TEHNIČNI IN ORGANIZACIJSKI UKREPI ZA ZAGOTAVLJANJE VARNOSTI OSEBNIH PODATKOV

2Mobile d.o.o. izvaja naslednje tehnične in organizacijske ukrepe za zagotovitev ustrezne ravni varnosti osebnih podatkov, ob upoštevanju narave, obsega, okoliščin in namena obdelave ter tveganj za pravice in svoboščine posameznikov:

I. Ukrepi, ki zagotavljajo »zaupnost« osebnih podatkov

I./1. Nadzor dostopa do prostorov

Namen nadzora dostopa do prostorov je preprečiti, da bi nepooblaščene osebe pridobile dostop do prostorov, v katerih se obdelujejo osebni podatki. Nadzor dostopa do prostorov se izvaja zlasti z naslednjimi ukrepi:

1. Nadzorovan dostop do poslovnih prostorov:
- Vsak obiskovalec mora najaviti svoj prihod in lahko v poslovne prostore vstopi samo v spremstvu zaposlenega.
2. Video nadzor poslovne stavbe:
- V poslovni stavbi se izvaja video nadzor.
- Z video nadzorom upravlja upravnik poslovne stavbe.
3. Upravljanje kartic in ključev:
- Vsak zaposleni ima svoj vstopni žeton za vstop v poslovno stavbo in del poslovne stavbe, v katerem se nahaja poslovni prostor podjetja. Poslovni prostor je zaklenjen s ključem, ki ga ima vsak zaposleni.
- Omare so zaklenjene, z omejenim dostopom do ključev samo za določene zaposlene.
- Če osebi preneha zaposlitev vstopno kartico in ključ vrne.

I./2. Nadzor dostopa do računalniških sistemov

Namen nadzora dostopa do računalniških sistemov je v preprečevanju uporabe računalniških sistemov za obdelavo osebnih podatkov s strani nepooblaščenih oseb. Nadzor dostopa do računalniških sistemov se izvaja zlasti z naslednjimi ukrepi:

1. Požarni zid in sistem zaznavanja vdorov
   Na delovnih postajah z operacijskim sistemom Windows se uporablja Windows Defender Firewall.
   Na delovnih postajah z operacijskim sistemom macOS se uporablja vgrajeni macOS Firewall.
   Požarni zid je privzeto vklopljen in konfiguriran za preprečevanje nepooblaščenih povezav.
2. Protivirusna in zaščitna programska oprema
   Na delovnih postajah z operacijskim sistemom Windows je nameščena in aktivna zaščita Windows Defender.

Na delovnih postajah z operacijskim sistemom macOS so aktivni vgrajeni varnostni mehanizmi Apple:

- XProtect, ki samodejno in tiho preverja aplikacije in datoteke glede znanih zlonamernih kod.
- Malware Removal Tool (MRT), ki samodejno odstranjuje zaznane grožnje.
- Gatekeeper, ki preprečuje zaganjanje aplikacij neznanih razvijalcev in preverja celovitost prenesenih aplikacij.
- Apple Notarization, ki preverja aplikacije glede zlonamerne vsebine in omogoča hitro blokado zaznanih groženj.

3. Posodabljanje sistema in varnostnih komponent
   Samodejno posodabljanje operacijskega sistema, varnostnih mehanizmov, protivirusnih definicij in brskalnikov je privzeto omogočeno.
   Na sistemih Windows posodobitve upravlja Windows Update.
   Na sistemih macOS se varnostne definicije XProtect, MRT in notarizacijski preklicni seznami posodabljajo samodejno in neodvisno od sistemskih posodobitev.
4. Vsak zaposleni ima svojo delovno postajo, ki je zavarovana z geslom. Vsak zaposleni ima svoje geslo za posamezne sisteme in aplikacije.
5. Zaposleni so dolžni zaklepati delovne postaje, ko niso v uporabi.
6. Geslo za ohranjevalnik zaslona deluje tako, da je zagotovljeno samodejno zaklepanje po 3 minutah, če zaposleni ne zaklene delovne postaje.
7. Za vsa orodja, ki jih uporabljamo za svoje poslovanje, je zagotovljena varna prijava z edinstvenim uporabniškim imenom, geslom in drugim faktorjem za preverjanje pristnosti (OTP, MFA, 2FA).
8. Minimalne zahteve za gesla in upravljanje gesel:

- Gesla morajo imeti več kot 8 znakov in vsebovati vse od sledečega: velike in male črke, številke in posebni znaki.
- Gesla se morajo zamenjati vsaj enkrat na 3 mesece.
- Posojanje gesel in uporaba skupinskih gesel je prepovedana.

