Podmienky poskytovania doplnkovej služby InLine Security

(ďalej iba „Podmienky")

Tieto Podmienky definujú pravidlá zriadenia a poskytovania doplnkovej služby Inline Security, na základe ktorých Podnik zabezpečuje Účastníkovi ochranu jeho mobilných dátových služieb za podmienok uvedených nižšie. V otázkach neupravených v týchto Podmienkach sa primerane použijú ustanovenia aktuálnych Všeobecných podmienok pre poskytovanie verejných služieb spoločnosti Slovak Telekom,a.s. (ďalej len „Všeobecné podmienky"), Podmienok pre spracovanie osobných, identifikačných, prevádzkových a lokalizačných údajov Účastníka a ďalších podmienok Účastníkom využívaných služieb a ponúk Podniku zverejnených na webových stránkach Podniku na adrese https://www.telekom.sk/info/dokumenty-a-pravne-informacie/informacie-pre-koncovych-uzivatelov ďalej platný Cenník služieb a ustanovenia platného právneho poriadku Slovenskej republiky.

Podmienky sú uverejnené na vyššie uvedených webových stránkach Podniku a samostatne bez splnenia ďalších podmienok nie sú návrhom na uzavretie zmluvy. V prípade rozporu medzi znením Podmienok uverejneným na internete a znením Podmienok uverejneným iným spôsobom je vždy rozhodujúce znenie uverejnené na vyššie uvedených webových stránkach.

Popis a rozsah Služby

1. Podmienkou aktivácie doplnkovej služby InLine Security (ďalej „InLine Security" alebo „Služba") je používanie mobilnej služby na základe platnej Zmluvy o poskytovaní služieb v programe Biznis Spojenie alebo na základe platnej Zmluvy o poskytovaní služieb - služba Mobilný Internet alebo Rámcovej zmluvy o spolupráci T-Biznis Flex alebo Dohody o voliteľnom volacom programe Biznis Data Partner.
2. Služba je určená výlučne pre Účastníka, ktorým je právnická osoba alebo fyzická osoba podnikateľ. S vopred udeleným súhlasom Účastníka má právo používať službu aj osoba, ktorá telefónne číslo (SIM) reálne používa na pracovné a prípadne aj súkromné účely (ďalej len „Koncový užívateľ").
3. Účastník je povinný informovať všetkých svojich Koncových užívateľov (najmä svojich zamestnancov a ďalšie osoby, ktorým udelil súhlas na používanie telefónneho čísla) o aktivácii Služby a jej podmienkach, vrátane možností zrušenia Služby. Účastník berie na vedomie a výslovne súhlasí s tým, že Podniku uhradí akúkoľvek škodu vzniknutú v súvislosti s neoprávnenou aktiváciou Služby alebo iným neoprávneným použitím a používaním Služby.
4. Koncový užívateľ má právo, na základe vopred udeleného súhlasu zo strany Účastníka a v jeho mene Službu aktivovať ako aj deaktivovať. Ak takýmto súhlasom nedisponuje, je povinný požiadať o aktiváciu alebo deaktiváciu prostredníctvom osoby na to oprávnenej za Účastníka.
5. O aktivácii aj deaktivácii Služby Podnik informuje Účastníka, resp. Koncového užívateľa prostredníctvom notifikačnej SMS.

6. Popis Služby InLine Security

6.1. Služba je viazaná na telefónne číslo Koncového užívateľa, pre ktoré bola aktivovaná (nie je využiteľná na inom telefónnom čísle).

6.2. Účelom Služby je zaistenie ochrany pred kybernetickými hrozbami na sieťovej úrovni ako sú vírusy, ransomware, phishing a pod. Služba nenahrádza ďalšie bezpečnostné opatrenia pre koncové zariadenia Koncového užívateľa (napr. antivírusový program), ale tieto nástroje vhodne dopĺňa. Služba chráni Koncového užívateľa iba v rámci prevádzky uskutočňovanej v mobilnej sieti Podniku v APN Internet (platí aj pre roaming) nie však pri využití dát prostredníctvom WiFi.

