norsk pasientskade-erstatning

Retningslinjer for logging

Revisjonstabell

Dato	Versjon	Skrevet av	Godkjent av	Beskrivelse av endring
13.04.2021	1.0	Arbeidsgruppe (TLA, GWE, GHA og MSM) med konsulentbistand fra Norconsult.	Ledelsens sikkerhetsforum (LSF)	

Innhold

1. Innledning

Logging er viktig for å oppdage misbruk, feil i systemer, eller for å ha kontroll på endringer i viktig informasjon. Disse retningslinjene stiller overordnede krav til hva systemer logger og hvordan logger blir behandlet.

1.1 Formål

Logging er nødvendig for å:

- Gi oversikt over autorisert bruk av personopplysninger i NPE og avdekke uautorisert bruk, eller forsøk på uautorisert bruk av personopplysninger eller annen beskyttelsesverdig informasjon.
- Oppdage unormal aktivitet.
- Forebygge, avdekke og forhindre drifts- og sikkerhetsbrudd i informasjonssystemer.
- Sikre endringshistorikk av viktig informasjon der dette er vurdert som nødvendig.

1.2 Virkeområde

Disse retningslinjene gjelder for alle systemer forvaltet av NPE. Hovedansvar for å definere krav og tilgangsstyring til logger ligger hos systemeier for systemet som produserer loggen, med mindre andre krav framgår.

Logging er nødvendig for å oppfylle krav i personopplysningsloven og personvernforordningen til ivaretakelse av personopplysningssikkerheten:

- krav til integritet og konfidensialitet i art. 5 (f)
- krav til behandlingsansvarlig i art. 24 (1)
- art. 32 om krav til sikring,
- art. 25 om innebygd personvern

Loggene benyttes blant annet til å sikre spor ved eventuelle sikkerhetsbrudd, som hjelpemiddel ved feilsøking og til dokumentasjon i forbindelse med eksterne revisjoner.

Oversikt over de spesifikke loggene vil være tilgjengelig i IT-seksjonen.

2. Definisjoner

Sporingslogg	logg som er ment å brukes til å kunne spore hvilke brukere som har slått opp personopplysninger i NPEs systemer. Begrepet «innsynslogg» brukes også.
Tjenestekall-logg	logg av kall mellom applikasjoner/tjenester
Sikkerhetslogg	logg over sikkerhetsrelaterte hendelser (brannmur, ruter mv.). Alle brudd på sikkerhetsregler (forsøk på ulovlig tilgang, brudd på regler for datatrafikk, hacking forsøk osv.). Benyttes til bl.a. analyser av eventuelle angrep eller ulovlige hendelser.
Applikasjonslogg	En fil over hendelser som er logget av et program/applikasjon. Kan bl.a. inneholde informasjon om programmets kjøretidsadferd, feil, informative hendelser, advarsler etc.

Annen logg	Annen logg som brukes til feilsøking, overvåking, kapasitetsplanlegging osv. Kan f.eks. være systemlogger. Bruk av administrator konto (brukere med utvidete rettigheter) skal også logges (dette kan også være en del av sikkerhetslogg). Logg av tildeling av rettigheter til brukere etc.
Personopplysninger	Dette er informasjon som er definert og regulert av Personvernforordningen som kan knyttes til eller identifisere en enkeltperson, herunder navn, personnummer, kontaktopplysninger, bilde, handlemønster, fingeravtrykk, irismønster, dynamisk IP-adresse.

3. Krav til logging og oppfølging av logger i NPE

3.1 Generelle krav

- All logg skal lagres og behandles på sikker måte, i hensiktsmessig miljø for loggen det gjelder. Logger skal sikres mot innsyn, endring og sletting av uautorisert personell. Autorisert personell skal ikke kunne endre/slette logger, dersom endring/sletting er mulig skal dette være sporbart.