9. V primeru suma varnostnih groženj administrator pošlje zahtevo vsem zaposlenim, da za določeno orodje takoj zamenjajo geslo.
10. Spremljanje varnostnih pomanjkljivosti kritičnih sistemov: Administrator je odgovoren za spremljanje statusa strani ponudnikov orodij v oblaku. Če so ugotovljene varnostne pomanjkljivosti, ukrepamo glede na navodila ponudnika orodja (npr. administrator pošlje zahtevo za menjavo gesla vsem uporabnikom določenega orodja).
11. V primeru prenehanja zaposlitve se osebi ukine dostop do vseh sistemov.

I.3. Nadzor dostopa do podatkov

Nadzor dostopa do podatkov vključuje ukrepe za zagotavljanje, da lahko uporabniki sistemov za obdelavo podatkov dostopajo do podatkov na podlagi dodeljene pravice dostopa in da se podatki med obdelavo, uporabo in hrambo nepooblaščeno ne berejo, kopirajo, spreminjajo ali odstranjujejo. Nadzor dostopa do podatkov se izvaja zlasti z naslednjimi ukrepi:

1. Dostop do sistemov z osebnimi podatki temelji na uporabniških računih. Zaposleni morajo pridobiti dovoljenje za dostop in imajo dodeljen točno določen segment sistema, do katerega lahko dostopajo. Vsi dostopi so omogočeni le z uporabniškim imenom, geslom in MFA.
2. Zaposleni imajo dostop samo do tistih podatkov, ki jih nujno potrebujejo za opravljanje svojih delovnih nalog in v skladu z načelom potrebe po seznanitvi. Splošne pravice dostopa veljajo samo za administratorja in direktorja.
3. Nosilce podatkov (npr. odpisane računalnike) pred odpisom popolno izbrišemo.

I./4. Nadzor ločene obdelave podatkov (separation control)

Nadzor nad ločevanjem vključuje ukrepe za zagotavljanje, da se podatki, zbrani za različne namene, obdelujejo ločeno. Nadzor ločene obdelave podatkov se izvaja zlasti z naslednjimi ukrepi:

1. Z ločitvijo razvojnega, testnega in produkcijskega okolja na zahtevo stranke.
2. Orodja v oblaku omogočajo logično ločitev strank.

II. Ukrepi, ki zagotavljajo »celovitost« osebnih podatkov

II./1. Nadzor prenosa

Nadzor prenosa vključuje ukrepe za zagotavljanje, da osebnih podatkov med elektronskim prenosom ali shranjevanjem ni mogoče nepooblaščeno brati, kopirati, spreminjati ali brisati. Nadzor prenosa se zagotavlja zlasti z naslednjimi ukrepi:

1. Zaščita dokumentov z geslom
2. VPN tuneli v primeru povezave na oddaljeno okolje partnerjev
3. Požarni zid in protivirusna zaščita kot je opisano pod točko I./2.

II./2. Nadzor vnosa

Nadzor vnosa vključuje ukrepe za zagotavljanje, da je mogoče za nazaj preveriti in ugotoviti, ali so bili osebni podatki vneseni v sisteme za obdelavo podatkov, spremenjeni ali odstranjeni (nadzor vnosa) ter kdo je to storil. Nadzor vnosa se zagotavlja zlasti z naslednjimi ukrepi:

1. Zagotavljamo osnovno sledljivost obdelave osebnih podatkov (vnos, brisanje, spremembe) preko orodja »Windows Activity History«, preko orodja »Windows App History«, preko preverjanja zgodovine brskanja v brskalnikih, preko orodja »Event Viewer«, preko Azure Admin Portala in pregleda uporabe e-pošte oz. dostopov do e-poštnega predala zaposlenih (samo administrator).
2. Zaposleni imajo dostop samo do tistih podatkov, ki jih nujno potrebujejo za opravljanje svojih delovnih nalog in v skladu z načelom potrebe po seznanitvi.

