

2Mobile d.o.o. – Tehnični in organizacijski ukrepi

I. Zaupnost

I./1. Nadzor fizičnega dostopa

I./1.1. Osebni podatki se shranijo in/ali obdelajo:

v prostorih 2Mobile d.o.o.

v podatkovnem centru ali strežniških prostorih 2Mobile d.o.o.

pri naslednjem ponudniku IT storitev (npr. ponudnik storitev v oblaku): SIEL d.o.o., LivePerson Netherlands B.V.

se ne uporablja

I./1.2. Objekti so zavarovani z naslednjimi ukrepi:

	Alarmni sistem	Video nadzor	Drugo (dodati opis)	Se ne uporablja
Poslovna stavba:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>
Podatkovni center ponudnika IT storitev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>

I./1.3. Dostop do prostorov je zavarovan z naslednjimi ukrepi:

	Ročno zaklepanje	Sistem pametnih kartic	Drugo (dodajte opis)*	Se ne uporablja
Pisarne:	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>
Podatkovni center ponudnika IT storitev	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>

*npr. dostopne točke za vstop, biometrični nadzor dostopa

I./1.4. Pooblaščen dostop je dokumentiran na podlagi imena osebe, ki vstopa:

da ne se ne uporablja

I./1.5. Pravila za dostop do stavbe za tretje osebe/goste/obiskovalce:

	Dokumentirano na podlagi imena	Vstop v spremstvu zaposlene osebe	Se ne uporablja
Pisarne	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Podatkovni center ponudnika IT storitev	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

I./1.6. Pravila o dostopu do stavbe osebja za čiščenje in vzdrževanje:

	Dokumentirano na podlagi imena	Vstop v spremstvu zaposlene osebe	Se ne uporablja
Pisarne	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Podatkovni center ponudnika IT storitev	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

I./1.7. Ob prenehanju pogodbe o zaposlitvi so za zaposlene vzpostavljena pravila za odvzem dovoljenja za dostop do stavbe in pravic za dostop do računalniških sistemov, vključno z njihovo dokumentacijo: da ne

I./2. Sistemski nadzor dostopa

I./2.1. Zasebno omrežje 2Mobile d.o.o. je pred javnim omrežjem zaščiteno s požarnim zidom:

da ne

če da:

	Dodajte opis
Postopek posodabljanja	Strežnik se avtomatsko posodablja za zadnjo programsko opremo.
Pogostost posodabljanja	1-krat do 2-krat na mesec

I./2.2. Preizkusi vstopa (penetration test) vseh IP naslovov, izpostavljenih spletu, se izvajajo redno:

da ne

I./2.3. Osebe mora izpolnjevati naslednje zahteve za zaščito gesel:

individualno računalniško geslo za vsakega zaposlenega, ki ga ne deli z nikomer

najmanjša dolžina gesla in z določenim številom znakov/zapletenostjo: 6 znakov, obvezno ena velika črka in poseben znak

pogostost spremembe gesla: 90 dni

samodejno zaklepanje zaslona po določenem časovnem obdobje: 3 minute

I./2.4. Protivirusna zaščita se uporablja pri naslednjih vmesnikih v omrežje 2Mobile d.o.o.

e-poštni račun FTP protokol splet

I./2.5. Protivirusna zaščita se uporablja na vseh strežnikih:

da; postopek in pogostost posodabljanja: samodejno ob nadgradnji sistema

ne; določite operacijski sistem in razlog: _____

se ne uporablja; razlog: _____

I./2.6. Protivirusna zaščita se uporablja na vseh računalnikih posameznih delovnih postaj:

da; postopek in pogostost posodabljanja: samodejno ob nadgradnji sistema

ne; določite operacijski sistem in razlog: _____

se ne uporablja; razlog: _____

I./2.7. Varnostne posodobitve programske opreme se za obstoječo programsko opremo namestijo redno in samodejno:

da ne

I./2.8. Naslednji zaposleni imajo lokalne skrbniške (administratorske) pravice na računalniku posamezne delovne postaje:

Administratorji, razvijalci, tehniki: da ne

Uporabniki: da ne

I./2.9. Zaposleni so pooblaščen za dostop do spleta:

da ne

če da: omejevalna konfiguracija brskalnika je nastavljena tako, da je zaposleni ne morejo spremeniti:

da ne se ne uporablja

I.3. Nadzor dostopa do podatkov

I./3.1. Kontrola dostopa na podlagi posameznikove vloge (role-based access) je vzpostavljena in dokumentirana:

da ne

I./3.2. Sistem dodeljevanja pravic za dostop je dokumentiran poimensko (name-specific basis); predvsem, kdo lahko dodeli katere pravice:

da ne

I./3.3. Pravice do dostopa so dodeljene po načelu najmanjšega obsega (need-to-know principle) in so posodobljene in dokumentirane poimensko:

da ne

I./3.4. Število skrbnikov, ki so pooblaščen za kopiranje/izvoz podatkovnih zbirk odjemalcev v celoti ali v velikih količinah:

