



PATVIRTINTA
"Orkla Care" UAB
Generalinio direktoriaus
įsakymu Nr.
Data

"Orkla Care" UAB

**ASMENS DUOMENŲ TVARKYMO
POLITIKA**

Vilnius
2018

"ORKLA CARE" UAB
ASMENS DUOMENŲ TVARKYMO POLITIKA

1. PAGRINDINĖS ŠIOS POLITIKOS SĄVOKOS

- 1.1. **ADTAI** - Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas.
- 1.2. **Atsakingas darbuotojas** – Duomenų valdytojo Darbuotojas, kuris pagal jo darbo pobūdį turi teisę vykdyti konkrečias su Duomenų tvarkymu susijusias funkcijas.
- 1.3. **BDAR** – Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).
- 1.4. **Duomenys/Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.
- 1.5. **Duomenų gavėjas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuriai atskleidžiami Asmens duomenys, nesvarbu, ar tai trečioji šalis ar ne.
- 1.6. **Duomenų saugumo pažeidimas** reiškia pažeidimą, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi Asmens duomenys arba prie jų be leidimo gaunama prieiga.
- 1.7. **Duomenų subjektas** – Duomenų valdytojo Klientas ar Darbuotojas arba bet koks kitas asmuo, kurio asmens duomenis tvarko Duomenų valdytojas.
- 1.8. **Duomenų tvarkymas** reiškia bet kurią operaciją ar operacijų rinkinį, automatiniais arba neautomatiniais būdais atliekamus su asmens duomenimis, tokius kaip: rinkimas, užrašymas, rūšiavimas, saugojimas, adaptavimas ar keitimas, atgaminimas, paieška, naudojimas, atskleidimas perduodant, platinant ar kitu būdu padarant juos prieinamus, išdėstymas reikiama tvarka ar sujungimas derinant, blokavimas, trynimasis ar naikinimas.
- 1.9. **Duomenų tvarkytojas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri Duomenų valdytojo vardu tvarko asmens duomenis.
- 1.10. **Duomenų valdytojas** - "Orkla Care" UAB, juridinio asmens kodas 301240827, registracijos adresas Trinapolio g. 9E, Vilnius.
- 1.11. **Informacijos vienetasis** – identifikuotas informacijos rinkinys, turintis Duomenų valdytojui kaip verslo subjektui tam tikrą vertę. BDAR atveju, tai bet koks Asmens duomenų rinkinys, turintis vertę Duomenų valdytojui.
- 1.12. **IT sistema** – sistema, palaikanti vieną ar daugiau Programų.
- 1.13. **IT sistemos savininkas** – įmonė atsakinga už IT sistemos valdymą.
- 1.14. **Kandidatas** – asmuo, pageidaujantis tapti Duomenų valdytojo Darbuotoju.
- 1.15. **Klientas** – asmuo, kuris naudojasi Duomenų valdytojo teikiamomis paslaugomis arba anksčiau jomis naudojosi.
- 1.16. **PDAV** – poveikio duomenų apsaugai vertinimas.

- 1.17. **Politika** reiškia šią Asmens duomenų tvarkymo Politiką.
- 1.18. **Programa** – programinė įranga, veikianti savarankiškai arba kaip didesnės programų grupės dalis.
- 1.19. **Pseudonimizavimas** – Asmens duomenų tvarkymas tokiu būdu, kuris neleistų Asmens duomenų susieti su konkrečiu Duomenų subjektų nenaudojant papildomos informacijos. Tai nėra tas pats kaip nuasmeninimas, kuris reikalauja negrįžtamo Duomenų subjekto tapatybės atskyrimo, kuri negali būti atkurta jokiais priemonėmis.
- 1.20. **Specialių kategorijų asmens duomenys** - asmens duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, genetiniai duomenys, biometriniai duomenys, skirti konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenys arba duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją.
- 1.21. Kitos Politikoje vartojamos sąvokos atitinka BDAR, ADTAĮ ir Lietuvos Respublikos elektroninių ryšių įstatyme (toliau – **ERĮ**) vartojamas sąvokas.

2. BENDROSIOS NUOSTATOS

- 2.1. Politikos tikslas – reglamentuoti asmens duomenų tvarkymo procedūras, duomenų subjektų teisių įgyvendinimą, technines ir organizacines priemones, skirtas apsaugoti asmens duomenis pagal BDAR, ADTAĮ, ERĮ ir kitus teisės aktus, nustatančius asmens duomenų apsaugą, ir šią Politiką.
- 2.2. Duomenų valdytojas užtikrina, kad jis atitinka šiuos esminius asmens duomenų tvarkymo principus:
 - 2.2.1. Asmens duomenys turi būti duomenų subjekto atžvilgiu tvarkomi teisėtu, sąžiningu ir skaidriu būdu (teisėtumo, sąžiningumo ir skaidrumo principas);
 - 2.2.2. Asmens duomenys turi būti renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu; tolesnis duomenų tvarkymas archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais nėra laikomas nesuderinamu su pirminiais tikslais (tikslų apribojimo principas);
 - 2.2.3. Asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi (duomenų kiekio mažinimo principas);
 - 2.2.4. Asmens duomenys turi būti tikslūs ir prireikus atnaujinami; turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi (tikslumo principas);
 - 2.2.5. Asmens duomenys turi būti laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi; asmens duomenis galima saugoti ilgesnius laikotarpius, jeigu asmens duomenys bus tvarkomi tik archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais pagal 89 straipsnio 1 dalį, įgyvendinus atitinkamas technines ir organizacines priemones, kurių reikalaujama šiuo reglamentu siekiant apsaugoti duomenų subjekto teises ir laisves (saugojimo trukmės apribojimo principas);
 - 2.2.6. Asmens duomenys turi būti tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas).

