Samen aanjagen van vernieuwing

Vergelijking SURF Juridisch Normenkader (Cloud)services en Data Pro Code van NLdigital

Auteur(s): SURF
Versie: 1.0
Datum: 1 november 2020

Inhoudsopgave

Inleiding

In deze notitie wordt een vergelijking gemaakt tussen de Data Pro Code van NLdigital[1] (voorheen Nederland ICT) en het SURF Juridisch Normenkader (Cloud)services[2]. Het betreft twee verschillende soorten documenten.

- Het SURF Juridisch Normenkader (Cloud)services (hierna: "JNK") is geschreven voor de doelgroep van SURF (de aangesloten onderwijs- en onderzoeksinstellingen). Het biedt hen handvaten om goede contracten met cloudleveranciers te kunnen sluiten. De Data Pro Code is geschreven voor verwerkers en vormt een nadere uitwerking van de verplichtingen voor verwerkers op grond van artikel 28 Algemene verordening gegevensbescherming (hierna: "AVG").
- De Data Pro Code is een gedragscode in de zin van artikel 40 lid 5 AVG.[3] Het JNK vormt niet een gedragscode in de zin van dit artikel, en is ook niet ter goedkeuring voorgelegd aan de Autoriteit Persoonsgegevens (hierna: "AP").

De Data Pro Code bestaat uit de volgende onderdelen:

- The Data Pro Code:
  - Informatieverplichtingen – Data Pro Statement
  - Toetsing en toezicht
  - Werking en aanpassing Data Pro Code
- Bijlage 1: Verwerkersovereenkomst, bestaande uit I) Data Pro Statement en II) Standaardclausules voor verwerkingen
- Bijlage 2: Uitgangspunten privacybeleid en Data Pro Statement met toelichting

Het JNK bestaat uit de volgende onderdelen:

- SURF Juridisch Normenkader (Cloud)services
- Bijlage A: Verwerkersovereenkomst
- Bijlage B: Instructie bij de verwerkersovereenkomst
- Bijlage C: Handreiking Beveiligingsmaatregelen
- Bijlage D: Handreiking Auditverplichting

In hoofdstuk 1 worden de belangrijkste verschillen tussen de Data Pro Code en het JNK uitgewerkt. In Hoofdstuk 2 worden vervolgens de belangrijkste verschillen tussen de twee bijbehorende verwerkersovereenkomsten uitgewerkt.

[1] Versie april 2019

[2] Versie april 2019, verwerkersovereenkomst 3.0

[3] De AP heeft in haar besluit ter goedkeuring van de Data Pro Code als opschortende voorwaarde opgenomen dat NLdigital een onafhankelijk toezichthoudend orgaan moet instellen ter controle op de naleving van de gedragscode op grond van artikel 41 lid 1 AVG. Dit toezichthoudende orgaan moet worden geaccrediteerd door de Autoriteit Persoonsgegevens.

1 Vergelijking Data Pro Code en JNK

1.1 Toepassingsgebied

- Het JNK ziet niet enkel op privacy, maar dat is wel waar het zwaartepunt ligt. Het JNK is breder en biedt “handvaten aan de sector om adequate waarborgen in te bouwen bij het afnemen van clouddiensten m.b.t. de omgang van persoonsgegevens, de vertrouwelijkheid van informatie, beschikbaarheid van de dienstverlening en eigendom van gegevens”. In het JNK worden standaardbepalingen (inclusief een toelichting) gegeven die kunnen worden opgenomen in de hoofdovereenkomst, de SLA en de verwerkersovereenkomst tussen partijen. Deze bepalingen zien op de onderwerpen Intellectuele eigendom en zeggenschap, beschikbaarheid en vertrouwelijkheid.
- De Data Pro Code is volledig gefocust op privacy en de AVG. In de Data Pro Code is niets opgenomen over intellectuele eigendom en zeggenschap. Beschikbaarheid en vertrouwelijkheid worden kort aangestipt, maar niet verder uitgewerkt.

1.2 Territoriaal toepassingsgebied

- De gedragscode bepaalt in de inleiding dat de Data Pro Code enkel van toepassing is op verwerkingen in Nederland. In de Data Pro Statement is echter wel de mogelijkheid opgenomen om aan te geven dat de verwerking (deels) plaatsvindt buiten de EER.
- Het SURF JNK kent deze beperking qua territoriaal toepassingsgebied niet. Wel is het JNK geschreven op basis van de Nederlandse implementatie van de AVG (de Uitvoeringswet Algemene verordening gegevensbescherming).