6.3 Obsahom Služby je prevencia pred kybernetickými hrozbami prostredníctvom blokovania potenciálne nebezpečnej dátovej komunikácie Koncového užívateľa. Súčasťou Služby je poskytnutie riešenia určeného k detekcii kybernetických bezpečnostných udalostí, overenie a kontrola prenášaných dát na sieťovom perimetri komunikačnej mobilnej siete Podniku a aktívne blokovanie nežiadúcej komunikácie v rámci perimetru komunikačnej mobilnej siete a inak nebezpečného obsahu na internete (ďalej iba „Riešenie"). Riešenie je momentom aktivácie Služby implementované medzi koncovým bodom mobilnej siete Podniku a koncovým zariadením Koncového užívateľa, tj. na sieťovom perimetre komunikačnej mobilnej siete Koncového užívateľa. Toto Riešenie kontroluje a monitoruje dátovú prevádzku na sieťovom perimetre komunikačnej siete Koncového užívateľa, bez toho, aby realizovalo dešifrovanie obsahu komunikácie. Pri šifrovanej komunikácii sú analyzované iba hlavičky dátových paketov a metadata. Strojové rozhodovanie o blokovaní komunikácie prebieha iba na základe IP adries, portov, protokolu alebo metadat v hlavičkách (napr. detekcia anomálií v správaní siete) za využitia kontinuálne aktualizovaných dát globálne uznávaných expertných spoločností a skupín v oblasti kybernetickej bezpečnosti. Pokiaľ príde k identifikácii hrozby a zablokovaniu komunikácie na sieťovom perimetre komunikačnej siete Koncového Užívateľa, je o takejto udalosti každý dotknutý Koncový užívateľ konkrétneho mobilného telefónneho čísla informovaný prostredníctvom SMS, cez ktorú sa dostane k informácii o konkrétnej blokovanej stránke. Súčasne má Účastník na portáli Moja firma a v Telekom aplikácii k dispozícii štatisticky zhrnuté informácie o celkovom počte zablokovaných hrozieb za každé telefónne číslo aktivované na Účastníka a to za aktuálny mesiac a 2 predchádzajúce mesiace.

6.4 Podnik negarantuje, že Služba zachytí všetku potenciálnu nebezpečnú komunikáciu. V prípade ak u Účastníka vzniknú pochybností, či je konkrétna doména alebo komunikácia skutočne potenciálne nebezpečná, má právo za týmto účelom kontaktovať Podnik telefonicky alebo e-mailom. Podnik si vyhradzuje právo neodblokovať prístup na jednotlivé zablokované domény na žiadosť Účastníka. Pokiaľ by aj naďalej Účastník/Koncový užívateľ trval na odblokovaní prístupu môže požiadať Podnik o deaktiváciu služby.

6.5 Účastník berie na vedomie a súhlasí, že prípadná porucha Služby môže ovplyvniť využívanie mobilných dát, aplikácií fungujúcich na mobilných dátach alebo aj iné riešenia Účastníka/Koncového užívateľa využívajúce mobilný dátový prenos, a to vrátane úplnej nefunkčnosti dátovej prevádzky a niektorých aplikácií na strane Účastníka/ Koncového užívateľa za sieťovým perimetrom komunikačnej siete Účastníka/Koncového užívateľa.

