



Podmínky služby Vodafone Chytrá budova

Podmínky pro poskytování služby Vodafone Chytrá budova společnosti Vodafone Czech Republic a.s. se sídlem náměstí Junkových 2, 155 00 Praha 5, IČO: 257 88 001, zapsané v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. B 6064 (dále jen „Vodafone“ nebo „Poskytovatel“)

1. Základní ustanovení

1) Služba Vodafone Chytrá budova (dále jen „Služba“) je soubor technického a programového vybavení realizující službu vnitřní lokalizace, v budovách včetně měření vybraných parametrů prostředí, např. obsahu CO₂ ve vzduchu. Dále také monitorování obsazenosti parkovišť v krytých parkovištích, případně venkovních parkovištích před budovami. Služba je poskytována společností Vodafone.

2) Službu mohou využívat zákazníci Vodafone, kteří požádají o aktivaci Služby Vodafone Chytrá budova.

3) Pokud tyto Podmínky nestanoví jinak, použijí se Všeobecné podmínky pro poskytování služeb elektronických komunikací, s výjimkou ustanovení, která s ohledem na povahu Služby nelze použít, a další smluvní dokumenty uvedené v Návrhu smlouvy o poskytování veřejně dostupných služeb elektronických komunikací, které jsou pro vás dostupné na internetové adrese www.vodafone.cz v sekci „dokumenty ke stažení“.

2. Popis Služby

I. Komponenty služby:

1) Základním hardwarovým prvkem je čidlo, tzv. Smart Stone, který obsahuje:

- Senzory – teploty, vlhkosti, CO₂, VOC
- Komunikační moduly:

2, 4 GHz max. výstupní výkon +4 DBM

iBeacon standard message

NB-IoT samostatné připojení nebo alternativně sub-Gigahertz komunikační modul na komunikaci s hubem

Bateriově napájené zařízení – předpokládána výdrž 3 až 8 let

Materiál: PC-ABS, bílá barva (možnost dodání jiných odstínů), nehořlavý

Instalace na různé povrchy (kov, omítka, beton, plast, sklo, dřevo,...) pomocí oboustranné samolepky.

Pokrytí podlahové plochy jedním čidlem – cca 30 m²

Smart stone neumí rozpoznávat zvuk, řeč a neobsahuje kameru.

2) Mobilní aplikace, která obsahuje tyto hlavní funkce:

- Rezervace místností
- Vnitřní navigace a lokalizace
- Reportování požadavků, například závady v budově, opravy IT techniky a úklid
- Ovládání teploty, světel a aktuální přehled hodnot v budově
- Provozní efektivita a spolupráce (např. sdílení událostí v budově)
- Building service (důležitá čísla, ztráty a nálezy, jídelní menu)

3) Webové rozhraní pro facility managery a administrátory

1 / 11



- Sledování obsazenosti místností (grafy, Excel export)
- Reportovací systém problémů v budově
- Push notifikace hromadně rozesílané uživatelům mobilní aplikace (upozornění)
- Přehled o reálných hodnotách prostředí v budově

II. Balíčky funkcí:

1) Occupancy Analytics: Balíček funkcí pokrývá potřeby sledování obsazenosti židlí. Čidlo (Smart Stone) se instaluje buď na kancelářskou židli, nebo pod desku kancelářského stolu. Čidla sledují polohu židlí a jejich obsazenost. Obsazení židle je sledováno zcela anonymně a to na základě drobných pohybů židle v době, kdy na nich sedí člověk. Variantně je dodáván sensor na desku stolu, který obsazenost místa detekuje na principu detekce tepla (PIR sensor). Stav pracovního místa je aktualizován v 10 minutových intervalech a zpřístupněn na webovém portálu včetně historie obsazenosti místa.

2) Indoor Location: Balíček funkcí umožňuje navigovat vnitřními prostorami budovy všechny uživatele s chytrými telefony Android (od verze 5.0+) nebo iOS (od verze 10+) podporující Bluetooth ver 4.2 instalovanou navigační aplikací, která je součástí služby. Mapové podklady tvoří floor plan dodaný Účastníkem ve formátu dwg (Autocad), pdf, jpg (v případě pdf a png je velmi důležitá kvalita obrázku-viditelnost detailů na mapě). Přesnost určení polohy je 1 až 3 metry.

Vnitřní prostory musí být pro správnou funkci navigace pokryty čidly – (Smart Stony). Každý z nich pokryje přibližně 30m² plochy budovy. Přesný počet a umístění čidel je určen na základě plánování provedeného nad plánem podlaží budovy nebo/a místního šetření.

