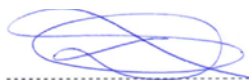


## DUOMENŲ APSAUGOS POLITIKA

<b>Tikslas:</b>	Ši politika apibrėžia „Affidea“ pasiryžimą laikytis Duomenų apsaugos įstatymų. Kiekvienas asmens duomenis tvarkantis „Affidea“ darbuotojas privalo aiškiai žinoti, kad Duomenų subjektai viso labo skolina mums asmens duomenis pasitikėjimo pagrindu ir kad mums tie duomenys nepriklauso. Duomenų subjektai yra pacientai, darbuotojai ir tiekėjai arba partneriai.
-----------------	---

Autorius (SME):



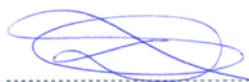
Daiva Adomaitienė

Duomenų apsaugos pareigūnė

Data:

2020-07-09

Proceso savininkas:



Daiva Adomaitienė

Duomenų apsaugos pareigūnė

Data:

2020-07-09

Patvirtina:



Vitalijus Orlovas

Direktorius

Data:

2020-07-09

Galioja nuo:

2020 m. liepos 10 d.

## 1. Apimtis

Ši politika galioja:

- Visiems darbuotojams, besikreipiantiems dėl darbo ir dirbantiems pagal kitas negu darbo ar partnerystės sutartis (mūsų vardu paslaugas teikiančių įstaigų darbuotojams); ir
- Visų BDAR apibrėžtų asmens duomenų tvarkymui. Ši sąlyga apima ir ne ES tvarkomus duomenis, kad „Affidea“ įstaigos galėtų perdavinėti duomenis viena kitai.

Šis dokumentas turėtų būti skaitomas kartu su kitomis susijusiomis „Affidea“ grupės politikomis ir tvarkomis. Šios politikos nesutapimų su kitais tvarkos dokumentais atvejais galioja tas dokumentas, kuriuo numatyti griežtesni reikalavimai.

Ši politika galioja visai UAB „Affidea Lietuva“ įmonių grupei, t.y. visiems šių grupę sudarantiems juridiniams asmenims ir jų visiems darbuotojams. UAB „Affidea Lietuva“ įmonių grupę sudaro: UAB „Affidea Lietuva“, kodas 300542299; UAB „Medicinos paslaugų grupė“, kodas 304148323; UAB „Alytaus Medea klinika“, kodas 300566791; UAB „Šilutės MCT“, kodas 300150444; UAB „MCT kompiuterinė tomografija“, kodas 302032665; UAB „Endemik“, kodas 220509380; UAB „Endemik didmena“, kodas 302244593, UAB „Kuncų ambulatorinė klinika“, kodas 141292840.