1.3 Doelgroep

- Het JNK is geschreven voor de doelgroep van SURF, die bestaat uit onderwijs- en onderzoeksinstellingen die doorgaans optreden als verwerkingsverantwoordelijke in de zin van de AVG.
- De Data Pro Code is geschreven voor verwerkers.

1.4 Handreiking beveiligingsmaatregelen

- Het JNK kent de bijlage ‘Beveiligingsmaatregelen’. Hierin is een uitgebreide set maatregelen opgenomen die zijn bedoeld als handreiking om het begrip ‘passende beveiligingsmaatregelen’ uit de AVG en de verwerkersovereenkomst concreet te maken. De volgende categorieën zijn hierin uitgewerkt: 1) beleid en organisatie, 2) toegangsbeveiliging, 3) beheer van technische kwetsbaarheden en anti-malware, 4) vertrouwelijkheid en integriteit van gegevens en privacy en 5) controle en logging.
- De Data Pro Code kent geen uitwerking of toelichting van beveiligingsmaatregelen, anders dan een beknopte opsomming van maatregelen die verwerkers kunnen gebruiken als inspiratie.

1.5 Handreiking auditverplichting

- Het JNK kent een auditverplichting, afhankelijk van het risiconiveau van de verwerking. Van de verwerker wordt gevraagd om periodiek een door hem aan te wijzen onafhankelijke IT-auditor of deskundige een onderzoek te laten uitvoeren naar de organisatie van de verwerker. Het doel daarvan is aan te tonen dat verwerker voldoet aan het bepaalde in de verwerkersovereenkomst, de AVG en andere toepasselijke wet- en regelgeving betreffende de verwerking van persoonsgegevens. In deze bijlage bij het JNK wordt een handreiking geboden voor de omgang met de auditverplichting in de praktijk.
- Bij de Data Pro Code heeft de verwerker niet standaard een periodieke auditverplichting. Wel heeft de Data Pro Code een vrijwillig certificeringsmechanisme, zoals toegelicht onder punt 6, waar een jaarlijkse toetsing onderdeel van is.

1.6 Externe toetsing en toezicht

- Een verwerker die aantoonbaar in voldoende mate voldoet aan het gestelde in de Data Pro Code, wordt opgenomen in het openbaar toegankelijke Data Pro Register. Deze verwerker onderwerpt zich hiermee aan externe toetsing. De toetsing vindt één keer per jaar plaats, waarbij additionele toetsingen mogelijk zijn op onregelmatige basis. Wanneer een verwerker minder dan 50 werknemers in dienst heeft, vindt de audit online plaats. Wanneer de verwerker meer dan 50 werknemers in dienst heeft, vindt de audit op locatie plaats. Er wordt toezicht gehouden op het toetsingsproces door de onafhankelijke Data Pro Toezichthouder.[4] De Data Pro Toezichthouder beheert het register, maakt het openbaar en kan verwerkers verwijderen uit het register als de omstandigheden daar aanleiding toe geven. De geregistreerde verwerker verkrijgt een gebruiksrecht om het Data Pro Certificate te gebruiken waarmee hij aantoont dat hij zich houdt aan het gestelde in de Data Pro Code. Het is niet duidelijk waar precies op wordt getoetst voor de certificering. Op de website van NLdigital staat dat er wordt getoetst of de verwerker voldoet aan de gedragscode Data Pro. De Data Pro Code laat echter wel enige keuzevrijheid aan verwerkers. Zo is het bijvoorbeeld toegestaan om een eigen verwerkersovereenkomst te hanteren en worden in Bijlage 2 uitgangspunten genoemd die door een verwerker in een privacybeleid kunnen worden opgenomen.
- Het JNK kent geen externe toetsing met een certificaat. Wel kent het JNK de auditverplichting zoals genoemd onder punt 1.5.

1.7 Verwerkersovereenkomst

- Zowel het JNK als de Data Pro Code bevat een standaardverwerkersovereenkomst.
- Bij de Data Pro Code bestaat de verwerkersovereenkomst uit de Data Pro Statement en de Standaardclausules. De Data Pro Code biedt de mogelijkheid aan verwerkers om de Standaardclausules te vervangen door een eigen, daarmee vergelijkbare, verwerkersovereenkomst.