3) Air Quality Analytics: Tento balíček umožňuje monitorovat rozšířené parametry prostředí a to:

- teplotu v rozsahu -40 až 125 st.Celsia s přesností +/- 1 st. celsia
- vlhkost v rozsahu 0 % až 100 % s přesností +/- 5 %
- TVOC – detekce těkavých organických sloučenin v rozsahu 0 až 60 000 ppm
- CO₂ – měření obsahu CO₂ ve vzduchu v rozsahu 0 až 10 000 ppm

Monitorování probíhá v místech instalace čidla (Smart Stone), které je určeno jen pro monitoring. Hodnoty jsou aktualizovány každých 30 až 60 minut a zpřístupněny na webovém portálu Služby včetně historie jejich vývoje, dále také v mobilní aplikaci (pouze aktuální hodnoty).

4) Parking Analytics: Tento balíček umožňuje monitorovat parkovací místa ve vnitřních i přilehlých venkovních parkovištích budov. Stav parkovacího místa (obsazeno/volno) je monitorován čidlem (Smart Stone) pro každé místo a je přenášen do webového portálu Služby a mobilní aplikace. Pokud je služba kombinována se službou Indoor Location, pak mobilní aplikace poskytuje i navigaci k volnému parkovacímu místu.

Uvedený rozsah služeb je maximální možný. Aktivní služby se mohou lišit podle konkrétně zakoupených balíčků služeb Účastníkem.

3.Podmínky využití Služby

1) Komunikace účastníka:

- Účastník bere na vědomí a souhlasí s tím, že je povinen komunikovat se Společností Vodafone prostřednictvím kontaktů, které si strany určily ve smlouvě. V případě, že bude Vodafone požádán o poskytnutí Služby prostřednictvím jiného než sjednaného telefonního čísla, je Vodafone oprávněn požadovat sdělení hesla, je-li heslo Účastníkem aktivováno. Bez sdělení hesla není Vodafone povinen Službu poskytnout. Heslo je rovněž nezbytné pro komunikaci prostřednictvím Webového Portálu a případnou změnu konfigurace služeb.
- Účastník je povinen uchovat heslo v tajnosti a chránit jej před vyražením a zneužitím, rovněž je povinen chránit před zneužitím telefonické a e-mailové kontakty. Odpovědnost za vyrazení a zneužití hesla a/nebo telefonických a e-mailových kontaktů nese Účastník. V případě ohrožení bezpečnosti či ztráty hesla a/nebo telefonických a e-mailových kontaktů je Účastník povinen neprodleně kontaktovat Vodafone a provést jejich změnu.
- Má se za to, že osoba, která se při komunikaci s Vodafone prokazuje sjednaným heslem, je osobou oprávněnou k provedení změn konfigurace služeb a ke sjednání změn smlouvy za osobu Účastníka. Vodafone není povinen ověřovat totožnost Účastníka i jinou formou než prostřednictvím zadání hesla.

2) Aktivace Služby:

- Pokud nesouhlasíte s podmínkami Služby anebo zpracováním údajů, které jsou nezbytné k poskytování Služby, Službu neaktivujte a nevyužívejte. Aktivací Služby potvrzujete, že jste se s výše uvedenými dokumenty podrobně seznámil a podmínky, za nichž je Služba poskytována, akceptujete.



- Vodafone je povinen zpřístupnit služby, k jejichž plnění se zavázal, do 60 dnů od účinnosti smlouvy, resp. od změny smlouvy, není-li dále uvedeno jinak. V případě Sjednání služby budou Účastníkovi rovněž sděleny přístupové údaje webového portálu systému. Služba bude dostupná od chvíle, kdy se Účastník – Administrátor přihlásí do portálu na adrese navevbudovy.spaceti.com (např. vodafone.spaceti.com). Administrátor se na portál může přihlásit, jakmile dojde k předání instalované služby pracovníkem Vodafone nebo jeho Servisního střediska.

3) Změna služby:

Službu může Účastník změnit v rámci balíčků funkcí uvedených v bodě 2:

- Změnu balíčku můžete udělat maximálně 1× do měsíce
- Změna balíčku proběhne v závislosti na náročnosti změny, např. v závislosti na dodávce a instalaci jiného druhu čidel.

4. Místo poskytování Služby

Služba Vodafone Chytrá budova je poskytována na území ČR.

5. Úhrada Služby

- Cena služeb je stanovena dohodou. Cena služeb je tvořena jednorázovými poplatky, měsíční paušální částkou (dále jen „měsíční paušál“) a dále položkovými cenami za zvlášť využívané služby. Aktuální Ceník služeb je umístěn na Vodafone OneNet Samoobsluha. Ceny jsou sjednány bez DPH.
- Pro případ prodloužení Účastníka s úhradou splatné pohledávky je Vodafone oprávněn zablokovat poskytování služby. Náhrada ceny služby v takovém případě Účastníku nenáleží.

