Ministerie van Justitie en Veiligheid

Beleidskader Logging

Informatiebeveiliging JenV

Versie v1.0

Documentbeheer:

Datum	29 april 2024
Status	Definitief met akkoord DOR

Eigenaar	: CIO JenV	
Ingestemd	: DOR	Datum : 29 april 2024
Vastgesteld	: BBR	Datum : dd mm 2024

Versie beheer:

Versie	Datum	Review
0.1		Review door ICS-IB
0.2		Review door BVA
0.3		Review door domeinhouders
0.3		Review door architecten
0.4		Review door Privacy-board
0.4		Review door CISO-board
0.5		1e vooroverleg met OR (mr. Lieke van Hees)
0.53		. 2e bespreking CISO board oktober 2021 . CTO-overleg
0.7		Aanbieden CIO Raad
0.7		Technisch vooroverleg met OR (mr. Lieke van Hees)
0.71		Vervolgoverleg met OR
0.99		Aanbieden voor formeel instemmingsverzoek aan DOR
0.999	15032024	Verwerkt advies DOR
1.0	28032024	Verwerkt finale advies DOR
1.0	29042024	Instemming DOR JenV
1.0	29042024	Doorgeleiden BBR JenV

Inhoudsopgave

MANAGEMENTSAMENVATTING 5

1 BESCHRIJVING 6

1.1 STRUCTUUR INFORMATIEBEVEILIGING 6
1.1.1 Relatie tot andere beleidsdocumenten 6
1.2 DOEL, SCOPE EN DOELGROEPEN 6

2 WERKING 8

2.1 VAN TOEPASSING ZIJNDE NORMEN VOOR LOGGING 8
2.1.1 BIO 2019 8
2.1.2 Algemene Verordening Gegevensbescherming (Avg) 9
2.1.3 Wet politiegegevens (Wpg) en Wet justitiële en strafvorderlijke gegevens (Wjsg) 10
2.1.4 Wet op de ondernemingsraden (WOR) 10
2.1.5 NEN 7513 11
2.2 BELEID EN MAATREGELEN M.B.T. LOGGING EN MONITORING 11
2.2.1 Randvoorwaarden en uitgangspunten 11
2.2.2 Welke gebeurtenissen moeten worden opgeslagen in logbestanden? 14
2.2.3 Welke gegevens wel en niet opslaan in logbestanden? 14
2.2.4 Wat wordt er met de logging gedaan? 15
2.2.5 Hoe worden logbestanden beschermd? 16
2.2.6 Hoe lang mogen/moeten logbestanden worden bewaard? 17
2.2.7 Verantwoordelijkheden voor logging 17
2.2.8 Speciale aandachtspunten bij logging in cloudomgevingen 17
2.2.9 Wat te doen bij uitvallen van de logging? 18
2.2.10 Hoe wordt over logging gecommuniceerd naar eindgebruikers? 19

BIJLAGE 1: WAT IS LOGGING? 20

LOGGING SOORTEN 21
WAT ZIJN DE MEEST VOORKOMENDE FOUTEN BIJ LOGGING? 21
LOGGING-CYCLUS EN -OPSLAG 22

BIJLAGE 2: SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) 23

BIJLAGE 3: COMMUNICATIE OVER LOGGING VAN TOEGANG TOT EN GEBRUIK VAN SYSTEMEN 25

Logging 25
Communicatie over logging naar eindgebruikers 25
OR 25

BIJLAGE 4: JURISPRUDENTIE T.A.V. PRIVACY ASPECTEN 26

RVS AFDELING BESTUURSRECHTSPRAAK 20-11-2011 *ECLI:NL:RVS:2011:BU6383* 26
RECHTBANK DEN HAAG 31-03-2021 *ECLI:NL:RBDHA:2021:3090* 26
RECHTBANK MIDDEN NEDERLAND 02-12-2020 27
ECLI:NL:RBMNE:2020:5410 27
AUTORITEIT PERSOONSGEGEVENS 26-11-2020 27

BIJLAGE 5: LIJST VAN GEBRUIKTE AFKORTINGEN 28

Managementsamenvatting

Dit beleidskader bevat de normen voor logging binnen het Ministerie van Justitie en Veiligheid, voor zover deze logging te maken heeft met informatiebeveiliging en privacy (bv. toegang tot bestanden, of het bezoeken van "besmette" websites). Logging betreft het proces van registreren van informatie over menselijke- en systeemactiviteiten binnen systemen en op netwerken, en het vastleggen daarvan. In het kader van informatiebeveiliging is logging ofwel gerelateerd aan use-cases die in het Security Information and Event Management (SIEM) systeem beschreven zijn, ofwel aan detectie van onjuist handelen door een medewerker in relatie tot persoonsgegevens. Dit kan betrekking hebben op zowel technische als applicatieve logging. Logging die om andere redenen dan informatiebeveiliging plaats vindt worden niet in dit document beschreven (Zie ook bijlage 1: Wat is logging?).

Goede beveiligingslogging kan o.a. gebruikt worden voor het (achteraf) ontdekken van indringers in systemen, en is de basis voor onderzoek naar beveiligingsincidenten en datalekken. Ook is logging van belang bij het aantonen van compliance aan geldende kaders en richtlijnen.

Logfiles bevatten o.a. (persoons-)gegevens van gebruikers, activiteiten van gebruikers, applicaties, netwerkcomponenten, servers en client-devices, evenals uitzonderingen en informatiebeveiligingsgebeurtenissen. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en controle op naleving van toegangscontrole. Deze logging-informatie kan dienen om specifieke dreigingen en informatiebeveiligingsincidenten te detecteren en bewijsmateriaal te verzamelen bij forensische onderzoeken.

Logging dient aan bepaalde richtlijnen/normen te voldoen; dit document geeft daarvoor een kader. Conform het Beleid informatiebeveiliging en het Privacybeleid JenV voldoet JenV aan Nederlandse wet -en regelgeving en met name aan de Baseline Informatiebeveiliging Overheid (BIO), de Algemene Verordening Gegevensbescherming (AVG), de Wet justitiële en strafvorderlijke gegevens (WJSG) en de Wet politiegegevens (Wpg). Organisaties kunnen afwijken van het beleidskader Logging, mits de afwijking bestuurlijk wordt geaccordeerd en de medezeggenschapsraad van de organisatie instemming heeft gegeven.

Deze normen bestrijken het gehele gebied van informatiebeveiliging: van de organisatie van beleid tot uitvoering inclusief kwaliteitszorg. Implementatie van de geldende normen en methoden is een randvoorwaarde voor informatiebeveiliging (verder steeds afgekort tot "IB") en privacy: "de basis op orde". De reguliere onderhoudscyclus (PDCA) is van toepassing hetgeen betekent dat herijking van dit document minimaal eens per 3 jaar plaatsvindt.

1 Beschrijving

Dit beleidskader beschrijft de normen voor logging binnen het Ministerie van Justitie en Veiligheid, voor zover deze logging te maken heeft met informatiebeveiliging en privacy (bv. toegang tot bestanden, of het bezoeken van "besmette" websites). In het kader van informatiebeveiliging is logging ofwel gerelateerd aan use-cases die in het Security Information and Event Management (SIEM) systeem (of ander soortgelijk systeem) beschreven zijn, ofwel aan detectie van onjuist handelen door een medewerker in relatie tot persoonsgegevens. Dat betekent dat logging die om andere redenen plaats vindt niet in dit document beschreven worden.

Dit document is geschreven om informatiebeveiligings- en privacymaatregelen met betrekking tot logging en controle uit te werken en daarbij handreikingen te geven voor het logging-beleid en logging-procedures. Het document stelt de verplichte kaders waar door de taakorganisaties uitvoering aan moet worden gegeven[1]. Hoofdstuk 2 beschrijft waar logging aan moet voldoen. In de bijlagen 1 en 2 wordt nader ingegaan op wat er onder logging wordt verstaan, en de inzet van het SIEM hierbij. In bijlage 3 is een communicatieopzet opgenomen die gebruikt kan worden als gecommuniceerd gaat worden over logging.

1.1 Structuur informatiebeveiliging

In onderstaand schema is de positie van dit beleidskader weergegeven.

Beleid Informatiebeveiliging	Kaderdocument Informatiebeveiliging [dit document]

1.1.1 Relatie tot andere beleidsdocumenten

Dit beleidskader staat niet op zich maar maakt onderdeel uit van het JenV brede stelsel met betrekking tot informatiebeveiliging en privacy. Dit document vindt zijn bestaansrecht in het *Kaderdocument informatiebeveiliging JenV* en het *Privacybeleid JenV*.

