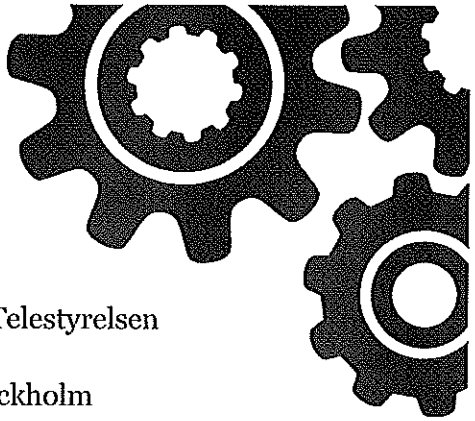


Post- och Telestyrelsen
Box 5398
102 49 Stockholm

Stockholm 2012-08-27

Remissvar – trafikdatalagring – PTS föreskrifter och allmänna råd om skyddsåtgärder för lagrade uppgifter för brottsbekämpande ändamål (Dnr: 12-4586)

.SE (Stiftelsen för Internetinfrastruktur har beretts möjlighet att lämna synpunkter på rubricerade remiss. .SE anser att förslagen till föreskrifter och allmänna råd saknar en del vitala inslag, framför allt när det gäller krav på skyddsåtgärder för uppgifterna med avseende på både karaktären på uppgifterna och den tid som dessa förväntas lagras. Vi saknar även tydliga krav när det gäller spårbarheten av behörighet och åtkomst till dessa uppgifter.

Förslag till föreskrifter om ersättning

Den föreslagna modellen med fast pris per utlämning kan förväntas drabba utlämnande organisationer olika. För vissa organisationer kan det kanske till och med komma att bli en vinstdrivande tjänst, för andra kommer dessa vara en ekonomisk belastning. .SE saknar ett utförligare resonemang kring detta i konsekvensanalysen.

.SE anser att det är bra att utlämnande organisation kan be om ytterligare ersättning om kostnaderna är högre än den fastställda ersättningen per uppgiftskategori. Även här saknar vi dock ett mer utförligt resonemang i konsekvensanalysen, gärna med exempel och typfall och gärna tillsammans med en överslagsberäkning av vad det kan komma att kosta att utveckla de system som krävs.

Det är rimligt att föreställa sig att standardiserade gränssnitt för utlämning resulterar i lägre kostnader och att det kan skapa incitament för de som hämtar ut uppgifter att implementera sådana gränssnitt. Det är dock oklart om det skapar något verkligt incitament för de som skall lämna ifrån sig information. De innebär att de ska göra en investering för att utveckla gränssnitt, samtidigt som det leder till att eventuella intäkter minskar.

Stiftelsen för Internetinfrastruktur
Box 7399, 103 91 Stockholm Tel 08-452 35 00 Fax 08-452 35 02 Org.nr. 802405-0190 www.iis.se

.SE betonar vikten av att enbart använda standardiserade gränssnitt och inte pekar ut någon specifik standard. Det är angeläget att marknadens aktörer, oavsett storlek, kan vara med och påverka utformningen av och fritt kan välja gränssnitt.

Förslag till föreskrifter och allmänna råd om skyddsåtgärder för lagrade uppgifter

3 §
Det är bra att PTS i 3 § föreskriver att den lagringsskyldige ska bedriva ett kontinuerligt och systematiskt säkerhetsarbete och att man ska ha dokumenterade rutiner och processer för att uppfylla kraven på skyddsåtgärder. Förutom detta skulle .SE gärna se ett krav på att det finns ett revisionsprogram där revisorer väljs och revisioner genomförs på ett sådant sätt att objektivitet och opartiskhet i revisionsprocessen säkerställs, inte bara att det finns särskilt utsedd personal inom organisationen för att kontrollera, godkänna och följa upp säkerhetsarbetet.

4 §
När det gäller behörighet och åtkomst specificerar föreskrifterna att "den lagringsskyldige ska ha rutiner som säkerställer att endast bemyndigad personal har tillgång till lagrade uppgifter och de system som hanterar dessa uppgifter".

.SE anser att behörighetshantering och behörighetskontroll för åtkomst till alla delar av system, utrustning och utrymmen som används för lagring av uppgifter är ett måste, inte bara ett bör-krav som det uttryckts i de allmänna råden. Utöver detta bör spårbarhet på individnivå vara ett krav (det vill säga inga gruppbehörigheter tillåts) och vi saknar även ett krav på rutiner för hantering av incidenter.

5 §
Det är viktigt att krav ställs på skydd mot obehörigt tillträde, men detta bör även kompletteras med krav på att inpasseringskontrollen har spårbarhet. Då vi kan anta att det utrymme som systemen för lagring av uppgifter och behandlingshistorik är en del i en datorhall som många har tillträde till blir det viktigt med spårbarhet på individnivå även för inpassering. I möjligaste mån bör man införa så kallad "separation of duties" med innebörden att det inte är samma personer som har tillträde till lagrade uppgifter som till behandlingshistoriken.

6 §
.SE anser det viktigt att loggning blir obligatoriskt, vi anser det även motiverat att både lagrade uppgifter och behandlingshistorik krypteras.

På samma sätt som man specificerar vilka uppgifter som ska lagras och kunna lämnas ut bör även uppgifter som ska lagras i behandlingsloggen specificeras utöver uppgifter om vem som har haft tillgång till lagrade uppgifter och vid vilken tidpunkt.

I föreskriften anges att behandlingshistoriken ska användas för att genomföra regelbunden och systematisk uppföljning och kontroll, och att detta ska ske innan uppgifterna utplånas enligt 6 kap. 16 § lagen (2003:389) om elektronisk kommunikation,

vilket innebär en tidsgräns om lagring i högst sex månader efter att kommunikationen avslutats, då den lagringsskyldige genast ska utplåna dem.

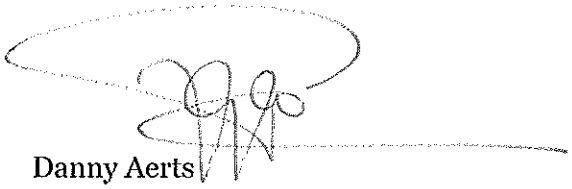
Det är inte uppenbart varför behandlingshistoriken ska utplånas samtidigt som de lagrade uppgifterna. Konstaterande av missbruk och oegentligheter kan ibland uppkomma i efterhand och då är behandlingshistoriken helt avgörande för att kunna fria eventuella misstänkta, alternativt finna någon skyldig. Det blir omöjligt att göra uppföljning av misstanke om eventuellt missbruk om behandlingsloggen utplånas. .SE saknar alltså en tydligare reglering av efter hur lång tid behandlingshistoriken ska utplånas och varför.

7 §
Förslaget i föreskriften är att lagrade uppgifter ska säkerhetskopieras och att också säkerhetskopior ska förstöras när den reglerade lagringstiden löpt ut. .SE är positiv till detta krav.

.SE anser det dessutom vara motiverat att:

- säkerhetskopior av lagrade uppgifter skyddas på samma sätt som ursprungsinformationen och ska förvaras i krypterad form,
- behandlingshistoriken ska säkerhetskopieras.

Övrigt
.SE saknar krav på uppföljning och statistik om utlämning av lagrade uppgifter över tiden så att det går att få en redovisning av hur ofta detta tillämpas och av vilken myndighet.



Danny Aerts

Vd