



**Algemene Inlichtingen - en  
Veiligheidsdienst**

Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties



# Databescherming met Privacy Enhancing Technologies

Technologie om vertrouwelijke data te beschermen  
bij gegevensverwerking

# Inhoudsopgave

Data gebruiken én beschermen	3
Casus: veilig informatie delen over cyberincidenten	4
Privacy Enhancing Technologies: een overzicht	5
Multi-party computation	6
Fully homomorphic encryption	8
Trusted execution environments	10
Federated learning	12
Synthetische data-generatie	14
Zero-knowledge proofs	16
Differential privacy	18
Overwegingen bij het gebruik van PET's	20
Bijlage: uitleg van de kenmerken	21

## Data gebruiken én beschermen

Personen en organisaties maken steeds vaker beslissingen op basis van data. Het is belangrijk om zorgvuldig met data om te gaan. Essentieel hierbij is *soevereiniteit*: personen en organisaties moeten de controle kunnen houden over hun eigen data. Tegelijkertijd heeft het in veel situaties meerwaarde om databronnen te combineren met andere data. Op deze manier kunnen nieuwe en waardevolle inzichten verkregen worden.

In het gebruik van data bieden *Privacy Enhancing Technologies* (PET's) uitkomst. PET's vormen een collectie aan krachtige technieken voor gegevensbescherming voor *data in use* (data in gebruik). PET's kunnen namelijk de risico's omtrent gegevensuitwisselingen in datasamenwerkingen verminderen door de veiligheidsgaranties technisch-organisatorisch te versterken.

Zo kunnen PET's datasamenwerkingen mogelijk maken door de benodigde randvoorwaarden te scheppen, zoals dataminimalisatie en proportionaliteit.

Voorbeelden van toepassingen voor PET's zijn:

- Op een veiligere manier gebruikmaken van de rekenkracht van clouddiensten;
- Een dataset op een veilige manier combineren met soortgelijke datasets van verschillende eigenaars, om gezamenlijk inzichten op te doen over deze gecombineerde dataset;
- Een AI-model trainen op data, en data door een AI-model laten verwerken, zonder de data zelf prijs te geven;
- Bewijzen dat je 18+ bent zonder je exacte leeftijd te onthullen;
- Controleren of een persoon voorkomt in een externe database, zonder dat de database-eigenaar weet om welke persoon het gaat;
- Publiceren van statistische analyses met de zekerheid dat individuele kenmerken niet kunnen worden herleid.

De inzet van PET's kan de digitale beveiliging bij gezamenlijke gegevensverwerking verhogen. De AIVD adviseert dan ook: overweeg om PET's te gebruiken als je data uitwisselt met een andere partij. Met deze publicatie wil de AIVD bijdragen aan de versterking van de digitale weerbaarheid en veerkracht van de Nederlandse overheid, de vitale sectoren, hightech-topsectoren en kennisinstellingen.

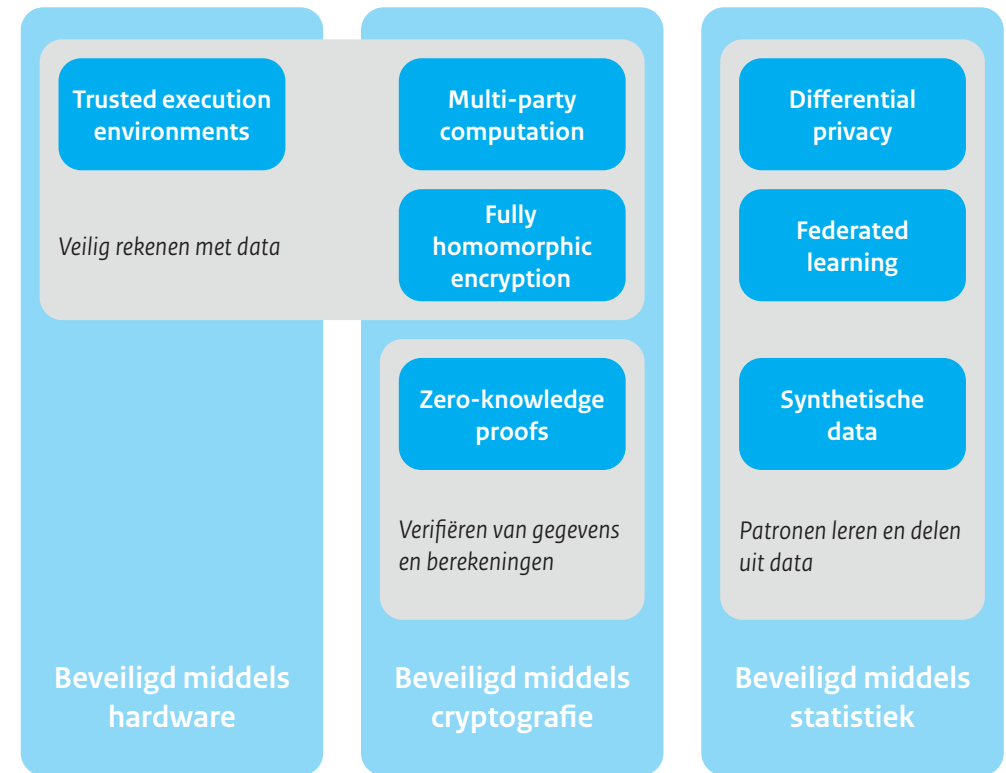
## Casus: veilig informatie delen over cyberincidenten

