

Klagomål till IMY

Detta är ett klagomål till Integritetsskyddsmyndigheten avseende Regeringskansliets användning av Cloudflare som underleverantör.

Har du kontaktat den som är personuppgiftsansvarig och fört fram dina klagomål?

Ja.

Beskriv vad du har gjort och vad resultatet blev

Jag kontaktade Regeringskansliet och informerade dem om att det saknade information på deras webbplats om deras användning av Cloudflare. Ni kan hitta hela samtalet [här](#).

Våra diskussioner handlade om:

- Bristen på information kring hur Cloudflare behandlar mina personuppgifter
- Möjligheten att mina uppgifter behandlas på amerikansk mark
- Övriga problem i deras PUB-avtal och dokument som verkar saknas

Svaren bekräftade min känsla att Regeringskansliet inte helt förstår vilka behandlingar sker när de använder Cloudflare, vilken roll Cloudflare har som underbiträde och vilken roll de har som personuppgiftsansvariga. Tyvärr ledde mitt meddelande endast till en liten förändring i informationen som finns på regeringen.se efter flera månader av tålamodiga mejl.

Du som anmäler

Förnamn och efternamn

Pierre Measure

E-postadress

pierre@mesu.re

Vad har inträffat?

På vilket sätt har personuppgifter behandlats felaktigt?

- **✓ Bristfällig information till exempel att den personuppgiftsansvariga inte har informerat om hur dina personuppgifter kommer att behandlas.**
- **✓ Personuppgiftsansvarig har felaktiga eller missvisande uppgifter**
- Personuppgiftsansvarig vägrar att ändra personuppgifter
- Bristande säkerhet hos personuppgiftsansvarig, till exempel för behörighetshantering eller organisationens rutiner
- Personuppgiftsansvarig har lämnat ut uppgifter felaktigt
- Kränkande uppgifter har spridits på internet
- **✓ Övrigt: Behandling av personuppgifter utan rättslig grund.**

Beskriv vad som hänt

Regeringskansliet använder en tjänst från Cloudflare för att skydda sig mot DDOS-attacker. Detta syns bland annat eftersom min webbläsare laddar regeringen.se från en av Cloudflares servrar i Kalifornien. Rättare sagt har Regeringskansliet ett avtal med sin huvudleverantör Nordlo Improve AB och de använder Cloudflare som underleverantör för att skydda Regeringskansliets webbsidor mot DDOS-attacker.

Detta betyder att min IP-adress och möjligtvis andra personuppgifter behandlas på amerikansk mark av ett amerikanskt företag. Genom ett snabbt test har jag till exempel kunnat se att min e-postadress skickas till Cloudflare när jag prenumerar mig till Regeringskansliets innehåll [på denna sida](#). Även min webbläsares *user agent* och min enhets språk finns i anropen som skickas till Cloudflare, vilket anses kunna vara personuppgifter och leda till så-kallad [fingerprinting](#).

I ett liknande fall [bestämde ert portugisiska syskon att tvinga den lokala statistiska centralbyrån](#) att sluta använda Cloudflare.

Under mina samtal med Regeringskansliet för att lösa detta märkte jag fler brister i deras dataskyddsarbete:

- Regeringskansliets PUB-avtal med Nordlo tecknades den 19:e oktober 2020 och innehöll redan då föråldrade formuleringar kring Privacy Shield (som upphörde redan 16:e juli 2020 på grund av Schrems II-domen). PUB-avtalet har inte uppdaterats sedan det tecknades enligt Regeringskansliet (se samtalet).
- Regeringskansliet och Nordlo verkar inte ha gjort någon riskanalys kring deras användares personuppgifter innan de började använda Cloudflares tjänst.
- Regeringskansliet verkar inte anse att Cloudflare är underbiträde till Nordlo och har därför inte beskrivit behandlingarna i PUB-avtalet.
- Regeringskansliet ska enligt PUB-avtalet få en kopia av Nordlos PUB-avtal med deras underbiträden. Enligt mina begäran har de inte fått en kopia av avtalet mellan Nordlo och Cloudflare som deras PUB-avtal. Och det är oklart om ett sådant avtal ens finns. **[UPPDATERING: Regeringskansliet skickade mig den 27:e mars 2023 ett addendum som beskriver Cloudflares behandling]**
- Regeringskansliet nämner att “[det] finns ytterligare en underleverantör, som avser en videotjänst, där personuppgifter inte behandlas”. Den sista delen av

påståendet kan mycket väl stämma eftersom den analytik-data som videotjänsten Qbrick skickar till adressen analytics.qbrick.com verkar inte innehålla uppgifter som kan lätt kopplas till användaren.

- Den 21:a mars 2023 har det dock dykt upp ytterligare en tjänst som verkar samla personuppgifter och innebär överföring till USA: [Azure Application Insights](#). Regeringens webbplats gör ett anrop till Microsofts servrar i USA för att ladda tjänsten och skickar sedan information om vad användaren gör på webbplatsen till Azurens servrar i Sverige. Jag har inte frågat Regeringskansliet om huruvida Nordlo Improve AB har ett underbiträdesavtal med Microsoft Azure och vad de tycker om kopplingen till USA. **[UPPDATERING: Jag frågade den 27:e mars, jag inväntar fortfarande ett svar]**