1.2 Doel, scope en doelgroepen

Dit beleidskader heeft betrekking op het beheer en gebruik van beveiligingslogging binnen alle onderdelen van JenV (zowel centraal als decentraal). Daarbij gaat het om *wat* er gelogd moet worden, niet *hoe* er gelogd wordt.

Goede beveiligingslogging kan o.a. gebruikt worden voor (niet-limitatief):

[1] In het geval de onderdelen ruimte hebben om af te wijken van dit kader en deze afwijkingen raken een formele bevoegdheid van de medezeggenschap, dan zullen deze voorgenomen afwijkingen formeel d.m.v. een instemmingsverzoek aan de OR van het onderdeel worden voorgelegd. Daarnaast dient het gebruik van systemen die als personeelsvolgsysteem kunnen worden gebruikt, aan de OR te worden voorgelegd.

- *threat hunting en monitoring*: signaleren van en acteren op specifieke dreigingen en incidenten, het ontdekken van indringers in systemen, en corruptie van data of programmatuur en antivirusmeldingen.
- *forensics*: het veiligstellen en analyseren van bewijsmateriaal.
- Het ondersteunen van onderzoek na een (beveiligings)incident.
- Het ondersteunen van Service Level Agreement (SLA) Compliance Monitoring.
- Het leveren van informatie ten behoeve van een wettelijk voorgeschreven audit.
- Het leveren van informatie om te onderzoeken of voldaan wordt aan beleid (bijvoorbeeld of er ongeautoriseerde apparaten aangesloten zijn geweest).
- Het leveren van informatie om onweerlegbaar aan te tonen dat een bepaald bericht wel of niet verzonden is, of dat een activiteit is uitgevoerd.
- Het mitigeren van door incidenten gebleken risico's in systemen en processen.
- Rapportage over incidenten aan de systeemeigenaar en de Chief Information Security Officer (CISO) van zowel de eigen organisatie als op Concern-niveau, zowel op incident- als op geaggregeerd niveau (trends).
- Rapportage over datalekken aan de hoogst leidinggevende van de organisatie, de Functionaris voor Gegevensbescherming (FG) en mogelijk de Autoriteit Persoonsgegevens (AP).

Monitoring betreft het actief gebruiken van gelogde informatie om de digitale veiligheid van de organisatie en de privacy van persoonsgegevens (medewerkers, burgers) te waarborgen. In de paragraaf "Wat wordt er met de logging gedaan?" wordt toegelicht hoe dit kan worden gedaan..

Dit beleidskader is allereerst van belang voor Chief Information Officers (CIO's), Chief Technology Officers (CTO's,als systeemeigenaar), CISO's, Privacy Officers (PO's), applicatie-, netwerk- en systeembeheerders, Integriteitscoördinatoren, leden van de diverse ondernemingsraden, en domeinhouders en ontwikkelaars. De afbakening in taken, verantwoordelijkheden en bevoegdheden tussen deze functionarissen kan per JenV-organisatie anders geregeld zijn.
Daarnaast is dit beleidskader voor alle medewerkers van JenV van belang, omdat logging o.a. gebaseerd is op informatie over gedrag en handelingen van medewerkers. Vandaar dat over logging ook altijd gecommuniceerd moet worden naar eindgebruikers (zie in dit verband: par. 2.2, sub "Randvoorwaarden en uitgangspunten", onder de bullet "communicatie over logging", en onder de sub paragraaf "Hoe wordt over logging gecommuniceerd naar eindgebruikers?").

2 Werking

De werking van dit beleidskader wordt onderverdeeld in een aantal aandachtsgebieden. Enerzijds zijn dat vigerende kaders, zoals de controls die vanuit de BIO relevant zijn voor het specifieke aandachtgebied. Anderzijds betreft het de maatregelen die geselecteerd kunnen worden op het gebied van organisatie (mens), proces en techniek.

2.1 Van toepassing zijnde normen voor logging

2.1.1 BIO 2019

Goed loggen is een eis uit de BIO en soms noodzakelijk om te kunnen voldoen aan een wettelijke eis, om bijvoorbeeld een audit op een systeem te doen. De eisen die gesteld worden aan logging worden zwaarder naarmate het te beschermen belang zwaarder is. Hiervoor beschrijft dit document m.b.t. logging de specifieke eisen. Dit document gaat uit van de minimale eisen aan logging op basis van de BIO.

BIO-controls in scope van dit beleidskader:

Controls

control	Beschrijving
Doelstelling	Onbevoegde toegang tot systemen en toepassingen voorkomen.
9.4.4.2-2	Het gebruik van systeemhulpmiddelen[2] wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.
Doelstelling	Gebeurtenissen vastleggen en bewijs verzamelen.
12.4.1-1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
12.4.1.1-1	Een logregel bevat minimaal: a. de gebeurtenis; b. de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; c. het gebruikte apparaat; d. het resultaat van de handeling; e. een datum en tijdstip van de gebeurtenis (gerelateerd aan een tijdzone).
12.4.1.2-1	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.

[2] Systeemhulpmiddelen met logging vallen dus binnen dit beleidskader.

control	Beschrijving
12.4.1.3-2	De informatie verwerkende omgeving wordt gemonitord door een SIEM en/of SOC[3] middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.
12.4.1.4-2	Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT[4] (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.
12.4.1.5-2	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.
12.4.2-1	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
12.4.2.1-1	Er is een overzicht van logbestanden die worden gegenereerd.
12.4.2.2-1	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.
12.4.2.3-2	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.
12.4.2.4-2	Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.
12.4.3-1	Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.
12.4.4-1	De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.
Doelstelling	Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.
16.1.7.1-2	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.
16.1.7-2	De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.

2.1.2 Algemene Verordening Gegevensbescherming (Avg)

[3] Security Operations Center

[4] Computer Emergency Response Team

De Avg stelt strenge eisen aan de beveiliging van persoonsgegevens en aan de manier waarop hierover verantwoording moet worden afgelegd. Hieruit zijn met name (maar zeker niet uitsluitend) de artikelen 5, 12, 24 en 42 van belang. Logging wordt niet expliciet in de Avg genoemd, maar de Avg vereist wel van organisaties dat ze passende technische en organisatorische maatregelen treffen om persoonsgegevens te beschermen (art. 32)). Logging wordt door de Autoriteit Persoonsgegevens (AP) aangemerkt als een technische maatregel en valt als verwerking van persoonsgegevens als zodanig onder de Avg. Daar waar passende technische en organisatorische maatregelen moeten worden genomen zodat een passende beveiliging gewaarborgd is, moet onder meer gedacht worden aan:

- het inbouwen van waarborgen om te kunnen aantonen dat de verwerking van persoonsgegevens wordt verricht in overeenstemming met hetgeen bij of krachtens wet (Avg) is bepaald;
- het kunnen bepalen van de waarschijnlijke oorzaken van de inbreuk op de beveiliging van gegevens.

Logging volgt als maatregel om een bepaald risico binnen een systeem te kunnen mitigeren (bijvoorbeeld ongeautoriseerde toegang). In de Data protection impact assessment (DPIA) die op dat systeem is uitgevoerd, moeten gegevens i.h.k.v. logging standaard worden meegenomen[5]. Daarbij komen alle elementen uit de DPIA aan bod. Raadpleeg de privacy officer bij de uitvoering van een DPIA.
Wanneer er voor JenV-dienstverlening gelogd wordt bij een leverancier, worden te loggen persoonsgegevens vastgelegd in een verwerkersovereenkomst.

2.1.3 Wet politiegegevens (Wpg) en Wet justitiële en strafvorderlijke gegevens (Wjsg)

In de *Richtlijn gegevensbescherming opsporing en vervolging*, de Wpg en de Wjsg geldt ook de eis dat gegevens beveiligd dienen te worden. Logging dient om aan te tonen dat de beveiligingsmaatregelen aanwezig zijn en functioneren (verantwoording). De Richtlijn bevat wel een verplichting tot logging (artikel 25). Per mei 2023 treedt in de Wpg artikel 32a en in de Wjsg artikel 26e in werking, waarin een specifieke loggingplicht is opgenomen. De persoonsgegevens die in het kader van de loggingplicht worden verwerkt, vallen onder de werking van de Avg. Daar waar verwezen wordt naar artikelen uit de Avg, zijn deze dus ook op de logginggegevens in het kader van de Wpg en de Wjsg van toepassing. In de Wpg zijn met name de artikelen 3 t/m 4b van belang. Voor de Wjsg zijn dat de artikelen 3, 7 t/m 7f, 17a t/m 26a en 7 jo. 1b Wjsg. Loggegevens die worden vastgelegd als zodanig vallen onder de Avg.