6.6 Hoci sa Podnik zaväzuje vynaložiť úsilie na identifikáciu a obmedzenie dopadu kybernetických udalostí,

vzhľadom na neustály vývoj nových typov útokov, ich kombinácií, modifikácií a rozsahu nemôže Podnik zaručiť, že ochrana poskytovaná prostredníctvom Služby bude vždy a bezpodmienečne plne účinná. Podnik nezodpovedá za prípadnú škodu (vrátane škody spôsobenej najmä nedostupnosťou Služby, stratou, narušením integrity či autenticity dát, zneprístupnením dát, prerušením prevádzky alebo únikom informácií, prípadne inej škody vzniknutej v dôsledku sankcií a nárokov tretích osôb, ako aj za ušlý zisk), ktorú Účastník/Koncový užívateľ utrpí v dôsledku akejkoľvek kybernetickej udalosti vedenej prostredníctvom mobilnej dátovej siete Podniku.

6.7 Účastník/Koncový užívateľ berie na vedomie a súhlasí, že Služba nie je kompatibilná s verejnou statickou IP adresou, privátnou statickou IP adresou a verejnou dynamickou IP adresou. Účastník/Koncový užívateľ berie na vedomie a súhlasí, že Služba nie je kompatibilná zároveň so službou OnNet Security – aktiváciou Služby sa služba On Net Security automaticky zruší.

6.8 Podnik na účely poskytovania Služby spracúva údaje o dátovej komunikácii Koncového užívateľa, a to výlučne na telefónnych číslach, pre ktoré je Služba aktívna. Osobné údaje sa spracúvajú výlučne na účel poskytovania Služby a nebudú sa využívať na iné účely. Podmienky spracovania osobných údajov tvoria prílohu č. 1 týchto Podmienok a predstavujú jej neoddeliteľnú súčasť. Ďalšie informácie k spracúvaniu osobných údajov sú uvedené na https://www.telekom.sk/osobne-udaje. Informácie o zablokovanej hrozbe sa uchovávajú 60 dní.

7 Rozsah Služby a jej základné funkcionality:

a) Dedikované pravidlá: Pravidlá vytvorené a spravované bezpečnostnými expertmi Podniku, využívajúce databázy indikátorov kompromitácie (IP adresy, domény, URL, hashe súborov a pod.) získané v rámci každodenných operácií kybernetické spravodajské činnosti (CTI).

b) Filtrovanie IP adries: Blokuje prístup ku škodlivým internetovým zdrojom odmietnutím pripojenia k IP adresám kategorizovaným ako *škodlivé webové stránky, phishing, spamové URL adresy a riadiace servery botnetov (C&C)*.

c) Blokovania riadiacich serverov botnetov (C&C): Deteguje a blokuje pokusy o pripojenie k riadiacim serverom *Command & Control*, ktoré kybernetický útočníci využívajú ku spravovaniu botnetov.

d) Filtrovanie DNS: Blokuje prístup ku škodlivým internetovým zdrojom odmietnutím DNS dotazov spojených s *škodlivými webovými stránkami, phishingem, spamovými URL adresami a riadiacími servermi botnetů (C&C)*.

e) Filtrovanie URL: Blokuje prístup ku škodlivým webovým stránkam prostredníctvom HTTP požiadaviek. Pokiaľ je aktívný DNS-over-HTTPS (DoH), analyzuje pole SNI v správach TLS *Client Hello*, bez toho aby pristupovalo k šifrovanému obsahu.

f) Antivírus: Deteguje a blokuje škodlivý software prenášaný na mobilné alebo stacionárne zariadenie prostredníctvom HTTP.

g) Antimalware (sandboxing): Analyzuje prenášené soubory vo virtuálnom izolovanom prostredí (sandboxu) za účelom detekcie škodlivého softwaru.

h) Detekcia a prevencia prieniku (IPS): Blokuje potenciálne kritické alebo vysoko závažné sieťové hrozby detekované v nešifrovanej prevádzke.

i) Reporty: Účastník môže pristupovať k reportom prostredníctvom portálu Moja firma alebo Telekom aplikácie.

.

