Krav på driftsäkerhet och skydd för behandlade uppgifter (integritetsskydd)

Varför finns det krav på driftsäkerhet och integritetsskydd?

I takt med att användningen av telefoni och internet ökar blir samhället, företag och individer alltmer beroende av att näten och tjänsterna fungerar. Operatörerna måste därför vidta åtgärder som säkerställer att verksamheten uppfyller rimliga krav på driftsäkerhet.

Operatörerna får vidare mycket information om användarna när de tillhandahåller elektroniska kommunikationsnät och tjänster. Det kan röra sig om bland annat personuppgifter, trafikuppgifter, inloggningsuppgifter och affärshemligheter. För att människor ska kunna känna sig trygga när de använder tjänster och nät är det viktigt att informationen skyddas.

Var finns det regler om krav på driftsäkerhet och integritetsskydd?

Regler om driftsäkerhet

Av 5 kap. 6b § lagen (2003:389) om elektronisk kommunikation, LEK, framgår att tillhandahållare av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster ska vidta lämpliga tekniska och organisatoriska åtgärder som säkerställer att verksamheten uppfyller rimliga krav på *driftsäkerhet*. I PTS föreskrifter om krav på driftsäkerhet, PTSFS 2015:2, förtydligas vilka åtgärder som ska vidtas för att leva upp till lagens krav. Syftet med reglerna är att nät och tjänster ska uppnå en grundläggande nivå av driftsäkerhet. Om en störning eller avbrott av betydande omfattning inträffar,

Post- och telestyrelsen

Postadress:
Box 5398
102 49 Stockholm

Besöksadress:
Valhallavägen 117 A
www.pts.se

Telefon: 08-678 55 00
Telefax: 08-678 55 05
pts@pts.se

ska detta rapporteras till PTS. När och hur rapportering ska ske och vad rapporterna ska innehålla framgår av lagen om elektronisk kommunikation och PTS föreskrifter PTSFS 2018:4 - Föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning.

Regler om integritetsskydd

Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster ska förutom driftsäkerhetsåtgärder även vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att de uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas (*integritetsskydd*), 6 kap. 3 § LEK. Förtydligande bestämmelser kring vilka säkerhetsåtgärder som ska vidtas finns i PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1). Syftet med reglerna är att tjänstetillhandahållarna ska skydda uppgifter om användare och deras kommunikation. Om en integritetsincident inträffar ska detta rapporteras till PTS. Hur och när rapportering ska ske framgår av Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott.

Regler om integritetsskydd finns även i EU:s dataskyddsförordning (EU) 2016/679 av den 27 april 2016 (GDPR). GDPR är den allmänna regleringen av behandling av personuppgifter och gäller för alla företag och organisationer i Sverige. LEK är däremot en särskild sektorreglering, s.k. lex specialis, när det gäller sektorn för elektronisk kommunikation. LEK är den reglering som ska tillämpas i första hand när ett företag behandlar uppgifter – såväl personuppgifter som andra uppgifter – i samband med tillhandahållandet av en elektronisk kommunikationstjänst. Först när en fråga inte specifikt regleras i LEK ska GDPR tillämpas. Vid osäkerhet kring om en inträffad incident ska rapporteras till PTS enligt LEK kan aktören kontakta PTS för att få hjälp att bedöma detta.

Vilka krav ställs på arbetet med driftsäkerhet?

Nedan följer en sammanfattning av några av de krav som ställs på operatörernas arbete med driftsäkerhet.

Definitioner

Allmänt kommunikationsnät: Ett allmänt kommunikationsnät definieras som ett elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster och som stödjer informationsöverföring mellan nätanslutningspunkter, 1 kap. 7 § LEK.

Elektronisk kommunikationstjänst: En elektronisk kommunikationstjänst definieras som en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät, 1 kap. 7 § LEK.

Tillgång: funktion som utgörs av en avgränsad del av ett kommunikationsnät eller kommunikationstjänst och som är nödvändig för att tillhandahålla ett sådant nät eller en sådan tjänst, samt som används för att sända, motta, bearbeta eller lagra information, 2 § Post- och telestyrelsens föreskrifter om krav på driftsäkerhet (PTSFS 2015:2). Exempel på funktioner som kan utgöra tillgångar är routrar, switchar, basstationer, media gateways etc.

Förbindelse: del av kommunikationsnät mellan två tillgångar eller mellan en tillgång och en anslutning till ett kommunikationsnät, 2 § PTSFS 2015:2. En förbindelse behöver inte gå mellan tillhandahållarens egna tillgångar för att omfattas, utan bör till exempel kunna utgöras av en svartfiberleverantörs uthyrda förbindelser mellan en annan parts tillgångar.