6. Provoz čidel Služby

- Služby poskytované společností Vodafone na základě smlouvy obsahují kromě údržby centrální infrastruktury (webových stránek, aplikace) také údržbu software čidel (Smart Stone) a dále záruční servis čidel.
- Účastník odpovídá za zajištění čidel Služby (Smart Stone) před působením vnějších vlivů včetně neoprávněných zásahů ze strany Účastníka nebo třetích osob.
- V případě, že příčinou závady čidla je působení vnějších vlivů provozem čidla v podmínkách nesplňujících jeho technickou specifikaci nebo neoprávněným zásahem do čidla, je Vodafone oprávněn účtovat cenu opravy nebo výměny čidla za nové v ceně až do výše aktuálně platné ceníkové ceny čidla. Pokud toto Vodafone zjistí při servisním zásahu technika přímo v místě instalace, je Vodafone oprávněn účtovat neoprávněný servisní zásah ve výši až 2500,- Kč bez DPH za každý jednotlivý případ.

7. Odpovědnost Vodafone

- Vodafone neodpovídá za škody nebo poruchy vzniklé neoprávněným zásahem do čidel nebo vystavením čidel působením podmínek prostředí, které neodpovídá běžným podmínkám v kancelářských budovách.
- Účastník je povinen neprodleně, nejpozději však do 7 dnů ode dne změny, oznámit Vodafone jakékoli změny svých identifikačních, fakturačních a kontaktních údajů.

8. Bezpečnost informací a ochrana osobních údajů

1) Vodafone dodržuje všechna bezpečnostní nařízení stanovená zákony a právními předpisy platnými v České republice a v rámci Evropské unie. Vodafone přijímá a aplikuje veškerá bezpečnostní opatření, na základě aktuálních a nejmodernějších poznatků v oblasti bezpečnosti, pro



zajištění důvěrnosti osobních údajů a eliminace rizik způsobených neoprávněným přístupem, smazáním, ztrátou nebo poškozením osobních údajů/informací.

2) Jsou-li v rámci Služby zpracovávány informace, jsou uloženy a uchovány v zabezpečených systémech, k nimž mají přístup pouze oprávnění pracovníci. Systémy jsou pod neustálým dohledem pro zajištění důvěrnosti, integrity a bezpečnosti informací včetně bezpečnosti proti průniku zvenčí. Vodafone v rámci Služby zajišťuje odpovídající technické a organizační zabezpečení.

3) Pro účely aktivace služby a komunikaci s Účastníkem v rámci poskytování Služby, Vodafone zpracovává jméno, příjmení, email, kontaktní telefonní číslo Účastníka a případně i fotografii, jež si Účastník nahraje do aplikace.

4) Údaje jsou zpracovávány po dobu poskytování Služby a dále po dobu šesti měsíců po ukončení poskytování služby. Účastník má kdykoliv možnost smazat veškeré údaje volbou smazání účtu v aplikaci.

5) Poskytovatel se při své činnosti řídí platnou právní úpravou o ochraně osobních údajů a zavazuje se veškeré osobní údaje, které mu budou Účastníkem sděleny, považovat za důvěrné, používat je výlučně k plnění smlouvy, tyto nezveřejňovat a neposkytnout je třetí osobě s výjimkou případů, kdy takové poskytnutí je nezbytné ke splnění účelu smlouvy. Třetí osoby, které mohou dle rozhodnutí Účastníka užívat Službu, nejsou pro Poskytovatele subjekty údajů, jelikož nejsou z pohledu Poskytovatele identifikované či identifikovatelné.

6) Účastník prohlašuje, že je seznámen s tím, že v rámci plnění služby může být v režimu real time zpracovávána poloha koncového zařízení uživatele aplikace. Takové zpracování je možné pouze na základě aktivace ze strany uživatele koncového zařízení, na němž je nainstalována příslušná aplikace. Poloha koncového zařízení uživatele aplikace je zpracovávána v tzv. real time režimu, tj. bez uchovávání záznamu do minulosti. Účastník je povinen na tuto skutečnost upozornit třetí osoby, kterým svěří službu nebo její části k užívání, a vyžadují-li toho zvláštní právní předpisy, je povinen vyžádat si souhlas těchto osob. Třetí osoby, které mohou dle rozhodnutí Uživatele užívat Službu, nejsou pro Vodafone subjekty údajů, jelikož nejsou z pohledu Vodafone identifikované či identifikovatelné.

7) Podmínky Ochrany soukromí společnosti Vodafone naleznete na <https://www.vodafone.cz/o-vodafone/ke-stazeni/ochrana-osobnich-udaju/>.

Vodafone jako zpracovatel

I. Předmět:

1) V rámci poskytování služby či produktu může nastat situace, kdy Vodafone jako zpracovatel zpracovává osobní údaje pro zákazníka jako správce. Pro vyloučení pochybností uvádíme, že se nejedná o poskytování služeb elektronických komunikací dle zákona č. 127/2005 Sb., kdy je Vodafone vždy v pozici správce, ale o údaje, které zákazník přímo vkládá či generuje v rámci poskytované služby či produktu.

2) Následující ustanovení upravují práva a povinnosti Správce a Zpracovatele při zpracování osobních údajů (dále jen „Údaje“) poskytnutých Správcem nebo vzniklých v rámci poskytování plnění, které zajišťuje Zpracovatel pro Správce na základě zvláštní smlouvy (dále jen „Služba“), kde je Správcem osobních Údajů Správce a kde je Zpracovatel v pozici zpracovatele nebo kde je Správce v pozici zpracovatele a Zpracovatel v pozici subzpracovatele, a to vždy s ohledem na konkrétní případ (dále jen „ustanovení“).

