Region Stockholm

Kulturförvaltningen
Regionarkivet

Datum
2023-02-22

ARK 2023/77

Dokumenttyp
Anvisning

Beslutad av
Kulturnämnden

Versionsnummer
1.0

Bevarande- och gallringsplan för loggar

Gäller inom Region Stockholm

Dokumentägare: Regionarkivet, enheten för Tillsyn och utredning

Innehållsförteckning

Dokumenthistorik

Rev. Nr	Datum	Kommentarer	Ansvarig
1.0	2023-02-22	Nytt styrdokument utan tidigare version.	Therése Almsätter

1. Omfattning, tillämpning och avgränsning

Detta är en generell bevarande- och gallringsplan för loggar. Med logg avses en automatiskt förd förteckning över händelser i ett IT-system. En logg kan visa hur information har hanterats, till exempel lästs eller ändrats, beroende på hur detaljerad loggen är. Planen omfattar inte manuellt förda register och förteckningar.

Planen gäller för Region Stockholms samtliga myndigheter, såsom förvaltningar, bolag och stiftelser (se *Riktlinje för informationshantering och arkiv*, RS 2019-0549, s. 3).

Huvudregeln är att allmänna handlingar ska bevaras. Gallring av allmänna handlingar får normalt bara ske med stöd av en generell bevarande- och gallringsplan eller genom ett gallringsbeslut av myndigheten som har tillstyrkts av Regionarkivet.

Informationen som loggarna rör omfattas av de generella bevarande- och gallringsplanerna, och gallras för sig enligt respektive gallringsbeslut.

Vid införande av nya system och utveckling av IT-tjänster är det viktigt att ta hänsyn till den generella bevarande- och gallringsplanen för loggar redan vid upphandling. De krav som verksamheten har (till exempel gallringsfunktionalitet) bör anges i en kravställning gentemot systemleverantören för att säkerställa att Regionarkivets regler för hantering av information i IT-system och applikationer efterföljs (se Regionarkivets webbplats, *Styrdokument för Region Stockholm*).

Om hanteringen av loggar innebär att personuppgifter behandlas ska detta hanteras utifrån kraven på personuppgiftsbehandling enligt Dataskyddsförordningen (GDPR). Se *6. Vid behov av förlängd gallringsfrist*.

Mer information om bland annat samråd, gallring och hantering av allmänna handlingar finns i vägledningen på Regionarkivets webbplats. Här finns också en ordlista med definitioner av begrepp rörande informationshantering och arkiv.

Bevarande- och gallringsplanen gäller från och med den 22 februari 2023. Planen kan användas retroaktivt.

2. Kontroll innan gallring

I många system kan en logg ha flera olika syften och innehålla uppgifter som hör till olika typer av loggar i denna bevarande- och gallringsplan. Innan gallring verkställs ska myndigheten därför säkerställa att alla relevanta användningsområden för den aktuella loggen har beaktats.

Handlingar i EU-projekt har i vissa fall en längre gallringsfrist än vad som anges i den här planen. Ingen gallring får därmed ske tidigare än vad som framgår av reglerna för respektive EU-projekt.

3. Gallringsfrister

Bevaras innebär att handlingar/information skall sparas för all framtid. Handlingar/information som ska bevaras ska uppfylla de krav som ställs i Regionarkivets regler om format.

Gallras innebär att förstöra allmänna handlingar eller uppgifter i allmänna handlingar.

Vid inaktualitet är en gallringsfrist som innebär att handlingen/informationen eller uppgifterna kan gallras när de har blivit inaktuella för verksamheten, det vill säga när verksamheten inte behöver dem längre.

Denna bevarande- och gallringsplan är ett stöd vid bedömning av gallringsfrister för generella loggar inom Region Stockholm. I de fall en myndighet önskar gallra loggar som inte omfattas av bevarande- och gallringsplanen eller önskar förlänga planens gallringsfrister, ska ett samråd med Regionarkivet initieras angående detta. Om Regionarkivet fattar ett beslut om att tillstyrka samrådet fungerar detta som ett myndighetsspecifikt gallringsbeslut, som ska tillämpas i första hand.

Observera att myndighetsspecifika gallringsbeslut inte får innehålla gallringsfrister som är kortare än för motsvarande handlingstyper i de generella bevarande- och gallringsplanerna.

4. Så läser du planen

I planens vänstra kolumn redovisas de olika handlingstyperna. I mittenkolumnen anges om handlingstypen ska bevaras eller om den ska gallras och i så fall när. Anmärkningskolumnen anger förtydliganden där sådana behövs.