Allmänt

PTS föreskrifter om krav på driftsäkerhet gäller för såväl tillhandahållare av allmänna kommunikationsnät som tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster. Driftsäkerhetsarbetet ska bedrivas långsiktigt, kontinuerligt och systematiskt och det ska finnas särskilt utpekade ansvariga för driftsäkerhetsarbetet. Såväl normala driftsförhållanden som extraordinära händelser måste beaktas och omfattas av driftsäkerhetsarbetet. Rutiner och processer för arbetet med driftsäkerhet ska dokumenteras.

Riskanalys

Av central betydelse i driftsäkerhetsarbetet är att riskanalyser genomförs avseende verksamhetens tillgångar och förbindelser. Risken för att tillgångarna och förbindelserna orsakar störningar och avbrott ska analyseras minst en gång per år samt vid vissa planerade förändringar och efter att rapporteringspliktiga störningar har inträffat. Riskanalyserna ska dokumenteras samt uppdateras kontinuerligt. Vid genomförandet av riskanalyser ska erfarenheter från inträffade incidenter beaktas. För att kunna genomföra relevanta riskanalyser krävs att samtliga tillgångar och förbindelser är identifierade. Dessa tillgångar och förbindelser ska vara dokumenterade och dokumentationen ska hållas uppdaterad.

Av PTS föreskrifter framgår närmare vilka delar en riskanalys måste innehålla. Bl.a. finns det krav på identifiering av hot mot tillgångar och förbindelser och en bedömning av vilka konsekvenser en störning eller avbrott kan få om ett hot realiseras. Vidare ska en bedömning av sannolikheten för att ett hot inträffar göras samt en sammanvägd bedömning av sannolikheten för att ett hot inträffar och de konsekvenser det kan medföra (riskbedömning).

Skyddsåtgärder

Riskbedömningen ska ligga till grund för att bedöma vilka skyddsåtgärder som är nödvändiga att vidta med hänsyn till de hot som föreligger mot tillgångarna och förbindelserna. Skyddsåtgärder ska vidtas på en nivå som är proportionerlig med hänsyn till riskbedömningen och de kostnader som är förenade med skyddsåtgärden samt verksamhetetens art och omfattning. Exempel på skyddsåtgärder är skydd mot intrång och yttre åverkan, skydd mot

väderrelaterade hot och åtgärder i samband med vissa planerade förändringar. Nivån på skyddsåtgärden ska dokumenteras och följs upp årligen och vid behov.

Rapportering av störningar och avbrott av betydande omfattning

I PTS föreskrifter, PTSFS 2015:2, finns krav på kontinuerlig övervakning av nät och tjänster samt system som genererar larm vid störningar och avbrott. Vidare finns krav på beredskap dygnet runt för att ta emot larm kring störningar och avbrott och att initiera relevanta åtgärder. Om en störning eller avbrott av betydande omfattning inträffar ska händelsen utan onödigt dröjsmål rapporteras till PTS. Detta framgår av 5 kap. 6c § LEK.

För att avgöra om en störning eller avbrott är betydande så ska hänsyn tas till hur många abonnenter, hur stort geografiskt område och hur stor andel av nätets eller tjänstens kapacitet, som berörs. Dessutom har det betydelse hur länge störningen har pågått. Detta innebär att även mer kortvariga händelser ska rapporteras om konsekvenserna är mycket omfattande. Om konsekvenserna inte är lika omfattande ska rapportering ändå ske om störningen varar en längre tid.

PTS har utfärdat föreskrifter och allmänna råd som mer i detalj anger hur omfattande en störning eller ett avbrott ska vara för att operatören ska vara skyldig att rapportera detta, Post- och telestyrelsens föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning, PTSFS 2018:4. Störning eller avbrott som når upp till nedanstående tröskelvärden ska rapporteras till PTS;

Tid som störningen eller avbrottet pågått	**Störningens eller avbrottets uppskattade omfattning**
≥ 1 timme	≥ 150 000 abonnenter eller ≥ 15 000 km² sammanhängande berört område eller ≥ 50 % kapacitetsbortfall
≥ 2 timmar	≥ 30 000 abonnenter eller ≥ 5 000 km² sammanhängande berört område eller ≥ 30 % kapacitetsbortfall
≥ 6 timmar	≥ 5 000 abonnenter eller

	≥ 2 500 km² sammanhängande berört område eller ≥ 20 % kapacitetsbortfall
≥ 24 timmar	≥ 2000 abonnenter eller ≥ 1 000 km² sammanhängande berört område eller ≥ 10 % kapacitetsbortfall

I föreskrifterna beskrivs närmare när och hur rapporteringen ska gå till. Det finns t.ex. bestämmelser kring tidpunkter för rapportering och krav på rapportens innehåll. Operatören ska lämna en inledande rapport till PTS senast den första vardagen efter den dag då störningen avhjälpts, dock aldrig senare än tre dagar efter den dag störningen eller avbrottet inträffade. En kompletterande rapport ska lämnas till PTS senast två veckor efter det att den inledande rapporten lämnades.