Cyberdreigingen spelen een grotere rol dan ooit in onze digitale samenleving. Met enige regelmaat komt er een kwetsbaarheid of dreiging aan het licht met gevolgen voor de Nederlandse overheid en het bedrijfsleven. Om dreigingen beter in kaart te brengen, is het belangrijk dat organisaties samenwerken en informatie over incidenten met elkaar delen.

Het Nationaal Cyber Security Centrum (NCSC) heeft onder meer als taak om op te treden als coördinator bij cybersecurity-incidenten. Om deze taak goed te vervullen en *lessons learned* te delen binnen het bredere cybersecuritylandschap, heeft het NCSC informatie nodig over het incident – terwijl getroffen organisaties vaak huiverig zijn om deze informatie te delen.

Het SecureNed platform is opgericht zodat organisaties veilig informatie kunnen delen over incidenten. Met PET's worden vervolgens alleen geaggregeerde analyses gedaan. De bedrijfsinformatie blijft verhuuld.

## Privacy Enhancing Technologies: een overzicht



Figuur 1. Een overzicht van populaire PET's die beschreven worden in deze brochure. Met PET's kan de vertrouwelijkheid van de data met verschillende eigenschappen worden gewaarborgd: via hardware, cryptografie en/of statistiek. Ook zijn de toepassingsmogelijkheden voor iedere PET verschillend.

In deze brochure licht de AIVD een aantal *Privacy Enhancing Technologies* (PET's) toe. Per PET wordt het toepassingsdomein benoemd en een schets van de werking gegeven. Ter illustratie worden de PET's besproken op een aantal kenmerken. Zie de bijlage op [pagina 21](#) voor een uitleg van de kenmerken.

# Multi-party computation

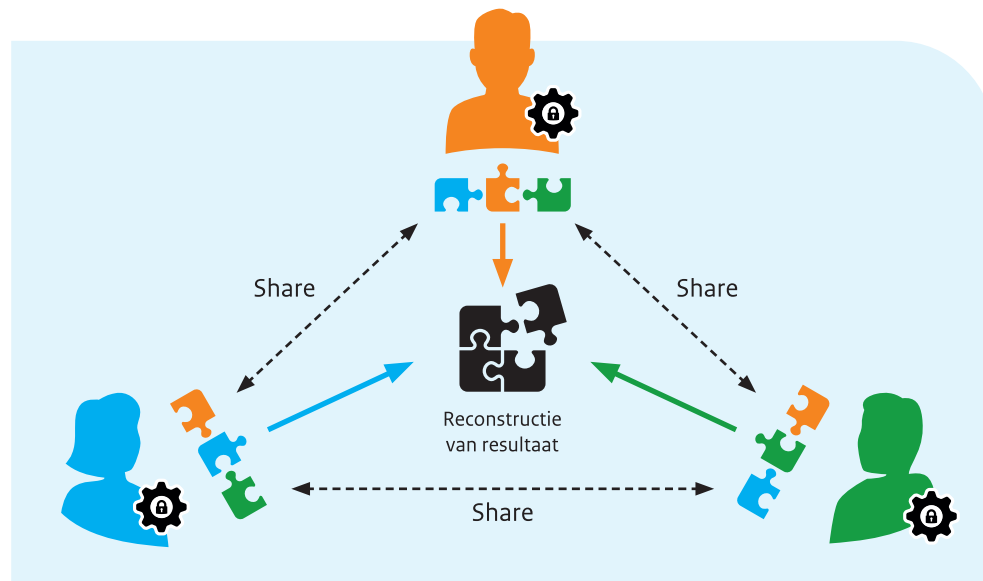
Secure multi-party computation (MPC) is een groep verschillende maar gerelateerde technieken met een overkoepelend idee: **met MPC kunnen verschillende partijen gezamenlijk een berekening doen, zonder iets over elkaars gegevens te weten te komen.**

Een populaire MPC-techniek is *secret sharing*. Het centrale idee is als volgt: iedere partij splitst de te delen gegevens (het *secret*) op in stukjes (*shares*) via een speciale constructie. Iedere individuele *share* geeft geen informatie prijs. Deze shares worden verdeeld over de deelnemende partijen. Elke partij verricht nu de afgesproken berekening op de ontvangen shares. Tenslotte combineren de partijen samen alle bewerkte *shares* weer tot een geheel.


