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; innskráningarfærslur (tími, IP-tala, vafri). Ekkert annað.

Unnið er með eftirfarandi flokka persónuupplýsinga: nafn, netfang, deild og hlutverk starfsmanns; framvindu námskeiða, prófniðurstöður og útgefin skírteini; og tæknilegar færslur um innskráningar og notkun (tímasetningar, IP-tölur, vafrategund). Skráðir einstaklingar eru starfsfólk og stjórnendur viðskiptavinarins. Þjónustan er ekki ætluð fyrir viðkvæmar persónuupplýsingar og viðskiptavinurinn skal ekki leggja slíkar upplýsingar inn í hana.

Vinnslan felst í að veita öryggisvitundarþjálfun: að halda utan um starfsmannalista, úthluta námskeiðum, skrá niðurstöður prófa, gefa út skírteini og útbúa tölfræði og endurskoðunarskýrslur fyrir viðskiptavininn. Vinnslan varir á meðan viðskiptavinurinn er með virkan reikning, að viðbættum eyðingarfresti samkvæmt kaflanum um eyðingu og skil gagna.

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 á Vercel og öll gögn eru geymd í PostgreSQL-gagnagrunni hjá Neon í Frankfurt í Þýskalandi, innan Evrópska efnahagssvæðisins. Tölvupóstur, svo sem innskráningartenglar og áminningar, er sendur í gegnum 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: Varhugi er eitt vefforrit sem keyrir hjá Vercel. Öll gögn viðskiptavina eru í einum PostgreSQL gagnagrunni hjá Neon í Frankfurt. Upstash Redis geymir aðeins skammlífa lykla fyrir aðgangstakmarkanir og athugun á aðgerðaleysi, aldrei gögn viðskiptavina, og Resend sendir tölvupóst. 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 geymdar á þjóni, stjórnendur skráðir út eftir fjögurra klukkustunda aðgerðaleysi.

Engin lykilorð: Varhugi geymir engin lykilorð. Innskráning fer fram með staðfestingartengli 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.

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 sólarhring, eða með Microsoft eða Google innskráningu (SSO). Varhugi geymir engin lykilorð. Lotur eru geymdar á þjóninum og 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 Entra app roles. SCIM er ekki enn í boði, svo stjórnandi fjarlægir þá sem hætta undir Starfsfólk.

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.

Sjá nánar: Leiðbeiningar um SSO

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, meðal annars 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

Stuttur listi nafngreindra starfsreikninga með rekstraryfirlit. 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 stuttan lista nafngreindra reikninga sem er geymdur sem stilling en ekki kóði, og veitir aðgang að rekstraryfirliti með tölum um reikninga og notkun; sá aðgangur er sem stendur ekki skráður í atvikaskrá viðskiptavinarins. Aðgangslyklar að hýsingu, gagnagrunni og póstþjónustu eru geymdir í umhverfisstillingum hýsingarinnar, aldrei í frumkóða, og þeim má skipta út án þess að breyta kóða.

Atvikaskrá: Öryggistengdar aðgerðir stjórnenda eru skráðar í atvikaskrá sem aðeins er bætt við, aldrei breytt: innskráningar, breytingar á hlutverkum, brottfelling notenda, boð, úthlutanir og breytingar á SSO stillingum, hver með geranda, viðfangi, tíma og IP-tölu. Skráin er afhent viðskiptavini sé þess óskað.

Aðskilnaður viðskiptavina: Viðskiptavinir deila gagnagrunni en hver færsla tilheyrir einu fyrirtæki. Allur lestur og allar breytingar í stjórnborðinu fara um eina heimildareiningu sem athugar aðild og hlutverk notandans áður en snert er við gögnum. Deildarstjóri sér og breytir aðeins eigin deild; einungis stjórnandi getur unnið með allt fyrirtækið.

Sjá nánar: Aðgangur starfsfólks Varhuga

7. Öryggisprófanir

Sjálfvirk yfirferð hugbúnaðarsafna við hverja breytingu og vikulega. Heildarrýni á kóða í júlí 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, eins og lýst er hér að neðan.

Ítarleg öryggisrýni á öllum kóða þjónustunnar fór fram í júlí 2026 og úrbætur voru innleiddar í kjölfarið. Rýnin er endurtekin reglulega. 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 síðunni Hafa samband og bregðumst hratt við.

Sjá nánar: Öryggisrýni

8. Viðbrögð við atvikum

Tilkynning innan 24 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 innan 24 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.

Verði Varhugi vart við öryggisbrot sem varðar persónuupplýsingar viðskiptavinarins tilkynnir Varhugi tengilið hans það án ótilhlýðilegrar tafar og eigi síðar en 24 klukkustundum eftir að Varhugi verður brotsins vart. Í tilkynningunni koma fram eðli brotsins, hvaða gögn og einstaklingar kunna að hafa orðið fyrir áhrifum, líklegar afleiðingar og þær ráðstafanir sem gripið hefur verið til, og henni er fylgt eftir þegar frekari upplýsingar liggja fyrir. Þannig getur viðskiptavinurinn uppfyllt eigin tilkynningarskyldu til Persónuverndar innan 72 klukkustunda þegar við á.

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 í Pro-áskrift 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), Neon (Gagnagrunnur, hýstur í Frankfurt), Resend (Sending tölvupósta), Stripe (Greiðsluvinnsla þegar áskrift er greidd), Upstash (Skyndiminni fyrir aðgangstakmarkanir).

Við lok þjónustu, eða samkvæmt beiðni, er persónuupplýsingum eytt innan 30 daga eða þeim skilað á algengu tölvutæku formi. Útgefin skírteini eru varðveitt áfram svo hægt sé að sannreyna þau á opinni staðfestingarsíðu, en þeim er eytt sé þess óskað sérstaklega.

Gögn þjónustunnar eru að jafnaði hýst innan Evrópska efnahagssvæðisins. Sumir undirvinnsluaðilar eru bandarísk félög og flutningur persónuupplýsinga út fyrir EES, eigi hann sér stað, byggist á stöðluðum samningsákvæðum framkvæmdastjórnar ESB (Standard Contractual Clauses, SCC) eða á þátttöku viðkomandi aðila í EU-US Data Privacy Framework, samkvæmt vinnslusamningi Varhuga við hvern aðila. Yfirlit yfir undirvinnsluaðila er í persónuverndarstefnunni.

Sjá nánar: Vinnslusamningur

10. Vottanir

Hvorki ISO 27001 né SOC 2 fyrir Varhuga sjálfan. Vercel og Neon hafa SOC 2 Type 2. Engin uppitímatrygging (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://varhugi.is/is/oryggi
Vinnslusamningur	https://varhugi.is/is/vinnslusamningur
Persónuverndarstefna	https://varhugi.is/is/personuvernd
Skilmálar	https://varhugi.is/is/skilmalar