3) Pro vyloučení pochybností platí, že tato ustanovení platí i pro futuro, a v okamžiku platnosti těchto podmínek nemusí být Služby, kde jsou osobní údaje zpracovávány, poskytována.

II. Práva a povinnosti:

1) Správce nese výhradní odpovědnost za posouzení, zda Údaje lze zpracovávat v souladu s platnou právní úpravou v oblasti ochrany osobních údajů, včetně nařízení EU 2016/679 obecné nařízení o ochraně osobních údajů (dále jen „Nařízení“) (společně jako „Aplikovatelné právo“), jakož i za ochranu práv subjektů údajů, a to zejména tak, aby Zpracovatel mohl poskytovat Služby dohodnutým způsobem, který není v rozporu s právními předpisy. Správce se zavazuje informovat Zpracovatele o jakémkoliv podezření, které může mít na poskytovanou Službu.

2) Pokud není výslovně dohodnuto jinak, činnosti ve formě podpory/součinnosti poskytované Zpracovatelem podle čl. II odst. 3, 10, 11, 13, 14 jdou na náklad Správce a hradí se zvlášť.

3) Zpracovatel je oprávněn prokázat plnění závazků z těchto ustanovení, zejména potom technických a organizačních opatření prostřednictvím následujících nástrojů, a to dle vlastního uvážení: a) schváleným etickým kodexem; b) závaznými podnikovými pravidly; c) certifikací v souladu se schváleným certifikačním postupem; d) aktuálními certifikáty, zprávami nebo výpisy ze zpráv od nezávislých instancí (např. auditorů, oddělení auditu); e) vhodnou certifikací ve formě auditu bezpečnosti IT nebo ochrany údajů; f) čestnými prohlášeními Zpracovatele.

4) Správce je oprávněn na vlastní náklady prověřovat soulad s plněním povinností podle těchto ustanovení a čl. 28 Nařízení. Správce se zavazuje oznamovat kontroly s přiměřeným předstihem, minimálně 20 pracovních dní předem, aby byla ze strany Zpracovatele zajištěna dostatečná součinnost. Správce je povinen kontroly provádět pouze v rozsahu nezbytně nutném pro ověření plnění ve vztahu ke zpracování osobních údajů pro jemu konkrétně poskytovanou Službu, a pouze pokud mu Zpracovatel nedoloží plnění závazků podle odst. 3 tohoto článku, a vždy tak, aby nenarušoval běžnou činnost Zpracovatele a aby byla vždy zachována důvěrnost. Správce nemůže mít přístup k informacím, které jsou předmětem obchodního tajemství Zpracovatele.



5) Má se za to, že Správce dal souhlas s využitím dalších zpracovatelů/subzpracovatelů. Zpracovatel informuje písemně nebo emailem Správce o veškerých zamýšlených změnách (přijetí/nahrazení), s tím, že Správce má právo vznést do 14 dnů vůči těmto změnám objektivní a odůvodněné námitky. Smluvní strany se výslovně dohodly, že v případě, že Správce bezdůvodně odmítá změnu, je Zpracovatel oprávněn ukončit poskytování Služby výpovědí bez výpovědní doby, aniž by Správci vznikal jakýkoliv nárok na finanční náhradu spojenou s takovým ukončením Služby.

6) Zpracovatel zajistí, že každá osoba, která bude mít přístup k Údajům, bude zavázána k povinnosti mlčenlivosti nebo se na ni bude vztahovat zákonná povinnost mlčenlivosti.

7) Zpracovatel se zavazuje zpracovávat Údaje výhradně v souvislosti s poskytovanou Službou a v souladu s pokyny Správce. Zpracovatel nepoužije Údaje k žádnému jinému účelu a neposkytne Údaje, které mu budou předloženy, žádným neoprávněným třetím stranám. Bez souhlasu Správce nesmí být pořizovány kopie a duplikáty - to nezahrnuje zálohování k zajištění řádného zpracování Údajů a/nebo řádnému poskytování Služby.

8) Zpracovatel se zavazuje ustanovit nezávislého, kvalifikovaného a spolehlivého Pověřence pro ochranu osobních údajů, pokud to vyžadují právní předpisy Evropské unie nebo členského státu, které se na Zpracovatele vztahují.

9) Jakékoli zpracování Údajů v tzv. třetích zemích (tj. zemích, které nejsou členskými státy Evropské unie a nedisponují patřičnou úrovní ochrany údajů) bude prováděno s řádným zřetelem k příslušným platným právním předpisům Evropské unie.

10) Zpracovatel bude v souladu s těmito ustanoveními a s přihlédnutím k charakteru zpracování a k informacím, kterými Zpracovatel disponuje – poskytovat Správci součinnost při plnění povinností Správce dle Aplikovatelného práva.