MPC kan bijvoorbeeld worden gebruikt voor het vergelijken van prestaties tussen concurrenten (benchmarken), zonder de individuele gegevens te delen.

MPC biedt veel flexibiliteit, omdat de techniek diverse soorten berekening ondersteunt: van relatief simpele berekeningen, zoals het vinden van een gemiddelde salaris in een groep, tot complexe berekeningen in het domein van AI.

Er zijn echter ook nadelen aan MPC. Zo is de ontwikkeling van MPC-software zeer specialistisch werk. Daarnaast is het inherent aan *secret sharing* dat meerdere partijen rekenwerk moeten verrichten en tegelijkertijd samen moeten communiceren. Het is dus niet voldoende om de software op één plek te draaien.



Figuur 2. Multi-party computation: samen rekenen zonder gegevens te delen.

MPC in het kort	
Toepassing	Meerdere partijen kunnen gezamenlijke berekeningen uitvoeren zonder elkaars data in te zien.
Aantal benodigde partijen	
Voordelen	Zeer flexibel en breed inzetbaar. Software en producten zijn commercieel beschikbaar.
Nadelen	Complexe software die bovendien door meerdere partijen gedraaid moet worden.
Veiligheids garanties	• • •
Volwassenheid & toepasbaarheid	• • (•)
Schaalbaarheid rekenkracht & geheugen	• •
Schaalbaarheid netwerkgebruik	•

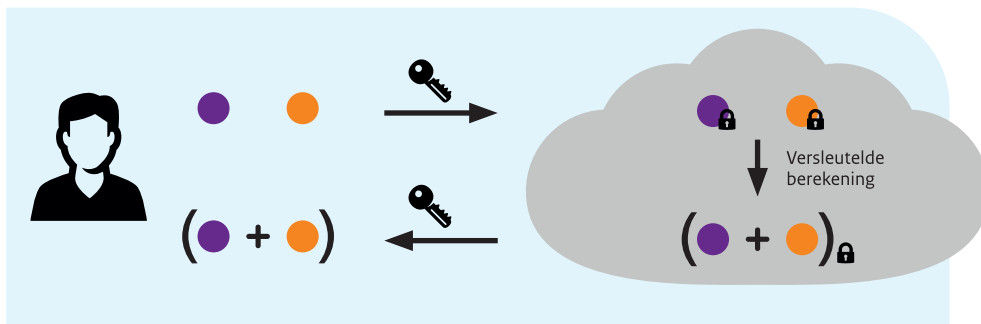
Zie de bijlage op [pagina 21](#) voor een uitleg van de kenmerken.

# Fully homomorphic encryption


*Fully homomorphic encryption* (FHE) is een speciale manier van versleuteling waarbij een bepaalde structuur van de data bewaard blijft. Anders dan bij 'normale' vormen van encryptie, kun je **met FHE rekenen met versleutelde waardes**. Pas na ontsleuteling wordt de uitkomst van de berekening zichtbaar.

Deze manier maakt het mogelijk dat je in feite 'blind' kunt rekenen. De gedroomde toepassing van FHE is dan ook *outsourced computation*: een gebruiker versleutelt lokaal de eigen gegevens en stuurt de versleutelde data met de gewenste rekeninstructies naar een clouddienst. De clouddienst verricht vervolgens de gevraagde berekening op de versleutelde data en stuurt het resultaat terug. Daarna kan de gebruiker deze lokaal ontsleutelen om het antwoord te zien. De gebruiker houdt zo de eigen gegevens vertrouwelijk, maar kan wel gebruikmaken van de grote rekenkracht van een cloud.

FHE is een zeer krachtige techniek, omdat het (net als MPC) allerlei verschillende berekeningen ondersteunt. FHE is echter nog relatief jong en zodoende zijn de producten minder volwassen. Momenteel kost FHE erg veel rekenkracht, waardoor gebruik voor toepassingen met veel data en complexe berekeningen nog niet altijd haalbaar is.



Figuur 3. Fully homomorphic encryption: rekenen in het versleutelde domein.