1 skrbnik

se ne uporablja

I./3.5. Število zaposlenih (ne skrbnikov!), pooblaščenih za kopiranje/izvoz podatkovnih baz v celoti ali v velikih količinah:

2 zaposlena

se ne uporablja

I./3.6. Vrste datotek, v katerih se lahko izvede izvoz (npr. csv, xlsx):

csv, pdf

se ne uporablja

I./3.7. Naslednje komponente delovne postaje (računalnika) so zaklenjene/onemogočene, tako da podatkov ni mogoče izvoziti:

USB vhodi

CD/DVD zapisovalnik

reže za pomnilniške kartice

druge mobilne naprave za shranjevanje podatkov; če se uporablja, kateri: _____

noben sestavni del ni onemogočen

I./3.8. Oddaljeni dostop za vzdrževanje/oddaljeni dostop do podatkov je vzpostavljen za:

druge ponudnike

zaposlene

se ne uporablja

Če je vzpostavljen oddaljeni dostop za vzdrževanje/oddaljeni dostop do podatkov, dodajte naslednje podatke:

vrsta preverjanja pristnosti (npr. geslo, PIN, žeton): geslo

kjer je identifikacija z geslom - odstopanje od informacij, podanih v točki I/.2.3: ne, velja enako pravilo

protokoli ali uporabljeni mehanizmi (npr., SSH, VPN, RDP): RDP, VPN

dodatni varnostni ukrepi (npr., posamična odobritev seje): _____

ni vzpostavljenega oddaljenega vzdrževanja/dostopa do podatkov

I./3.9. 2Mobile d.o.o. ima sprejeta pravila za mobilno delo (npr. delo od doma), ki zagotavljajo zaupnost, celovitost, razpoložljivost in robustnost obdelave podatkov:

da ne se ne uporablja

I./3.10. Zaposleni so usposobljeni za mobilno delo, takšno usposabljanje pa je poimensko dokumentirano:

da ne se ne uporablja

I./4. Zaupnost pisne komunikacije

I./4.1. Pisna dokumentacija se naslovníkom pošilja s priporočeno pošto ali osebno preko kurirja:

da ne

I./4.2. Pisna dokumentacija se hrani v zaklenjeni, ognjevarni omari/sefu v varovanem prostoru:

da ne

I./5. Nadzor ločene obdelave podatkov (separation control)

I./5.1. Kateri ukrepi se sprejmejo za ločevanje podatkov posameznih pogodbenih partnerjev 2Mobile d.o.o.?

namenski računalnik (dedicated client), posebej za to nalogo

delitev omrežja (network separation) z naslednjimi ukrepi: _____

se ne uporablja

I./5.2. Koncept dostopa na podlagi vloge je vzpostavljen za posamezne računalnike/omrežne segmente, kar onemogoča, da zaposleni, ki ne delajo na posameznem projektu, dostopajo do podatkov:

da ne se ne uporablja

I./5.3. Zaposleni so v pisni obliki zavezani, da ne uporabljajo podatkov iz baze podatkov posameznega projekta v drugih projektih/za druge namene:

da ne se ne uporablja

II. Integriteta

II./1 Nadzor razkritja

II./1.1. Če se podatki prenašajo prek digitalnih nosilcev podatkov (npr. trdi disk, USB ključ, CD):

podatki, ki se prenašajo prek digitalnih nosilcev podatkov, so šifrirani

če da, prosim opišite postopek: _____

digitalni nosilci podatkov se ne uporabljajo

II./1.2. Vrsta šifriranja, ki se uporablja za izmenjavo podatkov, če se podatki prenašajo elektronsko:

SFTP

S/MIME

HTTPS

SSL-VPN ali Citrix: _____ (dodaten opis)

drugo: Dropbox in Google Drive

podatki se ne prenašajo elektronsko

II./1.3. Ali so osebni podatki shranjeni pri 2Mobile d.o.o.?

da, nešifrirano da, šifrirano Ne

Če so podatki shranjeni v šifrirani obliki, opišite postopek: _____

II./1.4. Kako so podatki, ki so vključeni v varnostne kopije, zaščiteni (npr. varna hramba medija z varnostno kopijo, šifriranje varnostnih kopij)?

podatki Upravljavca so zaščiteni na naslednji način: varnostne kopije se izvajajo 1-krat dnevno.

