Drög — lögfræðileg yfirferð stendur yfir · Drög 0.9

VAKTO

Vinnslusamningur (DPA)

Samningur um vinnslu persónuupplýsinga samkvæmt 28. gr. reglugerðar (ESB) 2016/679 (GDPR) og 25. gr. laga nr. 90/2018.

Vinnsluaðili: BGL Ventures ehf., kt. 490806-0400, sem rekur VAKTO · hallo@vakto.is · Síðast uppfært 18. nóvember 2026 · Gildandi útgáfa: vakto.is/personuvernd/vinnslusamningur

1. Aðilar og gildissvið

- **Ábyrgðaraðili:** Viðskiptavinur VAKTO (fyrirtæki, stofnun eða sveitarfélag) sem hefur gert áskriftarsamning um VAKTO og skráir starfsfólk sitt í kerfið.
- **Vinnsluaðili:** BGL Ventures ehf., kt. 490806-0400, sem rekur VAKTO („VAKTO“).

Samningur þessi er hluti af skilmálum VAKTO (vakto.is/skilmalar) og gildir um alla vinnslu persónuupplýsinga sem VAKTO annast fyrir hönd ábyrgðaraðila. Gangi ákvæði þessa samnings lengra en skilmálarnir um vernd persónuupplýsinga gildir þessi samningur. Hugtök hafa sömu merkingu og í GDPR og lögum nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga.

2. Efni, eðli, tilgangur og tímalengd vinnslu

VAKTO vinnur persónuupplýsingar eingöngu til að veita þjónustuna: vaktaplan, stimpilklukku (app, vefur og kiosk), tímaskráningu, launaútreikning og útflutning í launakerfi, frí- og vaktaskiptabeiðnir, ráðningarsamninga og rafræna undirritun, skjalasafn, spjall og fréttaveitu innan vinnustaðarins, starfsmannaskírteini, tilkynningar og, ef ábyrgðaraðili leyfir, gervigreindaraðstoð (VAKTO AI).

Vinnslan felst í söfnun, skráningu, geymslu, uppflettingu, útreikningi, miðlun til notenda innan fyrirtækis ábyrgðaraðila, útflutningi að fyrirmælum hans og eyðingu. Vinnslan varir á meðan áskrift er virk og þar til gögnum hefur verið skilað og eytt samkvæmt 11. gr.

3. Flokkar skráðra einstaklinga

- Starfsfólk ábyrgðaraðila, þ.m.t. fyrrverandi starfsfólk, tímavinnufólk og verktakar sem skráðir eru í kerfið.
- Stjórnendur og vaktstjórar ábyrgðaraðila sem nota kerfið.
- Aðstandendur starfsfólks að því marki sem nafn og sími tengiliðs í neyð er skráð.
- Viðskiptavinir ábyrgðaraðila að því marki sem nöfn og heimilisföng verkkaupa eru skráð í VAKTO Verk.

4. Tegundir persónuupplýsinga

- Auðkenni og samskiptaupplýsingar: nafn, kennitala, netfang, sími, heimilisfang, prófílmynd, tengiliður í neyð.
- Ráðningarupplýsingar: staða, deild, vinnustaður, starfshlutfall, ráðningardagur og starfslok, ráðningarsamningar og undirritun þeirra.

- Launaupplýsingar: launaform, taxtar, kjarasamningur, lífeyrissjóður, bankareikningur, launaútreikningar, launaseðlar og launakeyrslur.
- Vinnutími: vaktir, stimplanir (tími og uppruni), frávik, tímabanki, orlofs- og veikindastaða, frí- og vaktaskiptabeiðnir.
- Staðsetning við stimplun, aðeins ef ábyrgðaraðili krefst þess: ein staðsetning við inn- og útstimplun, engin rakning þess á milli.
- Samskipti innan vinnustaðarins: spjallskilaboð, myndir, talskilaboð, færslur og athugasemdir.
- Tæknilegar upplýsingar: innskráningar, auðkenni tækis fyrir tilkynningar og aðgerðaskrá.

Sérstakir flokkar persónuupplýsinga (9. gr. GDPR, 3. tl. 3. gr. laga nr. 90/2018) geta verið unnir: aðild að stéttarfélagi (vegna kjarasamninga og iðgjalda) og upplýsingar um veikindi (veikindadagar og veikindi barna). Ábyrgðaraðili ber ábyrgð á heimild til vinnslunnar og á því að skrá ekki meira en nauðsynlegt er, t.d. ekki sjúkdómsgreiningar. Kennitölur eru unnar á grundvelli 13. gr. laga nr. 90/2018.