11) Pokud je Správce povinen poskytnout orgánům státní správy nebo osobám informace o zpracování Osobních údajů, Zpracovatel poskytne Správci při poskytování takových informací součinnost, pokud se tyto informace týkají zpracování údajů v souladu s těmito ustanoveními a poskytovanou Službou. Zpracovatel rovněž Správce vyrozumí – pokud to zákon připouští – o jakýchkoli sděleních dozorových orgánů (např. šetření, oznámení o opatřeních nebo požadavcích) Zpracovateli v souvislosti se zpracováním Údajů podle těchto ustanovení.

12) Zpracovatel je povinen Správce bez zbytečného odkladu informovat o jakýchkoli případech porušení zabezpečení Údajů, a to na kontakt uvedený ve smlouvě upravující poskytování Služby (administrátor systémových řešení).

13) V závislosti na druhu zpracování, Zpracovatel je Správci nápomocen, prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění Správcovy povinnosti, reagovat na žádosti o výkon práv subjektu údajů, a to v souladu s čl. 28 odst. 3 písm. e) Nařízení. V případě potřeby budou Správce a Zpracovatel koordinovat obsah a rozsah činnosti ve formě podpory poskytované Zpracovatelem podle tohoto odstavce. Pokud se subjekt údajů obrátí přímo na Zpracovatele a z podání bude možné určit, že se žádost týká Správce, Zpracovatel žádosti subjektu údajů bezodkladně postoupí Správci.

14) Pokud Správce provede posouzení dopadu na ochranu soukromí a/nebo konzultace s dozorovým orgánem k posouzení dopadu na ochranu soukromí, Správce a Zpracovatel budou koordinovat obsah a rozsah případné podpory poskytované Zpracovatelem, bude-li nutná.

15) Osobní údaje budou po ukončení poskytování Služby, vyjma osobních údajů, které musí být uchovány na základě zákonné povinnosti Zpracovatele, bez zbytečného odkladu vymazány, nebude-li výslovně dohodnuto jinak.

III. Technické a organizační zabezpečení

1) Správce a Zpracovatel jsou povinni přijmout veškerá vhodná technická a organizační opatření, aby zajistili úroveň ochrany odpovídající riziku. Opatření Zpracovatele, která jsou v současné době pokládána za adekvátní, jsou popsána v Příloze 1, kterou naleznete níže.

2) Pokud byly ve smlouvě, na základě, které jsou Služby poskytovány uzavřeny dohody ohledně technických a organizačních opatření, takové dohody mají přednost před ustanoveními tohoto článku. V opačném případě, jakékoli pokyny nebo opatření, která představují odchylku od technických a organizačních opatření, se pokládají za žádost o úpravu, jejíž náklady, pokud budou úpravy technicky realizovatelné a možné, nese Správce. Správce a Zpracovatel v takovém případě uzavřou samostatnou dohodu o rozsahu činností a výši a úhradě nákladů.

9.Reklamacie Služby a hlášení závad

1) Vodafone poskytuje na každé čidlo, které je předmětem Dílčí smlouvy záruku v délce 12 měsíců od uzavření Dílčí smlouvy.

2) Pro hlášení a řešení poruch a reklamaci Služby používá Účastník technickou podporu Vodafone OneNet.

3) Reklamacie čidla či jakéhokoli jiného zboží Účastník uplatňuje u společnosti Vodafone prostřednictvím servisního střediska na adrese:

Adresa servisního střediska: Spaceti, s.r.o., Purkyňova 2121/3, Praha 1, 110 00

4) Přičemž na uvedenou adresu musí být reklamovaný hardware či jiné zboží zasláno s označením přiděleným dříve technickou podporou.



10. Ostatní ujednání

- 1) Podrobné informace o tom, jak společnost Vodafone plní své povinnosti dle právní úpravy digitálních služeb podle nařízení EU 2022/2065 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách) (dále jen „nařízení DSA“), naleznete na webu www.vodafone.cz/digitalniodpovednost.
- 2) Smluvní strany se dohodly, že odpovědnost za újmu ze strany Poskytovatele, který jedná v souladu s nařízením DSA, je vyloučena.
- 3) Vodafone si vyhrazuje právo kdykoliv i bez uvedení důvodu omezit, ukončit nebo změnit podmínky této Služby, a to s účinností ode dne oznámení na internetových stránkách www.vodafone.cz, nebude-li výslovně uveden termín pozdější.
- 4) Tyto podmínky nabývají účinnosti dne 17. 2. 2024.

Příloha 1 - Technická a organizační opatření k zabezpečení ochrany Osobních údajů

Zpracovatel (dále v této příloze č. 2 „Vodafone“) chrání svá aktiva a informace a rozděluje je do skupin dle jejich důvěrnosti. Toto rozdělení definuje metody vytváření, ukládání, reprodukce, předávání a skartace a všichni uživatelé jsou v těchto pravidlech proškolení.