2.1.4 Wet op de ondernemingsraden (WOR[6])

De ondernemingsraad (OR) moet worden betrokken bij elk voorgenomen besluit tot vaststelling, wijziging of intrekking van een regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen[7].

---

[5] In geval van een systeem dat een gemeenschappelijke voorziening betreft, wordt de logging meegenomen in de JenV-brede DPIA's op die betreffende systemen.

[6] Zie WOR art. 27, 1e lid sub L en K.

[7] Zie ook: Autoriteit Persoonsgegevens (z.j.), *Het OR-privacyboekje: De rol van de ondernemingsraad bij privacy op de werkvloer*.

Logging is in het kader van de Wpg en Wjsg een wettelijke verplichting en logging is in het kader van de AVG een manier om te voldoen aan de verantwoordingsplicht. Voor de Wjsg is de DOR het aanspreekpunt; voor de Wpg de van toepassing zijnde medezeggenschapsorganen. De verantwoordelijkheden van de Medezeggenschapsraden ten aanzien van deze wetgeving zal dus beperkter zijn en vooral zien op de wijze waarop invulling wordt gegeven aan de wettelijke verplichting: staat de inbreuk van de werkgever in het 'privédomein' van de werknemer in verhouding tot het doel dat de werkgever moet bereiken (m.a.w.: kan de verwerking van persoonsgegevens en het monitoren/volgen van medewerkers, gegeven het doel, tot het hoogstnoodzakelijke worden beperkt?)? De afweging die de verantwoordelijke bestuurder hierin maakt, moet worden voorgelegd aan het van toepassing zijnde medezeggenschapsorgaan.

De Departementale Ondernemingsraad (DOR) wordt standaard betrokken bij huidige en toekomstige wijzigingen in het JenV-loggingsbeleid[8].
Indien de DOR vindt dat de controle op de logging afwijkt van het normale monitoringsbeleid, kan zij aangeven op welke onderdelen zij meent een instemmingsrecht te hebben. Dit instemmingsrecht geldt in ieder geval voor elk voorgenomen besluit tot vaststelling, wijziging of intrekking van een regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen. Wanneer bij de ontwikkeling van nieuwe logtoepassingen behoefte is aan een afwijkende invulling, met name ten aanzien van de vast te leggen gegevens of het gebruik daarvan, dan dient hiervoor instemming van de DOR te worden gevraagd.

Als JenV-onderdelen dit beleidskader willen wijzigen, dan wel aanvullen met organisatie-specifiek beleid op het gebied van informatiebeveiliging-gerelateerde logging, moeten deze wijzigingen/aanvullingen ter instemming worden aangeboden aan de betrokken ondernemingsraad.

2.1.5 NEN 7513

Logging moet voor wat betreft de gezondheidsgegevens (bv. m.b.t. justitiabelen) voldoen aan de specificaties zoals die zijn beschreven in de NEN 7513 voor de zorgsector. De Autoriteit Persoonsgegevens zal deze norm gebruiken als toetsingskader. De belangrijkste aspecten uit de NEN7513 zijn al opgenomen in dit beleidskader logging, voor de volledige set regels wordt verwezen naar de NEN 7513 norm zelf.

2.2 Beleid en maatregelen m.b.t. logging en monitoring

2.2.1 Randvoorwaarden en uitgangspunten

- *Basis van logging:* De aard en frequentie van logging en monitoring op informatiesystemen wordt vastgesteld op basis van risicomanagement. De risico's voor betrokkenen en het van toepassing zijnde Basis Beveiligings Niveau (BBN; zie BIO) worden hierin ook nadrukkelijk meegewogen. Logging is, naast andere noodzakelijke preventieve en detectieve maatregelen, een manier om risico's te mitigeren. Logging is daarom gebaseerd op dreigingsscenario's. Deze scenario's geven ook richting aan de selectie van de te loggen gegevens. In dat kader moet zijn vastgelegd welke gegevens gelogd worden, en bij welke drempelwaarden meldingen en

[8] In geval van gezamenlijke verwerkingsverantwoordelijkheid vormt het betrekken van meerdere ondernemingsraden een aandachtspunt. Zie tevens het kopje 'Verantwoordelijkheden voor logging'.

alarmoproepen gegenereerd worden bij welke systemen. Bij voorkeur geschiedt dit op basis van 'use cases' die in een SIEM (kunnen) worden vastgelegd en gebruikt. Input voor deze use cases komt uit risico-analyses IB, Quick Scans IB, DPIA's, audits, etc. Voor het maken van een use case wordt gebruik gemaakt van het MITRE attack framework.

- *Minimaal te loggen componenten:* In ieder geval moet voor de volgende componenten logging ingericht worden[9]:
  - de 'perimeter', de buitenkant van het netwerk van JenV en de systemen en netwerk componenten in de Demilitarized Zone (DMZ)
  - Besturingssytemen
  - Databases
  - Systemen voor toegangsbeheer, zoals Active Directory en MFA-systemen
  - Anti-malware oplossingen
  - Firewalls
  - Intrusion Detection Systemen
  - Applicaties (incl. Software-as-a-Service (SaaS))
  - Endpoints (zoals servers en werkstations)
  - Routers, switches en WiFi-apprartuur.

- *Afspraken met ICT-dienstverleners:* Met ICT dienstenleveranciers (verwerkers) worden maatregelen afgesproken over logging en monitoring, gebaseerd op de risicoafweging voor de afgenomen producten of diensten. SOC 2 type 2[10] en dit beleidsdocument zijn hierbij het uitgangspunt. Persoonsgegevens die i.h.k.v. logging worden verzameld bij een (externe) ICT-dienstverlener, worden vastgelegd in een verwerkersovereenkomst. Wanneer het gaat om cloud-dienstverleners: zie paragraaf "Speciale aandachtspunten bij logging in SaaS-omgevingen).

- *Communicatie over logging:* Op grond van artikel 12 AVG wordt over het doel en het gebruik van logging transparant gecommuniceerd richting betrokkenen (waaronder medewerkers). Kennisgeving is niet alleen van belang om te voldoen aan de AVG, maar kan ook bijdragen aan het verminderen van ongeautoriseerde toegang. Sowieso mogen medewerkers immers pas autorisaties krijgen voor bepaalde gegevens als ze die gegevens voor hun functie-uitoefening nodig hebben ("need-to-know"-principe). Daarnaast zullen medewerkers die wel geautoriseerd zijn om bepaalde gegevens te raadplegen, minder snel geneigd zijn dit onnodig te doen wanneer zij weten dat er logbestanden worden bijgehouden. Bij opgetreden incidenten worden waar mogelijk en gewenst eindgebruikers en/of klanten geïnformeerd.

- *Integriteitsschending:* Bij een integriteitsschending is het reguliere integriteitsbeleid van het betreffende JenV-onderdeel van toepassing. De zaak zal in dat geval worden overgedragen aan de integriteitscoördinator, die uitvoering geeft aan het integriteitsonderzoek. Er is sprake is van een integriteitsschending als een medewerker in strijd met de voorschriften van de organisatie handelt of op andere wijze de normen en waarden niet naleeft. Deze kernelementen zijn terug te vinden in artikel 6, eerste lid, van de Ambtenarenwet 2017. In artikel 6, eerste lid, van de Ambtenarenwet is

[9] Kan afhankelijk zijn van specifieke context/omgeving; welke gegevens en aspecten precies gelogd moeten worden, is afhankelijk van de risicoanalyses/use cases.

[10] Bij SOC2 Type 2 wordt door een onafhankelijke derde partij getoetst of er ook daadwerkelijk is gewerkt volgens de vastgestelde procedures en controles. Om een SOC2 Type 2 verklaring te kunnen behouden vindt een jaarlijks terugkerende audit plaats, waarbij gekeken wordt of de betreffende organisatie heeft voldaan aan de afgesproken processen en controles gedurende de voorgaande periode.

bepaald: De ambtenaar is gehouden de bij of krachtens de wet op hem rustende en uit zijn functie voortvloeiende verplichtingen te vervullen en zich ook overigens te gedragen zoals een goed ambtenaar betaamt. In hoofdstuk 15 van de CAO Rijk is bepaald dat als een medewerker toch iets doet wat niet mag of juist niets doet terwijl hij wel iets had moeten doen, de werkgever hem daarvoor een straf kan opleggen. Welke straffen kunnen worden opgelegd is in datzelfde hoofdstuk van de CAO Rijk opgenomen. In hoofdstuk 13.3.2 van het Personeelsreglement van het ministerie van Justitie en Veiligheid zijn nadere voorschriften opgenomen voor het melden van integriteitsschendingen en misstanden. In hoofdstuk 13.3.3 van dit reglement zijn nadere voorschriften opgenomen over welke stappen gezet moeten worden na het ontvangen van een melding van een integriteitsschending of misstand. In hoofdstuk 13.14 van dit reglement is de procedure voor ordemaatregelen en straffen uitgewerkt.