1.8 Contactpersoon met kennis van privacy

- De Data Pro Code stelt dat de verwerker een contactpersoon heeft aangewezen voor dataprotectie die kennis heeft van dataprotectie, of die kennis verkrijgt via opleiding.[5]
- De verwerkersovereenkomst van het JNK stelt het verplicht om een contactpersoon op te nemen voor de verwerkersovereenkomst en voor datalekken, maar niet dat deze persoon kennis moet hebben van dataprotectie.

1.9 Verwerkingsregister

- De Data Pro Code stelt dat de verwerker een accurate contractadministratie heeft en daarmee kan voldoen aan de verwerkingsregistratieplicht.[6]
- Het JNK stelt niet expliciet de verplichting dat verwerkers een verwerkingsregister moeten bijhouden.

4 Ten tijde van het schrijven van deze Vergelijking SURF JNK en Data Pro Code van NLdigital, is de onafhankelijke Data Pro Toezichthouder nog niet ingesteld.

5 Toelichting van Bijlage 2, Uitgangspunt 2, Data Pro Code.

6 Toelichting van Bijlage 2, Uitgangspunt 3, Data Pro Code.

1.10 Gescheiden verwerking persoonsgegevens

- De Data Pro Code stelt dat de verwerker de persoonsgegevens van de verwerkingsverantwoordelijke zal scheiden van persoonsgegevens van andere verantwoordelijke.[7]
- Het JNK kent een dergelijke bepaling niet.

[7] Toelichting van Bijlage 2, Uitgangspunt 3, Data Pro Code.

2 Vergelijking verwerkersovereenkomsten

In dit hoofdstuk is een vergelijking opgenomen tussen de Model Verwerkersovereenkomst “Data Pro”, opgesteld door NLdigital en de SURF Model Verwerkersovereenkomst 3.0, horend bij het SURF Juridisch Normenkader (Cloud)services.

2.1 Opzet en opbouw

De SURF verwerkersovereenkomst bestaat uit een aantal standaardbepalingen en drie bijlagen:

- Standaardbepalingen voor de verwerkersovereenkomst (overwegingen en 13 bepalingen)
- Bijlage A: specificering van de te leveren dienst. Bij meerdere diensten kunnen meerdere Bijlagen A worden toegevoegd.
- Bijlage B: Specificering van de beveiligingsmaatregelen van de te leveren dienst. Bij meerdere diensten kunnen meerdere Bijlagen B worden toegevoegd.

De Data Pro verwerkersovereenkomst bestaat uit twee delen:

- Deel 1: Data Pro Statement. In dit statement geeft de verwerker een specificering van de te leveren dienst/product, op het gebied van privacy en security.
- Deel 2: Standaardbepalingen voor de verwerkersovereenkomst (9 bepalingen)

Vergelijking opzet en opbouw:
Het Data Pro Statement is te vergelijken met Bijlage A en B van de SURF verwerkersovereenkomst. Daarin vindt men de specificering van de te leveren dienst/product op het gebied van privacy en security.

Verschillen:

- Het Data Pro Statement wordt opgesteld door de verwerker; de opdrachtgever/verwerkingsverantwoordelijke moet vervolgens beoordelen of dit goed genoeg is. Het invullen van Bijlage A en B van de SURF verwerkersovereenkomst is meer een inspanning van verwerker en verwerkingsverantwoordelijke gezamenlijk.
- De terminologie is anders. De SURF verwerkersovereenkomst is een overeenkomst tussen ‘verwerkingsverantwoordelijke’ en ‘verwerker’. De Data Pro verwerkersovereenkomst is een overeenkomst tussen ‘data processor’ en ‘opdrachtgever’. Door die terminologie is de Data Pro Code ook te gebruiken tussen verwerker en subverwerker.
- De inhoud en de vragen die gesteld worden zijn op sommige punten anders. Deze punten zijn hieronder verder uitgewerkt.

2.2 Verschillen specificering van de dienst/ het product

De inhoud en de vragen die gesteld worden in het Data Pro Statement en Bijlage A en B van de SURF verwerkersovereenkomst zijn op sommige punten anders. Dit zijn de verschillen:

- **Verzoeken van betrokkenen**: In het Data Pro Statement wordt gevraagd hoe de processor de opdrachtgever ondersteunt bij verzoeken van betrokkenen. In de SURF verwerkersovereenkomst staat in de standaardbepalingen wel dat een verwerker de verwerkingsverantwoordelijke moet ondersteunen, maar wordt er middels de specificatie niet een uitwerking gevraagd hoe dit wordt vormgegeven.