8 Podnik si vyhradzuje právo kedykoľvek aktualizovať a meniť tieto Podmienky v časti týkajúcej sa popisu a charakteristiky Služby, možností aktivácie a deaktivácie Služby a okruhu Koncových užívateľov, pre ktorých je Služba určená, tiež i súvisiace Podmienky spracovania osobných, identifikačných, prevádzkových a lokalizačných údajov. Podnik si zároveň vyhradzuje právo Službu čiastočne či v plnom rozsahu zrušiť. O tejto zmene bude Podnik Účastníka informovať spôsobom a za podmienok stanovených vo Všeobecných podmienkach pre poskytovanie verejných služieb spoločnosti Slovak Telekom, a.s.

9 Tieto Podmienky nadobúdajú platnosť a účinnosť dňom 1.7. 2026.

Pre všetky SIM využívajúce Službu platia rovnaké bezpečnostné pravidlá (Službu nie je možné upravovať pre jednotlivé SIM, ani jednotlivé IČO!

Príloha č. 1 k Podmienkam poskytovania doplnkovej služby InLine Security

Podmienky spracovania osobných údajov

1.1 Uchovávanie a iné spracovanie údajov, ktoré majú charakter osobných údajov v zmysle nariadenia (EÚ) 2016/679 Európskeho parlamentu a Rady z 27. apríla 2016 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov, a o zrušení smernice 95/46/ES (ďalej len „GDPR") a zákona č. 18/2018 Z.z. o ochrane osobných údajov v znení neskorších predpisov (ďalej len „Zákon o ochrane osobných údajov") (spoločne označované aj ako „Platný zákon"), v rámci služby sa riadia nižšie uvedenými podmienkami.

1.2 Pri poskytovaní Služby môžu byť spracovávané osobné údaje fyzických osôb, napríklad zamestnancov Účastníka alebo iných fyzických osôb využívajúcich Službu (ďalej len „Dotknuté osoby"). Účastník (ďalej len „Prevádzkovateľ") je pri spracovaní osobných údajov v pozícii prevádzkovateľa v súlade s ustanovením článku 4(7) GDPR. Podnik (ďalej len „Sprostredkovateľ“) je pri spracovaní osobných údajov v pozícii sprostredkovateľa v súlade s ustanoveniami článku 4(8) GDPR.

Spracovanie osobných údajov

1.3 Prevádzkovateľ poveruje Sprostredkovateľa spracovaním osobných údajov a Sprostredkovateľ bude tieto údaje spracovávať výlučne za účelom zabezpečenia poskytovania Služby na základe dohodnutého zmluvného vzťahu (ďalej len „Špecifikácia služby"). Sprostredkovateľ vždy spracováva osobné údaje transparentne, správne, len v nevyhnutnej miere, počas potrebného obdobia a v súlade s Platným zákonom. Sprostredkovateľ nebude používať osobné údaje na žiadny iný účel a nebude ich poskytovať žiadnym neoprávneným tretím stranám. Kópie a duplikáty osobných údajov nesmú byť vytvorené bez súhlasu Prevádzkovateľa – to neplatí v prípade zálohovania na zabezpečenie správneho spracovania osobných údajov a/alebo riadneho poskytovania Služby alebo aktivít na zabezpečenie dôvernosti, integrity, dostupnosti a odolnosti systémov Sprostredkovateľa alebo splnenia zákonnej povinnosti.

1.4 Predmetom spracovania sú osobné údaje prenášané Sprostredkovateľovi prostredníctvom alebo v súvislosti so poskytovanou Službou. Prevádzkovateľ rozhoduje o rozsahu spracovávaných osobných údajov.

1.5 Prevádzkovateľ je zodpovedný za zabezpečenie toho, že osobné údaje, ktoré sú predmetom spracovania, sú presné, boli zhromaždené v súlade so zákonom, najmä v súlade s GDPR a zákonom o ochrane osobných údajov.