## 2. Terminai

<b>BDAR</b>	Bendrasis asmens duomenų apsaugos reglamentas (2016/679) įsigalioja 2018 m. gegužės 25 d. Jis tiesiogiai taikomas nacionaliniu lygiu ir skirtas visų ES narių duomenų apsaugos įstatymams suderinti. Juo pakeičiama šiuo metu galiojanti 1995 m. Duomenų apsaugos direktyva (Direktyva 95/46/EB). BDAR taikomas ES įsteigtiems Duomenų valdytojams ir Duomenų tvarkytojams ir bus taikomas prekes ar paslaugas ES siūlantiesiems ar ES asmenų elgseną stebintiems Duomenų valdytojams ar tvarkytojams.
<b>„Affidea“</b>	Apima visus „Affidea“ grupės juridinius asmenis.
<b>„Affidea“ grupė</b>	Tiesiogiai ar netiesiogiai „Affidea Group BV“ valdomų įstaigų grupė.
<b>Duomenų valdytojas</b>	Duomenų valdytojas yra fizinis ar juridinis asmuo, viešoji įstaiga, agentūra ar kita institucija, viena pati ar su kitomis institucijomis nustatanti asmens duomenų tvarkymo tikslus ir priemones; tuo atveju, jei duomenų tvarkymo tikslai ir priemonės nustatyti Sąjungos ar Šalies narės įstatymais, valdytojo ar jo paskyrimo kriterijus gali nustatyti Sąjunga ar tos Šalies narės įstatymai.
<b>Duomenų privatumo pranešimas</b>	Informacinis pranešimas, kuriuo Duomenų subjektams ir „Affidea“ užtikrinamas su duomenų apsauga susijusios informacijos aiškumas ir suprantamumas.
<b>Duomenų tvarkytojas</b>	Duomenų tvarkytojas yra fizinis ar juridinis asmuo, viešoji įstaiga, agentūra ar kita institucija, tvarkanti asmens duomenis valdytojo vardu.
<b>Asmens duomenys</b>	Asmens duomenys yra bet kokia su identifikuotu ar galimai identifikuojamu fiziniu asmeniu (toliau - <b>Duomenų subjektas</b> ) susijusi informacija; galimai identifikuojamas fizinis asmuo yra tas, kurio tapatybę galima tiesiogiai ar netiesiogiai nustatyti, naudojantis identifikatoriumi pavyzdžiui, vardu, identifikavimo kodu, vietovės duomenimis, internetiniu identifikatoriumi arba vienu ar keliais to fizinio asmens fizinei, fiziologinei, genetinei, psichinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais požymiais. „Affidea“ Asmens duomenys reiškia toliau išvardintus dalykus (jais neapsiribojant):

- Pacientų duomenis: tyrimų vaizdus, medicininės ataskaitas, medicininių tyrimų laikus ir vietas, rinkodaros kampanijų metu naudojamas pacientų savybes;
- Darbuotojų duomenis: darbo sutartyse, darbo laiko ir darbo užmokesčio apskaitos dokumentuose, medicinos centų ir biurų vaizdo stebėsenos įranga padarytuose vaizdo įrašuose matomus asmens duomenis, prieigos kortelių duomenis ir darbuotojų elektroninio pašto adresus;
- Tiekėjų ar partnerių duomenis: paslaugų sutartyse nurodytus asmens duomenis, partnerių elektroninio pašto adresus ir kt.

**Asmens duomenų tvarkymas**

Tvarkymas reiškia bet kokį su asmens duomenimis ar jų rinkiniais automatinėmis ar neautomatinėmis priemonėmis atliekamą veiksma ar eilę veiksmų, pavyzdžiui, rinkimą, įrašymą, sisteminimą, formavimą, laikymą, adaptavimą ar keitimą, išgavimą, konsultavimą, panaudojimą, atskleidimą perduodant, platinant ar kitaip paviešinant, išdėstymą ar sujungimą, apribojimą, ištrynimą ar sunaikinimą.

**Asmens duomenų pažeidimas**

Asmens duomenų pažeidimas yra saugos pažeidimas, sukeliantis netyčinį ar neteisėtą perduotų, laikomų ar kitaip tvarkomų asmens duomenų sunaikinimą, praradimą, pakeitimą, neteisėtą atskleidimą ar neteisėtą prieigą prie jų.

**Asmens duomenų tvarkymo apsauga**

Asmens duomenų tvarkymo apsauga yra atitinkamos techninės ir organizacinės priemonės, skirtos asmens duomenų tvarkymo pavojingumą atitinkančiam apsaugos lygiui užtikrinti, siekiant išvengti: 1) fizinių asmenų teisių ir laisvių suvaržymo ir 2) asmens duomenų pažeidimų. Apsauga apima ir 1) bei 2) punktų incidentų ištaisymą.

**Asmens duomenų nuasmeninimas**

Asmens duomenų nuasmeninimas apibrėžiamas kaip tam tikrų elementų atsikratymas, kad Duomenų valdytojas, pasinaudodamas tvarkomais ar turimais duomenimis, daugiau nebegalėtų identifikuoti Duomenų subjekto. Šis procesas negrįžtamas. Jei jis grįžtamas, tai nėra nuasmeninimas.