1. Bezpečnost informací

- 1) Vodafone zajišťuje, že přístup k informacím pokrytým touto smlouvou mohou mít pouze osoby, které dané informace potřebují pro výkon své práce a pro účely plnění smlouvy. Informace nebudou použité pro jiné účely než plnění smlouvy, pokud právní úprava nestanoví výslovně jinak.
- 2) Vodafone vede řízenou dokumentaci relevantních bezpečnostních opatření týkajících se zajištění ochrany osobních údajů definovaných touto smlouvou.

2. Princip oddělení povinností

Vodafone v rámci nastavených pravidel odděluje neslučitelné povinnosti a odpovědnosti mezi vlastními zaměstnanci, aby se snížila příležitost k neoprávněné nebo neúmyslné modifikaci nebo zneužití aktiv Vodafone.

3. Záznamová povinnost

Vodafone pořizuje a uchovává (min. 3 měsíce) logy událostí ve vlastních systémech a aplikacích zaznamenávající aktivity uživatelů, výjimky, selhání a další události bezpečnosti informací.

4. Technická opatření

Vodafone má v rámci své sítě implementované firewally, antiviry a systémy pro detekci a/nebo předcházení průnikům (IDS/IDP), které jsou vždy pravidelně aktualizovány, udržovány na nejlepší možné úrovni a v souladu s oborovými best-practices. Jsou přijata opatření k identifikaci neoprávněného přístupu k Osobním údajům a/nebo Informačním Systémům i ve stádiu pokusu.

5. Instalování a provozování softwaru



Vodafone používá pouze legální software a má nastaveny postupy pro interní schvalování používaného softwaru. Vodafone zajišťuje včasnou instalaci oprav a bezpečnostních záplat na systémech kde jsou zpracovávány informace pokrývané touto smlouvou s přihlednutím k závažnosti zranitelnosti – pro kritické zranitelnosti v nejbližší možné době, pro vysoce závažné do 1 měsíce, pro středně závažné do 2 měsíců, pro méně závažné do 3 měsíců.

6. Antivirová ochrana

Všechny počítače Vodafone mají nainstalovaný a provozovaný antivirový program. Antivirový program lze vypnout pouze v odůvodněných případech – výjimku musí schválit oprávněný zaměstnanec Vodafone a jsou o ní vedeny záznamy. Jakmile pomine potřeba vypnutí antivirového programu, musí být antivirový program znovu bezodkladně uveden do provozu.

7. Testování s reálnými daty

Testování Informačních Systémů při jejich implementaci a/nebo modifikaci nepoužívá reálná (živá) data, pokud to není nezbytné. Použití reálných (živých dat) je možné pouze v případě, že neexistuje žádná jiná smysluplná alternativa. V případě, že reálná (živá) data musí být použita, je toto použití omezeno na nezbytné minimum.

8. Používání internetu a elektronických komunikačních sítí

Internet ani žádná elektronická komunikační síť nepatří mezi bezpečná média. Osobní údaje nesmí být nikdy posílány prostřednictvím internetu a/nebo elektronické komunikační sítě bez patřičného zašifrování nebo jiných opatření, které zajistí, že informace nebudou čitelné a/nebo modifikovatelné třetí stranou.

9. Veřejná úložiště

Osobní údaje nesmí být za žádných okolností ukládány na veřejná úložiště, ani v zašifrované formě.

10. Malware

Veškeré soubory stažené z internetu jsou považovány za nevěrohodné a před jejich prvním užitím je ověřeno, že neobsahují viry nebo škodlivý kód.

11. Používání e-mailu

Všechny přílohy elektronické pošty jsou kontrolovány na přítomnost virů. Potenciálně nebezpečné přílohy pošty jsou blokovány na serverech Vodafone. Zaměstnanci Vodafone především nesmí:

- užívat elektronickou poštu způsobem ohrožujícím Vodafone a/nebo Správce,
- používat poštu ke komentářům mimo Vodafone bez toho, aby bylo zcela jasné, že jde o osobní názory, a ne stanovisko Vodafone a Správce.

12. Přístupová oprávnění

1) Vodafone zajišťuje, že do informačních systémů a k datům Vodafone obecně, je umožněn přístup pouze osobám, které k tomu mají



příslušné oprávnění a které potřebují přístup do systémů k takovým údajům a zdrojům, které jsou nezbytné pro plnění jejich povinností („**Oprávněný uživatel**“).