Fully homomorphic encryption in het kort	
Toepassing	Het uitbesteden van berekeningen op gevoelige data, zonder de data prijs te geven.
Aantal benodigde partijen	
Voordelen	Zeer flexibel en breed inzetbaar.
Nadelen	<i>Fully homomorphic encryption</i> kost (zeer) veel rekenkracht en is voor veel toepassingen nog niet praktisch haalbaar.
Veiligheids garanties	• • •
Volwassenheid & toepasbaarheid	•
Schaalbaarheid rekenkracht & geheugen	•
Schaalbaarheid netwerkgebruik	• •

Zie de bijlage op [pagina 21](#) voor een uitleg van de kenmerken.

# Trusted execution environments

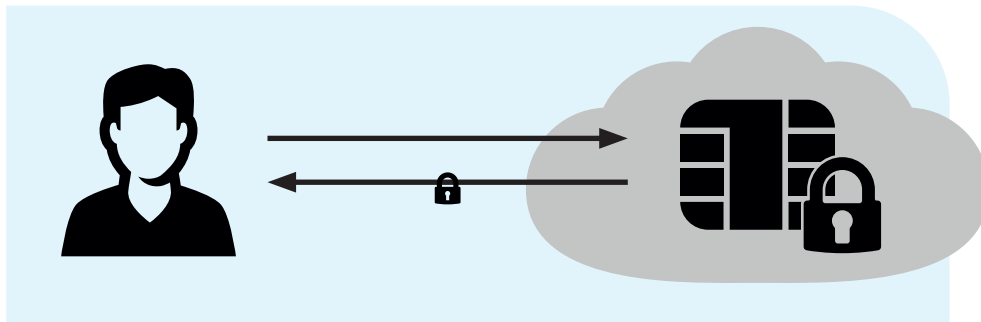
Trusted execution environments (TEE's) werken met speciale processors die een secure enclave ondersteunen: **een afgeschermd stukje hardware waarbinnen vertrouwelijk gerekend kan worden**. Gegevens en berekeningen in een TEE zijn niet toegankelijk voor processen of beheerders erbuiten.

TEE's zijn in zeker zin een buitenbeentje, omdat TEE's grotendeels hardware-oplossingen zijn. De meeste PET's zijn primair software-oplossingen.


Het gebruik van gespecialiseerde hardware binnen de cryptografie is niet nieuw: er bestaan al langer hardware-oplossingen voor bijvoorbeeld sleutelgeneratie en -opslag. Wat TEE's bijzonder maakt is dat ze niet beperkt zijn tot het veilig uitvoeren van één specifieke taak, maar allerlei berekeningen kunnen doen. Dit maakt ze breed toepasbaar.

De bekendste toepassing van TEE's is dezelfde als die van FHE: *outsourced computation*. Hiermee kun je berekeningen in de cloud laten uitvoeren, waarbij de TEE de gegevens afschermt van de clouddienst. Zelf een TEE implementeren vereist enige expertise.

Er worden af en toe kwetsbaarheden gevonden in TEE's, maar de technologie evolueert snel. Daarnaast zijn TEE's vaak 'gesloten' commerciële producten; het is lastig te achterhalen hoe ze precies werken.



Figuur 4. Trusted execution environment: afgeschermd, veilige rekenkracht.

Trusted execution environments in het kort	
Toepassing	Het uitbesteden van berekeningen op gevoelige data, zonder de data prijs te geven.
Aantal benodigde partijen	
Voordelen	Flexibel en relatief schaalbaar.
Nadelen	De technologie is al commercieel beschikbaar, maar nog in ontwikkeling. Ondanks hogere volwassenheid van producten worden er met enige regelmaat kwetsbaarheden gevonden.
Veiligheids garanties	• (•)
Volwassenheid & toepasbaarheid	• •
Schaalbaarheid rekenkracht & geheugen	• •
Schaalbaarheid netwerkgebruik	• •

Zie de bijlage op [pagina 21](#) voor een uitleg van de kenmerken.

