SURF Juridisch Normenkader (Cloud) services (JNK)

Utrecht, september 2018
Versienummer: versie 3.0, september 2018

Colofon

SURF Juridisch Normenkader (Cloud) services (JNK)

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

September 2018

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.
Deze publicatie is digitaal beschikbaar via de website van SURF: www.surf.nl/publicaties

Inhoudsopgave

1. Historie

April 2014 heeft het toenmalige SURF Platformbestuur ICT en Bedrijfsvoering het SURF Juridisch Normenkader (Cloud)services (afgekort JNK) vastgesteld. Het JNK biedt handvaten aan de sector om adequate waarborgen in te bouwen bij het afnemen van clouddiensten met betrekking tot de omgang van persoonsgegevens, de vertrouwelijkheid van informatie, beschikbaarheid van de dienstverlening en eigendom van gegevens. Het zwaartepunt van het JNK ligt bij de bepalingen omtrent de omgang van persoonsgegevens. Deze bepalingen bieden waarborgen van de privacy van de gebruiker en zijn gebaseerd op nationale en Europese regelgeving.

Actualisering

In verband met ontwikkelingen rond internationaal verkeer van persoonsgegevens (ongeldigverklaring van Safe Harbor door het Europese Hof) en de inwerkingtreding van de meldplicht van datalekken, is het JNK voor wat betreft de privacy bepalingen geactualiseerd.[1]

Er is gekozen om de geactualiseerde privacy bepalingen onder te brengen in een zogenaamde verwerkersovereenkomst. Op de instelling rust de wettelijke verplichting om bij de afname van diensten waarbij in opdracht van de instelling persoonsgegevens worden verwerkt een dergelijke verwerkersovereenkomst af te sluiten. De SURF-modelverwerkersovereenkomst biedt hierbij een praktisch instrument. De model verwerkersovereenkomst is vastgesteld in de Juridische Commissie (zie hoofdstuk 3) en met ondersteuning van het advocatenkantoor Project Moore.

De model verwerkersovereenkomst en de overige bepalingen uit het JNK zijn toe te passen bij alle dienstverlening in opdracht van de instelling waar privacy, beschikbaarheid, vertrouwelijkheid en eigendom een rol spelen. In het document wordt gesproken daarom gesproken van ‘leverancier’.

De opzet van het Juridisch JNK is ook veranderd. In deze notitie wordt uitleg gegeven wat het JNK inhoudt en hoe het tot stand is gekomen. En zijn de bepalingen omtrent vertrouwelijkheid, intellectueel eigendom en beschikbaarheid te vinden. Daarnaast zijn er verschillende bijlagen, zoals de eerdergenoemde verwerkersovereenkomst, maar ook handreikingen over bijvoorbeeld beveiliging en audits, om het JNK op een goede manier te kunnen toepassen.

[1] In verband met de inwerkingtreding van de Europese Algemene Verordening Gegevensbescherming op 25 mei 2018 en de invoering door de Europese Commissie van het EU-US Privacy Shield ter vervanging van het Safe Harbor verdrag, is het JNK voor wat betreft de privacy bepalingen in juni 2018 geactualiseerd.

2. Onderwerpen uit het JNK

Het JNK biedt onderwijsinstellingen een stevige basis voor contracten met leveranciers. Bij het gebruik van leveranciers van ICT-diensten voor onderwijs, onderzoek en bedrijfsvoering van een instelling, worden (bedrijfs)gegevens voor opslag en verwerking ondergebracht binnen de ICT-infrastructuur van de leverancier. Dat vraagt waarborgen met betrekking tot **zeggenschap, vertrouwelijkheid, beschikbaarheid en privacy** van deze gegevens.

Zeker als het persoonsgegevens betreft is het bestuur van een instelling volgens wet- en regelgeving aansprakelijk voor het respecteren van de privacy van de personen, ook als de gegevens worden verwerkt bij een derde partij zoals de leverancier.

Ook vragen zeggenschap over gegevens en de vertrouwelijkheid waarborgen om de belangen van de instellingen te verzekeren. De clausules uit het JNK bieden deze waarborgen.