- 2) Každému Oprávněnému uživateli je vydáván osobní a jedinečný identifikátor pro tyto účely („Uživatelské ID“). Uživatelské ID je ve vybraných případech doplněno vícefaktorovou autentizací.
- 3) Vodafone vede aktuální seznam Oprávněných uživatelů a jsou vytvořeny identifikační a ověřovací postupy pro veškeré přístupy do informačních systémů nebo pro provádění zpracování Osobních údajů.
- 4) Pro každého jednotlivého Oprávněného uživatele nebo pro stejnorodou skupinu Oprávněných uživatelů jsou vytvořeny autorizační profily, které jsou před započítím jakékoliv aktivity Oprávněného uživatele nakonfigurovány takovým způsobem, aby byl umožněn přístup pouze k údajům a zdrojům, jež jsou potřebné k plnění povinností Oprávněných uživatelů.
- 5) Přístup k jakýmkoliv datům Vodafone je Oprávněným uživatelům umožněn pouze po úspěšném ověření přístupových oprávnění.
- 6) Přístupová oprávnění jsou oprávnění přidělovat, měnit nebo odebírat pouze prověřeni a pověřeni pracovníci Vodafone. Schvalování přístupových práv je vícestupňové.
- 7) Přístupy do operačních systémů a databází jsou nakonfigurovány tak, aby umožňovaly přístup pouze Oprávněných Uživatelů po autorizaci.

13. Hesla

- 1) Uživatelská hesla jsou pravidelně měněna, minimálně 1× za 3 měsíce.
- 2) Hesla splňují následující kvalitativní požadavky:
 - minimální délka hesla je osm znaků,
 - hesla musí obsahovat velká a malá písmena,
 - hesla musí obsahovat číslice,
- 3) Hesla nesmí být uchovávána v nechráněném úložišti (např. papír, běžné textové soubory, ...).
- 4) Uživatelé mají za povinnost uchovávat autentizační údaje v tajnosti, toto se týká i prvků případné vícefaktorové autentizace.
- 5) V případě nepoužití přístupových oprávnění (mimo systémové a technické účty) po dobu 6 měsíců dochází k jejich deaktivaci.

14. Logování přístupů

- 1) V auditní stopě je uchovávána historie přístupu k Osobním údajům Oprávněnými Uživateli.
- 2) Tento logovací mechanismus je pod přímou kontrolou odpovědného zaměstnance Vodafone a není možné jej deaktivovat. Minimální doba uchování logů je 1 rok.

15. Čistý stůl a prázdná obrazovka

- 1) Zaměstnanci Vodafone dodržují nastavené obecné Zásady čistého stolu a prázdné obrazovky, což znamená, že v případě nepřítomnosti pracovníka na pracovišti nesmí zůstat volně přístupné položené definované dokumenty, přenosná média a softwarově neuzamčená zařízení (počítač, tablet, mobilní telefon, ...). V případě práce s klasifikovanými informacemi na počítači (nebo na displeji přenosného zařízení) je pracovník povinen se ujistit, že nikdo neoprávněný nemůže tyto informace vidět.
- 2) Např. v prostředí MS Windows je uživatel povinen vždy při opuštění pracoviště použít minimálně funkci Uzamčení počítače/Lock computer (klávesová zkratka Win+L).

16. Zákaz sdílení přístupových oprávnění

Vodafone nastavenými opatřeními zajišťuje, aby nedocházelo k používání systémových nástrojů, které by mohly vést k překonání systémové



nebo aplikační kontroly mimo situace, kdy se jedná o schválené testování buď těchto nástrojů, nebo příslušných systémů.

17. Vzdálený přístup

1) Zaměstnanci Vodafone jsou při využití technologií vzdáleného přístupu k prostředkům pro zpracování informací povinni dodržovat tyto zásady:

- připojovat se pouze schválenými zabezpečenými technologiemi,
- připojení využívat pouze v případech odůvodněných jejich pracovním zařízením, pro zabezpečení přístupu používat kvalitní hesla.

2) Pro práci se vzdáleným přístupem platí stejná pravidla jako pro práci v kanceláři. Při odchodu od notebooku je vždy nutné jej softwarově uzamknout, nebo se odhlásit. Přenosná zařízení ani tištěné dokumenty nesmí být nechávány bez dozoru.

3) Osobní vybavení, které se používá pro připojení k síti Vodafone, splňuje požadavky Vodafone na zařízení pro vzdálený přístup.

18. Výměnná média

1) Výměnnými počítačovými médii se rozumí zejména:

- diskety,
- CD/DVD/BluRay,
- USB flash disky,
- externí disky,
- mobilní telefony, tablety,
- obecně přenosné nosiče informací.

2) Každý zaměstnanec Vodafone je oprávněn na výměnná média umísťovat informace jen v těch případech, kdy je to nezbytně nutné pro výkon jeho pracovní činnosti; za takto vytvořené médium je přímo odpovědný.

3) Datové soubory uložené na ukládacích médiích (CD, DVD, paměťové karty, USB paměti apod.) musí být před přenosem na firemní HDD nebo osobní počítač prověřeny za pomoci aktuální verze firemního antivirového softwaru.

4) USB porty na zařízeních Vodafone jsou přístupné pro zápis pouze na základě výslovného povolení, v ostatních případech jsou read-only.