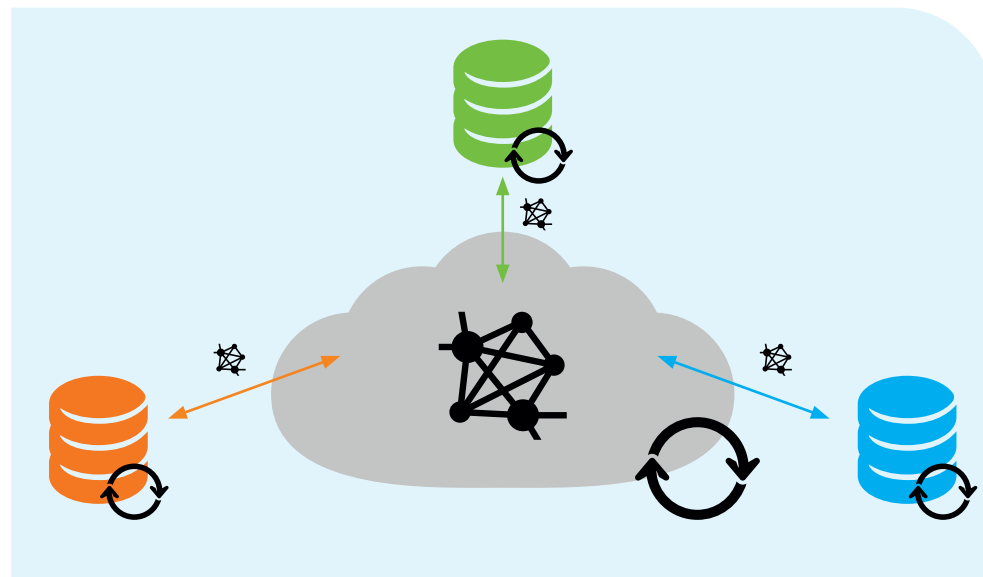
# Federated learning

Modellen voor kunstmatige intelligentie (AI) worden getraind op data: tijdens de trainingsfase ‘leert’ een AI-model aan de hand van een relevante database. Als deze trainingsdata niet op één centrale plek staat, maar verdeeld is over verschillende partijen, kan *federated learning* (FL) worden gebruikt.


De insteek van FL is als volgt: **in plaats van gegevens, delen de partijen getrainde ‘sub-modellen’ met elkaar**. Elke deelnemende partij traint een AI-model op eigen data. Deze modellen worden vervolgens bij elkaar gebracht tot één overkoepelend model. Dit overkoepelende model is dus getraind op alle data, maar zonder dat de partijen elkaars data hebben kunnen inzien.

Stel dat je een AI-model wilt trainen dat kan helpen diagnoses te stellen op basis van medische data. Hoe meer data, hoe beter het model - dus je zou idealiter de data van meerdere ziekenhuizen willen gebruiken. Met FL kun je een AI-model trainen zonder dat de ziekenhuizen gevoelige medische data hoeven te delen met elkaar.

FL beperkt het lekken van informatie, maar de precieze mate van vertrouwelijkheid is bij FL lastig te kwantificeren. Uit een sub-model, getraind op de data van één deelnemende partij, kan mogelijk informatie afgeleid worden. Hier dienen gebruikers rekening mee te houden.



Figuur 5. Federated learning: deel modellen in plaats van data.

Federated learning in het kort	
Toepassing	Het trainen van een AI-model op gedecentraliseerde data.
Aantal benodigde partijen	
Voordelen	Toepassingen vereisen weinig tot geen software op maat.
Nadelen	Het is lastig te kwantificeren hoe veilig FL is, omdat er informatie kan lekken uit de gedeelde sub-modellen.
Veiligheids garanties	● (●)
Volwassenheid & toepasbaarheid	● ●
Schaalbaarheid rekenkracht & geheugen	● ● ●
Schaalbaarheid netwerkgebruik	● ●

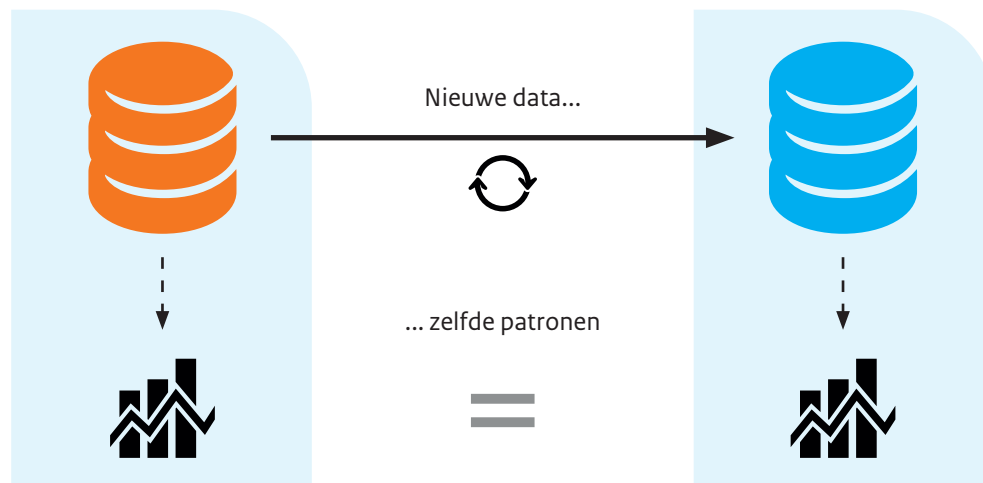
Zie de bijlage op [pagina 21](#) voor een uitleg van de kenmerken.