- *Privacy en Security By Design:* Voor de inrichting en toegang van logbestanden zijn privacy en security by design principes van toepassing (m.n. art. 25 AVG). Raadpleeg bij de toepassing van deze principes de CISO, privacy officer en eventueel een archivaris. Denk hierbij aan[11]:
    - Bewaartermijnen (niet langer bewaren dan noodzakelijk, afhankelijk van (al dan niet domeinspecifieke) vigerende wet- en regelgeving; te bepalen door CISO, PO en archivaris gezamenlijk)
    - Dataminimalisatie (alleen loggen wat noodzakelijk is; te bepalen d.m.v. risico-analyse)
    - Toegangsbeleid (need to know)
    - Cryptografische maatregelen
    - Integriteit van de loginformatie (onaanpasbaarheid)

- Centrale en decentrale logging: Op meerdere niveaus kan en moet worden gelogd. Centrale logging vindt in ieder geval plaats op JenV-brede dienstverlening, zoals Justitienet. Decentrale logging vindt vooral plaats op organisatie-specifieke dienstverlening, zoals systemen en databases ter ondersteuning van processen, en user-endpoints (waar de organisatie-CIO en systeemeigenaar verantwoordelijk voor zijn). Logging dient veilig te worden bewaard, als het kan op een centraal punt (bij voorkeur wordt aangesloten op het centrale logplatform binnen JenV). Als logging niet op een centraal punt wordt bewaard, dient deze wel zoveel mogelijk raadpleegbaar te zijn vanuit een centraal punt. Logging van systemen, infra en applicaties binnen JenV moeten namelijk met elkaar te correleren zijn: een dreiging of mogelijke besmetting bij een van de uitvoeringsorganisaties kan een risico voor een andere organisatie beteken. Door de logging centraal raadpleegbaar te maken, is het mogelijk een JenV breed risico beter in te schatten.

- *Herleidbaarheid:* Handelingen op informatie verwerkende systemen dienen, daar waar noodzakelijk, zoveel mogelijk terug te herleiden zijn tot natuurlijke personen[12]. Er mogen niet meer persoonsgegevens worden gelogd dan noodzakelijk (dataminimalisatie[13]).

- *Wijze van logging:* Zoveel als mogelijk wordt systeemgebruik *automatisch* gelogd.

[11] Zie in dit verband ook par. 2.1.4.

[12] De eisen voor Wpg en Wjsg zijn zwaarder: als verstrekkingen (waaronder bevragingen) daaronder vallen, dan zullen deze *verplicht* op een persoon herleidbaar vastgelegd dienen te worden als dit mogelijk is.

[13] Zie AVG, art. 5, lid 1, sub C

- *Werkinstructies en procedures:* Er zijn vastgestelde procedures en/of werkinstructies, waarin beschreven staat:
    - welke persoon en/of rol verantwoordelijk is voor het maken van lograpportages
    - welke persoon en/of rol verantwoordelijk is voor het beoordelen daarvan.
    - Hoe en met welke frequentie deze beoordeling moet worden uitgevoerd
    - Op welke wijze logging (indien nodig) extern veiliggesteld moet worden (bv. t.b.v. forensisch onderzoek).

- *Tijdsynchronisatie:* De klokken van alle relevante informatiesystemen van de organisatie behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron, zodat logs met elkaar vergeleken en gecorreleerd kunnen worden. De tijdzone is daarbij een belangrijke parameter.

2.2.2 Welke gebeurtenissen moeten worden opgeslagen in logbestanden?

De volgende gebeurtenissen worden *in ieder geval* opgenomen in de logs:

- Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instellingen: uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore.
- Gebruik van systeemhulpmiddelen.
- Gebruik van functies voor functioneel beheer, zoals het wijzigingen van configuraties en instellingen, release van nieuwe functionaliteiten, ingrepen in gegevenssets (waaronder databases).
- Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren van gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels.
- Autorisatieschema's van eindgebruikers, om te achterhalen welke rechten de gebruiker had ten tijde van de logging (anders is geen verantwoording mogelijk).
- Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, zoekacties op persoonsgegevens, gebruik van online transacties, en toegang tot bestanden door systeembeheerders.
- Online transacties. Hierbij wordt gelogd: het bericht-ID, datum en tijd, aanroepend en verzendend systeem en -proces.
- Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op kwetsbaarheden, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van Security Services).
- Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens het uitvoeren van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of -systemen).

Daarnaast kunnen gebeurtenissen worden opgeslagen o.b.v. risico-analyses.

2.2.3 Welke gegevens wel en niet opslaan in logbestanden?

In de BIO staat ook wat relevante input en output van een ICT-systeem of -service is. Op basis daarvan moeten de volgende gegevens in logbestanden worden opgeslagen:

- Een tot een natuurlijk persoon herleidbare unieke gebruikersnaam of ID van eindgebruikers

- De gebeurtenis (zie hiervoor paragraaf hierboven "Welke gebeurtenissen moeten/mogen wel en niet worden opgeslagen in logbestanden?**"**)
- Waar mogelijk de identiteit van het werkstation of de locatie. Denk aan: host naam, Operating System, naam van de toepassing, IP-adres(sen), locatie(s). *NB.: het systeem dat de logregel veroorzaakt staat vaak niet in de logregel zelf, in dat geval moet het logsysteem deze toevoegen aan de opgenomen logregel.*
- Het object waarop de handeling werd uitgevoerd
- Het resultaat van de handeling
- De datum en het tijdstip van de gebeurtenis
- De betrokken systemen of infrastructuur

In een logregel mogen géén gevoelige gegevens worden opgenomen! Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, et cetera). In de logregel moeten persoonsgegevens uit systemen van de organisatie zelf zoveel mogelijk worden vermeden (gebruikersnamen en/of inlog accounts mogen wel).

Soms is het echter onvermijdelijk of is JenV zelfs verplicht om wél personalia of wettelijke persoonsnummers op te nemen in een logregel:

- Onvermijdelijk is het bijvoorbeeld in die gevallen dat de logregel (mede) gebruikt wordt om te voldoen aan het recht van betrokkene om inzage te geven in de verstrekkingen van zijn gegevens (aan derden). Een identificerend gegeven is dan noodzakelijk om vast te stellen aan wie de gegevens zijn verstrekt.
- Er zijn ook andere gevallen denkbaar dat het vastleggen van die gegevens noodzakelijk zijn. De noodzakelijkheid moet (kunnen) blijken uit de DPIA die op de verwerking is uitgevoerd.

Raadpleeg de privacy officer en de CISO bij het bepalen van de inhoud van de logregel.

Ten aanzien van de gebruikersnamen en accounts is het goed om hier nog op te merken dat in mei 2023 artikel 26e van de Wjsg en artikel 32a van de Wpg in werking zal treden. Hierin is de verplichting opgenomen om, indien mogelijk, de gebruikersnamen of herleidbare identificerende gegevens van degene aan wie gegevens zijn verstrekt (dus ook de bevragers van systemen) vast te leggen. Bestaande systeem tot systeem koppelingen zullen in een aantal gevallen dus aangepast moeten worden om op een persoon herleidbare user-ID's op te nemen en aldus te voldoen aan deze nieuwe wettelijke verplichting.

2.2.4 Wat wordt er met de logging gedaan?

- Logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren bij voorkeur aangesloten op een Security Information and Event Management systeem (SIEM) of geschikt om op een later moment aan te sluiten op een SIEM. Hiermee worden (gecorreleerde) meldingen en alarmoproepen aan de beheerorganisatie gegeven.
- Logging wordt gecorreleerd en tegen dreigingsinformatie aangehouden. Periodiek, minimaal maandelijks, worden de logbestanden beoordeeld (bv. aanwezigheid, bewaartermijnen, systematische controle op ongeautoriseerd inzien en muteren van data, etc.). De Autoriteit Persoonsgegevens (AP) benadrukt het belang van controle op de logging in een boetebesluit uit 2020[14]. Op basis van deze logginggegevens wordt passende actie ondernomen om de dreigingen te mitigeren.

[14] Raadpleeg hier het boetebesluit. De visie van de AP staat verder uitgewerkt in bijlage 4

- Van deze samengevatte, gecorreleerde en beoordeelde logging informatie worden rapportages gemaakt.
- Rapportages die wijzen op afwijkingen/onregelmatigheden worden gerapporteerd aan de systeemeigenaren en de CISO.

