GDPR för Systemleverantörer

I maj 2018 infördes en ny europeisk förordning om skydd av personuppgifter, GDPR. GDPR har konsekvenser för dig som är systemleve-rantör av passerkontroll, inbrottslarm, CCTV, telefoni och andra system som hanterar personuppgifter. GDPR sätter användarna i fokus vilket innebär att:

- Användarna bör veta att ägaren till ett personuppgiftsystem inte sparar onödigt mycket information om dem
- Användarna ska ges möjlighet att kontrollera vad som lagras

Den nya lagen påverkar ägare av passerkontroll, inbrottslarm, CCTV, telefoni och andra system som hanterar personuppgifter, vilket även påverkar dig som leverantör på flera sätt:

- Ägarna av systemen kommer förmodligen behöva information från leverantören om de nya GDPR-reglerna
- Systemleverantören som ansvarar för driften och/eller service av systemet har ett delansvar för att bearbeta data enligt GDPR

Avgörande för avtal, leverans

GDPR specificerar att ägaren av personuppgiftsystem t.ex. ett passerkontrollsystem eller CCTV-system måste undersöka om system/ serviceleverantören kan utföra uppdraget, detta bekräftas av ett så kallat personuppgiftsbiträdesavtal mellan er som systemleverantör och ägaren av aktuellt system som personuppgiftsansvarig.

Rutiner för avvikelse är ett exempel på vad man behöver kunna

Om någon obehörig skulle komma åt personuppgifter i aktuella system via ex hackning, databas som har kommit på villovägar eller att man har brustit i att skydda personuppgifter, bör händelsen anmälas. Du som systemintegratör och servicepartner till kund måste ha rutiner för att upptäcka sådana avvikelser och meddela behandlingshanteraren, dvs. ägaren till åtkomstsys-temet. Det är ägaren som kom-mer att meddela myndigheterna.

Ansvar

Formellt är ägaren ansvarig för systemet och att uppgifterna behandlas ordentligt.
Men du går inte fri för det, både du som systemleverantör och servicepartner och kunden är solidariskt ansvariga för överträdel-ser som har negativa konsekvenser för en användare. I extrema fall kommer allvarliga överträdelser av GDPR att straffas med avgifter upp till fyra procent av den globala omsättningen för ett företag. Därför är det viktigt att du tar reda på vad du behöver veta inom de nya GDPR reg-lerna. Ditt ansvar är att se till att ägaren av systemet uppfyller kraven. Som nämnts måste du kunna avslöja dataöverträdelser och andra typer av avvikelser, så att ägaren uppfyller varningsskyldigheten. Dessutom måste du naturligtvis hitta orsaken till händelsen och stänga eventuella säkerhetshål.

Öppenhet och lagerhållningstid

En mindre dramatisk uppgift är att ge den nödvändiga insynen om lagrad trafikinformation. Här beskriver GDPR öppenhet om vem som är ansvarig dataprocesser. Om du anställs som underentreprenör ska det inte vara någon hemlighet för användarna. Hur personlig information behandlas bör vara helt öppet för berörda. De bör veta:

- Vilken typ av data om användningen av åtkomstsystemet som lagrats i loggen
- Hur länge informationen är lagrad
- Vad är lagringens syfte

Det här är uppgifter som ägaren är ansvarig för, men de kommer troligen att fråga leverantören för stöd för både kompetenshöjning och praktiska lösningar för öppenhet och insyn. Öppenheten kan enkelt lösas genom att lägga till relevanta delar av databehandlings-avtalet på kundens intranätsida. Inspektionen kan vara lite mer utmanande. Datainspektionen anger att systemägaren också måste ha en lösning eller metod för att hantera åtkomstförfrågningar. Det ska inte ske automatiskt per sekund, men senast 30 dagar efter att en användare har fått en sådan förfrågan.
Och att följa upp de tre punkterna med öppenhet:

- I loggen lagras endast trafikdata för passager gjorda med både åtkomstkort och PIN-kod.
- Lagringstiden är inte formellt avgjord, men Datainspektionen uppskattar att det kommer att bli en spegling av nuvarande praxis med högst 90 dagar.
- Syftet med lagringen är att kunna använda loggdata för att upprätthålla säkerhet och upptäcka fel i lösningen - och inget annat.

Information om Personuppgiftsbiträdesavtal som skall tecknas mellan Bravida och kund

Formellt är ägaren ansvarig för systemet och att uppgifterna behandlas ordentligt.

Information om Personuppgiftsbiträdesavtal som skall tecknas mellan Bravida och kund
Generellt så skall filialer/avdelningar som jobbar som systemleverantörer av system som hanterar personuppgifter såsom passerkon-troll, CCTV, patentsystem, telefonisystem och likande system teckna personuppgiftsbiträdesavtal med kunder enligt Bravidas mallar. .

Personuppgiftsbiträdesavtal

Bravida Personuppgiftsbiträde används när Bravida behandlar personuppgifter som något annat företag är ansva rig för, på uppdrag av det företaget, vilket sker när Bravida är leverantör och servicepart för system som hanterar personuppgifter såsom passerkontroll, CCTV, patentsystem och likande system. Bravidas mallavtal täcker alla bolag inom koncernen så det räcker med ett avtal per kund.
Kontor som hanterar slutkund ansvarar för att avtal upprättas.
När avtalet är undertecknat av båda parter ska avtalet laddas upp på BraGDPR. Detta är viktigt då Bravida enligt lag är tvunget att föra ett register över alla parter som behandlar personuppgifter på uppdrag av Bravida, eller för vilkas räkning Bravida behandlar uppgifter.
Observera att enbart personuppgiftsbiträdesavtal ska laddas upp på BraGDPR och ej annan avtalsinformation.
Vem som har rätt att underteckna personuppgiftsbiträdesavtalen för Bravidas räkning styrs av attestordningen.
BraGDPR har tagits fram som en central samlingsplats för de Personuppgiftsbiträdesavtal som Bravida har tecknat som Personuppgiftsansvarig och Personuppgiftsbiträde.
Vid frågor är du välkommen att kontakta Bravidas GDPR-grupp, bestående av representanter från juridik, HR och IT: gdpr@bravida.se