# Synthetische data-generatie


Synthetische data-generatie (SDG) is het proces om kunstmatige data te creëren die geen verband meer houdt met echte personen of entiteiten. Over het algemeen wordt synthetische data gegenereerd op basis van een bestaande, gevoelige dataset. **De kunst is om de nieuwe, synthetische dataset dezelfde statistische patronen en correlaties te laten bevatten als de originele, gevoelige dataset.**

Omdat een synthetische dataset geen gevoelige gegevens bevat, kan deze gemakkelijker gebruikt worden voor berekeningen en analyses. De datapunten zijn dan weliswaar fictief, maar in sommige toepassingen doet dat er niet toe. Zo zijn specifieke datapunten bij het trainen van AI-modellen van ondergeschikt belang. Het gaat uiteindelijk om de statistische patronen en correlaties die in de data voorkomen. Een data-eigenaar kan een synthetische dataset maken op basis van de eigen data en de synthetische dataset beschikbaar stellen aan derden om AI-modellen mee te trainen, bijvoorbeeld om de effectiviteit van medicijnen te verbeteren.

SDG is een methode die geen absolute vertrouwelijkheid garandeert. Hoewel de originele data niet gedeeld wordt met andere partijen, wordt de data gebruikt bij het genereren van de synthetische data. Naarmate de synthetische data meer patronen uit de originele data repliceert, groeit ook het risico dat de synthetische data onnodige informatie verklapt over de originele dataset. Het is belangrijk dat de data-eigenaar het risico op datalekkage uit de synthetische dataset analyseert, en bepaalt of dit risico aanvaardbaar is.



Figuur 6. Synthetische data: echte patronen in fictieve data.

Synthetische data in het kort	
Toepassing	Het trainen van een AI-model op gevoelige data.
Aantal benodigde partijen	
Voordelen	Met de synthetische dataset kan vrij gewerkt worden voor allerlei toepassingen, omdat deze niet langer gevoelig is.
Nadelen	Het genereren is een complexe taak: er is een balans tussen de kwaliteit van de gegenereerde data en het risico op informatie prijsgeven over de originele dataset.
Veiligheids garanties	● (●)
Volwassenheid & toepasbaarheid	● ●
Schaalbaarheid rekenkracht & geheugen	● ● ●
Schaalbaarheid netwerkgebruik	● ● ●

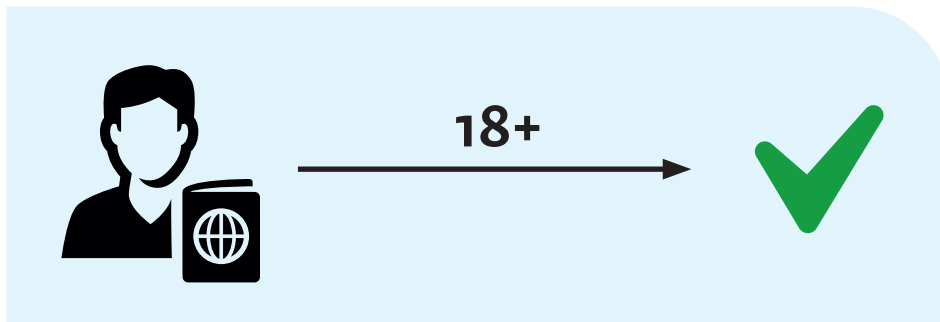
Zie de bijlage op [pagina 21](#) voor een uitleg van de kenmerken.

# Zero-knowledge proofs


Met behulp van een *zero-knowledge proof* (ZKP) kan een data-eigenaar bewijzen dat de data aan bepaalde voorwaarden of eigenschappen voldoet, zonder de onderliggende data te onthullen.

Een klassiek voorbeeld is dat van leeftijdscontrole. Als je ergens moet bewijzen dat je 18 jaar of ouder bent, doe je dit door een vorm van identificatie te laten zien. Hiermee deel je echter meer dan noodzakelijk is voor deze controle, zoals je volledige geboortedatum. Met behulp van een ZKP houd je meer controle op je eigen data. Je stelt de bewering 'ik ben ouder dan 18' op en produceert een bewijs. De controlerende partij kan dit bewijs vervolgens verifiëren zonder je exacte geboortedatum te weten te komen.