- **Privacy by design**: In het Data Pro Statement wordt gevraagd hoe de data processor bij het ontwerpen van het product/de dienst privacy by design/privacy by default heeft toegepast. Deze vraag komt in Bijlage A en B van de SURF verwerkersovereenkomst niet terug.
- **Medewerking DPIA**: In het Data Pro Statement wordt gevraagd hoe de processor medewerking verleent aan een Data Privacy Impact Assessment. In de SURF verwerkersovereenkomst staat in de standaard bepalingen wel dat een verwerker de verwerkingsverantwoordelijke moet ondersteunen, maar wordt niet een uitwerking gevraagd hoe dit wordt vormgegeven.
- **Bewaartermijnen**:
  - Bewaartermijnen na afloop overeenkomst: In de Data Pro Code staat een standaardtermijn van 3 maanden, waar eventueel van kan worden afgeweken met een toelichting. De SURF verwerkersovereenkomst kent een termijn van 1 maand na afloop van de verwerkersovereenkomst.
  - Bewaartermijnen tijdens de looptijd van de overeenkomst: In de Data Pro Code wordt niet gevraagd naar tussentijdse verwijdering van gegevens. In de SURF verwerkersovereenkomst wordt daar wel naar gevraagd in Bijlage A.
- **Datalekkenprotocol**: In het Data Pro Statement wordt gevraagd wat het datalekkenprotocol is van de data processor. Bij de SURF verwerkersovereenkomst is dit anders geregeld. Via artikel 7.3 wordt de verwerker verplicht gesteld om beleid en procedures te hebben omtrent datalekken en kan de verwerkingsverantwoordelijke op verzoek inzage in dit beleid krijgen. Beide overeenkomsten stellen beleid omtrent datalekken verplicht, alleen in de Data Pro Code dient het protocol opgenomen te worden. Een verdere inhoudelijke vergelijking over de afhandeling van datalekken staat verderop in dit document.
- **Toegang medewerkers**: In Bijlage A van de SURF verwerkersovereenkomst staat opgenomen welke medewerkers van verwerker toegang hebben tot de persoonsgegevens en welke acties zij kunnen uitvoeren. Dit is in het Data Pro Statement niet opgenomen.

2.3 Vergelijking invulling auditverplichting

- **Auditverplichting verwerker**: Bij de SURF verwerkersovereenkomst heeft de verwerker een verplichting om periodiek (één of twee jaarlijks, afhankelijk van de risicoklasse) een onafhankelijke, externe deskundige een audit te laten uitvoeren. Er is alleen geen verplichting bij een laag risico. De bevindingen van de audit moet de verwerker op verzoek aan de verwerkingsverantwoordelijke ter beschikking stellen. Bij de Data Pro verwerkersovereenkomst heeft de data processor geen periodieke auditverplichting. Wel kan de data processor er zelf voor kiezen om middels het Data Pro Certificaat of een daaraan ten minste gelijkwaardig certificaat of auditrapport van een onafhankelijke derde partij aan te tonen dat hij voldoet aan zijn verplichtingen op grond van de verwerkersovereenkomst: *"Data Processor kan desgewenst[8] de naleving van zijn verplichtingen op grond van de verwerkersovereenkomst aantonen door middel van een geldig Data Pro Certificaat of een daaraan ten minste gelijkwaardig certificaat of auditrapport (Third Party Memorandum) van een onafhankelijke, deskundige, indien hij over een dergelijk certificaat of auditrapport beschikt."*
- **Audit op verzoek van verwerkingsverantwoordelijke**: In beide overeenkomsten is een audit op verzoek van de verwerkingsverantwoordelijke/opdrachtgever mogelijk. Er zijn vier belangrijke verschillen:
  - In de Data Pro Code is opgenomen dat het maximaal één keer per jaar mag. In de SURF verwerkersovereenkomst staat dat een audit op verzoek maximaal één keer per jaar mag, en vaker bij een concreet vermoeden dat de verwerker de verwerkersovereenkomst, AVG of andere toepasselijke wet- en regelgeving niet nakomt.

8 Er wordt hier vanuit gegaan dat met 'desgewenst' wordt bedoeld: 'indien gewenst door de verwerker'.

- De audit ingevolge de Data Pro Code ziet enkel op naleving van de verwerkersovereenkomst. De audit uit de SURF verwerkersovereenkomst ziet op naleving van de verwerkersovereenkomst, de AVG en andere toepasselijke wet- en regelgeving.
- In de Data Pro Code staat dat de derde partij aan geheimhouding moet zijn gebonden. Dat staat niet in de SURF verwerkersovereenkomst.
- In de SURF verwerkersovereenkomst is opgenomen dat verwerkingsverantwoordelijke de verwerker ten minste 14 dagen voor aanvang van de audit schriftelijk in kennis moet stellen. In de Data Pro Code is geen minimumtermijn opgenomen.