- 2.2.7. Duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi aukščiau nurodytų principų, ir turi sugebėti įrodyti, kad jų yra laikomasi (atskaitomybės principas).
- 2.3. Duomenys saugomi laikotarpius, nurodytus šioje Politikoje kiekvienam Asmens duomenų tipui.
- 2.4. Jeigu Duomenys naudojami kaip įrodymai civilinėje, administracinėje ar baudžiamojoje byloje ar kitais įstatymų nustatytais atvejais, Duomenys gali būti saugomi tiek, kiek reikalinga šiems duomenų tvarkymo tikslams, ir sunaikinami nedelsiant, kai tampa nebereikalingi.
- 2.5. Sukaupti Duomenys saugomi (tvarkomi) vidiniame Duomenų valdytojo serveryje. Prieiga prie Duomenų suteikiama tik Atsakingiems darbuotojams ir duomenų tvarkytojams.
- 2.6. Duomenų tvarkytojo prieigos teisės prie Duomenų naikinamos nutraukus asmens duomenų tvarkymo sutartį, sudarytą su Duomenų valdytoju, ar šiai sutarčiai nustojus galioti.
- 2.7. Atsakingi darbuotojai privalo:
 - 2.7.1. tvarkyti Asmens duomenis vadovaudamiesi Europos Sąjungos ir Lietuvos Respublikos teisės aktais, taip pat šia Politika ir jos priedais;
 - 2.7.2. neatskleisti, neperduoti ir nesudaryti sąlygų bet kokiomis priemonėmis susipažinti su duomenimis nė vienam asmeniui, kuris nėra įgaliotas tvarkyti duomenų;
 - 2.7.3. nedelsiant pranešti Duomenų valdytojui apie bet kokią įtartina situaciją, kuri gali kelti grėsmę duomenų saugumui.
- 2.8. Atsakingas darbuotojas netenka teisės tvarkyti Asmens duomenis, kai pasibaigia Atsakingo darbuotojo darbo sutartis su Duomenų valdytoju, arba kai atitinkamai Duomenų valdytojo vadovas sprendimu atšaukia Darbuotojo paskyrimą tvarkyti duomenis ir informuoja apie tai Atsakingą darbuotoją.
- 2.9. Duomenys perduodami duomenų tvarkytojams ir duomenų gavėjams kai teisę ir (ar) pareigą tai daryti atitinkamais pagrindais suteikia teisės aktai.
- 2.10. Asmens duomenų perdavimas Tvarkytojams galimas tik sudarius tinkamas sutartis tarp Tvarkytojų ir Duomenų valdytojo.
- 2.11. Asmens duomenų perdavimas į trečiąsias šalis arba tarptautinėms organizacijoms įgyvendinamas pagal punktuose 13.5.-13.6. pateiktą informaciją.
- 2.12. Asmens duomenys Duomenų valdytojo gali būti pateikti ikiteisminio tyrimo įstaigai, prokurorui ar teismui dėl administracinių, civilinių, baudžiamųjų bylų, kaip įrodymai ar kitais įstatymų nustatytais atvejais.

3. DUOMENŲ KOKYBĖ

- 3.1. Duomenų valdytojas siekia, kad Duomenų subjektų asmens duomenys būtų:
 - 3.1.1. tvarkomi sąžiningai ir teisėtai;
 - 3.1.2. tvarkomi esant Duomenų subjekto sutikimui ar egzistuojant kitai teisėto asmens duomenų tvarkymo sąlygai;
 - 3.1.3. tinkami, aktualūs ir nepertekliniai, atsižvelgiant į nustatytus tikslus;
 - 3.1.4. tikslūs.
- 3.2. Duomenų valdytojas registruoja tvarkymo operacijas. Duomenų valdytojas skiria Atsakingiems darbuotojams pareigą registruoti tvarkymo operacijas naudojantis šablonais Duomenų valdytojo atsakomybe.

4. TEISĖTO DUOMENŲ TVARKYMO PAGRINDAS

- 4.1. Duomenų valdytojo Atsakingi darbuotojai, prieš pradėdami tvarkyti Asmens duomenis, privalo įsitikinti, kad egzistuoja teisėto duomenų tvarkymo pagrindas, pavyzdžiui:
- 4.1.1. Duomenų subjektas davė sutikimą, kad jo Asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais;
 - 4.1.2. Tvarkyti Duomenis būtina siekiant įvykdyti sutartį, kurios šalis yra Duomenų subjektas, arba siekiant imtis veiksmų Duomenų subjekto prašymu prieš sudarant sutartį;
 - 4.1.3. Tvarkyti Duomenis būtina, kad būtų įvykdyta Duomenų valdytojui taikoma teisinė prievolė;
 - 4.1.4. Tvarkyti Duomenis būtina siekiant teisėtų Duomenų valdytojo arba trečiosios šalies interesų, išskyrus atvejus, kai tokie Duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens Duomenų apsaugą, yra už juos viršesni.
- 4.2. Duomenų subjektams prieš pradėdant tvarkyti jų asmens duomenis pateikiama informacija apie Duomenų tvarkymą.

