PRILOGA 3 – INFORMACIJA O POSTOPKIH IN UKREPIH ZA INFORMACIJSKO IN ORGANIZACIJSKO VAROVANJE OBDELAVE PODATKOV, VKLJUČNO Z OSEBNIMI PODATKI

(1) Pošta je skladno z evropskimi in nacionalnimi predpisi s poštnega prometa, z Uredbo GDPR in drugimi nacionalnimi pravnimi predpisi, standardi in dobrimi praksami, ki urejajo prenos pošiljk, varnost in varstvo podatkov, vključno z osebnimi podatki, pri ročni in avtomatizirani obdelavi s pomočjo informacijskega sistema sprejela potrebne postopke in ukrepe. Pravne podlage in standardi, ki zavezujejo Pošto, so opredeljeni na spletni strani Pošte https://www.posta.si/zakoni-in-splosni-pogoji, https://www.posta.si/o-nas/predstavitev/pravno-obvestilo in https://www.posta.si/o-nas/predstavitev/trajnostni-razvoj/standardi-kakovosti.

(2) Pošta ima vzpostavljene varnostne postopke in ukrepe za varovanje in obdelovanje osebnih podatkov pri ročni obdelavi, pri strojni in programski opremi, kot je opisano v nadaljevanju:

a) Fizično varovanje

Ukrepi fizičnega varovanja so vzpostavljeni glede na oceno tveganja in varnostne načrte za posamezne objekte in območja, s katerimi upravlja Pošta. Pošta redno spremlja varnostno situacijo, korigira oceno tveganja in ustrezno prilagaja obseg nadzora in kontrol.

Pošta je vzpostavila nadzorni center, kjer se centralizirano upravlja s fizičnim varovanjem in nadzorom nad objekti prek video-nadzornega sistema, izvaja se tudi nadzor (sledenje) vozil, ki prevažajo poštne pošiljke. Zaposleni prijavljajo vse izredne dogodke neposredno v nadzorni center, ki ukrepa v skladu z določenimi protokoli.

Vstopanje v objekte in gibanje znotraj varovanih območij in ravnanje ob izrednih dogodkih je urejeno z navodilom za vstopanje v poštne objekte in ravnanje ob izrednih dogodkih.

Objekti in območja so zavarovani s tehničnimi sredstvi (video-nadzorni sistem, alarmni sistemi, kontrola pristopa), poslovne enote, oba logistična centra in sedež družbe pa imajo tudi receptorsko službo, ki preveri, ali imajo osebe, ki vstopajo, dovoljenje za vstop. Vsi vstopi v objekte se evidentirajo bodisi s pomočjo evidence delovnega časa za zaposlene bodisi z evidenco vstopov za vse ostale osebe, ki vstopajo.

Vsaka oseba, ki ni zaposlena v družbi, je dolžna pred vstopom v prostore družbe pridobiti dovoljenje za vstop, ki ga izdaja Pošta na podlagi vloge. Dovoljenja se izdajajo glede na veljavnost pogodbe (čas trajanja, objekti, območja).

Vstop v sistemske prostore, kjer je nameščena vsa ključna informacijsko-komunikacijska infrastruktura, je urejen s splošnim internim aktom »Informacijska varnostna politika »Vstop v varni sistemski prostor«. Proces izdaje dovoljenj in postopek vstopa imata vgrajene kontrole, ki preprečujejo, da bi v varne sistemske prostore vstopila nepooblaščena oseba, o vstopih se vodi poimenska evidenca. Vsi prostori podatkovnih centrov so pod videonadzorom in so dodatno varovani tudi s kontrolo pristopa in sistemom tehničnega varovanja.

b) Tehnični ukrepi pri varovanju informacijskega sistema

Protivirusna programska oprema je nameščena na vseh uporabniških računalnikih in se redno (samodejno) posodablja. Rešitev je centralizirana.

Sistem elektronske pošte je varovan s tehničnimi sredstvi, ki preverjajo vsa sporočila z namenom zaznavanja škodljive programske opreme, povezav na spletne strani, ki vsebujejo škodljivo programsko opremo, ter sistemom za odstranjevanje neželene pošte (t. i. spam).

