

VERWERKINGSSPECIFICATIE NATIONALE SUPERCOMPUTER

Deze Verwerkingsspecificatie is geldig vanaf 1 januari 2024.

Deze Verwerkingsspecificatie bestaat uit twee onderdelen:

- Hoofdstuk A Algemene specificaties
- Hoofdstuk B Beveiligingsmaatregelen

Deze Verwerkingsspecificatie vormt samen met de Annex Verwerkersafspraken een verwerkersovereenkomst zoals bedoeld in artikel 28 AVG. De Annex Verwerkersafspraken is te vinden via: www.surf.nl/annex-verwerkersafspraken.

In deze Verwerkingsspecificatie wordt aan de met hoofdletter geschreven begrippen de betekenis van de definitie in de Annex Verwerkersafspraken toegekend.

HOOFDSTUK A ALGEMENE SPECIFICATIES

1 Omschrijving van de Verwerking

De Nationale Supercomputer is een zogeheten “general purpose capability system” en is bij uitstek geschikt voor grootschalige berekeningen waarbij een grote hoeveelheid geheugen, hoge communicatiesnelheid tussen de processors onderling én veel en snelle schijfopslagruimte van belang zijn.

Afhankelijk van de manier waarop de Dienst wordt gebruikt door (onderzoekers werkzaam bij) Verwerkingsverantwoordelijke, kunnen diverse verwerkingen van persoonsgegevens plaatsvinden. Indien de Dienst wordt gebruikt om bestanden te verwerken die Persoonsgegevens bevatten, bijvoorbeeld om berekeningen uit te voeren op of met dergelijke bestanden, dan worden de Persoonsgegevens in die bestanden verwerkt.

Daarnaast vindt technische logging plaats van gebruiksgegevens zoals inlogacties en handelingen die Eindgebruikers door gebruikmaking van de Dienst uitvoeren, om de Dienst zo snel, betrouwbaar en veilig mogelijk te laten werken

2 Doeleinden van de Verwerking

Verwerker voert bij het verlenen van de Dienst de volgende Verwerkingen uit ten behoeve van Verwerkingsverantwoordelijke:

Uitvoeren van Dienstverleningsovereenkomst

Omschrijving van het doeleinde: Het bewerken en tijdelijk opslaan van onderzoeksgegevens ten behoeve van wetenschappelijk onderzoek. Het uitvoeren van de Dienstverleningsovereenkomst op grond waarvan Verwerker de Dienst ter gebruik beschikbaar stelt aan Verwerkingsverantwoordelijke, inclusief de beveiligingsmaatregelen om het gebruik van de Dienst voor alle Eindgebruikers zo veilig en betrouwbaar mogelijk te maken.

Categorie Persoonsgegevens: Verwerkingsverantwoordelijke beslist zelf of de Dienst wordt gebruikt om (bestanden met) Persoonsgegevens te verwerken en om welke categorieën Persoonsgegevens het dan gaat. Dat zal normaliter afhankelijk zijn van het betreffende onderzoeksproject. Om risico's in verband met de verwerking van Persoonsgegevens zo ver mogelijk te minimaliseren, raadt Verwerker Verwerkingsverantwoordelijke aan om (bestanden met) Persoonsgegevens zoveel mogelijk te pseudonimiseren of anonimiseren alvorens deze te verwerken bij gebruikmaking van de Dienst.

De beveiliging van de Dienst is ingericht op het (eventueel) verwerken van reguliere Persoonsgegevens en niet op het verwerken van Bijzondere categorieën Persoonsgegevens. Wanneer Verwerkingsverantwoordelijke de Dienst wil gebruiken om Bijzondere categorieën Persoonsgegevens of anderszins bijzonder gevoelige (onderzoeks)gegevens te verwerken, dient Verwerkingsverantwoordelijke zorg te dragen voor het nemen van aanvullende maatregelen om deze (Persoons)gegevens passend te beveiligen. Meer informatie over beveiliging is opgenomen in Hoofdstuk B van deze Verwerkingspecificatie.

Gebruiksgegevens die worden gelogd en gemonitord omvatten:

- Sessielogs (moment van inloggen en uitloggen, events die betrekking hebben op al dan niet succesvol inloggen);
- Operating system logs en applicatielogs;
- Applicatie gebruik en welke processen er uitgevoerd worden;
- Netwerkverkeer, file access monitoring en energiemonitoring;
- Monitoring die procesgedrag analyseert op basis van bekende dreigingen;
- Systeem resource verbruik (zoals batch systeem en accounting);
- De data die gelogd kan worden kan bestaan uit de volgende velden:
<https://www.elastic.co/docs/reference/integrations/endpoint#exported-fields>.