5. TINKAMAS DUOMENŲ SUBJEKTŲ INFORMAVIMAS

- 5.1. Duomenų subjektams prieš pradėdant tvarkyti jų asmens duomenis būtina pateikti šią informaciją:
- 5.1.1. Duomenų valdytojo tapatybę ir kontaktinius duomenis;
 - 5.1.2. Duomenų tvarkymo tikslus;
 - 5.1.3. Duomenų tvarkymo teisinį pagrindą;
 - 5.1.4. Asmens duomenų saugojimo laikotarpį arba, jei tai neįmanoma, kriterijus, taikomus tam laikotarpiui nustatyti;
 - 5.1.5. Informuoti apie Duomenų subjektų teisę prašyti, kad Duomenų valdytojas leistų susipažinti su Duomenų subjekto Asmens duomenimis ir juos ištaisyti arba ištrinti, arba apribotų duomenų tvarkymą, arba teisę nesutikti, kad Duomenys būtų tvarkomi, taip pat teisę į Duomenų perkeliamumą;
 - 5.1.6. Informuoti apie Duomenų subjektų teisę pateikti skundą kontroliuojančiai institucijai;
 - 5.1.7. Jei yra, Asmens duomenų gavėjus arba Asmens duomenų gavėjų kategorijas;
 - 5.1.8. Kai taikoma, apie Duomenų valdytojo ketinimą Asmens duomenis perduoti į trečiąją valstybę arba tarptautinei organizacijai;
 - 5.1.9. Kai taikoma, kad esama automatizuoto sprendimų priėmimo, įskaitant profiliavimą, ir, bent tais atvejais, prasmingą informaciją apie loginį jo pagrindimą, taip pat tokio Duomenų tvarkymo reikšmę ir numatomas pasekmes Duomenų subjektui;
 - 5.1.10. Esant skirtingiems Duomenų tvarkymo teisiniams pagrindams, turi būti pateikiama žemiau nurodyta informacija:

Teisinė prievolė ar sutartis	Sutikimas	Teisėti interesai
<ul style="list-style-type: none"> – Ar Duomenų subjektas privalo pateikti Asmens duomenis ir galimas pasekmes nepateikus tokių duomenų? – Ar Duomenų pateikimas yra teisės aktais arba sutartyje numatytas reikalavimas, ar 	<ul style="list-style-type: none"> – Teisė atsiimti savo sutikimą bet kuriuo metu. – Teisė pareikalauti skaitmeninio dokumento su savo asmenine informacija. 	<ul style="list-style-type: none"> – Susiję teisėti Duomenų valdytojo ar trečiosios šalies interesai.

reikalavimas, kurį būtina įvykdyti norint sudaryti sutartį?		
---	--	--

5.2. Tuo atveju, jei Asmens duomenys gauti ne iš Duomenų subjekto, turi būti pateikiama aukščiau išvardyta informacija, išskyrus nurodytąją, 5.1.10 punkte „Teisinė prievolė ar sutartis“ grafoje, bei papildomai ši informacija:

5.2.1. Asmens duomenų kategorijas, kurias planuojama tvarkyti;

5.2.2. Koks yra Asmens duomenų kilmės šaltinis ir ar Duomenys gauti iš viešai prieinamų šaltinių.

5.3. Duomenų gavimo ne iš Duomenų subjekto atveju, informacija pateikiama per:

5.3.1. Vieną mėnesį nuo Duomenų gavimo;

5.3.2. Jei Duomenys bus naudojami ryšiams su Duomenų subjektu palaikyti – ne vėliau kaip pirmą kartą susisiekiant su tuo Duomenų subjektu;

5.3.3. Jeigu numatoma Asmens duomenis atskleisti kitam Duomenų gavėjui – ne vėliau kaip atskleidžiant Duomenis pirmą kartą.

5.4. Informacija turi būti pateikiama trumpa, aiškia ir lengvai prieinama forma, aiškia ir paprasta kalba.

5.5. Informacijos pateikti nereikia tais atvejais, kai Duomenų subjektui yra akivaizdu, ką Duomenų valdytojas daro, ar darys su jo Duomenimis.

5.6. Sutikimas, gautas Duomenų subjektui pirmiausia nepateikus 5.1 ir/ar 5.2 punktuose išdėstytos informacijos, nėra laikomas tinkamu.

6. KLIENTŲ DUOMENŲ TVARKYMAS ELEKTRONINĖS PREKYBOS VYKDYMO TIKSLAIS

6.1. Duomenų valdytojas teikia informaciją apie savo platinamus produktus interneto tinklalapyje, sudarydama galimybę Vartotojams juos įsigyti nuotoliniu būdu, apsiperkant Duomenų valdytojo elektroninėje parduotuvėje. Šiems tikslams Duomenų valdytojas iš Klientų gauna, naudoja ir Tvarko asmens duomenis, be kita ko, susijusius su pirkinių krepšelio turiniu (įskaitant perkamos produkcijos rūšis, kiekius), mokėjimų statistika (įskaitant sumokėtas sumas), mokėjimų duomenimis (įskaitant Klientų bankų sąskaitų numerius, bankų pavadinimus ir pan.).

6.2. Atsižvelgiant į tai, elektroninės prekybos vykdymo tikslais Duomenų valdytojas tvarko tokias Klientų Duomenų grupes:

6.2.1. Vardas;

6.2.2. Pavardė;

6.2.3. Telefono numeris;

6.2.4. Elektroninio pašto adresas;

6.2.5. Gyvenamoji vieta (adresas);

6.2.6. Asmens kodas;

6.2.7. Jei asmuo atlieka pirkimą - banko sąskaitos numeris, mokėjimų duomenys, informacija apie pirktas prekes, jų rūšis, išleistas pinigų sumas.

6.3. Duomenų valdytojas aukščiau nurodytus Klientų Duomenis, išskyrus Duomenis, nurodytus punkte 6.2.7., trečiosioms šalims perduoda tik tais atvejais, kai su trečiąja šalimi yra pasirašyta Duomenų tvarkymo sutartis.

6.4. Duomenys tvarkomi elektroninės prekybos vykdymo tikslu saugomi ne ilgiau kaip 3 metus nuo paskutinio apsilankymo Duomenų valdytojo interneto svetainėje.

