info@readspeaker.com
www.readspeaker.com

ReadSpeaker och Interxion i relation till GDPR

Frågor och svar

Nedan följer några frågor och svar om affärsrelationen mellan ReadSpeaker och dess underleverantör av datacentertjänster Interxion Sverige (hädanefter Interxion) i relation till GDPR.

Vad är GDPR?

Dataskyddsförordningen, en EU-lag som implementerades den 25 maj 2018 och förkortas GDPR, kräver att organisationer hanterar personuppgifter på ett säkert sätt och upprätthåller rätten till personlig integritet för alla inom EU:s territorium. GDPR gäller inte enbart för organisationer inom EU utan även för organisationer utanför EU om de erbjuder varor eller tjänster till, eller övervakar beteendet hos, registrerade i EU. Förordningen innehåller sju principer för dataskydd som ska upprätthållas, samt åtta rättigheter för registrerade som måste främjas. Den ger också varje medlemsstats tillsynsmyndighet på området, vilket i Sverige är Integritetsskyddsmyndigheten, befogenhet att utfärda sanktioner i syfte att säkerställa efterlevnaden av GDPR. GDPR, som antogs i Europaparlamentet med överväldigande majoritet, förenar EU under ett och samma regelverk för dataskydd.

Vad är en personuppgiftsansvarig, ett personuppgiftsbiträde eller ett UNDERBITRÄDE enligt GDPR?

Begreppen personuppgiftsansvarig, gemensam personuppgiftsansvarig och personuppgiftsbiträde spelar en avgörande roll vid tillämpningen av GDPR, eftersom de avgör vem som ska ansvara för att olika dataskyddsregler följs och hur registrerade kan utöva sina rättigheter i praktiken. Begreppen personuppgiftsansvarig, gemensam personuppgiftsansvarig och personuppgiftsbiträde är funktionella begrepp genom att de syftar till att fördela ansvaret i enlighet med parternas faktiska roller och självständiga begrepp i den meningen att de huvudsakligen bör tolkas i enlighet med EU:s dataskyddslagstiftning.

En *personuppgiftsansvarig* är ett organ som bestämmer både ändamålen och medlen för behandlingen, dvs. varför och hur behandlingen ska utföras. Det är inte nödvändigt att

den personuppgiftsansvarige faktiskt har tillgång till de uppgifter som behandlas för att kvalificeras som personuppgiftsansvarig.

Ett *personuppgiftsbiträde* är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsbiträdet får inte behandla uppgifterna på annat sätt än enligt den personuppgiftsansvariges instruktioner. Den personuppgiftsansvariges instruktioner kan fortfarande lämna ett visst utrymme för bedömning när det gäller hur man bäst tjänar den personuppgiftsansvariges intressen, så att personuppgiftsbiträdet kan välja de bäst lämpade tekniska och organisatoriska åtgärderna för behandlingen.

Ett *underbiträde* är ett personuppgiftsbiträde som är underleverantör till ett personuppgiftsbiträde.

Vad av ovanstående begrepp gäller för ReadSpeaker, dess kunder och Interxion?

ReadSpeakers kunder är personuppgiftsansvariga för de personuppgifter som behandlas av ReadSpeaker och som lagras på servrarna i Interxions datahall. ReadSpeaker är personuppgiftsbiträde för sådana kunduppgifter.

Frågan om Interxion kvalificerar sig som underbiträde till ReadSpeaker eller inte adresseras i en fråga längre ner.

Vilken typ av datacentertjänster tillhandahåller Interxion ReadSpeaker?

ReadSpeaker upphandlar colocation-tjänster från Interxion, vilket innebär att ReadSpeaker äger sina servrar och hårdvaru-utrustning i vilka data lagras, men upphandlar tjänster för sin hårdvara av Interxion, såsom skåputrymme, strömförsörjning, temperaturreglering, bredbandsanslutning och andra korsanslutningstjänster.

I tillägg till att ReadSpeaker placerar sin hårdvara i Interxions datahallar inom EU, så kan Interxion, på ReadSpeakers begäran utföra så kallade Hands & Eyes-tjänster. Supporttjänsterna kan till exempel omfatta in - eller urkoppling av kablage, montering av en fabriksny server eller att trycka på en knapp för att starta eller stänga av en server. Hands & Eyes-tjänster kan även omfatta underhåll, installationsarbete, konfiguration eller felsökning. Hands & Eyes-tjänster får bara utföras på ReadSpeakers skriftliga begäran och enligt arbetsorder med närmare instruktioner för supporten.

Är Interxion ett personuppgiftsbiträde, och därmed ett underbiträde till ReadSpeaker?

Enligt GDPR aktualiseras specifika skyldigheter när ett personuppgiftsbiträde avser att anlita en underleverantör, och därigenom lägger till ytterligare en länk i kedjan, genom att anförtro sådan leverantör uppdrag som omfattar behandling av personuppgifter. Analysen av huruvida leverantören utgör ett sådant underbiträde enligt GDPR bör utföras i enlighet konceptet för personuppgiftsbiträde.

I ljuset därav är frågan om Interxion är ett personuppgiftsbiträde till ReadSpeaker när bolaget tillhandahåller ovan nämnda datacentertjänster?