**Profiliavimas**

Profiliavimas yra bet kokios formos automatinis asmens duomenų tvarkymas, sudarytas iš asmens duomenų panaudojimo tam tikriems su fiziniu asmeniu susijusiems aspektams įvertinti, tai yra, to fizinio asmens darbingumui, ekonominei būklei, sveikatai, pomėgiams, interesams, patikimumui, elgsenai, vietai ar judėjimui analizuoti ar numatyti.

**Automatinis sprendimų priėmimas**

Automatinis sprendimų priėmimas apima kitus aspektus, tačiau gali iš dalies sutapti su profiliavimu. Grynai automatinis sprendimų priėmimas yra galimybė priimti sprendimą technologinėmis priemonėmis, nedalyvaujant žmogui. Dažnai vadinamas Dirbtiniu intelektu.

### 3. Politika

#### 4.1 ĮVADAS

Ši politika skirta pagrindinėms rekomendacijoms apibrėžti; ją papildo kitos „Affidea“ politikos ir procedūros, kuriose specializuočiau ir išsamiau aprašytos įvairios temos. Darbuotojai įsipareigoja siekti išsamesnių konsultacijų, kadangi už Duomenų apsaugos įstatymų laikymąsi galiausiai atsakingas kiekvienas „Affidea“ grupės darbuotojas ir ši atsakomybė negali būti perleidžiama.

Politikos tikslas yra ir užtikrinti, kad „Affidea“ palengvins Duomenų subjektų galimybę pasinaudoti savo teisėmis ir laisvėmis ir padėti „Affidea“ tvarkyti asmens duomenis, laikantis ES reglamentų ir valstybių narių nacionalinių įstatymų reikalavimų.

Ši „Affidea“ Duomenų apsaugos politika skirta sukurti Duomenų apsaugos sistemos pagrindus, pasitelkiant Standartines veiklos procedūras:

Užtikrinant, kad:

- Visi Duomenų subjektai suprastų, kodėl, kaip, kur ir kaip ilgai „Affidea“ tvarkys jų asmens duomenis ir žinotų BDAR numatytas savo teises ir laisves;
- Visi asmens duomenis tvarkantys „Affidea“ darbuotojai, tiekėjai ir išorės partneriai gerai žinotų savo įsipareigojimus, numatytus BDAR ir galiojančiuose nacionaliniuose įstatymuose;
- „Affidea“ galėtų įrodyti ir patikrinti BDAR laikymąsi;
- „Affidea“ galėtų proaktyviai aptikti su duomenų apsauga susijusius incidentus, į juos reaguoti ir iš jų pasimokyti;
- Bet kokių asmens duomenų tvarkymo veiksmų atvejais „Affidea“ laikysis šešių BDAR principų ir įrodys, kad laikosi BDAR atskaitomybės principo.  
Suteikiant galimybę:
- „Affidea“ teisėtai tvarkyti asmens duomenis, laikantis BDAR ir galiojančių nacionalinių įstatymų reikalavimų, ir vykdyti profesiniu medikų elgesio kodeksu numatytus įsipareigojimus;
- Duomenų subjektams ir „Affidea“ aiškiai suvokti ir pasitikrinti asmens duomenų tvarkymo teisėtumą;
- Visai „Affidea“ grupei įgyvendinti BDAR numatytas Duomenų subjekto teises ir laisves;
- Teisėtai perduoti asmens duomenis „Affidea“ viduje ir už jos ribų;
- „Affidea“ atlikti poveikio duomenų apsaugai įvertinimą (PDAI);
- Darbuotojams, tiekėjams ir trečiosioms šalims prašyti pagalbos tais atvejais, kai, jų nuomone, duomenų tvarkymas gali pažeisti BDAR nuostatas ar kai tvarkant asmens duomenis nutinka kažkas neįprasto.

Darbuotojams visuomet privaloma laikytis šios politikos reikalavimų.