6.5. Klientų duomenys esantys Microsoft Dynamics Navision programoje saugomi 10 metų nuo sąskaitos faktūros išrašymo datos.

7. KLIENTŲ DUOMENŲ TVARKYMAS RINKODAROS TIKSLAIS

7.1. Duomenų valdytojas savo Klientų, davusių sutikimą tvarkyti jų Asmens duomenis tiesioginės rinkodaros tikslu, atžvilgiu vykdo tiesioginę rinkodarą.

7.2. Atsižvelgiant į tai, tiesioginės rinkodaros vykdymo tikslu Duomenų valdytojas tvarko tokias Klientų Duomenų grupes:

7.2.1. Vardas;

7.2.2. Pavardė;

7.2.3. Telefono numeris;

7.2.4. Elektroninio pašto adresas;

7.2.5. Gyvenamoji vieta (adresas);

7.2.6. Banko sąskaita;

7.2.7. Asmens kodas;

7.2.8. Informacija apie perkamus produktus, jų rūšis, kiekius, išleistas pinigų sumas.

7.3. Duomenų valdytojas aukščiau nurodytus Klientų Duomenis, išskyrus Duomenis nurodytus punkte 7.2.8., trečiosioms šalims perduoda tik tais atvejais, kai su trečiąja šalimi yra pasirašyta Duomenų tvarkymo sutartis.

7.4. Duomenys tvarkomi tiesioginės rinkodaros vykdymo tikslu saugomi ne ilgiau kaip 3 metus nuo paskutinio apsilankymo Duomenų valdytojo interneto svetainėje.

7.5. Klientų, davusių atitinkamą sutikimą Asmens duomenys gali būti įvedami į Orkla CRM duomenų bazę tam, kad būtų sukuriami individualūs Klientų profiliai, reikalingi specializuotai ir tiksliai tiesioginei rinkodarai bei kontaktui su Klientais. Tokie profiliai tam tikrais atvejais gali būti praturtinti Duomenimis, surinktais trečiųjų šalių tada, jei trečiųjų šalių duomenų šaltiniu yra sutikimo forma(-os), dėl kurių Klientas yra išreiškęs tinkamą sutikimą.

7.6. Be tiesioginės rinkodaros, Duomenų valdytojas taip pat vykdo ir rinkos tyrimus, kurių metu tiria Klientų kaip vartotojų elgesį siekdamas sukurti ar pritaikyti produktus ir rinkodarą siekdamas prisitaikyti prie vartotojų poreikių.

7.7. Rinkos tyrimų tikslais, be tiesioginei rinkodarai tvarkomų duomenų, Duomenų valdytojas taip pat tvarko arba atiduoda tvarkyti Duomenų tvarkytojui duomenis, gaunamus slapukų ir kitų panašių technologijų pagalba, kurių naudojimas plačiau aprašytas Politikos 9 skyriuje.

8. KANDIDATŲ Į DARBO VIETAS ASMENS DUOMENŲ TVARKYMAS

8.1. Duomenų valdytojas atrankos į darbo vietas tikslais tvarko tokius Kandidatų Asmens duomenis;

8.1.1. Vardas, pavardė;

8.1.2. Telefono numeris;

8.1.3. El. pašto adresas;

8.1.4. Gyvenimo aprašymas;

8.1.5. Įvairūs asmenybiniai testai;

- 8.1.6. Dalykinių ir itelektinių kompetencijų vertinimai;
- 8.1.7. Kiti Kandidato savanoriškai pateikti jo gyvenimo aprašyme ir/ar kituose pateiktuose dokumentuose esantys duomenys.
- 8.2. Tinkamo kandidatų informavimo užtikrinimas pasiekiamas pateikus informaciją skelbime dėl kandidatavimo į siūlomą pareigybės poziją.
- 8.3. Kandidatas turi duoti savo sutikimą dėl bet kokio tvarkymo ar dalijimosi jo Asmens duomenimis, kuris nėra būtinas, pavyzdžiui, Duomenų saugojimas ilgesnį laiką nei būtina prašymo išnagrinėjimui.
- 8.4. Kandidatų duomenys teikiami tretiesiems asmenims tik tokiu atveju, jei Duomenų valdytojas pasitelkia įdarbinimo agentūrų ar kitų panašias paslaugas teikiančių subjektų, pagalbą. Su tokiais Duomenų tvarkytojais iki įdarbinimo proceso pradžios sudaromos Duomenų tvarkymo sutartys.
- 8.5. Duomenys, tvarkomi įdarbinimo kontekste, bus laikomi jautriais ir keliančiais didelę riziką informacijos saugumo kontekste, todėl, remiantis Politikos 111 skyriuje nustatytomis taisyklėmis, prieigos teisė prie jų griežtai ribojama. Prieiga suteikiama tik žmogiškųjų išteklių skyriui, atsakingiems vadovams ar atrankos paslaugą teikiančiomis šalimis, su kuriomis pasirašyta Duomenų tvarkymo sutartis.
- 8.6. Atmestų Kandidatų Asmens duomenys sunaikinami pasibaigus atrankai per 30 kalendorinių dienų, išskyrus:
 - 8.6.1. Duomenis apie atmetimą ir jo priežastis būsimų įdarbinimo procesų tikslais.
 - 8.6.2. Duomenis, dėl Kandidatų duomenų bazės būsimoms atrankoms formavimo, kai gautas atskiras Kandidato sutikimas.
- 8.7. Priimtų Kandidatų Duomenys turi būti sunaikinami, išskyrus:
 - 8.7.1. Duomenis dėl sprendimo įdarbinti priežasčių.
 - 8.7.2. Darbuotojo gyvenimo aprašymą.
 - 8.7.3. Asmens duomenis, dėl kurių tvarkymo Kandidatas sutiko atskiru sutikimu.
 - 8.7.4. Duomenis, būtinus įdarbinimui.