Categorie
Betrokkenen:

Verwerkingsverantwoordelijke beslist zelf of de Dienst wordt gebruikt om (bestanden met) persoonsgegevens te verwerken en op welke categorieën Betrokkenen deze persoonsgegevens betrekking hebben. Dat zal normaliter afhankelijk zijn van het betreffende onderzoeksproject. Hierbij kan gedacht worden aan proefpersonen, patiënten, relaties of andere categorieën Betrokkenen die Verwerkingsverantwoordelijke zelf selecteert om Persoonsgegevens van te (laten) verwerken met behulp van de Dienst.

Ook de gebruikers van de Dienst zijn Betrokkenen van wie Persoonsgegevens kunnen worden verwerkt in het kader van het gebruik van de Dienst. Dat gebeurt als onderdeel van de authenticatie voor toegang tot de Dienst en de technische logging om de Dienst zo snel, betrouwbaar en veilig mogelijk te laten werken. Clusterverbruik kan inzichtelijk gemaakt worden in de vorm van een rapportsamenvatting voor de desbetreffende accounteigenaren van de instellingen. Hierin kunnen details verwerkt zijn zoals budgetverbruik en efficiëntie van job resources per user.

Bewaartermijn:

De bewaartermijn van databestanden en omgeving is tot uiterlijk 6 (zes) maanden nadat de Overeenkomst is geëindigd. Verwerker treft technische en organisatorische maatregelen om een correcte uitvoering van deze bewaartermijn te waarborgen.

Medewerkers
Verwerker:

De bestanden die worden verwerkt in het kader van technische logging worden voor een periode van 6 maanden bewaard.
Beheerder, adviseur en helpdeskmedewerker.

3 Sub-verwerkers

Verwerker schakelt bij de Verwerking ten behoeve van Verwerkingsverantwoordelijke de volgende Sub-verwerkers in:

Lenovo NL

Volledige naam Sub-verwerker: Lenovo Global Technology International B.V.
Lenovo NL schakelt in:

	Lenovo Duitsland Lenovo Frankrijk Lenovo Roemenië Lenovo USA Lenovo UK
Vestigingsland Sub-verwerker: (Categorieën) Persoonsgegevens:	Nederland Technische logs die verband houden met de werking van de hardware en aanverwante software (zoals firmware, drivers) en de Persoonsgegevens die zich daarin kunnen bevinden, zoals IP-adres, gebruikersnaam, en dergelijke.
Soort Verwerking:	Opslaan, analyseren, doorgeven, ten behoeve van het helpen waarborgen van een optimale werking van de Dienst.
Land van Verwerking:	Nederland, Duitsland, Frankrijk (zie overige landen onder 4)

EAR

Volledige naam Sub-verwerker:	Energy Aware Solutions S.L
Vestigingsland Sub-verwerker: (Categorieën) Persoonsgegevens:	Spanje Technische logs die verband houden met het energieverbruik per job binnen het cluster en persoonsgegevens die zich daarin kunnen bevinden, zoals gebruikersnaam, groep, job naam, applicatie en account.
Soort Verwerking:	Opslaan en analyseren ten behoeve van het helpen waarborgen van een optimale werking van de Dienst.
Land van Verwerking:	Nederland

4 Doorgiften buiten de Europese Economische Ruimte

Bij de Verwerking ten behoeve van Verwerkingsverantwoordelijke vinden de volgende doorgiften aan derde landen of internationale organisaties plaats:

Doorgifte #1:

Persoonsgegevens kan plaatsvinden, of technisch niet goed worden uitgesloten, doordat een zeer beperkt aantal hooggekwalificeerde medewerkers van Sub-verwerker Lenovo werkzaam voor Lenovo US (zie de volledige naam van de entiteit hiernaast) admin/root-toegang tot de Dienst nodig heeft om onderhoud en support te kunnen leveren ten behoeve van een optimale uitrol en werking van de Dienst. Daarbij kunnen technische logs worden verwerkt, en doorgegeven, die persoonsgegevens kunnen bevatten.

Entiteit die doorgeeft:	Lenovo Global Technology International B.V. (ook aangeduid als: "Lenovo NL"), Nederland.
Entiteit die ontvangt:	Lenovo US Inc (ook aangeduid als: "Lenovo US").
Land van Verwerking:	Verenigde Staten.
Doorgiftemechanisme:	Standard contractual clauses (SCCs).
Extra getroffen waarborgen:	Niet van toepassing

Doorgifte #2:

Idem als bovenstaande maar dan voor Lenovo UK.