Norėdamas tiksliausiai apibūdinti šią Duomenų apsaugos politiką, skaitytojas turėtų suprasti, kad asmens duomenys turi būti tvarkomi laikantis „Affidea“ Asmens duomenų raidos ciklo. Raidos ciklas bei techninės ir organizacinės priemonės, kurių ėmėsi „Affidea“, kad asmens duomenys būtų tvarkomi, laikantis BDAR, kitų ES reglamentų reikalavimų, Europos duomenų apsaugos kontrolierių, Europos duomenų apsaugos valdybos konsultacijų ir nuomonių ir atitinkamų ES direktyvų reikalavimų. Už atitiktį ES direktyvoms, perkeltoms į ES narių teisę ir ES narių nacionalinius įstatymus, atsako vietinės tų šalių „Affidea“ organizacijos.

## 4.2 AFFIDEA ASMENS DUOMENŲ RAIDOS CIKLAS

Toliau pateikiamos „Affidea“ asmens duomenų raidos ciklo pakopos ir jų paaiškinimai.

### 9. Duomenų subjektų prašymų įgyvendinti jų teises ir laisves vykdymas



### 10. Nuolat peržiūrimi atitinkamo PDAI rezultatai

1 pav.: „Affidea“ asmens duomenų raidos ciklas

1. **Asmens duomenų gavimas ir saugaus tvarkymo reikalavimų įgyvendinimas:** asmens duomenys gaunami tiesiogiai iš asmenų arba pateikiami „Affidea“ kito Duomenų valdytojo.

2. **Duomenų suklasifikavimas pagal „Affidea“ klasifikaciją:** visi „Affidea“ sistemose tvarkomi duomenys turi būti suklasifikuoti pagal „Affidea“ duomenų klasifikaciją. Šitaip, be kita ko, įdiegiamos tinkamos organizacinės ir techninės priemonės.
3. **Atsakingo asmens ir duomenų prižiūrėjo paskyrimas:** visiems „Affidea“ tvarkomiems duomenims paskiriamas prižiūrėtojas, atsakingas už duomenų priežiūrą ir tinkamumą numatyta paskirčiai, kuris taip pat prižiūri šios politikos laikymąsi.
4. **Saugus asmens duomenų tvarkymas tikslo įgyvendinimui užtikrinti:** asmens duomenys turi būti tvarkomi tik Duomenų privatumo pranešimu numatytam tikslui pasiekti ir tik laikantis Informacijos saugumo politikos reikalavimų.
5. **Asmens duomenų prieiga ir priežiūra:** asmens duomenys gali būti peržiūrėti ir tvarkomi tik pagrįstai ir tik tokią teisę turinčių darbuotojų. Pagrindinė priežastis turėtų būti Duomenų apsaugos pranešimu numatytų tikslų įgyvendinimas.
6. **Asmens duomenų laikymas ir saugojimas:** asmens duomenys saugojami kaip numatyta Duomenų saugojimo trukmės grafike. Pasibaigus saugojimo laikotarpiui, duomenys saugiai ištrinami.
7. **Asmens duomenų nuasmeninimas pagal poreikį:** „Affidea“ gali pasiekti numatytų tikslų, tvarkydama nuasmenintus duomenis. Jei asmens duomenys nuasmeninami, juos tvarkyti kur kas saugiau ir galima paprasčiau dalintis su kitomis šalimis.
8. **Asmens duomenų ištrynimasis ir atrinkimas:** pasibaigus saugojimo laikotarpiui, asmens duomenys (skaitmeniniai ir fiziniai) ištrinami tinkamiausiu būdu. Kaip numatyta Duomenų saugojimo trukmės grafike, prieš tai gali būti atrenkamos pavienės duomenų sritys ar fiziniai įrašai.
9. **Duomenų subjekto prašymo įgyvendinti jo teises ir laisves vykdymas:** asmens duomenų tvarkymo metu Duomenų subjektas turi galimybę pasinaudoti BDAR numatytomis savo teisėmis bei laisvėmis.
10. **Nuolatinis atitinkamų poveikio duomenų apsaugai vertinimų (DPIA) rezultatų peržiūrėjimas:** visus itin pavojingus asmens duomenų tvarkymo atvejus ir poveikio duomenų apsaugai įvertinimus būtina peržiūrėti, siekiant įsitikinti, kad nėra reikalo pakeisti pradinius jų rezultatus.