2.2.5 Hoe worden logbestanden beschermd?

Onweerlegbaarheid van een logregel is belangrijk. Van een gecollecteerde log regel, of log regel rapportage moet een 'chain of custody' aantoonbaar juist zijn. Dat betekent ook dat logbestanden dienen te worden beschermd tegen modificatie, inzien door onbevoegden en verwijdering. De volgende beleidsregels zijn daarom van toepassing:

- Het uitvoeren van een DPIA en een Quick Scan IB op de voorgestelde inrichting van logging-omgeving is noodzakelijk. Voor logging t.a.v. verschillende systemen of verwerkingen dienen afzonderlijke DPIA's en Quick Scan IB's te worden opgesteld. Aandachtspunten bij de DPIA zijn bijvoorbeeld de juridische grondslag en doelbinding.
- Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.
- Op grond van de BIO moeten de logbestanden zelf moeten worden geregistreerd. Dit betekent concreet dat van logbestanden onderstaande zaken worden gelogd in een nieuw logbestand (metalog):
    - Het (automatisch) overschrijven of verwijderen van logbestanden
    - Het openen van een nieuw logbestand
    - NB.: bij het inrichten van een systeem met als functionaliteit loggen over logging dient goed te worden nagedacht aan scheiding van functies. Een beheerder die op een systeem logfiles kan verwijderen, dient geen acties te kunnen uitvoeren op het systeem dat logt over logging.
- Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers die in de DPIA worden benoemd, en moet gerelateerd zijn aan het doel van beveiligingslogging. Hierbij is de toegang beperkt tot leesrechten. Het raadplegen van de logbestanden wordt zelf op zijn beurt ook weer gelogd.
- Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
- De instellingen van logmechanismen worden zodanig beschermd dat deze *aantoonbaar* niet aangepast of gemanipuleerd kunnen zijn. Indien de instellingen aangepast moeten worden zal daarbij altijd het 'vier ogen' principe toegepast worden.
- De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden[15], conform de eisen en wensen van de verwerkingsverantwoordelijke[16].
- Het goed functioneren van de logging wordt continue gemonitord voor alle systemen.
- Er wordt controle uitgevoerd op de opslag van de logs: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijvoorbeeld: een logserver die niet bereikbaar is).
- De logging wordt regelmatig gebackupped.

---

van deze Richtlijn.

[15] Vanuit de Wjsg geldt een minimumtermijn voor logging van 4 jaar op verstrekkingen.

[16] De verwerkingsverantwoordelijke bepaalt de doeleinden waarvoor en de middelen waarmee persoonsgegevens worden verwerkt. De verwerkingsverantwoordelijken onder de Wpg en Wjsg zijn door de wet aangegeven.

2.2.6 Hoe lang mogen/moeten logbestanden worden bewaard?

- De mimimum- en maximum bewaartermijnen van logging worden primair bepaald o.b.v. wettelijke verplichtingen[17] en de risico-analyse, bijvoorbeeld de Wsjg en Wpg. Deze wordt beschreven in de DPIA. Bij het vaststellen van de bewaartermijnen dient de privacy officer te worden geraadpleegd[18]. Doorgaans wordt als stelregel aangehouden dat logging minimaal een half jaar beschikbaar dient te zijn voor onderzoek (online of in archief). De CISO, PO (en soms archivaris) van een JenV-organisatie bepalen de bewaartermijnen gezamenlijk op grond van hun expertise.
- In geval van een (vermoed) informatiebeveiligingsincident moet de logging minimaal gedurende de totale duur van het onderzoek worden bewaard. Vaak wordt in deze gevallen een bewaartermijn van drie jaar[19] aangehouden.
- Logging die verzameld is in het kader van threat hunting dient minimaal een maand bewaard te worden op het centrale logplatform.

Belangrijk aandachtspunt hierbij is dat logging ook in de toekomst leesbaar moet blijven (bestandsformaten!)

Zie voor verdere informatie over bewaartermijnen van een log het BIO-OP product "Handreiking Dataclassificatie"[20].

2.2.7 Verantwoordelijkheden voor logging

De (eind)verantwoordelijkheid voor het bepalen van welke gegevens worden gelogd en op welke wijze deze gegevens worden gelogd ligt bij de verwerkingsverantwoordelijke organisatie (de hoogstleidinggevende binnen die organisatie). Hierbij wordt de verwerkingsverantwoordelijke geadviseerd door de systeemeigenaar.
De verantwoordelijkheid voor de wijze waarop de logging technisch wordt gerealiseerd ligt bij de systeemeigenaar.
De primaire verantwoordelijkheid voor het *bewaren* van logging is afhankelijk van de vraag of de logging centraal of decentraal is opgeslagen. De partij die de logging bewaart, is ook primair verantwoordelijk voor het adequaat *beveiligen* ervan. Wanneer twee of meer partijen gezamenlijk doel en middelen bepalen en er daarmee sprake van gezamenlijke verwerkingsverantwoordelijkheid is, of wanneer de verwerkingsverantwoordelijke tevens verwerker is, dient nadere aandacht aan dit onderwerp te worden besteed. De verwerkingsverantwoordelijke blijft te allen tijde *eind*verantwoordelijk voor het bewaren en beveiligen van de logging.

2.2.8 Speciale aandachtspunten bij logging in cloudomgevingen

[17] Bv.: Vanuit de Wjsg geldt een minimumtermijn voor logging van 4 jaar op verstrekkingen (artt. 18, 19, 39i, 39j, 44, 51c).

[18] In sommige organisaties dient niet alleen de privacy officer, maar ook de archivaris in dit geval te worden geraadpleegd.

[19] Dit kan langer zijn bij bijvoorbeeld een ontslag a.g.v. een ongeautoriseerde actie die in een logbestand is ontdekt (i.v.m. rechtzaken).

20 https://www.informatiebeveiligingsdienst.nl/product/handreiking-dataclassificatie-2/

Niet elke logging vindt on premise plaats. Als de logging gebeurt in een cloudomgeving, hanteert JenV dezelfde principes en normen voor logging als in een on premise-omgeving, maar wel met enkele speciale aandachtspunten. U zult zich daarom bij cloudomgevingen de volgende vragen moeten stellen en daarop antwoorden moeten krijgen:

- Welke logs (kunnen) worden gemaakt?
- Welke garanties krijgt u dat logs niet gewijzigd zijn?
- Welke afspraken maakt u opdat logs indien nodig dagelijks worden beoordeeld?
- Welke rapportages verwacht u omtrent logging?
- Kunnen logs automatisch naar u verzonden worden?
- Welke contractuele afspraken zijn met uw cloud-provider gemaakt over logging, zodat u kan voldoen aan de BIO en wettelijke verplichtingen omtrent auditing (bv. afspraken over pentesten, audits, etc.)?
- In welke bestandsindeling en van welke omvang zijn de logs?
- Zijn de gegevens binnen de log leesbaar, of te importeren in ander een logplatform dat u bezit?
- Hoe zijn de logbestanden beveiligd bij de leverancier? (Als bv. persoonsgegevens in logbestanden zitten, gelden de eisen die in dit document worden beschreven)
- Welke certificeringen moet de leverancier minimaal hebben?
- Welke afspraken zijn met de leverancier gemaakt over het melden van informatiebeveiligingsincidenten en datalekken?
- Alle bovenstaande punten dienen vastgelegd te zijn in het contract met de leverancier en de daarbij behorende verwerkersovereenkomst.

NB: Ook bij logging in cloudomgevingen blijft de verwerkingsverantwoordelijke eindverantwoordelijk voor het bepalen van welke gegevens moeten worden gelogd, en het bewaren en beveiligen van de aldus verkregen logging.

2.2.9 Wat te doen bij uitvallen van de logging?

Het inzetten van logging brengt een belangrijk vraagstuk met zich mee: wat te doen op het moment dat de logging uitvalt, dit geldt voor de centrale logging maar ook voor de decentrale logging.
Als er niet meer gelogd kan worden bestaat de kans dat niet meer kan worden aangetoond wie toegang heeft gehad tot een systeem of tot gegevens. Ook bestaat de kans dat niet meer vastgesteld kan worden of berichten ontvangen of verzonden zijn, of dat gegevens zijn ingevoerd en door wie.

Binnen het logplatform dienen signaleringen te zijn ingericht op het uitvallen van logging, om dit zo snel mogelijk te detecteren.

Op basis van een gedegen risicoafweging zijn verder de volgende keuzes te maken:

1. De component normaal te laten functioneren en geen logging opslaan
2. De component lokaal te laten loggen en later de logging te synchroniseren
3. De component acuut uit productie laten halen

Ad 1: De component normaal laten functioneren terwijl deze de logs niet kan opslaan. Consequentie hiervan is dat de logs verloren gaan, en dus niet voldaan kan worden aan het achteraf analyseren en vaststellen van incidenten.