De vier bovengenoemde onderwerpen zijn nader gespecificeerd en per onderwerp zijn standaardbepalingen geformuleerd. Daarbij volgt een uitleg hoe deze bepalingen te duiden en te gebruiken.

NB: in de standaardbepalingen in deze notities worden een aantal begrippen met hoofdletter genoemd. Deze begrippen dienen in de overeenkomst te worden gedefinieerd. Onderstaande definities kunnen worden gebruikt:

Te gebruiken definities:

Dienst: *de onder de Overeenkomst te leveren dienst van leverancier*

Gebruiker: *een op enigerlei wijze aan instelling verbonden (natuurlijke) persoon, zoals personeel, docenten en/of studenten, die door de instelling geautoriseerd is tot (een bepaald deel) van de Dienst.*

Gegevens*: alle gegevens, data, informatie en ander materiaal of content die de instelling en/of Gebruikers in het kader van de Overeenkomst invoeren, versturen, plaatsen of anderszins verwerken met behulp van de Dienst, waaronder mede begrepen Persoonsgegevens.*

Overeenkomst: *de onderhavige Overeenkomst die ziet op verlening van Diensten en op grond waarvan de leverancier ten behoeve van instelling Gegevens verwerkt.*

Persoonsgegevens: *elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, die op welke wijze dan ook door leverancier verwerkt wordt of zal worden in het kader van de Overeenkomst.*

1. Eigendomsrechten en zeggenschap

Te gebruiken bepaling:

(INTELLECTUELE) EIGENDOMSRECHTEN EN ZEGGENSCHAP

1. Alle (intellectuele) eigendomsrechten - daaronder begrepen enig auteursrecht en databankenrecht - op (het bestand c.q. de bestanden van) de Gegevens blijven te allen tijde berusten bij de instelling, de betreffende Gebruiker, dan wel hun respectievelijke licentiegever(s).

2. Leverancier heeft geen zelfstandige zeggenschap over de Gegevens die door haar worden verwerkt. De zeggenschap over de Gegevens berust bij de instelling en/of de betreffende Gebruiker.

Uitleg	
Welke onderdelen?	- Intellectueel eigendom - Zeggenschap over gegevens
Waarom belangrijk?	Regelen dat zeggenschap over gegevens niet wordt overgedragen aan de leverancier
Waar regelen?	Hoofdovereenkomst
Toelichting	Intellectueel eigendom: Het intellectuele eigendom op de gegevens (uitdrukkelijk alle gegevens en niet slechts persoonsgegevens) gaat nooit over naar de leverancier, maar blijft in handen van de instelling, gebruiker of de licentiegevers van de gebruiker of de instelling. Met deze bepaling is vastgelegd dat de leverancier de intellectuele eigendomsrechten dient te respecteren. Zeggenschap: Door de zeggenschap over de gegevens (uitdrukkelijk alle gegevens en niet slechts persoonsgegevens) te leggen bij de gebruiker en/of de instelling is expliciet vastgelegd dat de gegevens alleen mogen worden verwerkt voor zover de gebruiker/instelling daar opdracht toe geeft.
Praktijk	Het intellectuele eigendom van gegevens, bijvoorbeeld van werkstukken van studenten, behoort toe aan de student en/of instelling. Dit kan nooit overgaan op de leverancier. De gegevens die worden verwerkt blijven onder de zeggenschap van de instelling en/of gebruiker. In het Nederlands recht is de term eigendom en daarmee eigenaarschap verbonden met fysieke zaken. Nu van fysieke zaken bij clouddienstverlening geen sprake is, is hier niet voor de term eigenaarschap gekozen, maar voor termen die met betrekking tot gegevens gezamenlijk dezelfde lading dekken: (intellectuele) eigendomsrechten en zeggenschap.

2. Beschikbaarheid

Te gebruiken bepaling:

BESCHIKBAARHED VAN DE GEGEVENS

1. Leverancier is verantwoordelijk voor de beschikbaarheid van de Dienst aan de instelling overeenkomstig het bepaalde in deze Overeenkomst <en de service level agreement (SLA) welke daarvan onderdeel uitmaakt>.