9. SLAPUKŲ NAUDOJIMAS

- 9.1. Duomenų valdytojas savo interneto tinklapyje naudoja slapukus (ir panašias technologijas), kurie yra automatiškai patalpunami tinklapį naršančių Duomenų subjektų naršyklėse ar įrenginiuose tada, jei tokia funkcija yra aktyvuota jų naršyklės nustatymuose.
- 9.2. Duomenų valdytojas naudoja slapukus šiems tikslams pasiekti:
 - 9.2.1. Analizė: Duomenų valdytojas naudoja slapukus tam, kad galėtų suskaičiuoti unikalių tinklapio lankytojų skaičių ir rengti statistiką apie svetainės veikimą bei funkcionalumą. Naudojama programinė įranga išsaugo informaciją apie pateikiamus puslapio parodymus ir informaciją apie Duomenų subjektų geografinę padėtį, įrenginį, operacinę sistemą bei naršyklę.
 - 9.2.2. Prisijungimo paslaugos: Jei tinklapyje yra galimybė pasinaudoti prisijungimo paslauga, Duomenų valdytojas saugo ID numerį ir prisijungimo laiką slapuke Duomenų subjekto naršyklėje ar įrenginyje. Dėl to šiam nereikia iš naujo prisijungti kiekvieną kartą atidarius tinklapį.
 - 9.2.3. Interesais pagrįsta reklama internete: Duomenų subjektams gali būti pateikiamos bendrovių, priklausančių Orkla Group, reklamos dėl slapukų, išsaugotų jų naršyklėje ar

įrenginyje. Tokia reklama dažniausiai grindžiama naudotu turiniu, informacija apie Duomenų subjektą arba šio geografinę padėtimi. Tai pakartotinės rinkodaros technologija ir produktas, pateikiamas Duomenų valdytojui trečiųjų šalių, tokių kaip Google ar Facebook.

- 9.2.4. Dvigubi profiliai: Duomenų valdytojas grindžia dvigubų profilių kūrimą elgsenos duomenimis, surinktais iš jo tinklapių. Atsižvelgdamas į žinias, kurias turi apie vieną grupę Duomenų subjektų, Duomenų valdytojas siekia supažindinti Duomenų subjektus su naujais segmentais, kuriais besidomintieji turi panašius interesus bei elgesį kaip ir pradinė Duomenų subjektų grupė.
- 9.3. Konkretūs slapukai, jų funkcijos ir saugojimo terminai yra nurodyti Duomenų valdytojo svetainėje pateikiamame pranešime. Šiuo pranešimu Duomenų subjektai yra informuojami apie slapukų naudojimą ir išreiškia sutikimą dėl slapukų naudojimo. Duomenų valdytojo svetainė turi mechanizmus, kurių pagalba sutikimas būtų gaunamas anksčiau nei slapukai ar panašios technologijos yra aktyvuojami. Duomenų valdytojui tenka pareiga tinkamai įgyvendinti šias priemones praktiškai.
- 9.4. Duomenų subjektai, naršantys Duomenų valdytojo svetainę, gali savanoriškai pasirinkti sutikti su slapukų naudojimu per savo naršyklės ar įrenginio nustatymus. Savo svetainės nustatymuose Duomenų subjektai gali pasirinkti, kokius slapukus naršyklė atsisiunčia. Ten jie taip pat gali ištrinti visus esamus slapukus kurie yra saugomi naršyklėje ar įrenginyje.
- 9.5. Orkla ASA sudaro daug įmonių, gaminančių maisto papildus ir maisto produktus vartotojams bei įmonėms. Šios įmonės yra bendri slapukų pagalba gaunamų Asmens duomenų valdytojai.

10. DUOMENŲ SUBJEKTŲ TEISĖS

10.1. Duomenų subjektas BDAR ir ADTAĮ nustatyta tvarka gali įgyvendinti šias teises:

- 10.1.1. Teisės būti informuotam;
- 10.1.2. Prieigos teisės;
- 10.1.3. Ištrynimo teisės;
- 10.1.4. Teisės į patikslinimą;
- 10.1.5. Teisės apriboti duomenų tvarkymą;
- 10.1.6. Teisės į duomenų perkeliamumą;
- 10.1.7. Teisės prieštarauti;
- 10.1.8. Teisių, susijusių su automatiniu sprendimų priėmimu ir profiliavimu.

10.2. Aukščiau nurodyti ir BDAR įtvirtinti laikotarpiai yra tokie:

Duomenų subjekto prašymas	Laikotarpis
Teisė būti informuotam	Kai duomenys surenkami (jei pateikti Duomenų subjekto) arba per vieną mėnesį (jei pateikti ne Duomenų subjekto)
Prieigos teisė	Vienas mėnuo
Teisė į patikslinimą	Vienas mėnuo
Ištrynimo teisė	Nepagrįstai nedelsiant
Teisė apriboti duomenų tvarkymą	Nepagrįstai nedelsiant
Teisė į duomenų perkeliamumą	Vienas mėnuo
Teisė prieštarauti	Gavus prieštaravimą

Teisės, susijusios su automatiniu sprendimų priėmimu ir profiliavimu	Nenurodyta
--	------------

Lentelė 1 – Laikotarpiai Duomenų subjektų prašymams vykdyti

- 10.3. Duomenų valdytojas turi informuoti Duomenų subjektus apie jų teises aiškia, glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba.
- 10.4. Duomenų valdytojas turi teisę motyvuotai atsisakyti leisti Duomenų subjektui įgyvendinti jo teises arba imti pagrįstą mokesį esant BDAR 12 straipsnio 5 d. (b) punkte numatytoms aplinkybėms.