Ad 2: De component normaal laten functioneren en de logs lokaal laten opslaan. Veel componenten beschikken over een eigen mechanisme om lokaal te loggen. Daarmee kan de log tijdelijk worden veiliggesteld. Op het moment dat het centrale logmechanisme weer beschikbaar komt, sluist de component de verzamelde logs alsnog door. Dit voorkomt dat de component uit productie

genomen moet worden en voorkomt tevens dat logs verloren gaan. Er moet wel voor gewaakt worden dat de lokale logging er niet voor zorgt dat alle beschikbare ruimte van het systeem verbruikt wordt. Op het moment dat de lokale opslag volloopt, moet opnieuw besloten worden wat de component hierna doet (in productie blijven – zie bovenstaande optie - of uit productie halen – zie volgende optie).

Ad 3: De component acuut uit productie laten halen. Dit betekent dat gebruikers niet meer kunnen werken met het systeem. Stoppen met verwerking betekent dat compromitteren niet meer ongemerkt kan plaatsvinden en ook dat de audit log geen hiaten gaat vertonen. Er zijn maar enkele systemen die zo belangrijk zijn dat deze vorm van ingrijpen nodig is, bijvoorbeeld het systeem voor burgerzaken.

Het is een expliciet besluit van de risico-eigenaar (CTO) om één van deze drie opties te kiezen wanneer onverhoopt de logging uitvalt. Deze keuze dient schriftelijk vastgelegd te worden (risico-afweging o.b.v. risk appetite)!

2.2.10 Hoe wordt over logging gecommuniceerd naar eindgebruikers?

Logging van gebruikersactiviteiten valt onder de bescherming van persoonsgegevens. Daarom gelden de volgende regels:

- Een organisatie mag logginggegevens van medewerkers (van zowel de eigen organisatie als die van ketenpartners die gebruik maken van JenV-voorzieningen) in beginsel uitsluitend verwerken voor het oorspronkelijke doel waarvoor ze verkregen zijn. Loggegevens die zijn toegepast ter bevordering van de informatiebeveiliging mogen bijvoorbeeld niet gebruikt worden om medewerkers te beoordelen op algemeen functioneren. Logging mag dus in principe niet gebruikt worden als personeelsvolgsysteem of voor andere doeleinden die niet verenigbaar zijn met de AVG of andere wetgeving.
- Het Beleidskader Logging wordt ter instemming de DOR afgestemd middels een instemmingsverzoek; evenals toekomstige wijzigingen en/of intrekking. Uitbreidingen of wijzigingen van dit beleidskader door individuele JenV-onderdelen, worden ter instemming aan de betrokken ondernemingsraad aangeboden.
- Het bestaan, gebruik, doel en de manier van verwerking moeten duidelijk kenbaar worden gemaakt aan werknemers (transparantie, artikel 12 AVG), bijvoorbeeld via de Privacyverklaring voor werknemers en sollicitanten, of een paragraaf hierover in de arbeidsovereenkomst. Het verdient aanbeveling deze communicatie ook op te nemen op intranet.
- De gedragsregeling digitale werkomgeving.

In bijlage 3 staat een voorbeeld van communicatie over logging naar eindgebruikers.

Bijlage 1: Wat is logging?

Informatiesystemen en ICT-infrastructuur genereren loginformatie voor veel activiteiten, soms als normale statusmelding, soms als resultaat van een activiteit van een gebruiker of beheerder maar ook informatie als resultaat van onvoorziene omstandigheden of fouten. Logging wordt daartoe doelbewust ingebouwd in systemen en infrastructuur. Een log beschrijft wat er gebeurt binnen systemen. Tegenwoordig zijn de beschrijvingen van systemen soms zo gedetailleerd dat ze beschrijven waarom een gebeurtenis heeft plaatsgevonden.

Veel computersystemen gebruiken logging om informatie op te slaan over foutsituaties en andere gebeurtenissen die aandacht behoeven van de gebruiker of beheerder. Een log kan geschreven worden in tekstbestanden maar ook in databasetabellen.

Logging kan gebruikt worden voor (niet-limitatief):

- Het ondersteunen van capaciteitsbeheer door het krijgen van statusinformatie van systemen.
- Het ondersteunen bij het ontdekken van fouten in soft- en hardware.
- Het ontdekken van menselijke fouten, zoals fouten bij de bediening, maar ook het ontdekken van indringers in systemen (met inachtneming van de persoonlijke levenssfeer van medewerkers).
- Het ontdekken van corruptie van data of programmatuur en antivirusmeldingen.
- Het ondersteunen bij forensisch onderzoek van systemen.
- Het ondersteunen van onderzoek na een incident.
- Het ondersteunen van Service Level Agreement (SLA) Compliance Monitoring.
- Het leveren van informatie ten behoeve van een wettelijk voorgeschreven audit.
- Het leveren van informatie om te onderzoeken of voldaan wordt aan beleid (bijvoorbeeld of er vreemde apparaten aangesloten zijn geweest).
- Het leveren van informatie om onweerlegbaar aan te tonen dat een bepaald bericht wel of niet verzonden is, of dat een activiteit is uitgevoerd.
- Rapportage over systeemgebruik en incidenten aan de systeemeigenaar en de Chief Information Security Officer (CISO), de Privacy Officer en de Integriteitscoördinator.
- Voor het waarnemen van of controle op aanwezigheid, gedrag of prestaties van personeel c.q. gebruikers[21] (bv. t.b.v. BHV en veiligheid van de medewerkers en bezoekers).

Wanneer de logging op orde is en er is weinig tijd om de logs te analyseren, is het mogelijk om SOC. Monitoring af te nemen bij een andere organisatie. Zij zijn in staat om 24/7 de IT-omgeving te monitoren, logs te analysen en te rapporteren aan de organisatie.

[21] Hiervoor kàn logging worden gebruikt, maar krachtens dit beleidskader màg dit dus niet. Zie hiervoor de paragraaf "Hoe wordt over logging gecommuniceerd naar eindgebruikers?": "Loggegevens die zijn toegepast ter bevordering van de informatiebeveiliging mogen bijvoorbeeld niet gebruikt worden om medewerkers te beoordelen op algemeen functioneren. Logging mag dus in principe niet gebruikt worden als personeelsvolgsysteem of voor andere doeleinden die niet verenigbaar zijn met de AVG of andere wetgeving."

Logging soorten

In de BIO worden de volgende vormen van logging onderkend:
- Technische logging.
- Audit logging (ook wel applicatieve logging genoemd).

Logging wordt in de regel door systemen en netwerken zelf verzorgd (technische logging). Voor logging dienen instellingen op de verschillende systemen te worden geactiveerd.

Naast technische logging dienen ook de activiteiten van beheerders op uitgebreidere wijze gelogd te worden (bijvoorbeeld: gebruik van speciale en hoge privileges op het systeem). Dit heet **audit logging**. Bij het bepalen van instellingen wordt het gestelde beleid voor beveiliging en controle op logging als uitgangspunt genomen.

Wat zijn de meest voorkomende fouten bij logging?

Niet loggen: Veel systemen loggen niet standaard, je moet logging als optie aanzetten en configureren, bijvoorbeeld: een technische logging op systeem niveau werkt vaak nog wel, echter de audittrail van de webserver die draait, is niet standaard geactiveerd.

Niet kijken naar logging, bijvoorbeeld: Als er al wordt gelogd, dan wordt deze logging niet regelmatig bekeken, soms als het te laat is en soms helemaal niet. Terwijl uit wetgeving of uit een risicoanalyse blijkt dat logging en het regelmatig bekijken ervan verplicht is.

Verkeerde logging prioriteit: bijvoorbeeld er wordt besloten alleen bepaalde informatie in een log op te slaan en bij een incident vaststellen dat er informatie mist in de log. De juiste volgorde is: Log alles, bewaar alles wat nodig is, analyseer en rapporteer met regelmaat een subset van de gegevens.

Geen aandacht hebben voor logging van applicaties: Er zijn bijvoorbeeld vele soorten applicaties van legacy systemen tot moderne systemen die allemaal wel/niet loggen. Bovendien hebben ontwikkelaars van systemen vaak geen oog voor logging of er worden daaraan vaak geen eisen gesteld. Voor ieder kritiek systeem dienen logregels (beleid) te bestaan en te worden nageleefd.

Kijken naar bekende fouten, bijvoorbeeld; er wordt gezocht naar een bekende fout met een loganalyse-tool terwijl er vaak meer te ontdekken is door er met een andere bril (andere loganalyse-software of andere parameters) naar te kijken.