ZKP technieken zijn ook breder toepasbaar, bijvoorbeeld om te bewijzen dat een bepaalde berekening correct is uitgevoerd. Clouddiensten zouden dit bijvoorbeeld in de toekomst kunnen gebruiken om aan te tonen dat een AI-model correct wordt toegepast, of op de juiste data is getraind. Naar deze geavanceerde toepassingen is nog veel onderzoek nodig, omdat de berekeningen complex zijn.



Figuur 7. Zero-knowledge proofs: selectief gegevens onthullen.

Zero-knowledge proofs in het kort	
Toepassing	Het bewijzen van claims over gegevens zonder iets anders over de gegevens prijs te geven.
Aantal benodigde partijen	
Voordelen	Zeer flexibel en sterke garanties.
Nadelen	ZKP is een relatief complexe techniek die maatwerk vereist voor complexere toepassingen.
Veiligheids garanties	• • •
Volwassenheid & toepasbaarheid	• (•)
Schaalbaarheid rekenkracht & geheugen	• •
Schaalbaarheid netwerkgebruik	• •

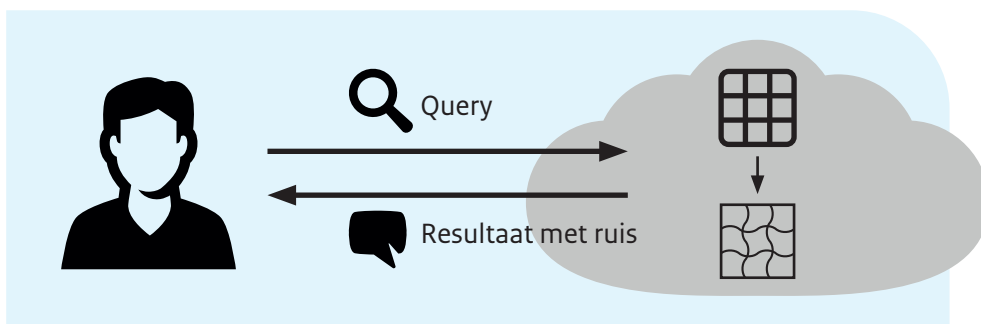
Zie de bijlage op [pagina 21](#) voor een uitleg van de kenmerken.

# Differential privacy


De PET's op de voorgaande bladzijden hebben het doel om gegevens tijdens een berekening vertrouwelijk te verwerken. Wel is het mogelijk dat de uitkomst van de berekening zelf informatie lekt over de gegevens - ongeacht de veiligheid waarmee de berekening is uitgevoerd. *Differential privacy* is een PET die juist als doel heeft om de informatie te verhullen die men kan achterhalen uit de uitkomst van een analyse.

Stel dat er binnen een organisatie jaarlijks een gemiddelde van de salarissen van werknemers wordt berekend en bekendgemaakt. Stel bovendien dat er in een gegeven jaar niemand vertrekt en er precies één nieuwe werknemer bijkomt. Als het nieuwe gemiddelde gepubliceerd wordt, dan lekt dit informatie over het salaris van die ene nieuwe werknemer.

Zulke situaties zijn te voorkomen: **differential privacy zorgt ervoor dat je statistische claims over een dataset kunt publiceren, zonder dat verschillen daarin kunnen worden teruggeleid naar een individu.** Dit gebeurt door ruis aan de uitkomst toe te voegen. De crux is om deze ruis zorgvuldig te kiezen. Het doel is om de statistische analyses nauwkeurig te houden, terwijl de achterliggende data beschermd blijven.



Figuur 8. Differential privacy: uitkomsten verhullen met ruis.

Differential privacy in het kort	
Toepassing	Het beschermen van individuele kenmerken bij (herhaalde) statistische analyses op een dataset.
Aantal benodigde partijen	
Voordelen	Er zijn geen (netwerk)interacties vereist en het kost weinig rekenkracht.
Nadelen	De analyse wordt minder nauwkeurig, vooral bij kleinere datasets.
Veiligheids garanties	• • •
Volwassenheid & toepasbaarheid	• •
Schaalbaarheid rekenkracht & geheugen	• • •
Schaalbaarheid netwerkgebruik	• • •

Zie de bijlage op [pagina 21](#) voor een uitleg van de kenmerken.

## Overwegingen bij het gebruik van PET's

De inzet van PET's kan van essentieel belang zijn bij de verwerking van vertrouwelijke gegevens. PET's verminderen de risico's voor *data in use*. De volgende zaken zijn hierbij echter van belang:

**1** Ten eerste heeft elke PET een eigen toepassingsgebied. Per casus moet worden verkend of en zo ja welke PET's relevant zijn. De inzet van PET's vereist bovendien maatwerk en in bepaalde gevallen het gebruik van speciale hardware of software.