1.6 Prevádzkovateľ je výlučne zodpovedný za posúdenie, či je možné osobné údaje spracovávať v súlade s platnou legislatívou v oblasti ochrany osobných údajov, najmä v súlade s Platným zákonom, ako aj za ochranu práv osôb, najmä aby Sprostredkovateľ mohol poskytovať služby dohodnutým spôsobom, ktorý nie je v rozpore s právnymi predpismi. Prevádzkovateľ sa zaväzuje informovať Sprostredkovateľa o akýchkoľvek podozreniach, ktoré by mohli ovplyvniť poskytovanú Službu.

1.7 Sprostredkovateľ sa zaväzuje spracovávať osobné údaje iba na základe týchto Podmienok spracovania osobných údajov a písomných inštrukcií Prevádzkovateľa. Pre vylúčenie pochybností sa spracovanie osobných údajov v súlade so záväzkami Sprostredkovateľa vyplývajúcimi zo špecifikácie Služieb považuje za spracovanie vykonané podľa pokynov Prevádzkovateľa alebo osôb oprávnených Prevádzkovateľom. Ak je určitá inštrukcia podľa názoru Sprostredkovateľa nezákonná, musí o nej bez zbytočného odkladu informovať Prevádzkovateľa. V takom prípade má Sprostredkovateľ právo pozastaviť vykonávanie inštrukcie, kým ju Prevádzkovateľ písomne nepotvrdí. V prípade, že Prevádzkovateľ trvá na splnení pokynu, ktorý Sprostredkovateľ naďalej rozumne považuje za nezákonný, má právo ukončiť poskytovanie služby bez upozornenia, bez práva Prevádzkovateľa na akúkoľvek finančnú kompenzáciu.

1.8 Sprostredkovateľ spracováva osobné údaje najmä automatizovaným spôsobom a v prípade potreby aj manuálne.

Bezpečnosť osobných údajov

1.9 Prevádzkovateľ a Sprostredkovateľ sú povinní prijať všetky vhodné technické a organizačné opatrenia na zabezpečenie úrovne ochrany primeranej riziku a poskytovanej Službe. Opatrenia Sprostredkovateľa, ktoré sú v súčasnosti považované za primerané, sú opísané v sekcii 1.22 týchto Podmienok spracovania osobných údajov. Akékoľvek pokyny alebo opatrenia, ktoré predstavujú odchýlku od uvedených opatrení, sa považujú za žiadosť o úpravu, ktorej náklady, ak je to technicky uskutočniteľné a možné, znáša Prevádzkovateľ. V takom prípade zmluvné strany uzavrú samostatnú dohodu o rozsahu činností, výške a preplácaní nákladov.

1.10 Sprostredkovateľ prijal a udržiava primerané technické a organizačné opatrenia na zabránenie neoprávnenému alebo náhodnému prístupu k osobným údajom Prevádzkovateľa, ich zmenám, zničeniu alebo strate, neoprávneným prevodom, inému neoprávnenému spracovaniu, ako aj inému zneužitiu osobných údajov, pričom berie do úvahy poskytovanú Službu.

1.11 Sprostredkovateľ má právo preukázať plnenie povinností, najmä technických a organizačných opatrení, pomocou nasledujúcich nástrojov: a) Kódex správania (článok 40 GDPR); (b) Záväzné firemné pravidlá; c) Certifikát (článok 42 GDPR); (d) aktuálne certifikáty, správy alebo výňatky zo správ nezávislých osôb (napr. audítorov, audítorských oddelení); (d) primeranú certifikáciu vo forme auditu IT bezpečnosti alebo ochrany údajov; e) čestné vyhlásenia Sprostredkovateľa.

1.12 Sprostredkovateľ je povinný informovať Prevádzkovateľa o akýchkoľvek únikoch údajov bez zbytočného odkladu na e-mailovú adresu kontaktnej osoby uvedenej v špecifikácii Služby.

