Manuál pre hlásenie a riešenie bezpečnostných incidentov a incidentov týkajúcich sa ochrany osobných údajov pre dodávateľov

1. Účel dokumentu

Účelom tohto manuálu je stanoviť postup pri identifikácii, oznamovaní a riešení bezpečnostných incidentov a incidentov týkajúcich sa ochrany osobných údajov, ktoré môžu vzniknúť pri poskytovaní služieb alebo plnení zmluvných povinností dodávateľa voči spoločnosti Deutsche Telekom Services Europe Slovakia s.r.o. (ďalej len „zákazník“).

Na účely tohto manuálu sa pojmom incident rozumie bezpečnostný incident alebo incident týkajúci sa ochrany osobných údajov, ak z kontextu nevyplýva inak.

2. Definícia incidentu

Incident predstavuje akúkoľvek udalosť na strane dodávateľa, ktorá ohrozuje alebo môže ohroziť bezpečnosť informácií, informačných systémov alebo ochranu osobných údajov zákazníka, najmä ich dôvernosť, integritu alebo dostupnosť.

Takýto incident môže zahŕňať najmä neoprávnený prístup k informáciám alebo systémom, porušenie bezpečnostných opatrení, porušenie právnych alebo zmluvných povinností, ako aj akékoľvek konanie, ktoré môže negatívne ovplyvniť ochranu osobných údajov alebo informačných aktív zákazníka.

Incident môže viesť k právnym sankciám, finančným stratám, prerušeniu prevádzky, poškodeniu dobrého mena organizácie alebo k zásahu do práv dotknutých osôb. Z uvedeného dôvodu je nevyhnutné zabezpečiť jeho včasné odhalenie, bezodkladné nahlásenie a prijatie primeraných nápravných opatrení.

2.1 Bezpečnostný incident

Bezpečnostným incidentom je akákoľvek udalosť alebo pokus o neoprávnený prístup, použitie, sprístupnenie, zmenu alebo zničenie informácií, informačných systémov alebo iných informačných aktív zákazníka, ako aj situácia, pri ktorej dôjde k zlyhaniu bezpečnostných opatrení určených na ich ochranu.

Za bezpečnostný incident sa považuje aj udalosť, ktorá naruší alebo môže narušiť poskytovanie služieb alebo bežnú prevádzku zákazníka.

Príklady bezpečnostných incidentov:

- Infekcia malvérom – zavedenie škodlivého softvéru (napr. vírusov, ransomvéru alebo spyware) do systémov organizácie, ktoré môže poškodiť integritu údajov alebo viesť k neoprávnenému prístupu k údajom.
- Útok sociálneho inžinierstva (phishing, smishing, vishing) – cielený pokus o získanie citlivých informácií vydávaním sa za dôveryhodný subjekt v elektronickej komunikácii, čo často vedie ku kompromitácii používateľských účtov.
- Neoprávnený prístup – získanie prístupu k systémom alebo údajom bez príslušného oprávnenia, napríklad zneužitím bezpečnostných zraniteľností alebo použitím odcudzených prihlasovacích údajov, kompromitácia prihlasovacích údajov. .

- Narušenie fyzickej bezpečnosti – neoprávnený fyzický prístup do zabezpečených priestorov, ako sú dátové centrá, ktorý môže viesť ku krádeži alebo poškodeniu hardvéru a citlivých údajov.
- Strata alebo krádež firemného zariadenia – strata alebo odcudzenie firemného notebooku alebo mobilného zariadenia obsahujúceho citlivé údaje zákazníkov alebo spoločnosti, čo môže viesť k ich sprístupneniu neoprávneným osobám a riziku zneužitia identity.

2.2 Incident týkajúci sa ochrany osobných údajov

Incidentom týkajúcim sa ochrany osobných údajov je akákoľvek udalosť vedúca k neoprávnenému prístupu, sprístupneniu, strate, zničeniu, zmene alebo inému neoprávnenému spracúvaniu osobných údajov.
Takýto incident môže predstavovať porušenie požiadaviek nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 (GDPR) alebo iných právnych predpisov upravujúcich ochranu osobných údajov.

Príklady incidentov, týkajúcich sa ochrany osobných údajov:

- únik osobných údajov,
- neoprávnené sprístupnenie osobných údajov,
- odoslanie e-mailu s osobnými údajmi nesprávnemu adresátovi,
- phishing vedúci ku kompromitácii osobných údajov,
- spracúvanie osobných údajov bez právneho základu,
- porušenie zásad GDPR (minimalizácia údajov, obmedzenie účelu, bezpečnosť spracúvania a pod.).

