DFRI:s Remissvar avseende Post och telestyrelsen Dnr: 12-4586 Trafikdatalagring - PTS föreskrifter och allmänna råd och skyddsåtgärder för lagrade uppgifter för brottsbekämpande ändamål

Föreningen DFRI (Föreningen för digitala fri- och rättigheter) har beretts möjlighet att lämna synpunkter på remiss från PTS avseende föreskrifter och allmänna råd och skyddsåtgärder för lagrade uppgifter för brottsbekämpande ändamål.

DFRI anser att de krav som ställs på skyddsåtgärder är otillräckliga på flera områden, särskilt med tanke på den långa lagringstiden och den typ av uppgifter som lagras.

Behörighet och åtkomst

Skyddsåtgärderna specificerar att ”den lagringsskyldige ska ha rutiner som säkerställer att endast bemyndigad personal har tillgång till lagrade uppgifter och de system som hanterar dessa uppgifter”. Dessa krav får anses som otillräckliga, av följande skäl:

1. Det saknas krav på oavvislighet rörande tillgång till systemet.
2. Det saknas krav på att systemet ska täckas av en IT-säkerhetspolicy.
3. Det saknas krav på att systemintegritet bevaras.
4. Det saknas krav på att rutiner för att hantering av IT-säkerhetsincidenter ska existera.
5. Det saknas krav på att IT-säkerhetsincidenter där lagrade uppgifter och behandlingshistorik eller misstankar om att dessa blivit komprometterat ska polisanmälas.
6. Det saknas krav på att lagrade uppgifter ska vara krypterade, ej heller att säkerhetskopior av lagrade uppgifter ska vara krypterade. Notera att ett behörighetssystem blir verkningslöst om lagrade uppgifter kan återställas på annan plats.

Behandlingshistorik (Logg)

DNR: 12-4586 beskriver att all behandling av lagrade uppgifter ska dokumenteras. DFRI anser att det är bra att en sådan logg blir obligatorisk, men har en del synpunkter. Behandlingsloggen ska krypteras, men det förklaras inte varför, och inte heller vad som ska finnas i behandlingsloggen, utöver vem som har haft tillgång till lagrade uppgifter och vid vilken tidpunkt. Detta måste uttryckligen regleras.

Det framgår också att behandlingsloggen ska förstöras, men inte efter hur lång tid, och inte heller varför, utöver en referens till LEK. Detta måste uttryckligen regleras.

1. Det saknas krav på att behöriga till lagrade uppgifter inte ska vara behöriga till behandlingshistoriken.
2. Det saknas krav på oavvislighet i behandlingsloggen.

3. Det beskrivs heller inte vilket data som ska finnas i behandlingsloggen. Vem som har haft tillgång till lagrade uppgifter kan vara ett namn, ett användarnamn eller även i vissa fall en funktion.
4. Det blir inte möjligt att göra uppföljning på ev. missbruk om behandlingsloggen förstörs.
5. Det blir betydligt enklare att missbruka om det finns vetskap om att behandlingsloggen förstörs efter viss tid.
6. Det blir svårt att få ut statistik om vad lagen om trafikdatalagring används till över tid om inte detta kontrolleras på annat sätt.

Säkerhetskopiering

Det framgår tydligt att lagrade uppgifter ska säkerhetskopieras och även att dessa säkerhetskopior ska förstöras när den obligatoriska lagringstiden upphört. DFRI anser att det är bra att det även ställs krav på förstörandet av säkerhetskopior. Utöver detta finns följande synpunkter:

1. Det saknas krav på att behandlingsloggen ska säkerhetskopieras.
2. Det saknas krav på skydd av säkerhetskopior av lagrade uppgifter, trots att återställande av säkerhetskopior gör det möjligt att kringgå att hamna i behandlingsloggen.
3. Säkerhetskopior av lagrade uppgifter ska krypteras.

Stockholm 24 augusti 2012
För DFRI genom styrelsen.