- **Acties n.a.v. bevindingen**: Beide overeenkomsten stellen dat de verwerker actie moet ondernemen als blijkt dat er niet (volledig) wordt voldaan aan de afspraken. In de Data Pro Code staat dat er enkel actie ondernomen hoeft te worden, als dat naar het oordeel van de data processor passend is. SURF verwerkersovereenkomst: *"Indien tijdens een audit wordt vastgesteld dat Verwerker niet aan het bepaalde in de Verwerkersovereenkomst en/of de AVG en/of andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet, neemt Verwerker onverwijld alle redelijkerwijs noodzakelijke maatregelen om te zorgen dat Verwerker hieraan alsnog voldoet."* Data Pro verwerkersovereenkomst: *"Partijen zullen zo snel mogelijk in overleg treden over de uitkomsten in het rapport. Partijen zullen de voorgestelde verbetermaatregelen die in het rapport zijn neergelegd opvolgen voor zover dat van hen in redelijkheid kan worden verwacht. Data Processor zal de voorgestelde verbetermaatregelen doorvoeren voor zover deze naar zijn oordeel passend zijn rekening houdend met de verwerkingsrisico's verbonden aan zijn product of dienst, de stand van de techniek, de uitvoeringskosten, de markt waarin hij opereert, en het beoogd gebruik van het product of de dienst."*
- **Kosten van de audit**: Bij de SURF verwerkersovereenkomst zijn de kosten voor de periodieke audit en voor het nemen van maatregelen n.a.v. de bevindingen voor rekening van de verwerker. De kosten voor een audit op verzoek van de verwerkingsverantwoordelijke zijn voor rekening van de verwerkingsverantwoordelijke, tenzij blijkt dat de verwerker afspraken niet is nagekomen. In de Data Pro verwerkersovereenkomst is dit anders geregeld. De data processor kan alle kosten verhalen op de verwerkingsverantwoordelijke: *"Data Processor heeft het recht om de kosten die hij maakt in het kader van het in dit artikel gestelde in rekening te brengen bij Opdrachtgever."*

2.4 Vergelijking beveiliging en risicoclassificering

- **Bijzondere persoonsgegevens**: In de SURF verwerkersovereenkomst geldt bij verwerking van bijzondere persoonsgegevens een jaarlijkse auditverplichting (risico hoog). In Bijlage A wordt vastgelegd of er bijzondere persoonsgegevens worden verwerkt en wat de auditfrequentie is. In de Data Pro overeenkomst is het uitgangspunt dat het product of de dienst niet is ingericht op de verwerking van bijzondere categorieën van Persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten of door de overheid uitgegeven persoonsnummers, tenzij in het Data Pro Statement expliciet anders is vermeld.
- **Technische & Organisatorische maatregelen**: In de Data Pro Code is openomen dat verwerker ernaar zal streven dat de genomen maatregelen passend zijn voor het door hem beoogde gebruik van de dienst, maar dat hij niet garandeert dat de maatregelen onder alle omstandigheden doeltreffend zijn. Bovendien is hier opgenomen dat het de verantwoordelijkheid van de opdrachtgever is om te bepalen of de door data processor opgenomen maatregelen toereikend zijn: *"Data Processor geeft uitvoering aan de AVG zoals neergelegd in deze Standaardclausules voor verwerkingen, het Data Pro Statement en de Overeenkomst. Het is aan Opdrachtgever om op basis van deze informatie te beoordelen of Data Processor afdoende garanties biedt met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van Data subjects voldoende zijn gewaarborgd"*, en *"De omschreven beveiligingsmaatregelen bieden, naar het oordeel van de Opdrachtgever, rekening houdend met de in artikel 3.1 genoemde factoren een op het risico van de verwerking van de door hem gebruikte of verstrekte Persoonsgegevens afgestemd*

beveiligingsniveau." In de SURF verwerkersovereenkomst is gekozen voor een andere aanpak: daarin staat dat de verwerker passende T&O-maatregelen zal treffen die een passend beveiligingsniveau waarborgen.