Den här bevarande- och gallringsplanen utgår från loggarnas syfte snarare än vilken benämning de har. I avsnitt *5. I vilket syfte används loggarna?* finns olika exempel på vilken typ av information loggarna kan innehålla, i vilket syfte de kan användas och vad de kan benämnas som.

En logg som används i flera olika syften kan benämnas likadant, liksom en logg som används i ett enda syfte kan benämnas på flera olika sätt. Begreppet *säkerhetsloggar* används till exempel ofta som benämning på loggar över säkerhetskritiska händelser, bland annat i Region Stockholms *Riktlinjer för informationssäkerhet*.[1] Ordet *säkerhetskritisk* kan ge en viss avgränsning i ett sammanhang medan det i ett annat sammanhang kan användas vidare. En bedömning av vilka loggar som används i vilka syften och sammanhang görs därför lämpligen av verksamheterna själva, då det inom regionen finns många olika system med varierande innehåll som hör till olika kärn- och stödverksamheter.

För referenser se *8. Referenslista* med källhänvisningar till lagar, föreskrifter, riktlinjer, fotnoter och övriga uppgifter som ligger till grund för gallringsfrister och information rörande loggar i denna plan.

5. I vilket syfte används loggarna?

Loggar skapar framför allt spårbarhet. Aktiviteter som loggas syftar inte enbart till att fälla utan kan även fria oskyldiga. Loggar kan bidra till bland annat att:

- Bedöma skadeverkningar
- Utreda inträffade händelser
- Kartlägga omfattningen av ett angrepp
- Kunna identifiera otillbörligt ändrad eller raderad information så att den kan återskapas

Nedan beskrivs några av de vanligaste benämningarna på loggar och vad de syftar till. Många av dessa loggar används för att dokumentera säkerhetskritiska händelser; det är alltså inte endast de loggar som benämns *säkerhetsloggar* som kan användas för detta ändamål.

5.1 Säkerhetsloggar

Uppgifter i loggar som registrerar händelser som kan påverka säkerheten i eller kring ett informationssystem, benämns ofta som *säkerhetsloggar*. Dessa loggar används i syfte att säkerställa informationssäkerhet.

Loggarna kan bland annat innehålla:

[1] Riktlinjer för informationssäkerhet (RS 2020-0148) s. 25.

- Information om systemfel, tekniska fel och avvikelser med betydelse för säker drift
- Information om systemoperatörers och systemadministratörers aktiviteter
- Information om användaraktiviteter
- Förändringar i behörighetsinformation och datorsystemets konfiguration som är kritiska ur säkerhetssynpunkt

För vidare information om säkerhetsloggning och ansvar kring detta, se vägledningen till Region Stockholms riktlinjer för informationssäkerhet.[2]

5.2 Loggar som används i syfte att dokumentera och utreda åtkomst

Loggar som används för att säkerställa informationssäkerhet kan även innefatta loggar som används i syfte att dokumentera och utreda åtkomst.

Dessa loggar benämns ofta som *åtkomstloggar* och avser loggar som dokumenterar tillgång eller försök till tillgång till information, mjukvara, hårdvara, lokal eller annan resurs. Loggarna används primärt i syfte att upptäcka och utreda obehörig åtkomst, men kan även användas för att upptäcka och utreda annan otillåten användning.

Loggarna kan bland annat innehålla:

- Information om åtkomst till information eller system (till exempel *åtkomstloggar*)
- Information om utskrifter från ett system (till exempel *utskriftsloggar*)
- Information om tillträde till lokaler (till exempel *tillträdesloggar*)
- Information om åtkomst till fysisk utrustning, till exempel processorer och lagringsmedia
- Information om åtkomst till loggar
- Information om in- och utloggningar i system (lyckade och misslyckade försök)
- Information om internettrafik

5.3 Loggar som används i syfte att dokumentera transaktioner och ändringar

Loggar som används för att säkerställa informationssäkerhet kan även innefatta loggar som används i syfte att dokumentera transaktioner och ändringar.

Dessa loggar kallas ofta för *transaktions-* och *ändringsloggar* och dokumenterar utförda bearbetningar i IT-system samt mottagna eller skickade meddelanden. Loggarna kan syfta till att uppfylla spårbarhetskrav,

[2] Vägledning till riktlinjer för informationssäkerhet (RS 2020-0148) s. 41-42

men kan även användas till att återställa information som gått förlorad. De kan också utgöra underlag för ekonomisk revision och annan granskning.