11. TECHNINĖS IR ORGANIZACINĖS ASMENS DUOMENŲ SAUGUMO PRIEMONĖS

- 11.1. Įgyvendinamos organizacinės ir techninės duomenų saugumo priemonės užtikrina tokį saugumo lygį, kuris atitinka Duomenų valdytojo valdomų duomenų pobūdį ir jų tvarkymo keliamą riziką.
- 11.2. Esminiai reikalavimai, keliami duomenų saugumui užtikrinti:
 - 11.2.1. Visi Informacijos vienetai, kuriuose yra Asmens duomenų, turi turėti savo savininką – duomenų valdytoją. Toks savininkas yra atsakingas už Asmens duomenų tvarkymo keliamos rizikos įvertinimą ir tinkamo saugumo lygio užtikrinimą.
 - 11.2.2. Duomenų saugumas turi būti įvertintas kiekvienai duomenų tvarkymo veiklai (kaip ji apibrėžta Politikoje) atskirai.
 - 11.2.3. Visos Duomenų tvarkymo sistemos (Programos ir IT sistemos) turi turėti savo savininkus, atsakingus už duomenų saugumo reikalavimų, nustatytų pagal Duomenų valdytojo atliktą rizikos vertinimą, įgyvendinimą.
 - 11.2.4. Visos naujos Duomenų tvarkymo sistemos turi atitikti BDAR keliamus reikalavimus. Jei tikėtina, kad IT sistemoje bus tvarkomi Asmens duomenys dideliu mastu ar toks tvarkymas kelia didelę grėsmę, turi būti atliekamas Poveikio duomenų apsaugai vertinimas.
- 11.3. Duomenų valdytojas visais atvejais bus savarankiškai atsakingas už tinkamą Duomenų saugumą, tačiau neretai tai gali būti pasiekta tik bendradarbiaujant su IT sistemų savininku, IT paslaugų teikėju, paslaugų teikimo partneriu ar kitu prieigą prie sistemų turinčiu subjektu, dažniausiai veikiančiu kaip Duomenų valdytojas. Duomenų tvarkytojas (IT sistemos ar Programos savininkas) atitinkamai turės savarankišką pareigą užtikrinti tinkamą Duomenų saugumo lygį. Su tokiais Duomenų tvarkytojais bus pasirašomos Duomenų tvarkymo sutartys.
- 11.4. BDAR informacijos saugumą apibrėžia per tris rizikos valdymo tikslus:
 - 11.4.1. Konfidencialumas – Asmens duomenys turi būti prieinami tik asmenims, turintiems teisėtą pagrindą tokiai prieigai ir tik tiek, kiek apima jų atliekamo tvarkymo tikslas. Identifikavimas ir prieigos valdymas yra esminės konfidencialumo užtikrinimo priemonės.
 - 11.4.2. Vientisumas – Asmens duomenys turi būti tikslūs ir išsamūs. Jei Duomenų vientisumas yra pažeistas, sprendimai priimami dėl Duomenų subjekto gali būti paremti klaidinga ar neišsamia informacija.
 - 11.4.3. Pasiiekiamumas – pasiekiamumo poreikį nulemia verslo poreikiai ir Duomenų subjektas. Pasiiekiamumas yra tiek galimybė atkurti prarastus duomenis (iš laiku sukurtų atsarginių kopijų), tiek ir veiklos tęstinumo užtikrinimas.
- 11.5. Turi būti atliekamas su visais tvarkomais Duomenimis susijusios rizikos vertinimas, remiantis tokiais principais:

- 11.5.1. Rizikos vertinimas, įskaitant ir tam tikroje IT Sistemoje tvarkomų Asmens duomenų apžvalgą, turi būti aprašomas. Tai apima tvarkomų Duomenų pobūdį ir apimtį, galimas galinčios kilti žalos Duomenų subjektams grėsmes ir registruotų Duomenų subjektų skaičių.
- 11.5.2. Vertinant riziką ir galimą žalą Duomenų subjektams, konfidencialumo praradimas įprastai yra esminė vertintina rizika, bet kitos grėsmės, susijusios su vientisumu ir pasiekiamumu taip pat turi būti įvertintos.
- 11.5.3. Tuo atveju, jei tvarkomi Specialių kategorijų asmens duomenys arba Duomenys apie apkaltinamuosius nuosprendžius ar nusikalstamas veikas, didelė grėsmė yra laikoma neatsiejama nuo tokios veiklos dėl potencialios Duomenų subjektui galinčios kilti žalos.
- 11.6. Rizika gali būti sumažinama naudojantis tokiomis priemonėmis:
 - 11.6.1. Užtikrinant adekvatų saugumo lygį tam, kad kiek įmanoma sumažinti fizinio praradimo ir konfidencialumo praradimo riziką.
 - 11.6.2. Duomenis perduodant už jų pradinės Programos ribų, Pseudonimizavimas turėtų būti standartiškai taikomas tada, jei tai techniškai įmanoma ir jei tokiu atveju galima įgyvendinti tvarkymo tikslus.
 - 11.6.3. Jei galima spręsti, kad Asmens duomenų tvarkymo rezultatu bus jautri informacija (pvz. tyrimas dėl sukčiavimo ar vagystės), arba jei Asmens duomenų apimtis yra didelė, Pseudonimizavimas ir šifravimas visais atvejais turėtų būti naudojamas už pradinės Programos ribų.
- 11.7. Atsižvelgiant į aukščiau išdėstytus tikslus ir rizikos valdymo priemones, kiekvienam Informacijos vienetui, kuriame yra Asmens duomenys, taikytini tokie reikalavimai:
 - 11.7.1. Prieigos valdymas turi būti įgyvendintas taip, kad Asmens duomenys būtų prieinami tik asmenims, turintiems teisėtą pagrindą tokiai prieigai ir tik tiek, kiek apima jų atliekamo tvarkymo tikslas.
 - 11.7.2. Jei suteikiamos prieigos teisės yra platesnės nei būtina, turi būti įgyvendintos priemonės, užtikrinančios, kad Asmens duomenų tvarkymas nebūtų atliekamas be Duomenų valdytojo nurodymų.
 - 11.7.3. Jei tvarkomi didelę riziką turintys Asmens duomenys, turi būti įgyvendinama dviejų pakopų autentifikavimo sistema ar kitos priemonės, užtikrinančios panašų autentifikavimo saugumą.
 - 11.7.4. Jei Duomenų pasiekiamumas ir tikslumas yra labai reikšmingi Duomenų subjektų interesų užtikrinimui, priemonės užtikrinančios tinkamą tęstinumą ir atsarginių kopijų darymą turi būti įdiegtos, išbandytos ir aprašytos.
 - 11.7.5. Informacijos saugumo priemonės turi būti aprašytos ir reguliariai testuojamos, siekiant užtikrinti pakankamą jų efektyvumą.
 - 11.7.6. Didelę riziką turinčių Asmens duomenų atveju, jų informacijos saugumas aprašytas šios Politikos skyriuje 11.
- 11.8. Duomenų valdytojas priima vidaus nuostatas ir įgyvendinti priemones, kuriomis visų pirma būtų paisoma pritaikytosios ir standartizuotosios duomenų apsaugos principų.
- 11.9. Duomenų valdytojas turi veikti atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms.