2.5 Vergelijking boetes en aansprakelijkheden

- In de Data Pro verwerkersovereenkomst staat het volgende: *"Een aan Opdrachtgever door de AP opgelegde bestuurlijke boete kan niet worden verhaald op Data Processor, tenzij er sprake is van opzet of bewuste roekeloosheid aan de zijde van de bedrijfsleiding van Data Processor."* En: *"Alle rechten en verplichtingen uit de Overeenkomst, waaronder begrepen de van toepassing zijnde algemene voorwaarden en/of beperkingen van aansprakelijkheid, zijn derhalve ook van toepassing op de verwerkersovereenkomst."*
- In de SURF verwerkersovereenkomst staat het volgende: *"Een Partij kan geen beroep doen op een aansprakelijkheidsbeperking, die is opgenomen in de Overeenkomst of andere tussen Partijen bestaande overeenkomst of regeling, ten aanzien van een door de andere Partij ingestelde: a. verhaalsactie op grond van artikel 82 AVG; of b. schadevergoedingsactie uit hoofde van de Verwerkersovereenkomst, indien en voor zover de actie bestaat uit verhaal van een aan de Toezichthoudende autoriteit betaalde geldboete die geheel of gedeeltelijk toerekenbaar is aan de andere Partij. Het bepaalde in dit artikel laat onverlet de rechtsmiddelen die de aangesproken Partij op grond van de geldende wet- of regelgeving ter beschikking staat."* En: *"Iedere Partij is verplicht de andere Partij zonder onnodige vertraging op de hoogte te stellen van een (mogelijke) aansprakelijkstelling of het (mogelijk) opleggen van een boete door de Toezichthoudende autoriteit, beiden in verband met de Verwerkersovereenkomst. Iedere Partij is in redelijkheid verplicht de andere Partij informatie te verstrekken en/of ondersteuning te verlenen ten behoeve van het voeren van verweer tegen een (mogelijke) aansprakelijkstelling of boete, zoals bedoeld in de vorige volzin. De Partij die informatie verstrekt en/of ondersteuning verleent, is gerechtigd om eventuele redelijke kosten dienaangaande in rekening te brengen bij de andere Partij, Partijen informeren elkaar zo veel mogelijk vooraf over deze kosten."*

2.6 Vergelijking afspraken bij inbreuk i.v.m. persoonsgegevens (datalek)

- **Informeren over datalek**: In de SURF verwerkersovereenkomst staat dat de verwerker de verwerkingsverantwoordelijke informeert zonder onredelijke vertraging en uiterlijk binnen 24 uur na kennisneming. De contactpersoon om te melden is opgenomen in Bijlage A. In de Data Pro Statement staat dat de data processor bij een datalek de opdrachtgever zonder onredelijke vertraging moet informeren. Er wordt geen termijn genoemd.
- **Melding aan AP/betrokkenen**: In beide overeenkomsten staat dat het in principe aan de verwerkingsverantwoordelijke is om een eventuele melding te doen.
- **Bijhouden register**: In de SURF verwerkersovereenkomst is opgenomen dat verwerker een register moet bijhouden van alle datalekken en dat de verwerkingsverantwoordelijke op verzoek een afschrift moet kunnen ontvangen. In de Data Pro verwerkersovereenkomst staat deze verplichting niet benoemd.
- **Datalekprotocol**: Zoals eerder beschreven wordt in het Data Pro Statement opgenomen wat het datalekkenprotocol van de data processor is. De SURF verwerkersovereenkomst kent deze verplichting niet.
- **Kosten**: In de Data Pro verwerkersovereenkomst staat dat data processor de redelijke kosten die in het kader van datalekken worden gemaakt, in rekening kan brengen bij de opdrachtgever tegen zijn geldende tarieven. Het gaat hier om kosten die worden gemaakt in het kader van een bij data processor ontdekt datalek. In de SURF verwerkersovereenkomst is niets opgenomen over eventuele kosten.

2.7 Vergelijking afspraken met subverwerkers

- **Toestemming voor subverwerkers**: In de Data Pro verwerkersovereenkomst wordt standaard uitgegaan van algemene toestemming voor de inzet van subverwerkers. In het Data Pro

Statement staat vermeld om welke subverwerkers het gaat. In de SURF verwerkersovereenkomst is slechts sprake van algemene toestemming als dit expliciet is opgenomen in Bijlage A. In bijlage A staan de subverwerkers opgenomen die zijn ingeschakeld en waar specifieke toestemming voor is.

