Öryggisspurningar birgja, svör Varhuga

Svörin eru þau sömu og birt eru á varhugi.is/oryggi og gilda þann dag sem skjalið er sótt. Nýjasta útgáfan er alltaf á þeirri síðu.

1. Hvaða gögn eru geymd

Nafn, netfang, deild og hlutverk starfsfólks; námsframvinda, niðurstöður prófa og skírteini; tilkynningar um grunsamleg skilaboð og staðfestingar á stefnum sem starfsfólk sendir inn; innskráningarfærslur (tími, IP-tala, vafri). Ekkert annað.

marketing.vinnslusamningur.sections.data_body

marketing.vinnslusamningur.sections.scope_body

Sjá nánar: Flokkar gagna í vinnslusamningi

2. Hvar gögnin eru hýst

Hjá Vercel, með gagnagrunn hjá Neon í Frankfurt, innan EES. Gagnagrunn má endurheimta á tiltekið tímamark og útgáfur má taka til baka samstundis.

Þjónustan keyrir hjá Vercel. Gögn eru geymd í gagnagrunni hjá Neon í Frankfurt í Þýskalandi og útgefin skírteini í skráageymslu Vercel, einnig í Frankfurt, hvort tveggja innan Evrópska efnahagssvæðisins. Tölvupóstur, svo sem innskráningarhlekkir og áminningar, fer um Resend.

Sumir undirvinnsluaðilar eru bandarísk félög. Eigi flutningur persónuupplýsinga út fyrir EES sér stað byggist hann á stöðluðum samningsákvæðum framkvæmdastjórnar ESB (Standard Contractual Clauses, SCC) eða þátttöku viðkomandi aðila í EU-US Data Privacy Framework.

Einingar: Forritið keyrir hjá Vercel í Frankfurt og öll varanleg gögn, gagnagrunnur og útgefin skírteini, eru hýst þar líka, innan EES. Skyndiminni fyrir aðgangstakmarkanir geymir aðeins tætt auðkenni (hash), aldrei netföng eða IP-tölur í hreinum texta. Varhugi rekur enga eigin netþjóna.

Sjá nánar: Hýsing

3. Auðkenning

Engin lykilorð. Innskráningarhlekkur í tölvupósti eða SSO með Microsoft og Google þar sem ykkar fjölþátta auðkenning gildir. Hlutverkin stjórnandi, deildarstjóri og starfsmaður. Lotur eru geymdar á þjóni og stjórnendur skráðir út eftir fjögurra klukkustunda aðgerðaleysi.

Engin lykilorð: Varhugi geymir engin lykilorð. Innskráning fer fram með innskráningarhlekk í tölvupósti eða innskráningarkerfi vinnustaðarins, svo það er ekkert lykilorðasafn sem getur lekið.

SSO með Microsoft og Google: Starfsfólk skráir sig inn með Microsoft Entra ID eða Google-reikningi vinnustaðarins og þá gilda fjölþátta auðkenning (MFA) og aðgangsreglur fyrirtækisins sjálfs við innskráningu. Varhugi er ekki með eigin fjölþátta auðkenningu; með innskráningarhlekk í tölvupósti byggist öryggið á aðgangi að pósthólfinu. Lokaður reikningur kemst ekki lengur inn, en viðkomandi er áfram skráður í Varhuga þar til hann er fjarlægður undir Starfsfólk eða gerður óvirkur með SCIM.

Hlutverkaskipt réttindi: Réttindi fara eftir hlutverki. Almennt starfsfólk sér aðeins eigin þjálfun og stjórnendur sjá stöðu síns fyrirtækis, ekki annarra.

Aðskilnaður milli fyrirtækja: Gögn hvers fyrirtækis eru aðskilin frá öðrum og allar fyrirspurnir eru bundnar við fyrirtæki innskráðs notanda.

Innskráning og lotur: Notendur skrá sig inn með einnota hlekk sem sendur er í tölvupósti og gildir í 15 mínútur, eða með Microsoft- eða Google-innskráningu (SSO). Varhugi geymir engin lykilorð. Réttindi sem byggja á netfangi, boð og skráningartenglar, eru aðeins veitt netföngum sem hafa verið sannreynd. Lotur eru geymdar á þjóninum, gilda að hámarki 30 daga og þeim lýkur um leið og notandi skráir sig út. Lotum stjórnenda og deildarstjóra er auk þess lokað eftir fjögurra klukkustunda aðgerðaleysi.