Šio raidos ciklo ir „Affidea“ juridinių asmenų techninių bei organizacinių priemonių tinkamumas tikrinamas, peržiūrint ir atnaujinant atitinkamų DPIA rezultatus, kurie yra „Affidea“ atitikties BDAR ir kitiems ES reglamentams pagrindas.

### 4.3 ŠEŠI BDAR NUMATYTI PRINCIPAI

Duomenų apsaugos taisyklių esmė – laikytis šešių toliau išvardintų principų ir galėti tai įrodyti. Bet kokie asmens duomenys turi būti:

1. Teisėtai, sąžiningai ir skaidriai tvarkomi (teisėtumo, sąžiningumo ir skaidrumo principas).
2. Tvarkomi Duomenų privatumo pranešime numatytais tikslais (ribotos paskirties principas).
3. Pakankami, aktualūs ir skirti Duomenų privatumo pranešime numatytiems tikslams pasiekti (duomenų minimizavimo principas).
4. Tikslūs ir pagal poreikį atnaujinami Duomenų privatumo pranešime numatytiems tikslams pasiekti (tikslumo principas).
5. Tvarkomi tik tol, kol reikia Duomenų privatumo pranešime ir ES valstybių narių įstatymais numatytiems tikslams pasiekti (riboto laikymo principas).
6. Tvarkomi taip, kad būtų užtikrintas „Affidea“ Informacijos saugumo politikoje numatytas asmens duomenų saugumas (vientisumo ir konfidencialumo principas).

Šių principų privalu laikytis visais bet kokių „Affidea“ asmens duomenų tvarkymo atvejais. BDAR numatytos tam tikros sankcijos – daugiau nei vieno principo pažeidimas skaudžiai atsilieptų „Affidea“, todėl privaloma laikytis šių principų.

Asmens duomenų tvarkymo teisėtumas užtikrinamas, pasirenkant tinkamą teisinį pagrindą juos tvarkyti. Šis pagrindas užfiksuojamas įstaigos vidaus dokumentais ir paaiškinamas Duomenų subjektui Duomenų privatumo pranešime. Duomenų privatumo pranešime Duomenų subjektui pateikiama skaidri informacija apie „Affidea“ aktualių duomenų tvarkymą.

#### 4.3.1 Duomenų privatumo pranešimas

Bet kuriame Duomenų privatumo pranešime turi būti pateikta tokia informacija:

- a) Duomenų valdytojo pavadinimas ir duomenys susisiekti ir duomenų apsaugos pareigūno kontaktiniai duomenys;
- b) Tvarkymo tikslai;
- c) Teisinis tvarkymo pagrindas (jei remiamasi „teisėto intereso“ pagrindu, reikia nurodyti, koks tas teisėtas interesas);
- d) Gavėjai ar gavėjų tipai, kuriems bus atskleidžiami asmens duomenys, įskaitant visus už Europos ekonominės erdvės (EEE) ribų esančius gavėjus;
- e) Duomenys bus perduodami trečiajai šaliai ar už EEE ribų esančiam gavėjui; pastaruoju atveju būtina nurodyti gavėjo duomenis, paskirties valstybę, tų duomenų apsaugos lygmenį ir numatomus įvairių kategorijų asmens duomenų ištrynimo laikotarpius (jei tai neįmanoma, nurodomi tokių laikotarpių nustatymo kriterijai);
- f) Duomenų subjekto teisės;
- g) Jei reikalingas Duomenų subjekto sutikimas tvarkyti duomenis, būtina paminėti jo/jos teisę bet kada atšaukti tokį sutikimą;
- h) Duomenų subjekto teisė skųstis priežiūros institucijai, jei iškiltų problemų;
- i) Asmens duomenų teikimas yra įstatyminis ar sutartinis reikalavimas ar reikalavimas, norint sudaryti sutartį; galimos duomenų nepateikimo pasekmės;
- j) Duomenis pateikti privaloma ar galima pasirinkti;
- k) Galimos duomenų nepateikimo pasekmės;
- l) Jei taikytina, bet kokio automatinio sprendimų priėmimo (tiksliau, profiliavimo) duomenis, prasmingus taikomos logikos duomenis ir galimas tokio tvarkymo pasekmes;
- m) Kai duomenys gaunami ne tiesiogiai iš Duomenų subjekto: atitinkamų asmens duomenų kategorijas, tų duomenų šaltiniai ir (kai taikytina), ar tie duomenys gauti iš viešai prieinamų šaltinių.