2. Leverancier zal zorgdragen voor adequate back-up en restore voorzieningen om beschikbaarheid van de Dienst (en daarmee van de statische en dynamische Gegevens) te waarborgen.

Uitleg	
Welke onderdelen?	- Beschikbaarheid - Back- up en restore voorzieningen
Waarom belangrijk?	Zorgen dat er overeenstemming is over de beschikbaarheid van de dienst en te garanderen dat er een adequate back-up is.
Waar regelen?	Hoofdovereenkomst en in de Service Level Agreement (SLA)
Toelichting	Beschikbaarheid: Met deze bepaling stemt de leverancier uitdrukkelijk (expliciet) in met de bepalingen in de overeenkomst. Wanneer de instelling constateert dat de dienstverlening niet aan de bepalingen voldoet, geeft dit artikel een extra mogelijkheid (naast de al niet nagekomen bepaling) om de leverancier in juridische zin aan te spreken. Back- up en restore voorzieningen: De leverancier is verplicht de gegevens of een kopie van de gegevens te bewaren voor het geval de dienstverlening uitvalt (om welke reden dan ook). Ook is de leverancier verplicht een recente back-up te kunnen gebruiken om de dienstverlening na de uitval weer te kunnen opstarten (restore-en). De gegevens blijven hierdoor beschikbaar voor de instelling.
Praktijk	Met verwijzing naar onder andere deze bepaling kan een ingebrekestelling worden opgesteld in het geval de leverancier de bepalingen niet nakomt. De tussen haakjes < > gezette tekst in lid 1 kan worden weggelaten indien er geen sprake is van een SLA.

3. **Vertrouwelijkheid**

Te gebruiken bepaling:

ARTIKEL VERTROUWELIJKHEID

1. Partijen zullen alle Gegevens waarvan zij het vertrouwelijk karakter kennen of redelijkerwijs kunnen vermoeden en die hen in het kader van de uitvoering van deze Overeenkomst ter kennis of beschikking komen, geheimhouden en op geen enkele wijze verder intern of extern bekendmaken en/of aan derden verstrekken, behalve voor zover:

a) bekendmaking en/of verstrekking van die Gegevens in het kader van de uitvoering van deze Overeenkomst noodzakelijk is;
b) enig dwingendrechtelijk wettelijk voorschrift of rechterlijke uitspraak partijen tot bekendmaking en/of verstrekking van die Gegevens of informatie verplicht, waarbij partijen eerst de andere partij hiervan op de hoogte stellen;
c) bekendmaking en/of verstrekking van die Gegevens geschiedt met voorafgaande schriftelijke toestemming van de andere partij; dan wel
d) het informatie betreft die al rechtmatig openbaar was op een andere wijze dan door het handelen of nalaten van een der partijen.

2. Bij elke schending van zijn geheimhoudingsverplichting zijn partijen een direct opeisbare boete van EUR 25.000 per overtreding verschuldigd, onverlet de overige rechten op schadevergoeding van de andere partij.

3. Partijen zullen voor hen werkzame personen (waaronder werknemers) die betrokken zijn bij de verwerking van vertrouwelijke Gegevens contractueel verplichten tot geheimhouding van die vertrouwelijke Gegevens.

4. Partijen verlenen op verzoek van de andere partij hun medewerking aan het uitoefenen van toezicht door of namens de andere partij op de bewaring en het gebruik van vertrouwelijke Gegevens door de andere partij.

5. Partijen stellen alle Gegevens die zij in het kader van de uitvoering van de Overeenkomst onder zich hebben, inclusief eventueel daarvan gemaakte kopieën, op eerste verzoek aan de andere partij ter beschikking.

6. Ieder der Partijen zal de andere partij onmiddellijk informeren nadat zij bekend is geworden met een vermoedelijk(e) of daadwerkelijk(e) (i) schending van de geheimhoudingsplicht; (ii) verlies van vertrouwelijke Gegevens; of (iii) schending van beveiligingsmaatregelen. De nalatige partij zal op eigen kosten alle benodigde maatregelen nemen om de vertrouwelijke Gegevens veilig te stellen, de tekortkomingen in de beveiligingsmaatregelen te herstellen om verdere kennisneming, wijziging, en verstrekking te voorkomen, onverminderd enig recht van constaterende partij op schadevergoeding of andere maatregelen. De nalatige partij zal op verzoek van de andere partij meewerken aan het informeren van betrokkenen.