19. Vynášení médií

1) Pokud to není nezbytně nutné z důvodu plnění pracovních povinností, nesmí informace Vodafone a jeho partnerů a zákazníků opustit prostory Vodafone. V případě vynášení informací mimo prostory Vodafone (i v případě např. údržby) musí být média zabezpečena proti zcizení a neoprávněnému kopírování, manipulaci či přístupu k informacím na médiu umístěnými. Zejména není povoleno ponechání média v prázdném automobilu nebo na jiném místě mimo uzamčené prostory bez dozoru. Toto pravidlo platí i pro přenosné počítače.

2) Vynášení médií obsahujících Osobní údaje mimo určené prostory musí být explicitně schváleno odpovědným zaměstnancem Vodafone.

20. Odstranění dat z médií

Pokud pomine důvod uložení informací na externím médiu, je zaměstnanec Vodafone odpovědný za jejich odstranění, které může mít podobu:

- fyzického zničení nosiče – nutno provést u nepřepisovatelných přenosných zařízení (např. skartace CD médií a disket). Pokud to je u konkrétního zařízení možné, je doporučena i jeho fyzická likvidace takovým způsobem, aby data z nosiče již nebyla dále čitelná.
- důsledného softwarového zničení zapsaných informací – vymazání dat na přepisovatelných zařízeních musí být prováděno speciálním nástrojem, který zajistí fyzické vymazání informace ze zařízení a jejich fyzické přepsání náhodnými daty – např. WIPE (min. 3× přepis náhodnými daty), prosté zformátování média se za dostatečné nepovažuje).

21. Fyzická bezpečnost



Média obsahující Osobní údaje musí být uložena v místech s omezeným přístupem pouze na osoby, které jsou k tomuto oprávněny v Bezpečnostní dokumentaci. Média musí být dostupná pouze Oprávněným uživatelům.

22.Notebooky

Informace uložené na notebookech Vodafone jsou vždy zašifrované.

23.Tisk

1) Vodafone má nastavena pravidla (s průběžnou kontrolou jejich plnění) týkající se listinných dokumentů, včetně pravidel odebírání výtisků z tiskáren ihned po jejich vytištění tak, aby bylo zamezeno možnému přístupu nepovolaných osob k vytištěným informacím. Z důvodu ochrany informací byl nastaven princip tisku SafeQ – vyzvednutí tisku a kopírování pomocí ID karty.

2) Po uplynutí použitelnosti vytištěných informací je zaměstnanec povinen provést skartaci, či jinak zabezpečit zničení výtisků.

24.Papírové dokumenty

Papírové dokumenty obsahující Osobní údaje mohou být předávány pouze v uzavřeném kontejneru a/nebo dvojité obálce a předány pouze do rukou Oprávněného uživatele.

25.Zálohování dat

Zpracovávané Osobní údaje jsou v pravidelných intervalech zálohované na zabezpečená úložiště s řízeným přístupem. Obnova dat ze záloh je pravidelně testována.

26.Noví zaměstnanci / osoby mající přístup k informacím

Noví zaměstnanci Vodafone mající přístup k Osobním údajům jsou při příchodu prověřeni s ohledem na potenciální rizika spojená s případným únikem informací. Se všemi zaměstnanci je uzavřena dohoda o mlčenlivosti. Zaměstnanci jsou po jejich příchodu bez zbytečného odkladu informováni a proškoleni o bezpečnostních opatřeních a požadavcích (vč. důsledků jejich porušení).

27.Změna pozice, pracovní náplně

V případě, že Oprávněný Uživatel přechází na jinou pracovní pozici, je nový manažer povinen ihned zrevidovat všechny přístupy do systémů a vstupy do prostor a zajistit jejich odebrání, pokud již nejsou nutné.

28.Ukončení práce

Pokud dojde k ukončení výkonu činností Oprávněného Uživatele, je manažer povinen zajistit, že všechna oprávnění (fyzické i logické přístupy) budou ihned zrušena. V závislosti na pracovní náplni se věnuje zvláštní pozornost zaměstnanci zejména v době od oznámení ukončení pracovního poměru do doby skutečného opuštění Vodafone.

29.Kontrola vstupu



1) Vstup do prostor Vodafone je zabezpečen a řízen. Jsou nastavena pravidla bránící pohybu neidentifikovaných osob. Přístup do prostor, kde dochází ke zpracování nebo kde jsou uloženy Osobní údaje, je povolen pouze Oprávněným uživatelům.

2) Vstup do prostor, kde jsou uchovávány média a Informační Systémy obsahující Osobní údaje je omezen pouze na prověřené osoby.

30. Umístění infrastruktury

Informační systémy jsou umístěny ve fyzicky zabezpečeném prostředí. Jsou přijata opatření k zamezení neautorizovaného fyzického přístupu do prostor, kde jsou Informační Systémy a data Vodafone umístěny.

31. Report incidentů

Vodafone má stanoveny, dokumentovány a v praxi dodržovány procesy pro řízení bezpečnostní událostí a incidentů (i ve stádiu pokusu a/nebo podezření). V případě, že by se bezpečnostní incident dotýkal Osobních údajů, bude o této skutečnosti Správce neprodleně informován.