5. Skyldur vinnsluaðila

- Fyrirmæli: VAKTO vinnur persónuupplýsingar eingöngu samkvæmt skjalfestum fyrirmælum ábyrgðaraðila. Notkun ábyrgðaraðila á kerfinu, stillingar hans (þ.m.t. Gagnastefna) og þessi samningur teljast fyrirmæli. Telji VAKTO fyrirmæli brjóta gegn persónuverndarlöggjöf lætur VAKTO ábyrgðaraðila vita án tafar.
- Trúnaður: starfsfólk VAKTO sem hefur aðgang að persónuupplýsingum er bundið þagnarskyldu. Aðgangur er aðeins veittur þegar þörf krefur, t.d. vegna þjónustubeiðni ábyrgðaraðila eða bilunar.
- Öryggi: VAKTO viðhefur tæknilegar og skipulagslegar ráðstafanir samkvæmt 32. gr. GDPR, sbr. 10. gr.
- Undirvinnsluaðilar: VAKTO notar aðeins þá undirvinnsluaðila sem taldir eru upp í 8. gr. og leggur á þá sambærilegar skyldur með skriflegum samningi.
- Réttindi skráðra einstaklinga: VAKTO aðstoðar ábyrgðaraðila við að svara beiðnum um aðgang, leiðréttingu, eyðingu, takmörkun og flutning gagna. Gögn má flytja út úr kerfinu (Excel, PDF, launaskrár). Berist beiðni beint til VAKTO er henni vísað til ábyrgðaraðila.
- Aðstoð: VAKTO aðstoðar ábyrgðaraðila við að uppfylla skyldur samkvæmt 32.–36. gr. GDPR, þ.m.t. mat á áhrifum á persónuvernd og fyrirframsamráð við Persónuvernd, eftir því sem sanngjarnt er miðað við eðli vinnslunnar.
- Upplýsingar og úttektir: sbr. 12. gr.

6. Skyldur ábyrgðaraðila

- Ábyrgðaraðili tryggir að heimild sé fyrir vinnslunni og að skráðir einstaklingar (starfsfólk) fái fræðslu um hana.
- Ábyrgðaraðili ákveður hvaða gögn eru skráð, hverjir fá aðgang í kerfinu (hlutverk og aðgangur vaktstjóra) og hvaða tengingar og gervigreindaraðgerðir eru leyfðar (Gagnastefna).
- Ábyrgðaraðili ber ábyrgð á réttmæti gagnanna og á gögnum sem hann flytur úr VAKTO í önnur kerfi.

7. Gervigreind og stýring ábyrgðaraðila (Gagnastefna)

Eigandi aðgangs ábyrgðaraðila getur í Stillingum → Tengingar → Gagnastefna ákveðið eftirfarandi. Stillingunum er framfylgt á þjónum VAKTO, ekki aðeins í viðmótinu, og hver breyting er skráð í aðgerðaskrá:

- VAKTO AI fyrir stjórnendur (sjálfgefið kveikt). Slökkt: engin gögn eru send til gervigreindarþjónustu af vefnum, þ.m.t. AI-vaktaplan, skýrslur og lestur kjarasamninga.
- VAKTO AI fyrir starfsfólk í appinu (sjálfgefið kveikt). Starfsmaður sér aðeins eigin vaktir og tíma og hverjir eru lausir, aldrei laun eða ástæður fjarveru annarra. Sé slökkt á VAKTO AI fyrir annan hvorn hópinn er þýðing spjallskilaboða einnig óvirk.
- Vefleit VAKTO AI (sjálfgefið kveikt): aðeins á síðum stéttarfélaga og opinberra aðila, t.d. til að finna launatöflur.

- Kennitölur og bankareikningar fjarlægðir úr gögnum sem fara til gervigreindar (sjálfgefið kveikt).
- Tengd forrit (MCP) og API-lyklar: þegar slökkt er hafnar VAKTO öllum tengingum og lyklum ábyrgðaraðila, líka þeim sem þegar eru til.

Gervigreindin (Anthropic) fær aðeins þau gögn sem þarf til að svara hverri spurningu, gögnin eru ekki notuð til að þjálfa líkön og þau eru geymd hjá Anthropic aðeins í takmarkaðan tíma samkvæmt skilmálum hennar. Tillögur gervigreindar að breytingum (t.d. vöktum) eru aldrei framkvæmdar nema notandi staðfesti þær, og hver framkvæmd aðgerð er skráð í aðgerðaskrá ásamt hverju kalli tengdra forrita (heiti verkfæris, notandi og forrit, en ekki gögnin sjálf).

Tengd gervigreindarforrit (t.d. Claude eða ChatGPT) sem stjórnandi tengir sjálfur að fengnu leyfi eiganda eru ekki undirvinnsluaðilar VAKTO. Þau fá lesaðgang, aldrei kennitölur, bankareikninga eða heimilisföng, og um gögnin gilda skilmálar þess sem rekur forritið.