Hranjene so na ločeni lokaciji, varovane v varnostnem sefu, z geslom

podatki Upravljavca niso varnostno kopirani

II./1.5. Brisanje podatkov Upravljavca:

Kako so podatki izbrisani (npr. v skladu s katerimi standardi/praksami)?

elektronski podatki v sistemih: Microsoft SQL Server, Dropbox in Google Drive

elektronski nosilci podatkov: _____

papirnati dokumenti: _____

se ne uporablja

II./1.6. Kdaj so podatki izbrisani oz. kdaj so nosilci podatkov odstranjeni?

skladno z določenimi roki hrambe

se ne uporablja

II./1.7. Kako je izbris podatkov oz. odstranitev nosilcev podatkov zabeležena?

izbris se zapiše v LOG

se ne uporablja

II./1.8. Ukrepi za zaščito podatkov Upravljavca (vključno z začasnimi) na mobilnih napravah:

vse naprave so zaščitene z gesli

ni ukrepov

se ne uporablja

II./1.9. Pametni telefoni, tablični računalniki itd. (npr. upravljanje mobilnih naprav, šifriranje; prosim navedite podatke o šifriranju, kjer je to potrebno):

vse naprave zaščitene z gesli

ni ukrepov

se ne uporablja

II./2. Nadzor vnosa

II./2.1. Za sledenje izbrisu ali spreminjanju podatkov Upravljavca se poimensko ustvarijo datoteke dnevnikov za vsakega zaposlenega:

da ne se ne uporablja

II./2.2. Za zgoraj navedene datoteke dnevnikov je vzpostavljen koncept omejevalnega dostopa:

da ne se ne uporablja

III. Dostopnost in odpornost

III./1. Nadzor dostopnosti

III./1.1. Podrobnosti varnostnih kopij podatkov:

pogostost (interval) izdelave varnostnih kopij: vsak dan

število ohranjenih generacij varnostnih kopij: vsakič za en dan nazaj

se ne uporablja

III./1.2. Lokacija shranjevanja varnostnih kopij:

varno

zunanje skladiščenje ≥ 5 km stran

se ne uporablja

III./1.3. Čas ponovnega zagona po popolnem uničenju podatkovnega centra v dneh:

- odvisno od ponudnika storitve v oblaku (SIEL)
se ne uporablja

III./1.4. Vzpostavljene so Pogodbe za vzdrževanje IT sistemov s strani tretjih oseb:

- da, samo v EU
da, dostop do podatkov iz tretjih držav je mogoč
ne

IV. Postopek rednega pregleda, ocenjevanja in vrednotenja

IV./1. Nadzor dela

IV./1.1. Ali so zaposleni v pisni obliki zavezani varovati zaupne podatke?

- da ne se ne uporablja

IV./1.2. Ali so v pogodbeno obdelavo vključeni podobdelovalci?

- da ne se ne uporablja

IV./1.3. Ali je s podobdelovalci sklenjena ustrezna pogodba oz. veljajo splošni pogoji?

- da ne se ne uporablja

IV./1.4. Ali obstajajo podobdelovalci zunaj EU?

- da ne se ne uporablja

IV./1.5. Ali podobdelovalci, ki imajo dostop do osebnih podatkov, zagotavljajo skladnost obdelave osebnih podatkov z veljavnimi predpisi s področja varstva osebnih podatkov?

- da ne se ne uporablja

IV./1.6. Zaposleni se usposabljujejo glede varstva osebnih podatkov, tovrstno usposabljanje pa je dokumentirano poimensko:

- da ne

IV./1.7. Za 2Mobile d.o.o. trenutno veljajo naslednji certifikati/koncepti varovanja zaupnosti podatkov (prosim, navedite naslov in datum):

- se ne uporablja

IV./2 Razno

IV./2.1. Pri 2Mobile d.o.o. se uporablja naslednji postopek za redno pregledovanje, ocene in vrednotenje učinkovitosti tehničnih in organizacijskih ukrepov:

ISMS, v skladu z naslednjim standardom (npr. ISO 27001/2): _____

alternativni postopek (navedite):

se ne uporablja (navedite razlog): Obdelovalec sam redno spremlja učinkovitost svojih tehničnih in organizacijskih ukrepov

IV./2.2. Pri zagotavljanju storitev ali razvoja programske opreme (npr. programska oprema kot storitev), veljajo pri 2Mobile d.o.o. pravila:

o »vgrajenem in privzetem varstvu podatkov«, da se pri razvijanju in oblikovanju izdelkov, storitev in aplikacij upošteva pravica do zasebnosti (npr. z ukrepi kot je psevdonimizacija):

o uporabi osebnih podatkov pri razvoju programske opreme:
podatkovne baze in anonimiziramo osebne podatke.

Pri nadgradnji sistema naredimo kopijo

se ne uporablja

IV./2.3. Ali je zagotovljeno obveščanje v primeru varnostnega incidenta?

da ne