Sjá nánar: Innskráning og aðgangsstýring

4. Stofnun og brottfelling notenda

SSO-notendur bætast sjálfkrafa við og hlutverk fylgja þeim sem skilgreind eru í Entra (app roles). SCIM-tenging við Entra ID stofnar notendur og gerir þá óvirka sjálfkrafa þegar aðgangur á ekki lengur að vera virkur; óvirkir halda sögunni og losa sætið.

Starfsfólk skráir sig inn með Microsoft Entra ID eða Google-reikningi vinnustaðarins og þá gilda fjölþátta auðkenning (MFA) og aðgangsreglur fyrirtækisins sjálfs við innskráningu. Varhugi er ekki með eigin fjölþátta auðkenningu; með innskráningarhlekk í tölvupósti byggist öryggið á aðgangi að pósthólfinu. Lokaður reikningur kemst ekki lengur inn, en viðkomandi er áfram skráður í Varhuga þar til hann er fjarlægður undir Starfsfólk eða gerður óvirkur með SCIM.

Sjá nánar: Leiðbeiningar um SCIM

5. Dulkóðun

TLS á allri umferð, dulkóðun í hvíld í gagnagrunninum.

Dulkóðun á ferð og í hvíld: öll umferð fer um TLS og gögn í gagnagrunninum eru dulkóðuð í hvíld.

Öryggishausar á öllum síðum: þvinguð Content-Security-Policy með nonce sem leyfir aðeins skriftur vefsins sjálfs, HSTS með preload, X-Frame-Options: DENY, nosniff, Referrer-Policy og Permissions-Policy.

Aðgangstakmarkanir (rate limiting) á innskráningu og öðrum viðkvæmum endapunktum verja gegn ágiskunartilraunum og ruslumferð.

Öryggisuppfærslur á hugbúnaðarsöfnum eru hluti af föstu viðhaldi þjónustunnar.

Sjá nánar: Tæknilegar varnir

6. Hverjir hjá Varhuga komast í gögnin

Fáir nafngreindir reikningar með aðgang að rekstrarumhverfinu. Starfsfólk Varhuga skráir sig ekki inn í vinnusvæði viðskiptavina. Aðgerðir stjórnenda viðskiptavinar eru skráðar í atvikaskrá.

Aðgangur starfsfólks Varhuga og leyndarmál: Starfsfólk Varhuga skráir sig ekki inn í vinnusvæði viðskiptavina; aðgangur að rekstrarumhverfinu er bundinn við fáa nafngreinda reikninga. Öll leyndarmál eru geymd í stillingum hýsingarinnar, aldrei í frumkóða, og þeim má skipta út án kóðabreytingar.

Atvikaskrá: Öryggistengdar aðgerðir stjórnenda eru skráðar í atvikaskrá sem aðeins er bætt við, aldrei breytt: innskráningar, breytingar á hlutverkum, brottfelling notenda, boð, úthlutanir, SCIM-atburðir, staðfestingar stefna og tilkynningar, hver með geranda, viðfangi, tíma og IP-tölu. Stjórnendur skoða hana undir Stillingar og sækja sem CSV.

Aðskilnaður viðskiptavina: Aðskilnaði fyrirtækja er framfylgt í hverri einustu fyrirspurn: notandi kemst aðeins í gögn síns vinnusvæðis og deildarstjóri aðeins í sína deild. Vald yfir öllu fyrirtækinu er bundið við stjórnendur.

Sjá nánar: Aðgangur starfsfólks Varhuga

7. Öryggisprófanir

Sjálfvirk yfirferð hugbúnaðarsafna við hverja breytingu og vikulega. Heildarrýni á kóða í júlí og september 2026. Engin óháð innbrotsprófun enn.

Veikleikastjórnun: Hugbúnaðarsöfn eru yfirfarin sjálfvirkt við hverja kóðabreytingu og aftur í hverri viku. Alvarlegur veikleiki stöðvar útgáfu þar til hann hefur verið lagaður. Allur kóði þjónustunnar var öryggisrýndur í júlí 2026 og aftur í september 2026 með áherslu á aðskilnað fyrirtækja, eins og lýst er hér að neðan.

Ítarleg öryggisrýni á öllum kóða þjónustunnar fór fram í júlí 2026 og aftur í september 2026, þá með áherslu á aðskilnað fyrirtækja, réttindastig og auðkenningu, og úrbætur voru innleiddar í kjölfarið. Rýnin er endurtekin reglulega. Sjálfvirk heimildapróf keyra við hverja breytingu á kóðanum og staðfesta að gögn eins fyrirtækis sjáist aldrei öðru, að deildarstjórar sjái aðeins sína deild og að óvirkir notendur komist ekki inn. Óháð innbrotsprófun (penetration test) hefur ekki enn farið fram; þegar hún verður gerð birtist samantekt hér.