#### 4.4 DUOMENŲ SUBJEKTŲ TEISĖS IR LAISVĖS

Duomenų apsaugos pranešime nurodomos visų Duomenų subjektų Teisės ir laisvės, o tai yra:

1. **Teisė gauti duomenis:** Duomenų subjektas turi teisę patvirtinti mūsų tvarkomus jo/jos asmens duomenis ir gauti jų elektroninę ar fizinę (popierinę) kopiją. Būtina paaiškinti visus techninius terminus. Yra parengtos vietinės ES valstybių narių gairės, kuriose nurodyta, kokius duomenis galima pateikti sveikatos priežiūros įstaigoms ir darbdaviams. Teisė gauti duomenis dar vadinama SPP – Subjekto prieigos prašymu. Ši teisė pavojinga, kadangi nevykdant SPP Duomenų subjektas gali pateikti skundą Priežiūros institucijai, kuri privalo atlikti tyrimą. Tokio pobūdžio prašymus privaloma profesionaliai įvykdyti, laikantis atitinkamų procedūrų.
2. **Teisė taisyti duomenis:** Duomenų subjektas turi teisę pareikalauti pataisyti netikslius ar papildyti neišsamius asmens duomenis.
3. **Teisė ištrinti duomenis:** Duomenų subjektas turi teisę pareikalauti ištrinti jo/jos asmens duomenis. Vis dėlto, „Affidea“ gali turėti teisinę prievolę tam tikrą laikotarpį saugoti asmens duomenis; ši prievolė aprašyta „Affidea“ Duomenų saugojimo grafike. Tokiu atveju „Affidea“ neprivalės ištrinti to asmens duomenų.
4. **Teisė apriboti tvarkymą:** Duomenų subjektas turi teisę pareikalauti sustabdyti bet kokį duomenų tvarkymą, išskyrus jų laikymą ir prieigą. Paprastai taip nutinka ginčo su Duomenų subjektu atvejais, yra laikina ir pasikeičia, kai tik ginčas išsprendžiamas.
5. **Teisė perduoti:** Duomenų subjektas turi teisę pareikalauti elektroninės asmens duomenų kopijos sau arba perduoti tiesiogiai kitam Duomenų valdytojui.
6. **Teisė prieštarauti:** Kai teisinis pagrindas tvarkyti duomenis yra teisėtas interesas, Duomenų subjektas gali paprieštarauti tokiam tvarkymui ir, jei jam/jai pasiseks, „Affidea“ privalės nustoti tvarkyti jo/jos asmens duomenis.
7. **Teisė uždrausti automatinių sprendimų priėmimą:** BDAR aiškiai atskiriamas profiliavimas ir automatinių sprendimų priėmimas. Prieš pradėdam bet kokius profiliavimo ar automatinių sprendimų priėmimo veiksmus būtina pasikonsultuoti su DAP ir atlikti DPIA. Apie tai būtina pranešti Duomenų subjektui, kuris/-i turi teisę uždrausti tokį duomenų tvarkymą.

Duomenų subjekto teisės ir laisvės nėra absoliučios; Duomenų subjekto reikalavimai svarstomi pagal galiojančias taisykles ir įstatymus. Jei reikalavimas įgyvendinti Duomenų subjekto teises ir laisves atmetamas, jam/jai būtina nurodyti dokumentais pagrįstas atmetimo priežastis. Reikalavimą atmesti galima tik gavus Duomenų apsaugos pareigūno (DAP) leidimą.