Uitleg	
Welke onderdelen?	- Vertrouwelijkheid - Schending vertrouwelijkheid - Geheimhouding - Toezicht vertrouwelijkheid
Waarom belangrijk?	Regelen dat bepaalde (persoons)gegevens vertrouwelijk worden behandeld, niet intern en extern mogen worden verspreid en er een geheimhoudingsplicht geldt voor werknemers.
Waar regelen?	Hoofdovereenkomst en eventueel in de verwerkersovereenkomst.
Toelichting	1. Met toepassing van dit artikel worden gegevens die als vertrouwelijk worden bestempeld door de instelling of door de gebruiker als zodanig te worden behandeld. De vertrouwelijkheid van gegevens heeft tot gevolg dat de leverancier deze gegevens geheim dient te houden en niet mag verspreiden/bekendmaken (noch intern, noch extern). Persoonsgegevens kunnen worden onderscheiden van vertrouwelijke gegevens (maar persoonsgegevens kunnen tegelijkertijd ook vertrouwelijke gegevens zijn). Daar waar het persoonsgegevens betreft dient te worden voldaan aan de Algemene Verordening Gegevensbescherming (AVG). Ad a. Het kan voorkomen dat bekendmaken of verstrekking van vertrouwelijke gegevens noodzakelijk is voor de uitvoering van de dienstverlening en/of de overeenkomst. In dat geval en tot zover is bekendmaking en verspreiding van vertrouwelijke gegevens toegestaan. Ad b. De vertrouwelijkheid van gegevens mag niet in de weg staan bij het voldoen van de leverancier aan dwingendrechtelijke wet- en regelgeving. Ook hier geldt weer dat bekendmaking en verstrekking van de vertrouwelijk gegevens is toegestaan om te voldoen aan de dwingendrechtelijke wet- en regelgeving door de leverancier. Ad c. Alleen met schriftelijke toestemming van de verantwoordelijke mogen vertrouwelijke gegevens worden bekendgemaakt/ verstrekt. Ook hier geldt weer dat de bekendmaking en de verspreiding alleen mag conform de schriftelijke toestemming en niet verder dan waarvoor de toestemming gegeven is. Ad d. Wanneer vertrouwelijke gegevens al openbaar zijn (door toedoen of nalaten van de instelling) is de geheimhouding niet meer van toepassing. 2. Op het schenden van de geheimhoudingsplicht staat een direct opeisbare boete, daar schending van de geheimhoudingsplicht niet meer kan worden teruggedraaid. Bij de hoogte van de boete is ook gekeken naar de ARBIT-voorwaarden. Deze is niet overgenomen. Er is besloten een lager bedrag van € 25.000,-- per overtreding te hanteren. 3. Niet alleen de leverancier maar ook de voor haar werkzame personen dienen een geheimhoudingsverklaring te ondertekenen om aan dit artikel te kunnen voldoen. Dit om de geheimhoudingsplicht verder te effectueren en de aansprakelijkheid ten aanzien van het schenden van de geheimhoudingsverplichting vast te leggen.