- **Afspraken met subverwerkers**: In de SURF verwerkersovereenkomst staat dat verwerker de verplichtingen uit de verwerkersovereenkomst doorzet naar subverwerkers. In de Data Pro Code staat enkel dat subverwerkers hetzelfde beveiligingsniveau moeten leveren als de data processor. In de SURF verwerkersovereenkomst staat daarnaast dat verwerker verantwoordelijk blijft voor het nakomen van verplichtingen door subverwerkers. Dit staat niet in Data Pro Code.
- **Wijzigen subverwerker**: In de Data Pro verwerkersovereenkomst staat dat opdrachtgever wordt geïnformeerd over een wijziging in ingeschakelde derde partijen en dat opdrachtgever het recht heeft om bezwaar te maken. Er staat niet bij binnen welke termijn er geïnformeerd moet worden, of wat het gevolg is van bezwaar maken. Wel staat er in een andere bepaling het volgende (wellicht relevant omdat de subverwerkers in het statement staan opgenomen): *"Het Data Pro Statement, en met name de daarin opgenomen beveiligingsmaatregelen, kan van tijd tot tijd door Data Processor worden aangepast aan veranderende omstandigheden. Data Processor zal Opdrachtgever van significante aanpassingen op de hoogte stellen. Indien Opdrachtgever in redelijkheid niet akkoord kan gaan met de aanpassingen, is Opdrachtgever gerechtigd binnen 30 dagen na kennisgeving van de aanpassingen de verwerkersovereenkomst schriftelijk gemotiveerd op te zeggen."* Er wordt in het midden gelaten of wijziging van een subverwerker een 'significante aanpassing' is. In de SURF verwerkersovereenkomst staat dat, in geval van algemene toestemming, de verwerker de verwerkingsverantwoordelijke informeert uiterlijk binnen 3 maanden voorafgaand aan de wijziging. Bezwaar is mogelijk binnen 1 maand, partijen treden hierop in onderhandeling.
- **Verwerking buiten de EER**: In de Data Pro Statement kan worden aangeven of persoonsgegevens buiten de EER worden verwerkt en zo ja, op welke manier is geborgd dat een passend beschermingsniveau van toepassing is. Uitgangspunt is dat verwerking buiten de EER is toegestaan. In de SURF verwerkersovereenkomst is opgenomen dat doorgifte van persoonsgegevens buiten de EER pas is toegestaan als verwerkingsverantwoordelijke daar expliciete toestemming voor heeft verleend in Bijlage A. Tevens staat in de SURF verwerkersovereenkomst het volgende: *"De doorgiften van Persoonsgegevens buiten de Europese Economische Ruimte of aan internationale organisaties ter uitvoering van de Overeenkomst, zijn nader omschreven in Bijlage A. Verwerker is uitsluitend gerechtigd tot deze in Bijlage A gespecificeerde doorgiften aan derde landen of internationale organisaties, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt."* In de Data Pro Code staat een dergelijke bepaling niet.

2.8 Vergelijking overige punten

- **Kosten**: Aanvullend op de eerder in het document genoemde kosten, is in de Data Pro verwerkersovereenkomst opgenomen dat de kosten voor een DPIA en verzoeken van betrokkenen voor rekening van de opdrachtgever komen. Ook kosten voor het verwijderen of overdragen van persoonsgegevens kunnen na het einde van de overeenkomst in rekening worden gebracht bij opdrachtgever. Nadere afspraken kunnen worden gemaakt in het Data Pro Statement. In de SURF verwerkersovereenkomst is niets opgenomen over de kosten van een DPIA en verzoeken van betrokkenen. Wel is hier over het verwijderen of overdragen van persoonsgegevens opgenomen dat die kosten in principe voor rekening van de verwerker komen. Wanneer verwerkingsverantwoordelijke extra eisen stelt aan bijvoorbeeld het bestandsformaat, overleggen partijen over de verdeling van de extra kosten.