8. Undirvinnsluaðilar

Ábyrgðaraðili veitir almenna skriflega heimild til að nota eftirfarandi undirvinnsluaðila:

Aðili	Tilgangur	Gögn	Staðsetning	Hvenær
Supabase Inc.	Gagnagrunnur, auðkenning, skráageymsla og rauntímatengingar	Öll gögn sem skráð eru í VAKTO	ESB — Írland (AWS eu-west-1)	Alltaf
Vercel Inc.	Hýsing vefsins og keyrsla kerfisins (þjónar, CDN)	Öll gögn sem fara um kerfið á leið til og frá notanda; aðgangsskrár (IP-tala)	ESB (Dublin); stýrilag í Bandaríkjunum undir SCC	Alltaf
Resend Inc.	Sending tölvupósta úr kerfinu (boð, plan birt, samningar, skýrslur)	Nafn, netfang og efni póstsins	Bandaríkin/ESB undir SCC	Alltaf
Anthropic PBC	Gervigreind: VAKTO AI fyrir stjórnendur og starfsfólk, AI-vaktaplan, lestur kjarasamninga, drög að samningsákvæðum, skýrslur og þýðing spjallskilaboða	Spurningin og þau rekstrargögn sem þarf til að svara (vaktir, tímar, launakostnaður, nöfn). Kennitölur og bankareikningar eru fjarlægðir sjálfgefið. Ekki notað til að þjálfa líkön.	Bandaríkin undir SCC	Aðeins þegar gervigreind er notuð. Ábyrgðaraðili getur slökkt á henni í Gagnastefnu; þýðing spjalls stöðvast ef slökkt er á VAKTO AI fyrir annan hvorn hópinn.
650 Industries Inc. (Expo)	Sending push-tilkynninga í VAKTO-appið; áframsent til Apple (APNs) og Google (Firebase Cloud Messaging)	Auðkenni tækis, fyrirsögn og texti tilkynningar	Bandaríkin undir SCC	Ef notandi leyfir tilkynningar í appinu
Apple Inc., Google LLC, Mozilla (vafratilkynningar)	Push-tilkynningar í vafra (Web Push) og Wallet-skírteini	Auðkenni áskriftar vafra, texti tilkynningar; á skírteini: nafn, staða, deild, starfsmannanúmer	Bandaríkin/ESB samkvæmt skilmálum hvers aðila	Aðeins ef notandi kveikir á tilkynningum í vafra eða setur skírteini í veskið
Taktikal ehf.	Undirritun ráðningarsamninga með rafrænum skilríkjum	Nafn, kennitala og símanúmer undirritara og skjalið sjálft	Ísland	Aðeins ef ábyrgðaraðili velur rafræn skilríki

Aðili	Tilgangur	Gögn	Staðsetning	Hvenær
Já hf. (Gagnatorg)	Uppfletting í Þjóðskrá eftir kennitölu við skráningu starfsmanns	Kennitala (fyrirspurn); nafn og heimilisfang (svar, ekki vistað nema stjórnandi vistar)	Ísland	Aðeins þegar stjórnandi notar uppflettinguna

VAKTO tilkynnir ábyrgðaraðila um fyrirhugaða nýja eða breytta undirvinnsluaðila með a.m.k. 30 daga fyrirvara (tölvupóstur til eiganda og á þessari síðu). Ábyrgðaraðili getur andmælt á því tímabili; náist ekki sátt getur hann sagt áskrift upp án kostnaðar. VAKTO ber ábyrgð gagnvart ábyrgðaraðila á efndum undirvinnsluaðila.

Ekki undirvinnsluaðilar

- Straumur (Kvika banki hf.) — greiðslusíða og kortageymsla fyrir áskriftargjald ábyrgðaraðila. VAKTO er ábyrgðaraðili þeirrar vinnslu.
- Payday ehf. — reikningar VAKTO til ábyrgðaraðila (bókhald BGL Ventures ehf.).
- Cloudflare Turnstile — vörn gegn sjálfvirkum nýskráningum á opna vefnum.
- Google Analytics og Meta Pixel — aðeins á opna vefnum og aðeins með samþykki gests; aldrei inni í kerfinu.
- OpenStreetMap (Nominatim) og OpenFreeMap — kort og leit að heimilisföngum vinnustaða.
- Tengingar sem ábyrgðaraðili velur sjálfur (Payday, DK eða H3 Laun fyrir laun, Inventra, kassakerfi um API-lykla og tengd gervigreindarforrit um MCP): gögnin fara þangað að fyrirmælum ábyrgðaraðila og um vinnsluna gilda samningar hans við viðkomandi aðila.