PTS tillhandahåller en e-tjänst för rapportering av avbrott och störningar. Det går även bra att lämna incidentrapporter per e-post till incidentrapport@pts.se.

Vilka krav ställs på arbetet med integritetsskydd?

Nedan följer en sammanfattning av några av de krav som ställs på operatörernas arbete med skydd för behandlade uppgifter (integritetsskydd).

Definitioner

Elektronisk kommunikationstjänst: En elektronisk kommunikationstjänst definieras som en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät, 1 kap. 7 § LEK.

Informationsbehandlingstillgångar: system, databaser och fysiska tillgångar som används för informationsbehandling

Behandlade uppgifter: uppgifter som behandlas i samband med tillhandahållande av tjänsten enligt 6 kap. 3 § LEK. Med behandling avses t.ex. insamling, registrering, lagring och bearbetning. Uppgifter är t.ex. det innehåll som överförs i kommunikationstjänsten, abonnentuppgifter, trafikuppgifter och lokaliseringsuppgifter som kan kopplas till den överförda informationen, till abonnemangsinnehavare eller till de användare som kommunicerar.

Uppgifterna ska normalt röra eller kunna hänföras till en abonnent eller användare för att omfattas.

Integritetsincident: en händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring, eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster, LEK 6 kap 1 §. Begreppet integritetsincident är relativt brett och kan t.ex. handla om att en faktura skickas till fel person, förlust av uppgifter i samband med mjukvaruuppdateringar eller att uppgifter tillfälligt inte kan kommas p.g.a. en överbelastningsattack.

Allmänt

PTS föreskrifter och allmänna råd om skydd för behandlade uppgifter innehåller bestämmelser riktade mot tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster. Arbetet med skydd för behandlade uppgifter ska bedrivas långsiktigt, kontinuerligt och systematiskt och det ska finnas särskilt utpekade ansvariga för detta arbete. Rutiner och processer för arbetet med skydd för behandlade uppgifter ska dokumenteras.

Riskanalys

Av central betydelse i arbetet med skydd för behandlade uppgifter är att riskanalyser genomförs avseende verksamheten och dess informationsbehandlingstillgångar. Risken för att integritetsincidenter inträffar för informationsbehandlingstillgångarna ska analyseras minst en gång per år. Inträffade integritetsincidenter och dess orsaker ska beaktas i samband med genomgången av riskanalyserna. Riskanalyserna ska dokumenteras samt följas upp årligen och vid behov. Vid uppföljningen av riskanalyserna ska inträffade integritetsincidenter och dess orsaker beaktas. För att kunna genomföra relevanta riskanalyser krävs att samtliga informationsbehandlingstillgångar där behandlade uppgifter förekommer är identifierade. Det finns ett krav på att föra en uppdaterad förteckning över dessa informationsbehandlingstillgångar.

Skyddsåtgärder

I PTS föreskrifter och allmänna råd pekas ett antal skyddsåtgärder ut som ska vidtas av alla tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, t.ex. åtgärder kring åtkomst- och behörighetshantering, loggning, skydd mot utplåning och förlust och kryptering. Därutöver ska även andra nödvändiga skyddsåtgärder vidtas, på en nivå som är lämplig för att hantera de identifierade riskerna. Vidtagna skyddsåtgärder samt bedömning av lämplig nivå ska dokumenteras och följas upp årligen och vid behov.

Rapportering av integritetsincidenter

I PTS föreskrifter och allmänna råd finns krav på att det ska finnas dokumenterade rutiner för identifiering, intern rapportering, hantering och uppföljning av integritetsincidenter. Om en integritetsincident inträffar ska detta utan onödigt dröjsmål rapporteras till PTS. Detta framgår av 6 kap. 4a § LEK.

Hur och när rapportering av integritetsincidenter ska göras framgår inte av LEK, utan regleras i Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott. I EU-förordningen används begreppet "personuppgiftsbrott" med samma innebörd som begreppet "integritetsincident" har i LEK. Av förordningen framgår bland annat att en första rapport ska lämnas senast 24 timmar efter att integritetsincidenten/personuppgiftsbrottet upptäckts, där så är möjligt. Om inte alla uppgifter vid den tidpunkten finns tillgängliga och ytterligare utredning krävs, ska en uppföljande rapport lämnas så snart som möjligt och inom tre dagar från den inledande rapporten. Av förordningen framgår också vad rapporterna ska innehålla.

PTS tillhandahåller en e-tjänst för rapportering av integritetsincidenter. Det går även bra att lämna incidentrapporter per e-post till incidentrapport@pts.se.

Observera att detta endast är ett urval av de regler och skyldigheter som finns för aktörer på området driftsäkerhet och integritet.

För mer fördjupad läsning - se länkar i mailet till fördjupad information på PTS hemsida och tillämpliga bestämmelser.