Foute aannames op basis van loggen, bijvoorbeeld: De relatie tussen een event en een transactie van een gebruiker is niet altijd makkelijk vast te leggen. In veel gevallen levert een transactie een veelvoud aan log events op, die niet altijd herleidbaar zijn tot een transactie.

Samenhang van logs: Logbestanden komen van diverse netwerkapparatuur, systemen en applicaties met daarbij mogelijk allemaal verschillende beheerders. De samenhang tussen deze logbestanden kan hierdoor moeilijk worden ingeschat indien logbestanden niet worden samenbebracht of niet goed wordt samengewerkt.

Logging-cyclus en -opslag

Het maken van een log dient in een cyclus te gebeuren. Dit omdat anders de logbestanden of -tabellen in een database te groot worden. Het is vaak ook niet direct nodig om erg ver in de tijd terug te kunnen kijken. In systemen kan men soms bepalen hoe vaak een logbestand moet worden vernieuwd, dat kan bijvoorbeeld op loggrootte, op -tijdstip of -datum en dit is tevens systeemafhankelijk. Dus als er een grens overschreden wordt, start een nieuw logbestand en het oude logbestand wordt bewaard. Het is raadzaam om goed na te denken over de rotatie van de log en de bewaarlocatie van de logbestanden, dit omdat logbestanden door hun omvang ook de prestaties van een systeem kunnen degraderen en ruimte innemen die noodzakelijk is voor de werking van een systeem.
Meestal probeert men logbestanden op een andere plaats (centraal) neer te zetten; dit heeft een aantal voordelen:

1. De grootte op een productiesysteem is in de hand te houden.
2. Logbestanden kunnen makkelijker beveiligd worden tegen onbevoegd wijzigen. Separate opslag kan apart worden beveiligd.
3. De bewaartermijn van een log kan beter worden nageleefd. Een log moet soms gedurende een minimum termijn bewaard worden, maar er zijn ook maximum termijnen.

Bijlage 2: Security Information and Event Management (SIEM)

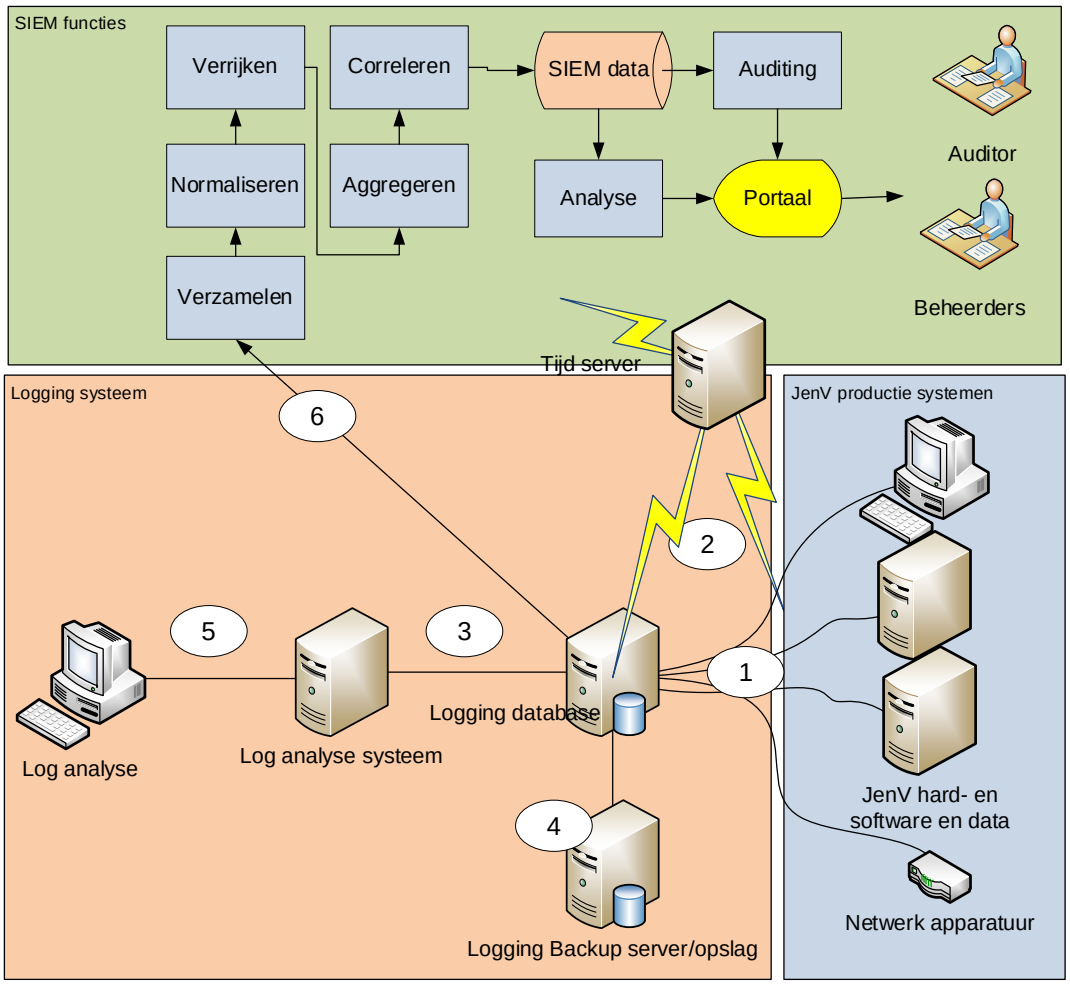
Omdat er op veel plaatsen gelogd wordt, kan de logging versnipperd raken, en een organisatie kan dan gemakkelijk het overzicht over alle gebeurtenissen verliezen, hetgeen er weer voor kan zorgen dat aanvallen niet worden gedetecteerd. Daarom is het belangrijk deze logs vanaf één centraal punt te kunnen inzien. Hierdoor, en door filtering toe te passen op deze logs, ontstaat een heldere blik op alle informatie vanuit de verschillende componenten uit de infrastructuur. Dit kan in platte tekst maar ook in een database zijn. Doorgaans wordt hier een Security Information and Event Management (SIEM) voor gebruikt. Het voordelen van centraal inzicht in de verzamelde loginformatie zijn:

- Gebruiksgemak: Er hoeft maar op één plaats gekeken te worden.
- Beschikbaarheid: De logging is beschikbaar, ook als het systeem dat logt niet beschikbaar is.
- Veiligheid: De logging is ook beschikbaar als het bronsysteem gehackt of besmet is.
- Veiligheid: De logging kan worden afgeschermd tegen onbevoegd inzien en modificatie, bijvoorbeeld door digitaal ondertekenen.
- Eenvoud: Een centrale logging is eenvoudiger veilig te stellen op bijvoorbeeld een back-up.
- Automatische analyse van logbestanden geeft sneller de samenhang van incidenten weer en maakt het mogelijk om logische verbanden tussen geïsoleerde incidenten te detecteren, zoals een systeeminbraak die zich in meerdere, verschillende stappen laat herkennen.

Het logging systeem is gescheiden van de rest van de JenV-systemen. Er is alleen toegang voor de medewerkers die logging moeten beoordelen of voor auditors.

In figuur 2 is de centrale logging (figuur 1) gecombineerd met een SIEM.

Een SIEM-systeem voert de volgende bewerkingen uit:
- Verzamelen
- Normaliseren
- Verrijken
- Aggregeren
- Correleren



Figuur 2: Logging in combinatie met een SIEM

Legenda bij figuur 2:

1. Logging wordt vanuit de systemen naar een centrale logging database gezonden
2. Alle systemen hebben dezelfde tijd en gebruiken een tijd synchronisatie bron
3. De logging database wordt benaderd vanuit een loganalyse systeem
4. Logging die langere tijd ongebruikt blijft wordt apart gezet in een back-up server
5. Het loganalyse systeem wordt gebruikt door loganalyse werkstations
6. Logging wordt doorgestuurd naar de collector van de SIEM

Bijlage 3: Communicatie over logging van toegang tot en gebruik van systemen

Logging

Het tegengaan en controleren van onrechtmatige, onregelmatige of doel overschrijdende verwerking van gegevens:

1. Ter ondersteuning van verplichte audits over bepaalde systemen.
2. Wetenschappelijke en/of statistische doeleinden.

De organisatie heeft rapportages ontwikkeld omtrent de logging van het gebruik van de systemen. De organisatie is verplicht om gegevens te loggen waarmee het gebruik van applicaties per medewerker van de organisatie kan worden nagegaan.
De volgende gegevens worden gelogd:

1. Het tijdstip van iedere login en logout en andere acties.
2. De gebruikersnaam van degene die inlogt/uitlogt.
3. Persoonsgegevens (of enige andere zoeksleutel) waarvan gegevens worden opgevraagd. Dit wordt als actie geregistreerd.