Povinnosť mlčanlivosti

1.13 Sprostredkovateľ musí zabezpečiť, že každá osoba, ktorá má prístup k osobným údajom, je viazaná povinnosťou mlčanlivosti alebo je viazaná zákonnou povinnosťou mlčanlivosti. Povinnosť mlčanlivosti platí aj po ukončení hlavnej zmluvy.

Poskytovanie spolupráce

1.14 Sprostredkovateľ musí, s ohľadom na povahu spracovania a informácie dostupné Sprostredkovateľovi, poskytnúť Prevádzkovateľovi spoluprácu pri plnení povinností Prevádzkovateľa podľa platného zákona.

1.15 Sprostredkovateľ je povinný zabezpečiť spoluprácu v nasledujúcich oblastiach:

1.15.1 Prevádzkovateľ má právo overiť dodržiavanie povinností podľa zmluvy o spracovaní osobných údajov a článku 28 GDPR (povinnosti Sprostredkovateľa osobných údajov) na vlastné náklady. Sprostredkovateľ umožní Prevádzkovateľovi vykonať inšpekciu alebo audit na jeho žiadosť, ale nie častejšie ako raz za kalendárny rok. Prevádzkovateľ sa zaväzuje oznámiť inšpekcie primerane vopred, minimálne 30 (tridsať) pracovných dní vopred, aby zabezpečil dostatočnú spoluprácu zo strany Sprostredkovateľa. Prevádzkovateľ je povinný vykonávať kontroly len v rozsahu nevyhnutnom na overenie splnenia spracovania osobných údajov pre Službu, ktorá mu bola špeciálne poskytnutá, a len v prípade, že Sprostredkovateľ nepreukáže splnenie povinností: a) Kódex správania (článok 40 GDPR); (b) Záväzné firemné pravidlá; c) Certifikát (článok 42 GDPR); d) aktuálne certifikáty, správy alebo výňatky zo správ z nezávislých inštancií (napr. audítori, audítorské oddelenia); (d) primeranú certifikáciu vo forme auditu IT bezpečnosti alebo ochrany údajov; e) podľa čestných vyhlásení Sprostredkovateľa, a vždy tak, aby nezasahovali do bežných činností Sprostredkovateľa a aby bola zachovaná dôvernosť. Prevádzkovateľ nemôže mať prístup k informáciám, ktoré podliehajú obchodným tajomstvám Sprostredkovateľa. Zároveň má Sprostredkovateľ právo podmieniť poskytovanie kontroly alebo auditu uzavretím špeciálnej dohody o ochrane dôvernosti informácií a dodržiavaní interných pravidiel Sprostredkovateľa, ktoré boli vopred oznámené.

1.15.2 Ak je Prevádzkovateľ povinný poskytnúť štátnym správnym orgánom alebo osobám informácie o spracovaní osobných údajov, Sprostredkovateľ poskytne Prevádzkovateľovi spoluprácu pri poskytovaní týchto informácií, ak sa tieto informácie týkajú spracovania údajov v súlade so špecifikáciou Služby a poskytovanou Službou. Sprostredkovateľ musí tiež informovať Prevádzkovateľa – ak to zákon povoľuje – o akejkoľvek komunikácii od dozorných orgánov (napr. vyšetrovania, oznámenia o opatreniach alebo požiadavkách) Sprostredkovateľovi v súvislosti so spracovaním osobných údajov podľa špecifikácie služby.

1.15.3 Sprostredkovateľ je povinný poskytnúť Prevádzkovateľovi spoluprácu v súvislosti so svojou povinnosťou odpovedať na žiadosť o uplatnenie práv dotknutých osôb podľa článkov 15 až 22 GDPR, pokiaľ je to možné vzhľadom na podmienky príslušnej služby a technické a organizačné podmienky. V prípade potreby budú strany koordinovať obsah a rozsah činnosti formou podpory poskytovanej Sprostredkovateľom podľa tohto odseku. Ak osoba kontaktuje Sprostredkovateľa priamo a je možné z podania zistiť, že žiadosť sa týka Prevádzkovateľa, Sprostredkovateľ okamžite postúpi žiadosť dotknutej osoby Prevádzkovateľovi.