**2** Ten tweede bieden PET's een krachtige methode voor dataminimalisatie. Het is van belang op te merken dat PET's geen garantie bieden dat de gebruiker daarmee automatisch voldoet aan de wet- en regelgeving omtrent gegevensverwerking.

**3** Ten derde verschillen de veiligheidsgaranties per PET. PET's zijn immers technisch-organisatorische oplossingen en daarmee maximaal zo veilig als de implementatie en het gebruik ervan.

PET's zijn geen totaaloplossing bij het omgaan met vertrouwelijke gegevens. PET's kunnen echter wel degelijk datasamenwerkingen mogelijk maken door de benodigde randvoorwaarden te scheppen.

Wil je meer informatie over PET's? Bezoek dan de website van het Nationaal Innovatie Centrum Privacy-Enhancing Technologies (NICPET): [www.nicpet.pleio.nl](http://www.nicpet.pleio.nl)

## Bijlage: uitleg van de kenmerken

**Veiligheidsgaranties:** hoe sterk zijn de garanties rondom vertrouwelijkheid die deze PET (opzichzelfstaand) biedt?

1. Geen garanties. De gegevensbescherming is lastig te beargumenteren of te kwantificeren, of er zijn grote (risico's op) kwetsbaarheden.
2. Enige garanties. Er is goede gegevensbescherming haalbaar (afhankelijk van de gekozen parameters en methoden). Wel is er kans op lekkage of er moet rekening gehouden worden met statistische aanvallen.
3. Sterke garanties. Wiskundig onderbouwde vertrouwelijkheids garanties.

**Volwassenheid & toepasbaarheid:** hoe volwassen is de techniek?

1. Er wordt (op academisch niveau) geëxperimenteerd met software. Eventueel enkele toepassingen met echte data. Het vereist nog veel onderzoek om de functionaliteit in de praktijk te brengen.
2. Wordt op echte casussen toegepast of gemaakt door één of enkele (startende) leveranciers.

*of*

Genoeg uitgewerkt op academisch vlak, maar er zijn nog weinig tot geen toepasbare implementaties.

3. Wordt breed toegepast in de praktijk in verschillende sectoren / er zijn verscheidene leveranciers.

*of*

Er zijn meerdere toepasbare en stabiele implementaties beschikbaar.

**Schaalbaarheid rekenkracht & geheugen:** hoeveel rekenkracht en/of geheugen vereist deze techniek?

1. Vereist buitengewone rekenkracht/geheugen of specialistische hardware.
2. Vereist significante rekenkracht/geheugen.
3. Vereist weinig extra rekenkracht en geheugen.

**Schaalbaarheid netwerkgebruik:** hoeveel netwerkgebruik vereist deze techniek?

1. Veel interactie via netwerkverbinding.
2. Weinig interacties en/of weinig volumes.
3. Geen interacties of netwerkverbinding.

Meer informatie over het verhogen van de cyberweerbaarheid van je organisatie of bedrijf is te vinden in onder andere deze publicaties. Deze zijn te raadplegen via [www.aivd.nl](http://www.aivd.nl).



Publicatie: **Verdedigbaar Netwerk**  
Hoe doe je dat?



Publicatie: **Generatieve AI:**  
een transformatieve impact  
op cybersecurity



Publicatie: **AI-systemen:**  
ontwikkel ze veilig



Publicatie: **Het PQC-migratie handboek**  
Richtlijnen voor het migreren naar  
Post-Quantumcryptografie

Deze brochure is met de grootst mogelijke zorg samengesteld door de AIVD, en is mede tot stand gekomen door de input van onafhankelijke experts van TNO. Het doel van deze publicatie is om bewustwording en begrip te creëren bij een breder publiek over het gebruik van *Privacy Enhancing Technologies* (PET's). Deze publicatie is niet gericht op het verschaffen van een volledig beeld of universele aanpak, enkel op het verschaffen van inzicht in het gebruik en de (on)mogelijkheden van de verschillende PET's. De in deze brochure beschreven PET's zijn niet een op een met elkaar te vergelijken, daar de relevantie afhangt van de toepassing. Aangezien PET's volop in ontwikkeling zijn, kan de informatie uit deze brochure verouderd raken na publicatie.

Algemene Inlichtingen- en Veiligheidsdienst  
Postbus 20010 | 2500 EA Den Haag  
aivd.nl

November 2025