- 11.10. Pritaikytoji duomenų apsauga reiškia, kad kiekviena nauja programa ar sistema naudojanti asmens duomenis turi būti kuriama atsižvelgiant į tokių duomenų apsaugą. Į privatumą turi būti atsižvelgiama per visą programos ar sistemos gyvavimo laiką.
- 11.11. Kaip priemonių, skirtų pritaikytajai duomenų apsaugai įgyvendinti, pavyzdžiai paminėtini:
- 11.11.1. Surinkto duomenų kiekio ribojimas;
 - 11.11.2. Kontrolės galimybė;
 - 11.11.3. Skaidrumas;
 - 11.11.4. Vartotojui draugiškos sistemos;
 - 11.11.5. Duomenų konfidencialumas;
 - 11.11.6. Duomenų kokybė;
 - 11.11.7. Pseudonimų suteikimas;
 - 11.11.8. Kuo skubesnis duomenų anonimizavimas;
 - 11.11.9. Galimybės stebėti duomenų tvarkymą suteikimas duomenų subjektams;
 - 11.11.10. Galimybės kurti ir tobulinti apsaugos priemones suteikimas;
 - 11.11.11. Tinkamas darbuotojų mokymas;
 - 11.11.12. Auditas ir politikos peržiūros asmens duomenų apsaugos kontekste;
 - 11.11.13. Duomenų naudojimo ribojimas.
- 11.12. Standartizuotoji duomenų apsauga kelia reikalavimą taikyti griežčiausius privatumo nustatymus tam tikrai programai ar sistemai kai tik ta programa ar sistema tampa prieinama.
- 11.13. Kaip priemonių, skirtų standartizuotajai duomenų apsaugai įgyvendinti, pavyzdžiai paminėtini:
- 11.13.1. Standartizuotai tvarkomi tik tie duomenys, kurie yra būtini konkrečiam duomenų tvarkymo tikslui;
 - 11.13.2. Technologiniai sprendimai turi būti kuriami taip, kad būtų galima išvengti nereikalingo duomenų tvarkymo;
 - 11.13.3. Duomenų apsaugai draugiški numatytieji nustatymai;
 - 11.13.4. Funkcijos, kurios nėra būtinos paslaugos teikimui, turi būti konfigūruojamos.
- 11.14. Šiomis priemonėmis siekiama veiksmingai įgyvendinti duomenų apsaugos principus, kaip antai duomenų kiekio mažinimo principą, ir į duomenų tvarkymą integruoti būtinas apsaugos priemones, kad jis atitiktų BDAR reikalavimus ir apsaugotų duomenų subjektų teises.
- 11.15. Duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kuriomis užtikrina, kad standartizuotai būtų tvarkomi tik tie Asmens duomenys, kurie yra būtini kiekvienam konkrečiam duomenų tvarkymo tikslui. Ta prievolė taikoma surinktų asmens duomenų kiekiui, jų tvarkymo apimčiai, jų saugojimo laikotarpiui ir jų prieinamumui. Visų pirma tokiomis priemonėmis užtikrinama, kad standartizuotai be fizinio asmens įsikišimo su Asmens duomenimis negalėtų susipažinti neribotas fizinių asmenų skaičius.
- 11.16. Duomenų valdytojas gali remtis patvirtintu sertifikavimo mechanizmu, jei toks bus, kaip priemone įrodyti aukščiau išdėstytų reikalavimų laikymąsi.
- 11.17. Jei nauja Programa ar IT sistema apima naujus Asmens duomenų tvarkymo metodus, Duomenų tvarkymą dideliu mastu ir/ar Specialių kategorijų asmens duomenis arba duomenis apie teistumą, turi būti atliekamas PDAV. Toks vertinimas turi būti atliekamas vadovaujantis šiomis gairėmis:

- 11.17.1. BDAR kelia tam tikrus reikalavimus PDAV, be kita ko išankstinę konsultaciją su priežiūrą atliekančia institucija;
 - 11.17.2. Kai rizikos vertinimas leidžia spręsti apie didelę riziką, turi būti konsultuojamasi su grupės teisės/atitikties skyriaus atstovais dėl PDAV atlikimo būtinybės ir šie įtraukiami į patį vertinimą.
 - 11.17.3. Duomenų valdytojas atsakingas už PDAV atlikimą, kai toks yra reikalingas.
 - 11.17.4. Programos savininkas yra atsakingas už PDAV poreikio įvertinimą ir atlikimą analizės etapo metu, o tokios veiklos aprašymas turėtų būti saugomas kaip BDAR atitikties dokumentacijos dalis.
- 11.18. Duomenų valdytojas naujos ar atnaujintos programos ar sistemos kūrimo pradžioje įvertina, ar yra reikalingas poveikio duomenų apsaugai vertinimas.

12. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO IR REAGAVIMO Į TOKIUS PAŽEIDIMUS TVARKA

- 12.1. Duomenų valdytojo Darbuotojai, turintys prieigos teisę prie Duomenų, pastebėję Duomenų saugumo pažeidimus (asmens neveikimą ar veiksmus, galinčius sukelti ar sukeliančius grėsmę Duomenų saugumui), turi informuoti Atsakingą darbuotoją ir (ar) savo tiesioginį vadovą.
- 12.2. Įvertinęs Duomenų apsaugos pažeidimo rizikos veiksnius, pažeidimo poveikio laipsnį, žalą ir padarinius, Duomenų valdytojas priima sprendimus dėl priemonių, reikiamų Duomenų apsaugos pažeidimui ir jo padariniams pašalinti.

13. DUOMENŲ PERDAVIMAS

- 13.1. Duomenų valdytojas, norėdamas skirti trečiąjį asmenį Duomenų tvarkytoju, privalo:
 - 13.1.1. sudaryti su Duomenų tvarkytoju sutartį, kurioje būtų pateikta punkte išvardyta informacija;
- 13.2. Asmens duomenų perdavimas Duomenų tvarkytojams galimas tik sudarius tinkamas sutartis tarp Tvarkytojų ir Duomenų valdytojo.
- 13.3. Duomenų valdytojas privalo kontroliuoti, ar Duomenų tvarkytojas vykdo sutartyje nurodytus įsipareigojimus.
- 13.4. Sutartys privalo apimti šią informaciją:
 - 13.4.1. Duomenų tvarkymo dalykas;
 - 13.4.2. Duomenų tvarkymo trukmė;
 - 13.4.3. Duomenų tvarkymo pobūdis;
 - 13.4.4. Duomenų tvarkymo tikslas;
 - 13.4.5. Duomenų rūšys;
 - 13.4.6. Duomenų subjektų kategorijos;
 - 13.4.7. Šalių teisės ir pareigos, kylančios iš asmens duomenų apsaugos teisinio reguliavimo;
 - 13.4.8. Duomenų tvarkytojo darbuotojų konfidencialumo įsipareigojimai;
 - 13.4.9. Duomenų tvarkymo saugumo priemonės;
 - 13.4.10. Kitų Duomenų tvarkytojų pasitelkimas;
 - 13.4.11. Pagalba įgyvendinant Duomenų subjektų teises;
 - 13.4.12. Pagalba teikiant pranešimus apie Duomenų saugumo pažeidimus;

13.4.13. Auditavimo galimybė.

- 13.5. Asmens duomenys gali būti perduodami į trečiąją šalį arba tarptautinei organizacijai, kurios teisinis reglamentavimas Europos Komisijos pripažintas užtikrinančiu adekvatų Asmens duomenų apsaugos lygį. Perdavimas į adekvatų subjektą gali vykti be jokio papildomo Komisijos ar valstybių narių leidimo.
- 13.6. Asmens duomenys į trečiąsias šalis arba tarptautinėms organizacijoms taip pat gali būti perduodami pritaikius vieną ar daugiau iš žemiau nurodytų tinkamų apsaugos priemonių:
- 13.6.1. Standartinės sutarčių sąlygos dėl Duomenų apsaugos, priimtose Europos Komisijos;
- 13.6.2. Standartinės sutarčių sąlygos dėl Duomenų apsaugos, priimtose Priežiūros institucijos, arba Priežiūros institucijos pripažintos sutarties sąlygos;

14. ATSAKOMYBĖ

- 14.1. Darbuotojams, kurie pažeidžia BDAR, VDAĮ, ERĮ ir kitus teisės aktus, reglamentuojančius Asmens duomenų tvarkymą bei apsaugą, arba Politikoje nurodytas pareigas, taikoma Lietuvos Respublikos įstatymų nustatyta atsakomybė.

15. BAIGIAMOSIOS NUOSTATOS

- 15.1. Už Politikos patvirtinimą atsakingas Duomenų valdytojo vadovas. Už įgyvendinimą, jos vykdymo kontrolę, atnaujinimą, kitų šiose Taisyklėse įvardintų veiksmų atlikimą yra atsakingas Duomenų valdytojo vadovas ar jo paskirtas darbuotojas savo kompetencijos ribose.
- 15.2. Politika įsigalioja jas patvirtinus Duomenų valdytojo vadovui.
- 15.3. Politika gali būti peržiūrima kartą per kalendorinius metus Duomenų valdytojo iniciatyva ir (arba) keičiantis teisės aktams, reguliuojantiems asmens duomenų tvarkymą.
- 15.4. Politika ir jos pakeitimai įsigalioja nuo jų patvirtinimo dienos.
- 15.5. Paskutinė Politikos peržiūra vykdyta 2018 m. gegužės 25 d.