Remiantis BDAR nuostatomis, atsakymai į Subjekto prieigos prašymus negali būti mokami, nebent tie reikalavimai būtų aiškiai nepagrįsti ar pertekliniai. Svarbiausia patikrinti prašančiojo tapatybę, prieš imantis kokių nors veiksmų.

Su Duomenų subjektu turi būti bendraujama glaustai, skaidriai, suprantamai ir lengvai pasiekiamą forma, aiškiai ir paprastai paaiškinant visus medicininius terminus. Prie susirašinėjimo pridedamas Duomenų privatumo pranešimas, kad Duomenų subjektą žinotų savo teises. „Affidea“ atsisakius įgyvendinti kokią nors teisę, būtina informuoti Duomenų subjektą, išdėstant priežastis ir primenant galimybę pateikti skundą Priežiūros institucijai bei kreiptis į teismą.

Kai kurios teisės ir laisvės įgyvendinamos „Affidea“ pacientų portalų pagalba; juose pacientams suteikiama prieiga prie jų asmens duomenų. Jei „Affidea“ perdavė asmens duomenis trečiosioms šalims (Duomenų tvarkytojams), „Affidea“ privalo informuoti tuos Duomenų tvarkytojus apie Duomenų subjekto prašymus pataisyti, ištrinti asmens duomenis ar apriboti jų tvarkymą.

#### 4.5 DUOMENŲ TVARKYTOJO PAREIGOS IR SUTARTYS

„Affidea“ vardu veikiančioms Duomenų tvarkytojams privaloma sudaryti sutartis su mumis. Duomenų tvarkymo sutartyje turi būti BDAR ir vietos įstatymų numatytos dalys. Naudojamas patvirtintas sutarties šablonas, nebent Duomenų apsaugos pareigūnas nurodo kitaip. Mūsų Duomenų tvarkytojai, siekdami užtikrinti duomenų tvarkymo saugumą, privalo įdiegti mūsų reikalaujamas technines ir organizacines priemones.

#### 4.6 ASMENS DUOMENŲ PERDAVIMAS KITOMS ŠALIMS

Asmens duomenys perduodami tik pagal galiojančias sutartis ir tik patvirtintais saugiais perdavimo būdais. Jei duomenys perduodami už ES ribų, taikomos naujausios Europos duomenų apsaugos valdybos numatytos standartinių ES sutarčių sąlygos.

#### 4.7 AFFIDEA VYKDOMI POVEIKIO DUOMENŲ APSAUGAI ĮVERTINIMAI (DPIA)

Jei tikėtina, kad duomenų tvarkymas gali kelti didelį pavojų asmenų teisėms ir laisvėms, prieš imantis bet kokių duomenų tvarkymo veiksmų būtina atlikti Poveikio duomenų apsaugai įvertinimą.

Dideliu pavojumi „Affidea“ laiko atvejus, kai tvarkomi tokie duomenys:

- a) Asmens tapatybės duomenys;
- b) Asmens finansiniai duomenys;
- c) Asmens buvimo vietos duomenys;
- d) Asmens įrenginių atpažinimo duomenys.

Labai dideliu pavojumi „Affidea“ laiko atvejus, kai tvarkomi tokie duomenys:

- a) Specifiniai asmens duomenys (Duomenų subjekto fizinės ar psichikos sveikatos arba medicininės būklės duomenys);
- b) Asmens biometriniai duomenys;
- c) Asmens genetiniai duomenys;
- d) Vaiko asmens duomenys;
- e) Pažeidžiamų asmenų asmens duomenys.

DPIA yra atitikties kūrimo ir demonstravimo procesas ir Atskaitomybės priemonė. DPIA procesas fiksuojamas dokumentais. Prieš pradėdant bet kokius su naujų tipų labai pavojingų duomenų tvarkymu susijusius veiksmus, būtina atlikti DPIA.