För att Interxion ska utgöra ett personuppgiftsbiträde enligt GDPR måste Interxion behandla personuppgifter för ReadSpeakers räkning, och indirekt för ReadSpeakers kunders räkning i egenskap av personuppgiftsansvariga. Enligt Integritetsskyddsmyndigheten uppstår rollen som personuppgiftsbiträde i samband med att ett uppdrag av en leverantör innefattar behandling av personuppgifter för den personuppgiftsansvariges räkning.

Innehållet i tjänsterna och hur de utförs kommer att avgöra om behandlingsaktiviteten utgör behandling av personuppgifter för den personuppgiftsansvariges räkning i den mening som avses i GDPR. I enlighet härmed beror svaret på ovanstående fråga på vilken typ av tjänster Interxion utför för ReadSpeaker. Det ovan beskrivna erbjudandet för ett colocation-datacenter berör IT-infrastrukturen – utrymme, elförsörjning, kylning, säkerhet och uppkoppling – varav inget påverkar behandlingen av de personuppgifter som lagras på ReadSpeakers servrar. Sådana tjänster inkluderar inte någon behandling av personuppgifter och gör således inte Interxion till ett underbiträde till ReadSpeaker.

I Interxions tjänsteportfölj ingår även ovan beskrivna s.k. Hands & Eyes-supporttjänster. Sådana tjänster används i begränsad omfattning av ReadSpeaker och aldrig på ett sätt som omfattar behandling av personuppgifter lagrade på ReadSpeakers servrar. Teoretiskt framstår det som att sådana tjänster kan innefatta att Interxions tekniska personal med fysisk tillgång till servrarna kan logga in på dessa och behandla personuppgifter som lagras av ReadSpeaker. Interxions Hands & Eyes-supporttjänster är dock inte avsedda att användas på det sättet, något som både ReadSpeaker och Interxion är överens om och klargjort i avtalet bolagen emellan. Därtill tillhandahålls Hands & Eyes-tjänsterna endast efter och baserat på ReadSpeakers uttryckliga instruktioner. En faktisk åtkomst till personuppgifter på ReadSpeakers servrar kräver inloggningsuppgifter, inklusive lösenord, som förmedlas av ReadSpeaker. Sådana tekniska och organisatoriska säkerhetsåtgärder som tillämpas på ReadSpeakers och dess kunders data resulterar i att Interxion skulle behöva utföra dataintrång för att behandla personuppgifter på ReadSpeakers servrar. Mot bakgrund därav och utan

någon specifik åtkomst till personuppgifterna kan Interxion varken anses behandla personuppgifter för ReadSpeakers räkning eller utgöra ett underbiträde till ReadSpeaker.

Till följd av att Interxion inte kan anses utgöra ett personuppgiftsbiträde till ReadSpeaker, har ReadSpeaker ingen skyldighet enligt GDPR att informera sina kunder om, eller inhämta samtycke på förhand från sina kunder, för de tjänster som upphandlas från Interxion. ReadSpeaker har dock oavsett det åtagit sig att fortsätta upprätthålla en nära och transparent relation med sina kunder, samt att kommunicera sin upphandling av datacentertjänster från Interxion och sin analys av rättsläget inom dataskydd som tillämpas på sådan upphandling. Alla organisationer hanterar personuppgifter på ett eller annat sätt i denna datadrivna värld och bör lägga stor vikt vid att följa regelverken. Att ha kunder som ifrågasätter och utmanar oss i dessa ämnen är ett tecken på att organisationer tar dataskydd på allvar, i alla aspekter av sin verksamhet. ReadSpeaker välkomnar sina kunder att kontakta företaget för ytterligare frågor om dessa ”Frågor och svar”.

Medför Interxions datacentertjänster som ReadSpeaker upphandlar överföring av personuppgifter till ett tredjeland utanför EU/EES?

Om en tredje part utanför EU/EES ges tillgång att behandla personuppgifter som ReadSpeaker antingen är personuppgiftsansvarig eller personuppgiftsbiträde för, utgör det en tredjelandsöverföring av personuppgifter enligt GDPR. Huvudregeln i GDPR är att inga sådana överföringar är tillåtna, såvida inte vissa villkor uppfylls. Anledningen till det är att det utanför EU/EES inte finns några generella regler likt GDPR som ger likvärdigt skydd för registrerades rätt till personlig integritet, förutom i vissa länder för vilka EU-kommissionen har beslutat om adekvat skyddsnivå för överföring av personuppgifter med den effekten att personuppgifter kan strömma fritt från EU-medlemsstater till sådana icke-EU-länder utan att några ytterligare skyddsåtgärder behövs. Enligt GDPR och Integritetskyddsmyndigheten är det fråga om överföring av personuppgifter till ett tredje land när personuppgifter görs tillgängliga för någon utanför EU/EES.

Interxion ingår i den globala koncernen Digital Realty, och ägs och kontrolleras därmed indirekt och ytterst av en amerikansk enhet. Interxions datacentertjänster medför dock ingen överföring av personuppgifter till ett tredjeland utanför EU/EES eftersom Interxion inte behandlar några personuppgifter i samband med sina datacentertjänster (såsom analyserats och presenterats under ovanstående fråga), och eftersom inga personuppgifter görs tillgängliga för varken Interxion, eller indirekt dess kontrollerande utländska enhet, inom ramen för tjänsterna.