GDPR via ombud och vem är ansvarig?

2023-01-10 [sv] Joaquim Homrighausen, gdprtech@webbplatsen.se

GDPR fångar allt fler människors, myndigheters och företags uppmärksamhet och det är numera väldigt viktigt att hålla reda på var data behandlas, hur data behandlas och var data lagras, om den påverkas av GDPR.

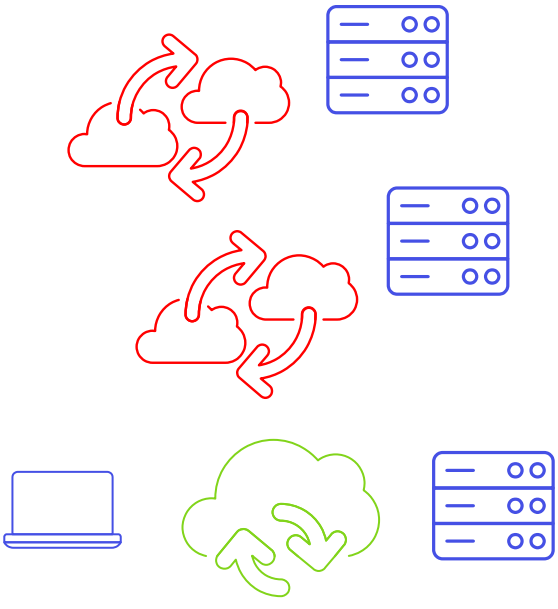
Många webbsajter och molntjänster bryter mot GDPR. Detta är, förmodligen, inte medvetet i de flesta fall, men många av dem använder t ex en ombudsmekanism (“proxy”) som gömmer eller maskerar var och hur data från och till användaren hanteras. En sådan mekanism är nästan omöjlig att upptäcka om du inte har direkt insyn i hur sajten eller tjänsten är uppbyggd. Att använda sig av externa resurser för en webbsajt eller molntjänst är också ett sätt att skaffa sig GDPR-problem.

På begäran från kunder, och för att jag är nyfiken av mig, så analyserar jag ofta webbsajter och molntjänster. Det är, för mig, häpnadsväckande att se hur många problem med GDPR och integritet vad gäller personlig information som dessa har. Många av problemen skulle kunna åtgärdas ganska enkelt, men ändå så fortsätter dessa sajter och tjänster att läcka personuppgifter, alternativt hantera personuppgifter på ett mycket nonchalant sätt, år efter år.

En del av texten i den här artikeln kan kännas för teknisk för många, men jag skall försöka att beskriva problematiken så okomplicerat som möjligt. Ställ gärna frågor eller kom med annan feedback; synpunkter om felaktigheter tas tacksamt emot!

Jag har inga intentioner att ta upp ämnen som kakor (”cookies”), gömda pixlar eller andra metoder som används för att spåra användare, som t ex fingeravtryck (”fingerprinting”). Artikeln förutsätter att klienten/besökaren/användaren lyder under och är skyddad av europeisk lagstiftning så som den är utformad inom EU.

Användning av molntjänster inom EU (grön), som sedan utbyter data med infrastruktur utanför EU (röd). Molntjänsten på insidan av EU är ombud.



Användning av molntjänster inom EU (grön), som sedan instruerar användarens webbläsare att hämta externa resurser från infrastruktur utanför EU (röd)

Dessa två illustrationer visar två scenarier:

1. **Back-end-tjänster med front-end som ombud:** En webbsajt eller molntjänst som inte nödvändigtvis har några referenser till externa resurser, men som skickar data fram och tillbaka till back-end infrastruktur, inklusive personlig information om/från användaren.

2. **Referenser till externa resurser:** En webbsajt eller molntjänst som använder sig av referenser till externa resurser, som t ex CSS, bilder, JavaScript-ramverk och/eller webbtypsnitt, vilket får användarens webbläsare att hämta dessa från den angivna adressen (URL). Detta är vanligt när utvecklare vill använda CDN eller *”Content Distribution Network.”*

Back-end-tjänster med front-end som ombud

Det här sättet att bygga webbsajter och molntjänster blir allt vanligare och det är extremt svårt, för att inte säga omöjligt, att upptäcka.