	4. Ter zekerstelling van een juiste uitvoering van de geheimhoudingverplichting door de leverancier is de leverancier verplicht medewerking te verlenen aan het toezicht dat de instelling hierop uit kan voeren. De leverancier is op grond van deze bepaling verplicht mee te werken aan het toezicht op de naleving van deze geheimhoudingsverplichting. 5. De instelling kan (vertrouwelijke) gegevens op verzoek opvragen. Ook eventuele kopieën van de gegevens zodat vertrouwelijke gegevens niet meer worden verwerkt bij de leverancier. Op deze wijze kan de instelling de verwerking van de (vertrouwelijk) gegevens controleren en beheersen. 6. Voor de leverancier geldt een onmiddellijke informatieplicht ter zake van beveiligingsincidenten betreffende vertrouwelijke gegevens. Het gaat hierbij om vermoedelijk en daadwerkelijk incident zodat de geheimhoudingsplicht zoveel als mogelijk kan worden gewaarborgd. Onder incidenten vallen onbevoegde kennisneming en inbreuken op de beveiliging die leiden tot onrechtmatig verlies, vernietiging of wijziging van gegevens. Naast de informatieplicht is de leverancier verplicht om te reageren op de incidenten door de vertrouwelijke gegevens veilig te stellen, maatregelen nemen om het incident te beëindigen en/of te voorkomen en mee te werken aan verdere afhandeling van een incident.
Praktijk	1. De instelling of gebruiker kan expliciet aangeven dat gegevens vertrouwelijk zijn. Op dat moment vallen de gegevens onder de regeling van dit artikel. Wanneer de vertrouwelijkheid niet expliciet is aangegeven, maar de leverancier wel kan vermoeden dat het vertrouwelijke gegevens betreft dienen de gegevens ook als vertrouwelijk behandeld te worden. In de praktijk is het aan te bevelen de vertrouwelijkheid van gegevens expliciet aan te geven, zodat daaromtrent geen discussie kan ontstaan. Een oordeel van vertrouwelijkheid ligt in dat geval bij de instelling en/of gebruiker zelf. Daar waar het gaat om gegevens waarvan redelijkerwijs vermoed kan worden dat de gegevens vertrouwelijk zijn, is dat uiteindelijk ter beoordeling van de rechter. Voor de leverancier betekent de geheimhoudingsplicht dat de vertrouwelijke gegevens niet door de leverancier verder worden verspreid dan nodig voor de uitvoering van de dienstverlening. Deze gegevens mogen niet intern of extern bekend worden gemaakt of verder worden verspreid. 2. Wanneer de leverancier de geheimhoudingsplicht schendt is een direct opeisbare boete op zijn plaats. Een schending van de geheimhoudingsplicht kan vaak niet worden teruggedraaid. Er is dan al direct sprake van schade. 3. De geheimhoudingsverklaring dient voorafgaand aan het starten van de dienstverlening gecontroleerd te worden. Dat kan door de betreffende contractuele verplichting op te vragen bij de leverancier. 4. De instelling kan toezicht op de naleving van de geheimhoudingsverplichting uitvoeren door bijvoorbeeld de geheimhoudingsverklaring met medewerkers van de leverancier op te vragen of procedures die betrekking hebben op de uitvoering van de geheimhoudingsverplichting in te zien.

4. Privacy

De AVG stelt zowel de instelling als de leverancier verantwoordelijk voor het waarborgen van de privacy van de personen wiens gegevens het betreft (de betrokkenen). Als een leverancier gegevens namens een instelling verwerkt, schrijft de AVG voor dat er schriftelijke afspraken moeten worden gemaakt tussen de verantwoordelijke voor de verwerking van de persoonsgegevens (de instelling in dit geval) en de verwerker (de leverancier), om zo een goede omgang met persoonsgegevens te waarborgen en af te spreken wat een verwerker wel en niet mag doen met de persoonsgegevens.

Belangrijk daarbij is dat persoonsgegevens door de instelling worden geclassificeerd naar risiconiveau. In overeenstemming met de richtlijnen van de Autoriteit Persoonsgegevens, de Nederlandse toezichthouder op de uitvoering van de AVG, stelt het JNK toenemende eisen aan de leverancier, naar gelang een hoger risiconiveau van gegevens wordt vastgesteld.JNK) De bepalingen geven de instelling de zekerheid dat de eigen wettelijke verantwoordelijkheid genomen is en verantwoord kan worden naar de toezichthouder. Ook rechten van de betrokkenen worden gewaarborgd. Verder regelen de bepalingen dat de leverancier ook bij inschakeling van hulpleveranciers (sub-verwerkers) aan rechten en plichten blijft voldoen in het licht van de verantwoordelijkheid van de instelling. Dit geldt ook als de leverancier of hulpleveranciers zich buiten de Europese Economische Ruimte (EER) bevindt.

Bepalingen over privacy en de bescherming van persoonsgegevens worden in een verwerkersovereenkomst opgenomen. De verwerkersovereenkomst kan als losse overeenkomst naast de hoofovereenkomst worden afgesloten, of als bijlage bij de hoofdovereenkomst waarin de dienstverlening wordt geregeld. Een Model Verwerkersovereenkomst is onderdeel van het JNK.