3. Dostop do sistemov z osebnimi podatki temelji na uporabniških računih.

III. Ukrepi, ki zagotavljajo »razpoložljivost« osebnih podatkov

Nadzor razpoložljivosti vključuje ukrepe, ki zagotavljajo, da so osebni podatki zaščiteni pred nenamernim uničenjem ali izgubo. Nadzor razpoložljivosti se izvaja zlasti z naslednjimi ukrepi:

1. Vsi dokumenti so shranjeni v oblaku v orodjih, ki jih dnevno uporabljamo za svoje delo. Ponudniki orodij v oblaku zagotavljajo varnostno shranjevanje podatkov. Dostop do orodij v oblaku je omogočen na podlagi uporabniških računov, ki zagotavljajo MFA, OTP in 2FA.
2. V poslovni stavbi je vgrajen sistem za zaznavanje dima in ognja, ki se redno testira.
3. Požarni zid in protivirusna zaščita kot je opisano pod točko I./2.
4. V primeru varnostnih groženj oziroma varnostnih kršitev administrator vsem zaposlenim pošlje obvestilo o grožnji preko skupnih pogovornih kanalov in lahko zahteva ponastavitev gesel vseh zaposlenih.

IV. Organizacijski ukrepi

IV./1. Zaposleni in drugi sodelavci

1. Postopki zaposlovanja so zastavljeni tako, da je zagotovljena skrbna izbira zaposlenih (npr. pošiljanje podrobnega življenjepisa in razgovor za službo z dodatnimi vprašanji).
2. Zaposleni, ki obdelujejo osebne podatke, ali imajo do njih dostop, so se pisno obvezali, da v zvezi z obdelavo osebnih podatkov ohranijo zaupnost.
3. Zaposleni znajo prepoznati socialni inženiring.
4. Zaposleni se držijo politike gesel.
5. Zaposleni se držijo politike čistega zaslona in čiste mize.
6. Zaposleni se usposabljajo za ozaveščanje o varnosti in zasebnosti:

- Vsak novo zaposleni mora v 7 dneh od zaposlitve rešiti spletni seminar "Varni v Pisani" dostopen na naslednji povezavi: https://www.varnivpisarni.si/, certifikat mora shraniti na svojo napravo.
- Preko orodja Wizer (https://www.wizer-training.com/) vsi zaposleni enkrat letno prejmejo poziv k rešitvi "Security Annual Training", ki zajame vse aktualne trende v zvezi z varnostjo podjetij. Administrator lahko preverja ali so vsi zaposleni zaključili s treningom, zaposleni prejmejo tudi e-maile z opozorilom, da morajo zaključiti ta trening.

7. Zaposleni so seznanjeni z navodili upravljavca in zavezani, da ravnajo skladno s njimi, kar se tudi redno preverja. Upravljavci imajo po pogodbi pravico do izvajanja pregledov in revizij
8. Vzpostavljene imamo procese za skrbno izbiro ponudnikov storitev in spremljanje izpolnjevanja pogodb. S podobdelovalci imamo sklenjene ustrezne pogodbe za

obdelavo podatkov, ki vključujejo ustrezne tehnične in organizacijske varnostne ukrepe ter pravico do izvajanja pregledov in revizij.

IV./2 Revizija tehničnih in organizacijskih ukrepov

1. Najmanj 1-krat letno interno ocenjujemo učinkovitost tehničnih in organizacijskih ukrepov. Ob ugotovljenih pomanjkljivostih uvedemo nove ukrepe oziroma prilagodimo obstoječe.
2. Pri razvoju programske opreme je vzpostavljeno načelo o »vgrajenem in privzetem varstvu podatkov«, tako da se pri razvijanju in oblikovanju izdelkov, storitev in aplikacij upošteva pravica do zasebnosti.

IV./3. Ukrepi v primeru kršitve varstva osebnih podatkov

1. V primeru seznanitve s kršitvijo varstva osebnih podatkov, bomo upravljavca pisno obvestili brez nepotrebnega odlašanja, najkasneje pa v 24-ih urah potem, ko se bomo seznanili s kršitvijo. Pisno obvestilo bo vsebovalo:

- naravo kršitve varnosti osebnih podatkov, po možnosti tudi kategorije in približno število posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število evidenc osebnih podatkov;
- verjetne posledice kršitve varnosti osebnih podatkov;
- ukrepe, ki naj jih upravljavec sprejme ali katerih sprejetje upravljavcu predlagamo za obravnavanje kršitve varnosti osebnih podatkov, pa tudi, kadar je smiselno, ukrepe za ublažitev morebitnih škodljivih učinkov kršitve.

2. Obvestilo bo poslano po elektronski pošti na naslov pooblaščene osebe za varstvo osebnih podatkov pri upravljavcu ali druge kontaktne osebe, če upravljavec nima imenovane pooblaščene osebe za varstvo osebnih podatkov.

Ljubljana, 27.01.2026

2Mobile d.o.o.

Matjaž Možina, direktor