Från ett tekniskt perspektiv kan det uppfattas som ett bra sätt att bygga tjänster på det här sättet, och det är inte nödvändigtvis fel att göra det. Den första servern kan vara en webbserver, den andra servern en databasserver, eller den första servern kan vara en webbserver och den andra servern en API-server med vilken webbservern utväxlar data.

Så vad är problemet? Jo, om den första servern finns inom EU och den andra servern eller annan infrastruktur är utanför EU så kan det, enligt GDPR, förekomma en överföring av information till ”tredje land”. Det är problemet.

Referenser till externa resurser

Utvecklare av webbsajter och molntjänster använder ofta externa ramverk och andra förpaketerade komponenter som CSS och webbtypsnitt. Inte för att det är nödvändigt eller för att det gör så stor skillnad 2023, men för att, tja, de tycker det är en fantastisk idé när de utvecklar sajter och tjänster. Det är det inte. Åtminstone inte när dessa ramverk och komponenter hämtas från extern infrastruktur.

Alla sådana ramverk och komponenter kan läggas på samma ställe som webbsajten eller molntjänsten. Detta kan komma att öka belastningen marginellt på den lokala infrastrukturen och det skulle möjligen kunna vara en av de få motiverbara anledningar bland högen av ursäkter och förklaringsmodeller utvecklare använder när de anser att dessa resurser skall hämtas externt.

Motiveringar som ”det kommer att öka tiden det tar att visa webbsajten” och ”det ökar mängden komponenter vi måste hantera internt” är, för det mesta, inte helt överensstämmande med verkligheten. Inte heller är argumentet för att använda CDN (”Content Distribution Network”) särskilt starka, då det ofta motiveras med att ”Det går snabbare för användarens webbläsare att hämta resurserna då eftersom de förmodligen redan finns lagrade lokalt i webbläsaren.” Det argumentet baseras på förutsättningen att användaren har besökt en annan webbsajt som hänvisar till exakt samma externa resurs. Den situationen kan naturligtvis uppstå, men inte i närheten så ofta som utvecklare skulle vilja göra gällande.

Varje gång en användares webbläsare hämtar sådana externa resurser så skickas information såsom IP-adress (bland annat) till infrastrukturen som huserar den externa resursen och det finns väldigt lite användaren eller användarens webbläsare kan göra för att förhindra detta. Om man som användare väljer att blockera hämtningen av sådana resurser, så fungerar väldigt sällan webbsajten eller molntjänsten som det är tänkt.

Vad betyder ”i EU”?

Leverantörer av molntjänster och webbsajter använder ofta uttryck som ”driftas i EU” eller att infrastrukturen finns på ”GDPR-säker plats”. Detta räcker inte för att molntjänsten eller webbsajten skall anses efterleva GDPR.

Vad som betyder mer är vilket företag som äger infrastrukturen, och var det företaget har sitt säte.

Ett amerikanskt företag som tillhandahåller tjänster från ett datacenter i Amsterdam är fortfarande ett företag som lyder under amerikansk lagstiftning. Detta lämnar utrymme för en överföring av personlig information till ”tredje land”, t ex om amerikanska myndigheter kräver att få ta del av data i det amerikanska företagets infrastruktur. Det spelar ingen roll om en server är fysiskt placerad ”i EU”.

Vem är ansvarig?

Du, som företagsägare eller företagsledare är ansvarig för GDPR-incidenter och brott mot GDPR. Du kan inte ”outsourca” ansvaret eller ”skylla på utvecklarna eller webbyrån”.

Det kan vara en bra idé att ställa frågor om just sådant som tas upp i den här artikeln innan du hoppar i båten med båda fötterna. Det är inte så svårt eller komplicerat att hålla sig på rätt sida om GDPR när det kommer till webbsajter och molntjänster, faktiskt.

Ta gärna kontakt med mig om du har frågor, förslag eller annan feedback. Min e-postadress finns i början av texten på första sidan.

Illustrationerna i denna artikel använder grafik från Streamline-samlingen, www.streamlinehq.com