De Model Verwerkersovereenkomst kent de volgende onderwerpen:

- Verwerken in opdracht en volgens instructies van de verwerkingsverantwoordelijke;
- Geheimhouding;
- Toegang tot persoonsgegevens;
- Inzet van hulpleveranciers/sub-verwerkers ;
- Beveiligingsmaatregelen;
- Meldplicht datalekken;
- Auditverplichting;
- Doorgifte aan derde landen
- Behandelen van opsporingsverzoeken;
- Verlenen van bijstand en medewerking door verwerker;
- Afhandelen van verzoeken van betrokken;
- Aansprakelijkheid en vrijwaring;
- Wijziging in verwerking van persoonsgegevens;
- Duur en beëindiging;
- Toepasselijk recht en geschillenbeslechting;
- Specificatie van verwerking, waaronder de persoonsgegevens en beveiligingsmaatregelen.

De Model verwerkersovereenkomst is bijlage A bij het JNK.

Een aparte bijlage, horend bij het JNK, bevat een toelichting bij elke bepaling van de verwerkersovereenkomst en een instructie voor het invullen van de bijlage A behorend bij de Model verwerkersovereenkomst (specificatie van de persoonsgegevens en beveiligingsmaatregelen).

3. Juridische commissie

Bij het vaststellen van het JNK heeft SURF besloten tot de inrichting van een Juridische Commissie. De commissie houdt zich bezig met de verdere ontwikkeling van het JNK en bespreekt het toepassen van het JNK in de praktijk.

De commissie bestaat uit minimaal 5 en maximaal 10 leden. Leden van de commissie zijn aangesteld voor de looptijd van 2 jaar. De commissie kiest een voorzitter uit haar midden. SURF zorgt voor een secretaris. Bij een vergadering van de commissie zal een jurist van SURFmarket aanwezig zijn en de Corporate Privacy Officer van SURF. De medewerkers van SURF waaronder ook de secretaris zijn geen lid van de commissie.

Bij de benoeming van de leden van de commissie worden de CSC's betrokken. Benoeming van leden van de commissie is een besluit van het bestuur van SURF. De samenstelling van de commissie wordt gepubliceerd op de website.

De Juridische Commissie komt 4 keer per jaar bijeen. De Juridische Commissie adviseert het bestuur van SURF over inhoud en toepassing van het JNK. De commissie bereidt aanpassingen voor en zorgt voor aansluiting van het JNK bij ontwikkelingen op het gebied van wet en regelgeving en andere relevante ontwikkelingen.

SURF kan door haar gewenste aanpassingen van het JNK ter advies bij de commissie voorleggen. Substantiële aanpassingen zowel wat betreft inhoud als met betrekking tot de werkwijze legt de commissie voor aan het bestuur die besluit over de aanpassingen.

Het bestuur legt verantwoording af aan de Ledenraad over de manier waarop deze met het advies omgaat. Kleine aanpassingen die de commissie voorstelt kunnen worden voorgelegd aan het lid van het bestuur met privacy en security in portefeuille die hierover een besluit kan nemen.

De commissie stelt een jaarverslag op voor het bestuur dat zal worden gedeeld met de Ledenraad

4. Praktische instrumenten en andere handreikingen

Het JNK bevat een aantal bijlagen, die zijn opgesteld om te helpen bij het gebruiken en toepassen van het kader:

Bijlage A: SURF Model verwerkersovereenkomst
Bijlage B: Instructie bij Model verwerkersovereenkomst
Bijlage C: Handreiking beveiligingsmaatregelen
Bijlage D: Handreiking Auditverplichting leverancier

Het JNK blijft zich ontwikkelen en er wordt naar gestreefd om het JNK verder aan te vullen met handreikingen en praktische instrumenten voor de toepassing van het kader in de praktijk. In deze versie van het JNK heeft met name privacy veel aandacht gekregen maar ook voor de andere onderwerpen – zoals beschikbaarheid en vertrouwelijkheid – staan voor verdere uitwerkingen op de agenda.