Loggarna kan bland annat innehålla:

- Information om spårbarhet (till exempel *spårbarhetsloggar*)
- Information om ändringar (till exempel *ändringsloggar*)
- Information om skickade och mottagna meddelanden

5.4 Loggar som används i syfte att dokumentera förvaltning av system

Loggar som används för att säkerställa informationssäkerhet kan även innefatta loggar som används i syfte att dokumentera förvaltning av system.

Dessa loggar över drift och förvaltning används för att övervaka drift och tekniska händelser eller för att undersöka systemfel och funktionsstörningar. Hit hör också loggar i de särskilda IT-miljöer som används för systemutveckling samt loggar i test- och utbildningsmiljöer.

Loggarna kan bland annat innehålla:

- Teknisk information
- Information om fel i systemet (till exempel *felloggar*)
- Information om drift av systemet (till exempel *driftloggar*)
- Information om systemadministratörer (till exempel *administratörsloggar*)
- Information om lösenordsbyten

5.5 Loggar som används i syfte att dokumentera granskning och uppföljning av loggar

Loggar som används för att säkerställa informationssäkerhet kan även innefatta loggar som används i syfte att dokumentera granskning och uppföljning av loggar.

Loggar som används i syfte att dokumentera granskning och uppföljning av loggar kan bland annat innehålla:

- Information om elektronisk åtkomst till uppgifter om en patient som har förekommit i ett IT-system som används av vårdgivare.
- Information om loggar som framställs med hjälp av logganalysverktyg
- Information om loggar som har överförts till system för logguppföljning

5.5.1 Loggutdrag för analys och uppföljning av loggar som registrerar händelser som kan påverka säkerheten i eller kring ett informationssystem

Ett loggutdrag är i sig inte en logg, men kan innehålla uppgifter ur loggar som identifierats, samlats in eller kopierats i syfte att ligga till grund för analys och/eller uppföljning. Se till exempel Integritetsskyddsmyndighetens (IMY) webbplats gällande systematisk logguppföljning.

Uppgifter i analyser kan bestå av beskrivningar av händelser som till exempel förändringar och störningar i driften, bedömd orsak och vidtagen åtgärd. Analyserna kan ingå i en myndighets incidenthantering.

6. Vid behov av förlängd gallringsfrist

Om verksamheten bedömer att gallringsfristen behöver förlängas med hänsyn till preskriptionstider (till exempel för brottet grovt dataintrång som preskriberas efter 10 år) och behov av spårbarhet, rekommenderar Regionarkivet att loggarna sparas under längre tid än vad som anges under *Bevaras/Gallringsfrist* i planen.

I ett sådant beslut ska alltid principerna om uppgiftsminimering och lagringsminimering utifrån Dataskyddsförordningen (GDPR) vägas in. I enlighet med GDPR ska lämpliga skyddsåtgärder vidtas vid behandling av personuppgifter och kan i vissa fall inbegripa bland annat pseudonymisering och kryptering. En förutsättning för detta är att myndigheten bedömer att loggens syfte bibehålls samt tar hänsyn till hur skyddsåtgärden eventuellt påverkar gallringen.

Ett beslut om förlängd gallringsfrist ska dokumenteras i myndighetens verksamhetsbaserade informationsredovisning (VIR).

7. Bevarande- och gallringsregler

Typ av logg/uppgift i logg	**Bevaras/ Gallrings-frist**	**Anmärkning**
Loggar hos verksamhetsutövare som bedriver säkerhetskänslig verksamhet.	Minst 10 år, se anmärkning.	Se PMFS 2022:1, 4 kap. 25-29 §§. Se *6. Vid behov av förlängd gallringsfrist*.
Loggar i IT-system som är avsett för att behandla säkerhetsskyddsklassificerad information i säkerhetsskyddsklassen kvalificerat hemlig.	Minst 25 år, se anmärkning.	Se PMFS 2022:1, 4 kap. 25-29 §§. Se *6. Vid behov av förlängd gallringsfrist*.
Uppgifter i loggar som registrerar händelser som kan påverka säkerheten i eller kring ett informationssystem.	Minst 5 år, se anmärkning.	Kan benämnas som *säkerhetsloggar*. Avser automatisk registrering av uppgifter i loggar som syftar till att upptäcka och utreda sådant som skadlig eller otillåten påverkan, obehörig åtkomst och funktionsstörningar i informationssystem. Se *6. Vid behov av förlängd gallringsfrist*.
Uppgifter i loggar som registrerar händelser som kan påverka säkerheten i eller kring ett informationssystem och som leder till åtgärd.	5 år, se anmärkning.	Kan benämnas som *säkerhetsloggar*. Se *6. Vid behov av förlängd gallringsfrist*.
Loggar över åtkomst till system där patientinformation behandlas.	5 år, se anmärkning.	Kan benämnas som *säkerhetsloggar*. Se HSLF-FS 2016:40, 4 kap. 9 § gällande bland annat vårdgivarens ansvar, gallringsfrist och vad som ska framgå av loggarna. Se *6. Vid behov av förlängd gallringsfrist*.

