Asmens duomenų teikimo sutarties su ūkio subjektu, sudariusiu sutartį dėl medicinos priemonių įsigijimo išlaidų apmokėjimo Privalomojo sveikatos draudimo fondo biudžeto lėšomis, Nr. 2 priedas

ORGANIZACINIŲ IR TECHNINIŲ PRIEMONIŲ SĄRAŠAS

Siekdamas apsaugoti duomenų subjektų asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, nuo bet kokio kito neteisėto tvarkymo ir vadovaudamasis Asmens duomenų teikimo sutartimi su ūkio subjektu, sudariusiu sutartį dėl medicinos priemonių įsigijimo išlaidų apmokėjimo Privalomojo sveikatos draudimo fondo biudžeto lėšomis (toliau – Sutartis), ūkio subjektas taiko toliau išdėstytas organizacines ir technines duomenų saugumo priemones:

1. Užtikrinama prieigos prie asmens duomenų apsauga, valdymas ir kontrolė. Prieiga prie asmens duomenų suteikiama tik tam darbuotojui, kuriam asmens duomenys yra reikalingi jo darbo funkcijoms vykdyti. Darbo santykiams pasibaigus, prieiga buvusiam darbuotojui panaikinama.
2. Su asmens duomenimis galima atlikti tik tuos veiksmus, kuriems atlikti darbuotojui yra suteiktos teisės.
3. Užtikrinama asmens duomenų apsauga nuo neteisėto prisijungimo prie vidinio kompiuterių tinklo elektroninių ryšių priemonėmis. Vidinis tinklas yra apsaugotas ugniasienėmis.
4. Užtikrinama, kad visi su asmens duomenų tvarkymu susiję darbuotojai būtų įsipareigoję neatskleisti asmens duomenų. Šiam tikslui pasiekti darbuotojai pasirašo įsipareigojimus dėl asmens duomenų tvarkymo.
5. Kiekvienam darbuotojui, kuriam suteikta prieiga prie asmens duomenų, tvarkomų automatiniu būdu, suteikiamas unikalus prisijungimo vardas ir vienkartinis slaptažodis, kurį pirmojo prisijungimo metu privalu pakeisti nuolatiniu slaptažodžiu. Nuolatinis slaptažodis negali būti trumpesnis nei 8 simbolių ir negali būti sudaromas naudojant asmeninio pobūdžio informaciją. Slaptažodis keičiamas ne rečiau kaip kartą per 3 mėnesius. Tas pats slaptažodis negali būti kartojamas kelis kartus. Darbuotojas yra atsakingas už slaptažodžio konfidencialumą ir įsipareigoja neatskleisti jo tretiesiems asmenims.
6. Sutarties šalių patalpos rakinamos. Į Sutarties šalių patalpas, kuriose tvarkomi asmens duomenys, patenka tik įgaliotieji asmenys. Įgaliotieji asmenys, kurie nėra Sutarties šalių darbuotojai, ir klientai į nurodytas patalpas patenka tik kartu su įgaliotaisiais Sutarties šalių darbuotojais.
7. Naudojamos tik tinkamai licencijuotos (teisėtos) kompiuterių programos. Nuolat atliekama kompiuterinėse darbo vietose naudojamų kompiuterių programų kontrolė.
8. Užtikrinamas tinkamas techninės įrangos saugojimas ir priežiūra, informacinių sistemų priežiūra, tinklo valdymas, naudojimosi internetu saugumas, kompiuterinės įrangos apsauga nuo kenksmingos programinės įrangos (diegiamos ir atnaujinamos antivirusinės programos).
9. Darbuotojų kompiuteriuose tvarkoma informacija, susijusi su asmens duomenimis, yra nepertekline, būtina tik kasdienėms darbo funkcijoms atlikti. Informacija, kuri nebėra aktuali ir reikalinga darbo funkcijoms atlikti, periodiškai ištrinama.

10. Jei darbuotojas abejoja įdiegtų saugumo priemonių patikimumu, jis privalo kreiptis į tiesioginį vadovą, kad būtų įvertintos turimos saugumo priemonės ir, jei reikia, įsigytos ir įdiegtos papildomos priemonės.

11. Įvykus gedimui, asmens duomenys, esantys serveryje, atkuriami iš atsarginių kopijų. Duomenų serverio atsarginės kopijos daromos kartą per 24 valandas.

12. Visuose serveriuose įdiegta antivirusinė programa ir įrengta ugniasienė. Duomenų bazės apsaugotos vartotojų slaptažodžiais (toliau – IP). Prisijungti galima tik pagal nurodytus vartotojų IP adresus.

13. Asmens duomenų saugumo pažeidimų valdymo tvarkos apraše detaliai reglamentuota asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarka.

14. Įvykus duomenų saugumo incidentui, apie incidentą ir saugumo priemones, kurių imtasi siekiant apsaugoti asmens duomenis, nedelsiant informuojami atsakingi asmenys ir kita Sutarties šalis.

Ūkio subjektas	VLK
_____	_____
(Parašas)	(Parašas)
A.V.	A.V.
202_ m. _____ d.	202_ m. _____ d.