- Logger for ulike behov skal skilles på en måte som gjør det mulig å lage tekniske sperrer for hvem som kan se hvilke logger

- Tekniske rutiner for logging beskrives i generell systemdokumentasjon

- Logger skal *ikke* brukes til andre formål enn det de er samlet inn for, som for eksempel å kartlegge hvor mye tid hver enkelt arbeidstaker bruker på ulike oppgaver.

- Dersom logger indikerer straffbare forhold, skal forholdet vurderes iht. Personalhåndboken

- Dersom oppføringer i logger kan knyttes til enkeltpersoner, skal loggene slettes når de ikke lenger er nødvendige for utførelse av NPEs oppgaver.

3.2 Sporingslogg

- Sporingsloggen skal vise hvilke brukere som har behandlet (slått opp, søkt på, endret eller eksportert) personopplysninger om en identifisert (eller identifiserbar) person

- Sporingslogg skal lages i alle systemer som inneholder personopplysninger («skarpe data»)

- Tilgang til sporingslogg skal være strengt kontrollert og administrert. Kun personer med tjenstlig behov skal gis tilgang (f.eks. internrevisjon, systemadministrator). Tilgangsstyring til sporingslogg skal godkjennes av seksjonssjef IT-seksjonen

- Sporingsloggen er i seg selv personopplysninger, og tilgang til denne skal også logges

- Sporingslogg skal oppbevares i minimum 90 dager.

- Sporingsloggen skal kun inneholde nødvendig informasjon for formålet med loggen. Eksempler på dette kan være:
    - Dato og klokkeslett
    - Systemnavn
    - Brukernavn, eller tilsvarende unik identifikasjon av brukeren
    - Rolle (brukerens aktive rolle i systemet)
    - Personnummer (11 siffer) til den registrerte, eller andre entydig identifikator for den registrerte. Personnummer skal kun brukes dersom annen entydig identifikator ikke er egnet.
    - Hvilken informasjon som er berørt
    - Klientens IP-adresse
    - Status/resultat, hvorvidt operasjonen brukeren forsøkte var vellykket

3.3 Tjenestekall-logg

- Tjenestekall-loggen vil kunne inneholde personopplysninger og må i slike tilfeller sikres på bakgrunn av dette.
- Systemeier beslutter hvem som skal ha tilgang til tjenestekall-logg. Tilgangen til disse loggene må begrenses til kun de med tjenstlig behov.
- Systemeier beslutter hvor lenge tjenestekall-logg skal lagres.

3.4 Annen logg

- Annen logg skal så langt det er mulig ikke inneholde personopplysninger.
- Det skal være tilgangsstyring til logger. Tilgangen til disse loggene må begrenses til kun de med tjenstlig behov.
- Applikasjonslogg brukes til feilsøking, kapasitetsplanlegging, SLA-overvåking eller å avdekke forsøk på innbrudd.
- Systemeier beslutter hvem som skal ha tilgang til applikasjonslogg
- Systemeier må i samråd med drift/driftspartnere (NHN mv.) beslutte hvor lenge applikasjonslogg skal lagres

3.5 Innsyn i logg

Enhver har krav på innsyn i NPEs behandling av sine personopplysninger. Ansatte og borgere har krav på innsyn i alle registrerte opplysninger om dem selv.

- Det må i hvert enkelt tilfelle vurderes om den som krever innsyn kan få det i logger som inneholder sine personopplysninger.
- I tilfeller der en utlevering av loggdata vil kunne svekke informasjonssikkerheten bør en ikke gi innsyn. Et eksempel kan være at logger avslører sikkerhetsmekanismer som potensielt kan omgås om disse blir kjent.

3.6 Bruk av logger

- Elektroniske logger skal enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd på interne retningslinjer og personopplysningsloven.
- Det skal være prosedyrer for håndtering av brudd og for når personalmessige reaksjoner skal iverksettes.
- Logger som inneholder personopplysninger skal ha en definert oppbevaringstid, og skal slettes når oppbevaringstiden utløper.
- Analyser av logger skal i så stor grad som mulig basere seg på behandling av anonyme opplysninger.