Entiteit die doorgeeft:	Lenovo Global Technology International B.V. (ook aangeduid als: "Lenovo NL"), Nederland.
Entiteit die ontvangt:	Lenovo Technology Limited United Kingdom Ltd (ook aangeduid als: "Lenovo UK").
Land van Verwerking:	Verenigd Koninkrijk.
Doorgiftemechanisme:	Standard contractual clauses (SCCs).
Extra getroffen waarborgen:	Niet van toepassing

5 Inbreuken in verband met persoonsgegevens

Inbreuken in verband met persoonsgegevens worden gemeld aan de bij Verwerker bekende contactgegevens van de Instellingscontactpersoon (ICP) en contactpersoon 'Meldpunt datalekken SURF'.

HOOFDSTUK B BEVEILIGINGSMAATREGELEN

1 Uitwerking van de beveiligingsmaatregelen:

Technische maatregelen:

Nationale Supercomputer

- Strikte toegangsprocedure tot gebouwen en het datacenter.
- Netwerk zonering: de Dienst is geplaatst in een eigen netwerksegment.
- De Dienst is geplaatst achter een firewall met specifieke regels voor de Dienst.
- Voor het verkrijgen van root-rechten is **multifactorauthenticatie** nodig.
- Voor Eindgebruikers zonder root-rechten kan **multifactorauthenticatie** op verzoek worden ingeschakeld.
- Verwerker maakt gebruik van beveiligde verbindingen (TLS/SSL/HTTPS, SSH) waarbij gegevensstromen ('in transit') worden versleuteld met behulp van een actueel en als veilig beschouwd encryptiealgoritme.
- De Dienst is een multi-user systeem waar groepen van Eindgebruikers veelal met elkaar samenwerken. Het rechtenmodel is in beginsel een standaard Unix-model. Eindgebruikers kunnen hun data desgewenst zelf op een hoger niveau beveiligen. Op het systeem is het Posix ACL mechanisme aanwezig. Indien wenselijk kan daar gebruik van worden gemaakt om een uitgebreider access-/rechtenmodel te realiseren.
- Bij het aanmaken van het gebruikersaccount staat de home directory dicht voor 'group' en 'other'.
- Het gebruik van bestanden, m.a.w. access op bestandsniveau, wordt niet gelogd.
- Eindgebruikers kunnen op Unix-niveau en met ACL's rechten instellen, uiteraard alleen voor bestanden en directories waarvan ze de eigenaar zijn.
- Opslag is standaard niet versleuteld, de Eindgebruiker kan daar zelf voor kiezen, wel met gebruik van eigen tools en keys. Standaard basis encryptie-tools zoals GPG zijn aanwezig op het systeem.
- Indien Verwerkingsverantwoordelijke bijzonder gevoelige (Persoons)gegevens wil verwerken bij gebruikmaking van de Dienst dient hij zelf zorg te dragen voor passende aanvullende beveiligingsmaatregelen. Het is de verantwoordelijkheid van Verwerkingsverantwoordelijke om daarvoor passende instructies te geven aan diens medewerkers als Eindgebruikers van de Dienst.
- Systeemlogs worden centraal opgeslagen voor proactieve security monitoring en alerting:
 - Processen die draaien op het cluster worden bijgehouden;
 - Filetoegang wordt bijgehouden;
 - Netwerkgebruik wordt bijgehouden;
 - Securitymaatregelen zijn van toepassing zoals malware detectie en verdacht gedrag van processen worden geanalyseerd op basis van bekende dreigingen;
 - Op basis van de bovenstaande monitoring kunnen dashboards gebouwd worden en proactieve alerting ingesteld worden;

Organisatorische maatregelen:

- Security-organisatie is opgezet en de rollen en verantwoordelijkheden zijn toegekend.
- Rollen- en rechtenmodel (autorisatiematrix) wordt periodiek geëvalueerd.
- Verwerker is ISO27001 gecertificeerd.

2 Beschikbare certificeringen

De volgende certificaten zijn beschikbaar ter zake van de Verwerking:

Verwerker is ISO 27001 gecertificeerd. Afhankelijk van de Dienst kunnen aanvullende audits en/of pentests worden uitgevoerd. Het betreft audits die door onafhankelijke, deskundige externe partijen uitgevoerd worden.

Certificaten	Organisatieonderdeel / dienst waarop certificaat betrekking heeft	Geldigheidsduur certificaat	Verklaring van toepasselijkheid
ISO 27001	Leveren van computing, data opslag en -analyse, visualisatie, authenticatie, autorisatie, cloud en grid diensten	2/12/2022-31/10/2025	v. 6.0