Elke actie, zoals de bekeken applicatie pagina's, overzichten en mutaties.

Communicatie over logging naar eindgebruikers

De eindgebruikers van systemen (inclusief de medewerkers van ketenpartners en burgers die JenV-systemen gebruiken) moeten weten dat over hen gegevens worden verzameld en vastgelegd. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. Met het oog hierop moet de navolgende informatie worden verstrekt aan de medewerkers die (gaan) werken met onze systemen:

1. Het bestaan van de logging-applicatie;
2. De (aard van de) gegevens die binnen deze applicatie worden gelogd;
3. Doelen van de logging;
4. De wijze en het moment waarop en door wie een onrechtmatig of doel overschrijdend gebruik van onze systemen wordt geconstateerd;
5. Dat bij bovenstaande constatering dit door het afdelingshoofd wordt gecommuniceerd met de betreffende medewerker(s)[22].

OR

Dit loggingbeleid is d.m.v. een instemmingsverzoek geaccordeerd door de OR dd. DD-MM-YYYY.

[22] Dientengevolge kunnen er ook disciplinaire maatregelen worden getroffen. Dit wordt beschreven in par. 2.2 van het *Beleidskader Logging Informatie beveiliging JenV*, sub "Integriteitsschending". Zie voor verwijzingen naar relevante bronnen 'Integriteitsschending' onder paragraaf 2.2.

Bijlage 4: Jurisprudentie t.a.v. privacy aspecten

RvS Afdeling bestuursrechtspraak 20-11-2011
ECLI:NL:RVS:2011:BU6383

Betrokkene heeft een ziekenhuis verzocht om een overzicht te geven van de zorgverleners die toegang hebben gehad tot haar medisch patiëntendossier. Het ziekenhuis heeft dat verzoek afgewezen. Zij motiveert dat persoonsgegevens enkel worden verstrekt aan derden voor zover die verstrekking voortvloeit uit het doel van de verwerking. Er hebben geen onbevoegden inzage gehad in het medisch dossier. De rechtbank wijst het verzoek toe, nu in artikel 35 Wbp staat dat n.a.v. een inzageverzoek onder meer *de ontvangers of categorieën van ontvangers* moet worden vermeld.

De RvS overweegt dat personen die het dossier raadplegen niet aan te merken zijn als ontvangers in de zin van de Wbp. Desondanks wijst de RvS het verzoek toe, nu het inzagerecht betrokkene in beginsel het recht toekent op een overzicht van namen van degenen die haar medisch dossier hebben geraadpleegd. Tevens overweegt de RvS dat het doel dat betrokkene met het verzoek voor ogen heeft irrelevant is, nu de Wbp aan eenieder het recht geeft zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden, behoudens misbruik en andere uitzonderingen. De uitzondering waar het ziekenhuis zich in casu op beroept ("noodzakelijk in het belang van de bescherming van de betrokkene of van de rechten en vrijheden van anderen") slaagt niet. Het verweer is volgens de RvS onvoldoende gemotiveerd.

Rechtbank Den Haag 31-03-2021
ECLI:NL:RBDHA:2021:3090

De AP heeft aan een ziekenhuis een bestuurlijke boete van € 460.000,- en een last onder dwangsom opgelegd. Het ziekenhuis had volgens de AP artikel 32 van de AVG overtreden, omdat er niet genoeg maatregelen waren genomen om de persoonsgegevens van patiënten te beschermen. Zo had het ziekenhuis de tweefactor authenticatie moeten invoeren en heeft het ziekenhuis de logging van de toegang tot de patiëntendossiers niet regelmatig gecontroleerd. De rechtbank is van oordeel dat de AP een boete en een last onder dwangsom mocht opleggen.

Wel was de boete volgens de rechtbank te hoog. Het basisboetebedrag van €310.000,- acht de rechtbank op zichzelf niet onredelijk. De rechtbank is het ook eens met de AP dat het boetebedrag verhoogd mocht worden vanwege de aard, ernst en duur van de overtreding en de opzettelijke/nalatige aard van de overtreding. Met deze twee boeteverhogende omstandigheden (tweemaal €75.000,) was het totale boetebedrag vastgesteld op €460.000,-. De rechtbank vindt het bedrag in dit geval te hoog en ziet aanleiding de boete te matigen tot €350.000,-. De rechtbank acht het namelijk van belang dat het ziekenhuis wel een aantal maatregelen heeft genomen om te voorkomen dat persoonsgegevens in het digitale patiëntendossier worden ingezien door onbevoegde medewerkers. Ook heeft het ziekenhuis nog tijdens de bezwaarfase alsnog de tweefactor authenticatie ingevoerd en de logging geïntensiveerd. De door het ziekenhuis getroffen maatregelen tonen volgens de rechtbank in ieder geval de bereidwilligheid om met de problematiek in de organisatie aan de slag te gaan en nuanceren de nalatigheid die het ziekenhuis wordt verweten.

Rechtbank Midden Nederland 02-12-2020

ECLI:NL:RBMNE:2020:5410

In december 2016 heeft de directeur van de school van [minderjarige] een zorgmelding gedaan bij Veilig Thuis, die een paar maanden later is afgehandeld en afgesloten. Op 3 maart 2020 heeft verzoekster (ouder van minderjarig kind) Samen Veilig verzocht om haar "afschriften van alle volledige logoverzichten tot het moment van verstrekken met daarin opgenomen alle namen van personen die inzage hebben gehad in het dossier" te verstrekken (een inzageverzoek o.g.v. de AVG).

Samen Veilig verstrekt een overzicht van de loggingoverzichten, maar laat daarbij enkel functietitels zien en geen namen van personen. Op basis van een belangenafweging komt zij tot de conclusie dat het recht op privacy van haar medewerkers zwaarder weegt dan het recht op inzage van verzoekster.

De rechtbank concludeert dat het delen van de functietitel zonder namen niet voldoet en dat dit betrokkene beperkt in de mogelijkheid om te controleren of de verleende toegang rechtmatig is geweest. Zij kan immers op basis van die informatie niet opmaken of haar contactpersoon inzage in het dossier heeft gehad, dan wel een andere persoon die zich toegang tot het dossier heeft verschaft.

Het recht op inzage is niet beperkt; er zal een belangenafweging moeten worden gemaakt. De rechtbank concludeert dat een uitzondering op het inzagerecht alleen mogelijk is als dit strikt noodzakelijk is in het *individuele geval*. De belangen die Samen Veilig naar voren heeft gebracht zijn van algemene aard en voldoen dus niet.

Autoriteit Persoonsgegevens 26-11-2020
Raadpleeg hier.

In een boetebesluit aan het Amsterdamse ziekenhuis OLVG uit november 2020 benadrukt de Autoriteit Persoonsgegevens (AP) het belang van controle op de logging (p12-13). De AP zegt daarover het volgende:

"*Het uitgangspunt van de AP is dat controle van de logging systematisch en consequent moet plaatsvinden, waarbij een steekproefsgewijze controle en/of controle op basis van klachten niet voldoende is. De fijnmazigheid van het gehanteerde autorisatiemodel en de controle op de juistheid van de autorisaties zijn mede bepalend voor de intensiteit van de controle op de logging. Bij een willekeurig steekproefsgewijs controleren is er geen sprake van een systematiek gericht op onrechtmatig gebruik en risico's. Daarmee heeft OLVG niet aan het vereiste van het regelmatig beoordelen van logbestanden voldaan, wat in de context van deze verwerking in het kader van artikel 32 van de AVG wel is vereist. Een dergelijke controlemaatregel acht de AP, ook gezien de huidige stand van de techniek en de uitvoeringskosten, passend. Daarbij neemt de AP in aanmerking dat algemeen geaccepteerde beveiligingsstandaarden, zoals de Nederlandse norm voor informatiebeveiliging in de zorg, regelmatige logging voorschrijven*."

Bijlage 5: Lijst van gebruikte afkortingen

AVG	Algemene Verordening Gegevensbescherming
BBN	Basis Beveiligings Niveau
BIO	Baseline Informatiebeveiliging Overheid
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COR	Centrale Ondernemingsraad
CTO	Chief Technology Officer
DOR	Departementale Ondernemingsraad
DPIA	Data protection impact assessment
IB	Informatiebeveiliging
MFA	Multi Factor Authenticatie
PO	Privacy Officer
SIEM	Security Information and Event Management systeem
SLA	Service Level Agreement
SOC	Security Operations Center
WJSG	Wet justitiële en strafvorderlijke gegevens
Wpg	Wet politiegegevens