Notranje omrežje družbe je pred javnim omrežjem zavarovano s sistemom tehničnih zaščit, ki obsega: požarno pregrado, IDS/IPS-sistem in posredovalni strežnik s filtriranjem.

Dogodki se iz sistemskih dnevnikov zbirajo centralno v SIEM, kjer so na voljo za nadaljnjo analizo in aktivno spremljanje delovanja sistemov.

Vzpostavljeni so sistemi samodejnega alarmiranja in obveščanja pristojnih (dežurstvo) v primeru izrednih dogodkov.

c) Pravila uporabe informacijskega sistema

Za dostop do podatkov, ki se hranijo v elektronski obliki, so se uporabniki dolžni avtorizirati (prijava z uporabniškim imenom in geslom). Uporabniška imena so vezana na točno določeno osebo. Politika gesel je določena in prek nastavitev sistema tudi vsiljena (Informacijska varnostna politika "Uporaba informacijskega sistema Pošte Slovenije d. o. o."). Družba dodeljuje pravice dostopa do informacijskih storitev (virov) v skladu s procesom opredeljenim s splošnim internim aktom, ki vključuje ustrezne kontrole, s katerimi se prepreči, da bi dostop do podatkov pridobile osebe, ki za to niso pooblaščene. Proces je informacijsko podprt. Pooblastila se posameznikom dodeljujejo na podlagi njihovih delovnih zadolžitev in dostop do osebnih podatkov dobijo le tiste osebe (njegovi zaposleni in druge osebe, ki bodo pod njegovim vodstvom obdelovale osebne podatke), za katere je to zaradi njihove funkcije oziroma delovnih zadolžitev nujno potrebno.

Zaposleni so dolžni spoštovati pravilo čiste mize in čistega zaslona ter v svoji odsotnosti ustrezno poskrbeti za zavarovanje delovne postaje (zaklepanje).

d) Dostopi in posredovanje podatkov

Do podatkov, ki so predmet obdelave za potrebe opravljanja poštnih storitev, imajo dostop izključno zaposleni, ki izvajajo procese, ki so potrebni za izvedbo poštne storitve. Obseg dostopa je omejen na minimalni nabor, da lahko nemoteno izvajajo aktivnosti, potrebne za izvedbo storitve.

Pošta posreduje podatke pogodbenim sodelavcem, s katerimi sodeluje, da izvedejo dostavo, pri tem je obseg podatkov omejen izključno na dostavne podatke za pošiljke, ki jih pogodbeni sodelavec dostavlja.

Podatki se ne izvažajo v druge oblike in se po zakonsko določenih rokih (Zakon o poštnih storitvah) izbrišejo ali anonimizirajo, razen v primerih, ko so predmet posebnih postopkov, kjer obstaja zakoniti interes ali zakonska podlaga (npr. podatki služijo kot dokazno gradivo). Podatki se pri prenosih prek javnega telekomunikacijskega omrežja kriptirajo.

e) Zavarovanje podatkov pred izgubo

Podatki, ki so shranjeni v elektronski obliki, so fizično locirani v varnih podatkovnih centrih Pošte. Podatkovni centri imajo visok nivo protipožarne zaščite, neodvisne vire napajanja z energijo (UPS in generatorje) ter primerno zmogljive sisteme za hlajenje. Primarna lokacija je certificirana po standardu TIER III za neprekinjeno poslovanje, procesi pa so vzpostavljeni v skladu z dobrimi praksami, ki sledijo standardu ISO 27001. Podatki se redno arhivirajo ter hranijo na dveh ali celo več lokacijah.

(3) Uporabnik in Pošta lahko opredelitve glede varovanja podatkov podrobneje določita tudi v pogodbi, ki jo skleneta po pogojih iz teh ali drugih obvestil, ki jih je objavila Pošta z namenom informiranja uporabnikov skladno z obveznostmi, ki jih določa zakonodaja.