijatá k tomu, aby zajistila, že uživatelé mají přístup pouze k údajům, k nimž mají oprávnění přistupovat, a že osobní údaje nelze bez oprávnění přečíst, zkopírovat, změnit nebo smazat v průběhu zpracovávání nebo používání a poté, co byly uloženy.

Kontrola přístupu v našich provozních areálech

Definovali a zdokumentovali jsme vnitřní normy pro udělování oprávnění. Dle nich se řídí práva, která mají administrátoři při provozu klientských systémů. Tyto normy stanovují například požadavky na bezpečnost hesel.

Kontrola přístupu u provozovatele datového centra

V případech, kdy uzavřeme smlouvu s provozovatelem datového centra, aby převzal nastavení uživatelů a autorizací na aplikační vrstvě, bude tento provozovatel vázán stejnými bezpečnostními normami, které platí pro naše vlastní provozní areály. Odchylky jsou povoleny pouze tehdy, pokud je písemně nařídíme. Stanovujeme i formulaci směrnic, pokud jde o to, jak má provozovatel datového centra koncipovat pojetí autorizace specifické pro danou aplikaci.

Kontrola přenosu

Kontrola přenosu zahrnuje opatření, která zajišťující, aby během elektronického přenosu nebylo bez dovolení možné osobní data přečíst, zkopírovat, změnit nebo vymazat, zatímco jsou přenášena nebo ukládána na datová média, a aby bylo možné ověřit a prokázat, jak se mají osobní data přenášet pomocí zařízení datové komunikace.

Kontrola přenosu v našich provozních areálech

S ohledem na obecné zpracování dat (údaje o zaměstnancích, údaje o dodavatelích, údaje o klientské základně) je kontrola přenosu (kontrola přenosu, kontrola komunikace) zajišťována pomocí náležitých technických opatření. Ta zahrnují firewall, antivirovou ochranu, tunel VPN, šifrování dat a ochranu heslem pro jednotlivé dokumenty. Pro logistickou přepravu dat jsou zaměstnáváni pouze vhodní poskytovatelé služeb. Pokud jde o komerční zpracování údajů, příjem a poskytování údajů klientů v průběhu našeho informačního podnikání, je kontrola přenosu zajišťována na evidováním všech stádií zpracování údajů. Pokud je dojednáno s klientem zařazení dat do kategorie „obzvlášť důvěrné" jsou data dále šifrována pro účely přenosu prostřednictvím veřejných sítí.

Kontrola přenosu u provozovatele datového centra

Provozovatel datového centra je vázán stejnými povinnostmi ohledně kontroly přenosu, jako jsme my. Pro provozně zásadní kopie (záloha), zejména v souvislosti se zabezpečením zcela nepostradatelných údajů, se používají pouze standardizované a zdokumentované postupy. Vytváření všech záloh je evidováno.

Kontrola vkládání dat

Vstupní kontrola zahrnuje opatření zajišťující, aby bylo možné následně ověřit a prokázat, zda došlo k vložení, pozměnění nebo vymazání osobních údajů do systémů zpracování dat a kým. Vložit údaje smí pouze pracovníci, kteří mají přístup k datům. Také se u systémů automaticky vytvářejí protokoly „určitých procesních kroků". Protokolování „určitých procesních kroků" se vztahuje na procesy, které slouží k zajištění kontinuity podnikání, které slouží k účelům účetnictví a splnění zákonných požadavků na uchování údajů.

Kontrola dostupnosti

Kontrola dostupnosti zajišťuje, že jsou osobní údaje chráněny před náhodnou (neúmyslnou) ztrátou nebo zničením.

Základem kontroly dostupnosti je subdodavatelské zadání provozování IT zařízení maximálně střeženému datovému centru provozovatele datového střediska. Datová centra mají záložní napájecí zařízení s nepřerušitelným zdrojem napájení a generátorovou jednotku pro případ nouze (využívající například záložní dieselové generátory). Dostupnost dat, především ochrana před ztrátou dat kvůli technickému selhání nebo náhodnému vymazání, se také zajišťuje pomocí pravidelných bezpečnostních opatření a záloh dat všech relevantních databází a systémů, aby v případě poruchy bylo možné data obnovit alespoň na měsíční bázi.

Separační pravidlo

Separační pravidlo zajišťuje možnost, aby data shromážděná k různým účelům byla zpracována odděleně.

Separační pravidlo v našich provozních areálech

S ohledem na obecné zpracování údajů (údaje o zaměstnancích, údaje o dodavatelích, údaje o klientské základně) se separační pravidlo realizuje například fyzickým oddělením a uložením do oddělených zařízení nebo datových médií, oddělením výrobního, testovacího a vývojového prostředí pro naše aplikace a IT systémy, vhodnými autorizačními koncepcemi a zároveň databázovými právy. Navíc je na straně softwaru zaveden systém logistického oddělení klientů.

Separační pravidlo u provozovatele datového centra

Provozovatel datového centra odděluje všechna data jak fyzicky, tak logicky alespoň na úrovni klienta. V případě dat, která jsou subdodavatelsky zadaná provozovateli datového centra jsou k dispozici další oddělená rozhraní na úrovni systému nebo databáze.