Pasikeitus pavojingumo Duomenų subjektui lygmeniui, būtina peržiūrėti visų turimų labai pavojingų duomenų tvarkymo DPIA. Peržiūrėjimo tikslas – patikrinti, ar reikia keisti technines ir organizacines priemones. Ypač daug dėmesio būtina skirti profiliavimui ir automatiniam sprendimų priėmimui, dirbtiniam intelektui (DI), kadangi šių tipų duomenų tvarkymui būtinas DPIA atitikčiai ir pavojaus Duomenų subjekto teisėms ir laisvėms sumažinimui įrodyti.

#### 4.8 APSAUGOS INCIDENTAI IR GALIMI BDAR PAŽEIDIMAI

Visi asmens duomenų pažeidimai (PDB) laikomi saugumo incidentais, tačiau ne visi saugumo incidentai yra asmens duomenų pažeidimai. Dėl to apie kiekvieną saugumo incidentą pranešama „[Informacijos saugumo incidentų valdymo](#)“ procedūros tvarka. Informacijos saugumo incidentų valdymo procedūra susijusi su procedūra, skirta gauti, patikrinti, įvertinti, reaguoti ir pranešti apie Asmens duomenų pažeidimus Priežiūros institucijai. Pranešti būtina per 72 valandas nuo akimirkos, kai „Affidea“ gavo



pranešimą kaip Duomenų valdytojas; visas personalas ir trečiosios šalys privalo pradėti saugumo patikrą, kai tik sužino apie problemą.

Jei kuris nors darbuotojas ar trečioji šalis mano, kad gali pažeisti BDAR nuostatas, prieš perduodant ar tvarkant tokius asmens duomenis būtina pasitarti su DAP. Personalui dėmesingai primenama, kad, turint abejonių, konsultuotis su DAP būtina ne tik imantis eilinių darbinių veiksmų, bet ir vienkartinį ar nestandartinių duomenų tvarkymo veiksmų atvejais.

#### 4.9 PROAKTYVUS APTIKIMAS, REAGAVIMAS IR PASIMOKYMAS IŠ DUOMENŲ APSAUGOS INCIDENTŲ

„Affidea“ tvarko asmens duomenis nuolat besikeičiančiame pasaulyje, kuriame technologijos ir grėsmės saugumui tobulėja nuolatos. Po kiekvieno reikšmingo apsaugos incidento DAP komanda patikrins apsaugos registrus su vyriausiuoju informacijos saugumo pareigūnu ir pateiks rekomendacijas dėl saugesnio duomenų tvarkymo, atsižvelgdami į besikeičiantį pavojingumo kontekstą. Šitaip techninės ir organizacinės priemonės papildomos mokymusi ir pagerėja proaktyvus apsaugos incidentų aptikimas bei reagavimas į juos.

## 4. Mokymų reikalavimai

Su dokumentu supažindinami ar apmokinami šių funkcijų darbuotojai:

- Visi darbuotojai.

Jrašai apie supažindinimą su dokumentu ar mokymus atliekami ir laikomi pagal SOP-QM-LT-003 Kokybės įrašų kontrolė.

## 5. Auditas / Metrikai

Šalies vadovas yra atsakingas už tai, kad būtų vykdomas vidinis (valstybės lygmens) auditas, skirtas įvertinti atitiktį šiai politikai. Atitiktis politikai apima darbuotojų mokymų ir sąmoningumo įrodymą.

Siekiant įvertinti atitiktį politikai, gali būti vykdomas išorinis auditas (centrinio biuro arba trečiųjų šalių).

## 6. Nuorodos / Susiję dokumentai

**P-IT-LT-001** Informacijos saugumo politika

**SOP-IT-LT-001** Informacijos saugumo incidentų valdymo procedūra

## 7. Versijų istorija

Versija	Pakeitimo aprašymas	Pakeitimo priežastis
01	Pirminis dokumentas	
02	Išplėsta politikos taikymo apimtis	Įmonių prisijungimas