9. Flutningur út fyrir EES

Gagnagrunnur og skráageymsla eru á Írlandi. Þegar undirvinnsluaðili vinnur gögn utan EES byggir flutningurinn á staðlaðum samningsskilmálum framkvæmdastjórnar ESB (SCC) og, eftir atvikum, EU–US Data Privacy Framework, ásamt viðbótarráðstöfunum eins og dulkóðun í flutningi.

10. Öryggisráðstafanir

- Hýsing á EES (Írland); öll samskipti dulkóðuð (TLS) og gögn dulkóðuð í hvíld hjá hýsingaraðila.
- Aðskilnaður fyrirtækja í gagnagrunni með row level security: hver fyrirspurn er afmörkuð við fyrirtæki og hlutverk notanda.
- Aðgangsstýring eftir hlutverkum (eigandi, vaktstjóri, starfsmaður, verktaki) og aðgangur vaktstjóra per svæði. Starfsfólk sér aldrei laun, kennitölur eða bankareikninga samstarfsfólks.
- Lyklar þjónustunnar eru aðeins á þjóni. API-lyklar og aðgangslyklar tengdra forrita eru geymdir sem SHA-256 tætigildi; lotur tengdra forrita eru dulkóðaðar (AES-256-GCM).
- Kortanúmer fara aldrei um kerfi VAKTO (tokenization hjá greiðsluveitu).
- Aðgerðaskrá yfir mikilvægar aðgerðir, þ.m.t. launakeyrslur, breytingar á starfsfólki, aðgerðir gervigreindar og köll tengdra forrita.
- Vörn gegn sjálfvirkum nýskráningum, takmörkun á fjölda fyrirspurna og kiosk-stimpilklukka varin með leynilykli fyrirtækisins.
- Regluleg öryggisafrit hjá hýsingaraðila.

11. Öryggisbrestir, varðveisla og eyðing

Öryggisbrestir

Verði VAKTO var við öryggisbrest sem varðar persónuupplýsingar ábyrgðaraðila tilkynnir VAKTO honum það án ótilhlýðilegrar tafar og eigi síðar en 48 klukkustundum eftir að VAKTO varð hans var, svo ábyrgðaraðili geti tilkynnt Persónuvernd innan 72 klukkustunda. Tilkynningin lýsir eðli brestsins, flokkum og áætluðum fjölda skráðra einstaklinga og færslna, líklegum afleiðingum og ráðstöfunum sem gripið hefur verið til, og VAKTO veitir frekari upplýsingar jafnóðum.

Varðveisla og eyðing

- Gögn eru varðveitt á meðan áskrift er virk. Ábyrgðaraðili getur eytt einstökum gögnum (t.d. starfsfólki, samtölum við VAKTO AI) í kerfinu.
- Við lok áskriftar getur ábyrgðaraðili flutt gögnin út. Gögnum er eytt innan 90 daga frá lokum áskriftar nema lög krefjist lengri varðveislu; eyðing úr öryggisafritum fylgir hringrás þeirra.
- Aðgerðaskrá og öryggisskrár eru varðveittar í allt að 12 mánuði.

12. Upplýsingar og úttektir

VAKTO veitir ábyrgðaraðila þær upplýsingar sem nauðsynlegar eru til að sýna fram á að skyldur samkvæmt 28. gr. GDPR séu uppfylltar og heimilar úttektir ábyrgðaraðila eða úttektaraðila á hans vegum, með sanngjörnum fyrirvara (að jafnaði 30 dögum), á venjulegum vinnutíma og að hámarki einu sinni á ári nema öryggisbrestur gefi tilefni til. Ábyrgðaraðili ber kostnað af úttekt. Úttektaraðili skal bundinn trúnaði.

13. Gildistími, lög og varnarþing

Samningurinn gildir á meðan VAKTO vinnur persónuupplýsingar fyrir ábyrgðaraðila. Ákvæði sem eðli máls samkvæmt eiga að gilda áfram (trúnaður, eyðing) gilda eftir lok hans. Um samninginn gilda íslensk lög. Ágreiningur sem ekki leysist með samkomulagi skal rekinn fyrir Héraðsdómi Reykjavíkur.

Ábyrgðaraðili sem þarf undirritað eintak (t.d. sveitarfélag eða ríkisstofnun) getur óskað eftir því á hallo@vakto.is; samningurinn er þá undirritaður af báðum aðilum og fylgir áskriftarsamningi.

Undirritun

Fyrir hönd ábyrgðaraðila

Nafn, kennitala ábyrgðaraðila

Staður og dagsetning

Fyrir hönd vinnsluaðila

BGL Ventures ehf., kt. 490806-0400

Staður og dagsetning