Finnir þú veikleika í þjónustunni þiggjum við ábendingu á info@varhugi.is eða á netfangið í öryggisyfirlýsingu vefsins, varhugi.is/.well-known/security.txt, og bregðumst hratt við.

Sjá nánar: Öryggisrýni

8. Viðbrögð við atvikum

Tilkynning án ótilhlýðilegrar tafar og að jafnaði innan 48 klukkustunda frá því að Varhugi verður vart við brot sem varðar ykkar gögn, með eftirfylgni eftir því sem rannsókn miðar.

Verði vart við öryggisbrot sem varðar gögn viðskiptavinar er honum tilkynnt það án ótilhlýðilegrar tafar og að jafnaði innan 48 klukkustunda frá því að Varhugi verður brotsins vart, með lýsingu á eðli brotsins, líklegum áhrifum og þeim ráðstöfunum sem gripið hefur verið til, og síðan sendar viðbótarupplýsingar eftir því sem rannsókn miðar. Þannig hefur fyrirtækið svigrúm til að uppfylla eigin tilkynningarskyldu til Persónuverndar innan 72 klukkustunda þegar við á.

marketing.vinnslusamningur.sections.breach_body

Sjá nánar: Öryggisbrot

9. Persónuvernd

Vinnslusamningur gildir sjálfkrafa. Fimm nafngreindir undirvinnsluaðilar, 30 daga fyrirvari á breytingum. Gögnum eytt eða þau afhent innan 30 daga frá lokum samnings.

Vinnslusamningurinn gildir sjálfkrafa fyrir öll fyrirtæki sem nota þjónustuna. Fyrirtæki með Pro-áskrift eða sérsamning geta óskað eftir undirrituðu eintaki.

Varhugi notar fáa og vel þekkta undirvinnsluaðila. Hver þeirra fær aðeins þau gögn sem þjónusta hans krefst og er bundinn af vinnslusamningi við Varhuga. Breytingar á listanum eru tilkynntar viðskiptavinum með 30 daga fyrirvara. Vercel (Hýsing og keyrsla hugbúnaðarins og geymsla útgefinna skírteina, Frankfurt), Neon (Gagnagrunnur, hýstur í Frankfurt), Resend (Sending tölvupósta), Stripe (Greiðsluvinnsla þegar áskrift er greidd), Upstash (Skyndiminni fyrir aðgangstakmarkanir og rekstrarmerki, hýst í Frankfurt).

Við lok þjónustu hefur fyrirtækið 30 daga til að sækja gögn sín á algengu tölvutæku formi; að þeim tíma liðnum, eða fyrr sé þess óskað, er persónuupplýsingum eytt. Útgefin skírteini fylgja starfsmanninum sjálfum og eru varðveitt áfram svo hægt sé að sannreyna þau á opinni staðfestingarsíðu; um þá varðveislu er Varhugi sjálfstæður ábyrgðaraðili og skírteinishafi getur óskað eyðingar hvenær sem er.

marketing.vinnslusamningur.sections.transfers_body

Sjá nánar: Vinnslusamningur

10. Vottanir

Hvorki ISO 27001 né SOC 2 fyrir Varhuga sjálfan. Vercel og Neon hafa SOC 2 Type 2. Engin trygging um uppitíma (SLA) í núverandi áskriftarleiðum.

Vottanir: Varhugi hefur hvorki ISO 27001 né SOC 2 vottun og heldur öðru ekki fram. Þau fyrirtæki sem reka innviðina, Vercel og Neon, hafa SOC 2 Type 2 vottun og birta skýrslur sínar á eigin öryggissíðum. Engin formleg trygging um uppitíma (SLA) fylgir núverandi áskriftarleiðum.

Afrit og endurheimt: Gagnagrunnsþjónustan heldur samfelldri sögu allra breytinga svo hægt er að endurheimta gagnagrunninn á tiltekið tímamark, ekki bara síðasta næturafrit. Forritið er sett upp beint úr útgáfustýringu og hver útgáfa er geymd, þannig að gallaða útgáfu má taka til baka á nokkrum mínútum.

Sjá nánar: Vottanir

Tengd skjöl

Öryggi Varhuga	https://www.varhugi.is/is/oryggi
Vinnslusamningur	https://www.varhugi.is/is/vinnslusamningur
Persónuverndarstefna	https://www.varhugi.is/is/personuvernd
Skilmálar	https://www.varhugi.is/is/skilmalar