Typ av logg/uppgift i logg	**Bevaras/ Gallrings-frist**	**Anmärkning**
Loggar över åtkomst till lokaler och hårdvara (till exempel medicinteknisk utrustning och skalskydd) med information om händelser som kan påverka säkerheten.	5 år, se anmärkning.	Se *6. Vid behov av förlängd gallringsfrist*.
Loggar som utgör behandlingshistorik i myndighetens ekonomiska redovisning	Bevaras/10 år, se anmärkning.	Avser uppgifter som kan ingå i beskrivningar över genomförda bearbetningar inom systemet som gör det möjligt att följa och förstå de enskilda bokföringsposternas behandling, enligt lag (2018:597) om kommunal bokföring och redovisning 3 kap. 11 § och bokföringslagen (1999:1078) 5 kap. 11 §. Bevaras i de delar som är nödvändiga för att presentera de ekonomiska händelserna som huvudbokföring samt den sidoordnade bokföring som ska bevaras (till exempel anläggningsregister). Resterande gallras efter 10 år. Se även *Bevarande- och gallringsplan för ekonomiinformation* (LA 2019-0122).
Övriga transaktions- och ändringsloggar i ekonomi- och lönesystem.	7 år, se anmärkning	Se 7 kap. 2 § bokföringslagen (1999:1078) och 3 kap. 13 § lagen (2018:597) om kommunal bokföring och redovisning. Se *6. Vid behov av förlängd gallringsfrist*.
Transaktions- och ändringsloggar i diarier och motsvarande dokument- och ärendehanteringssystem	10 år, se anmärkning.	Se *6. Vid behov av förlängd gallringsfrist*.

Typ av logg/uppgift i logg	**Bevaras/ Gallrings-frist**	**Anmärkning**
Loggar över systemadministrativa åtgärder	5 år, se anmärkning	Se *6. Vid behov av förlängd gallringsfrist*.
Loggar i utvecklings- och testmiljöer	Vid inaktualitet	
Loggar i utbildningsmiljöer	Vid inaktualitet	Med utbildningsmiljöer avses kopior av system eller program som används uteslutande för utbildning i hur systemet eller programmet fungerar. Ett system för att skapa webbutbildningar är inte en utbildningsmiljö.
E-postloggar	3 månader, se anmärkning.	Se *6. Vid behov av förlängd gallringsfrist*.

8. Referenslista

8.1 Lagar och föreskrifter

Bokföringslag (1999:1078).

Lag (2018:597) om kommunal bokföring och redovisning.

Polismyndighetens författningssamling, PMFS 2022:1 *Säkerhetspolisens föreskrifter om säkerhetsskydd*.

Riksarkivet, RA-FS 2021:3 *Riksarkivets föreskrifter och allmänna råd om gallring av säkerhetshandlingar*.

Socialstyrelsen, HSLF-FS 2016:40 *Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården*.

8.2 Riktlinjer och övriga styrdokument

Regionarkivet, *Bevarande- och gallringsplan för ekonomiinformation* (LA 2019-0122).

Regionarkivet, *Regler för informationshantering och arkivering i IT-system/applikationer* (LA 2017-0112).

Regionarkivet, *Riktlinje för informationshantering och arkiv* (KN 2018/1243, RS 2019-0549).

Regionarkivets webbplats, *Styrdokument för Region Stockholm*. Startsida - Regionarkivet Stockholm (regionstockholm.se) (hämtad 2023-01-24).

Regionstyrelsen, *Riktlinje för informationssäkerhet* (RS 2020-0148).

Regionstyrelsen, *Vägledning till riktlinje informationssäkerhet* (RS 2020-0148).

8.3 Övrigt

Riksarkivet, RA-KS 2021/879 *PM Gallring av säkerhetshandlingar*.

Integritetsskyddsmyndigheten, *Systematisk logguppföljning*. Systematisk logguppföljning |IMY (hämtad 2022-11-16).