1.15.4 Sprostredkovateľ je povinný na základe žiadosti Prevádzkovateľa zaslanej Sprostredkovateľovi (najmenej 10 pracovných dní vopred) poskytnúť informácie potrebné na preukázanie splnenia povinností Sprostredkovateľa podľa článku 28 GDPR (povinnosti Sprostredkovateľa osobných údajov).

1.15.5 Sprostredkovateľ je povinný spolupracovať pri zabezpečení dodržiavania povinností Prevádzkovateľa podľa článkov 32 a 36 GDPR na základe žiadosti Prevádzkovateľa zaslanej Sprostredkovateľovi (najmenej 10 pracovných dní vopred), pričom berie do úvahy povahu spracovania a informácie dostupné Sprostredkovateľovi od Prevádzkovateľa.

1.15.6 Ak Prevádzkovateľ vykoná hodnotenie dopadu na súkromie (osobné údaje) a/alebo konzultácie s dozorným orgánom na posúdenie vplyvu na ochranu súkromia, strany budú koordinovať obsah a rozsah akejkoľvek podpory poskytovanej Sprostredkovateľom, ak to bude potrebné.

1.16 Vyššie uvedené aktivity a spolupráca Sprostredkovateľa sú na náklady Prevádzkovateľa a platia sa samostatne podľa potrebného času alebo využitých zdrojov, spätne za mesiac, v ktorom boli poskytnuté zmluvnému partnerovi.

Zodpovedná osoba pre ochranu osobných údajov

1.17 Sprostredkovateľ sa zaväzuje vymenovať nezávislého, kvalifikovaného a spoľahlivého pracovníka pre ochranu údajov, ak to vyžaduje legislatíva Európskej únie alebo členského štátu, ktorému je Sprostredkovateľ podriadený.

Prenos do tretích krajín

1.18 V prípade, že Sprostredkovateľ prenesie osobné údaje do tzv. tretích krajín (t.j. krajín, ktoré nie sú členmi Európskej únie a nemajú primeranú úroveň ochrany osobných údajov) alebo medzinárodných organizácií, Sprostredkovateľ spracováva osobné údaje v súlade s

príslušnou legislatívou Európskej únie. V takom prípade musí Sprostredkovateľ vopred informovať Prevádzkovateľa, pokiaľ takéto informácie nie sú zákonom zakázané z dôležitých dôvodov verejného záujmu.

Ďalší sprostredkovateľ

1.19 Sprostredkovateľ môže do spracovania zapojiť aj ďalších sprostredkovateľov. Na žiadosť Prevádzkovateľa musí Sprostredkovateľ poskytnúť zoznam ďalších zapojených sprostredkovateľov. Prevádzkovateľ súhlasí s možnosťou zapojenia spoločností v rámci skupiny Deutsche Telekom. Sprostredkovateľ informuje Prevádzkovateľa o akýchkoľvek plánovaných zmenách (zapojenie/náhrada) a Prevádzkovateľ má právo vzniesť relevantné, objektívne a odôvodnené námietky voči takýmto zmenám do 14 (štrnástich) dní. Zmluvné strany sa výslovne dohodli, že v prípade, že Prevádzkovateľ neoprávnene odmietne zmenu, je Sprostredkovateľ oprávnený ukončiť poskytovane Služby výpoveďou bez výpovednej doby a Prevádzkovateľovi v takom prípade nevznikne akýkoľvek nárok na finančnú náhradu spojenú s takýmto ukončením služby.