3. Hlásenie incidentov

Dodávateľ je povinný oznámiť každý incident bez zbytočného odkladu po jeho zistení, a to aj v prípade, ak:

- nie je isté, či ide o incident,
- rozsah incidentu zatiaľ nie je známy,
- incident bol medzičasom odstránený,
- nebolo ešte ukončené interné preverovanie.

Incident sa oznamuje miestnemu:

- Security Officerovi (SO) alebo Data Privacy Officerovi (DPO), podľa povahy incidentu.

Ak nie je možné jednoznačne určiť kategóriu incidentu, dodávateľ kontaktuje ktorúkoľvek z uvedených osôb.
Do času prevzatia riešenia incidentu zákazníkom je dodávateľ povinný:

- prijať primerané opatrenia na obmedzenie ďalších následkov incidentu,
- zachovať všetky dostupné dôkazy,
- neposkytovať informácie o incidente tretím osobám bez predchádzajúceho súhlasu zákazníka, ak takú povinnosť neukladá právny predpis.

4. Proces riešenia incidentu

4.1 Detekcia incidentu

Incident je identifikovaný na základe zistených skutočností alebo dôveryhodného oznámenia, ktoré nasvedčuje možnému porušeniu bezpečnosti informácií, ochrany osobných údajov alebo iných právnych či zmluvných povinností.

4.2 Počiatočné posúdenie

Security Officer alebo Data Privacy Officer vykoná počiatočné posúdenie oznámeného incidentu a overí jeho dôvodnosť.

4.3 Vyšetrovanie

V prípade potvrdenia incidentu sa začne vyšetrovanie v spolupráci s príslušnými organizačnými útvarmi.
Cieľom vyšetrovania je najmä:

- určiť príčinu incidentu,
- identifikovať rozsah dopadov,
- určiť dotknuté osoby alebo systémy,
- navrhnúť nápravné opatrenia.

4.4 Nápravné opatrenia

Na základe výsledkov vyšetrovania sa prijmú primerané technické, organizačné alebo právne opatrenia na odstránenie príčin incidentu a minimalizáciu jeho následkov.
Všetky prijaté opatrenia musia byť zdokumentované.

4.5 Uzatvorenie incidentu

Incident sa uzatvorí po:

- ukončení vyšetrovania,
- prijatí všetkých potrebných opatrení,
- splnení oznamovacích povinností,
- zdokumentovaní celého priebehu riešenia incidentu.

5. Kategórie incidentov

Typ incidentu	Kategória
Infekcia malvérom	Bezpečnostný incident
Útok sociálnym inžinierstvom (phishing/smishing/vishing)	Bezpečnostný incident / Incident týkajúci sa ochrany osobných údajov*
Neoprávnený prístup	Bezpečnostný incident
Narušenie fyzickej bezpečnosti	Bezpečnostný incident
Strata alebo krádež firemného zariadenia	Bezpečnostný incident
Strata alebo krádež osobných vecí zamestnancov	Bezpečnostný incident**
Strata alebo krádež prístupových kariet	Bezpečnostný incident
Únik a zneužitie osobných údajov	Incident týkajúci sa ochrany osobných údajov
Náhodné zdieľanie alebo sprístupnenie osobných údajov	Incident týkajúci sa ochrany osobných údajov

Typ incidentu	Kategória
Porušenie požiadaviek GDPR	Incident týkajúci sa ochrany osobných údajov

* **Útok sociálnym inžinierstvom** môže byť klasifikovaný ako bezpečnostný incident, pričom v prípade kompromitácie osobných údajov súčasne predstavuje aj incident týkajúci sa ochrany osobných údajov.

** Ak ide o stratu alebo krádež osobných vecí zamestnanca bez dopadu na informačnú bezpečnosť (napr. súkromná peňaženka), nejde spravidla o bezpečnostný incident spoločnosti. Ak však ide o vec obsahujúcu firemné informácie, identifikačné prvky alebo prístupové prostriedky (napr. notebook, mobilný telefón, USB kľúč alebo identifikačná karta), ide o bezpečnostný incident.

6. KONTAKTY

Secutity Officer	angelika.kodhajova@telekom.com
Data Privacy Officer	j.balik@telekom.com