Vymazanie osobných údajov

1.20 Pokiaľ nie je dohodnuté inak a právne predpisy nevyžadujú dlhšie uchovávanie osobných údajov, tieto budú nenávratne vymazané v prípade ukončenia Špecifikácie služby. Prevádzkovateľ berie na vedomie, že Sprostredkovateľ nie je schopný oddeliť osobné údaje od iných údajov, a preto v prípade žiadosti o vrátenie údajov splní svoje povinnosti podľa tohto ustanovenia vrátením alebo sprístupnením údajov.

Špecifikácia spracovania

1.21 Osobné údaje budú spracovávané za účelom poskytovania Služby v súlade so Špecifikáciou služby a Podmienkami poskytovania doplnkovej služby InLine Security (ďalej len „Podmienky"). Kategórie spracovávaných osobných údajov, príslušné dotknuté osoby, súvisiace operácie alebo doba uchovávania, ako aj ďalšie detaily vyplývajú z povahy a spôsobu poskytovania Služby a sú podrobnejšie opísané v Podmienkach.

1.22 Technické a organizačné opatrenia

a) Dôvernosť (článok 32(1)(b) Všeobecného nariadenia EÚ o ochrane osobných údajov (GDPR)
   - **Kontrola prístupu**
     Zabezpečenie systémov na spracovanie dát proti prístupu neoprávnených osôb, napríklad pomocou magnetických alebo čipových kariet, kľúčov, elektrických otváračov dverí, bezpečnostných služieb a/alebo concierge, alarmov, video systémov a podobne.
   - **Kontrola prístupu**
     Zabezpečenie systémov pred neoprávneným použitím, napríklad prostredníctvom (bezpečnostných) hesiel, automatických zamykacích mechanizmov, dvojfaktorovej autentifikácie, šifrovania dátových nosičov a podobne.
   - **Kontrola prístupových oprávnení**
     Zabezpečenie, aby osoby bez príslušného oprávnenia nemôžu čítať, kopírovať, meniť alebo mazať údaje, napríklad prostredníctvom autorizačných konceptov, prístupových práv na základe príslušných potrieb a prístupových záznamov

b) Integrita (článok 32(1)(b) GDPR)
   - **Kontrola zverejňovania údajov**
     Zabezpečenie, aby počas elektronického prenosu alebo prenosu osoby bez príslušného oprávnenia nemohli takéto údaje čítať, kopírovať, meniť alebo mazať, napríklad prostredníctvom šifrovania, virtuálnych súkromných sietí (VPN), elektronických podpisov a podobne.
   - **Kontrola zadávania údajov**
     Zabezpečenie, aby bolo možné spätne overiť a zistiť, či a kým boli osobné údaje zadané, upravené alebo vymazané zo systémov spracovania údajov, napríklad registráciou autorizácií, vedením záznamov o zadávaní údajov a podobne.

c) Dostupnosť a odolnosť systémov (článok 32(1)(b) GDPR)
   - **Kontrola dostupnosti**
     Ochrana dát pred náhodným alebo úmyselným poškodením a/alebo stratou, napríklad prostredníctvom záloh (online/offline; on-site/off-site), neprerušiteľných zdrojov napájania (UPS), antivírusovej ochrany, firewallov, záznamu prenosových trás a núdzových plánov
     Schopnosť obnoviť dostupnosť dát (článok 32(1)(c) GDPR)

d) Periodický proces testovania, hodnotenia a hodnotenia (článok 32(1)(d) GDPR; článok 25(1) GDPR)
   - Riadenie ochrany údajov
   - Riadenie reakcií na incidenty
   - Predvolené nastavenia, ktoré zabezpečujú ochranu údajov (článok 25(2) GDPR)
   - Kontrola zmluvnej strany
     Zákaz zmluvného spracovania údajov v zmysle článku 28 GDPR bez príslušných pokynov od zákazníka, napr. jednoznačná zmluva, formálne výberové konanie, prísny výber poskytovateľa služieb, povinnosti vykonať dôkladné kontroly vopred a vykonávanie následných kontrol