- **Geheimhouding**: Beide overeenkomsten kennen een artikel over geheimhouding/vertrouwelijkheid. De Data Pro Code kent een extra bepaling die de SURF verwerkersovereenkomst niet kent: *"Alle door Data Processor aan Opdrachtgever verstrekte toegangs- en/of identificatiecodes, certificaten, informatie omtrent toegangs- en/of wachtwoordenbeleid en alle door Data Processor aan Opdrachtgever verstrekte informatie die invulling geeft aan de in het Data Pro Statement opgenomen technische en organisatorische beveiligingsmaatregelen zijn vertrouwelijk en zullen door Opdrachtgever als zodanig worden behandeld en slechts aan geautoriseerde medewerkers van Opdrachtgever kenbaar worden gemaakt. Opdrachtgever ziet erop toe dat zijn medewerkers de verplichtingen uit dit artikel naleven."*
- **Opsporingsverzoeken**: De SURF verwerkersovereenkomst kent een uitgebreide bepaling over opsporingsverzoeken. De Data Pro verwerkersovereenkomst is beperkt op dit punt en kent enkel de volgende bepaling: *"Data Processor is gerechtigd de Persoonsgegevens te verstrekken aan derden, indien en voor zover verstrekking noodzakelijk is ingevolge een rechterlijke uitspraak, een wettelijk voorschrift of op basis van een bevoegd gegeven bevel van een overheidsinstantie."*
- **Wijziging overeenkomst**:
  - Data Pro verwerkersovereenkomst: *"Het Data Pro Statement, en met name de daarin opgenomen beveiligingsmaatregelen, kan van tijd tot tijd door Data Processor worden aangepast aan veranderende omstandigheden. Data Processor zal Opdrachtgever van significante aanpassingen op de hoogte stellen. Indien Opdrachtgever in redelijkheid niet akkoord kan gaan met de aanpassingen, is Opdrachtgever gerechtigd binnen 30 dagen na kennisgeving van de aanpassingen de verwerkersovereenkomst schriftelijk gemotiveerd op te zeggen."* Er staat niet in wat de gevolgen voor de hoofdovereenkomst zijn.
  - SURF verwerkersovereenkomst: *"Verwerker is verplicht Verwerkingsverantwoordelijke onmiddellijk te informeren over voorgenomen wijzigingen in de Dienst, de uitvoering van de Overeenkomst en de uitvoering van de Verwerkersovereenkomst die betrekking hebben op de Verwerking van Persoonsgegevens en die (mogelijk) een wijziging van de Verwerkersovereenkomst en/of de Bijlagen vereisen. Hieronder wordt in ieder geval verstaan: Wijzigingen die invloed (kunnen) hebben op de te verwerken (categorieën) Persoonsgegevens; Wijziging van de middelen waarmee de Persoonsgegevens worden verwerkt; Het inschakelen van andere Sub-verwerkers; Wijziging in de doorgifte van Persoonsgegevens."*
    En: *"Verwerker is pas gerechtigd tot het uitvoeren van een wijziging in de Dienst, een wijziging in de uitvoering van de Overeenkomst, een wijziging in de uitvoering van de Verwerkersovereenkomst en/of een wijziging die aanpassing van Bijlage A of Bijlage B tot gevolg heeft, indien Verwerkingsverantwoordelijke daaraan voorafgaand Schriftelijk toestemming voor deze wijziging(en) heeft gegeven. Onder een wijziging in de Dienst wordt verstaan een substantiële wijziging die gevolgen kan hebben voor de Verwerking van Persoonsgegevens. Verwerker kan in afwijking van voorgaande zonder voorafgaande Schriftelijke toestemming van Verwerkingsverantwoordelijke direct noodzakelijke verbeteringen uitvoeren, bijvoorbeeld met betrekking tot adequate beveiliging van de dienst. Verwerker zal Verwerkingsverantwoordelijke zo spoedig mogelijk informeren over de wijziging."*
    De looptijd van de SURF verwerkersovereenkomst is gelijk aan de looptijd van de hoofdovereenkomst, en kan niet los worden beëindigd.
- De SURF verwerkersovereenkomst kent een aantal verplichtingen voor de verwerker die de Data Pro Code niet kent:
  - *"Verwerker brengt Verwerkingsverantwoordelijke onverwijld op de hoogte indien Verwerker reden heeft om aan te nemen dat Verwerker niet langer aan de Verwerkersovereenkomst kan voldoen."*
  - *"Verwerker en Verwerkingsverantwoordelijke leven de AVG en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens na. Verwerker stelt de Verwerkingsverantwoordelijke onmiddellijk in kennis indien naar mening van Verwerker*

een instructie van Verwerkingsverantwoordelijke inbreuk oplevert op de AVG en/of andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens."

- *"Indien Verwerker in strijd met de Verwerkersovereenkomst en/of de AVG en/of andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens het doel en de middelen van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker voor die Verwerkingen als Verwerkingsverantwoordelijke beschouwd."*
- *"Indien Verwerker de Dienst rechtstreeks aanbiedt aan Betrokkene, is Verwerker verplicht om Betrokkene namens de Verwerkingsverantwoordelijke te informeren over de Verwerking van de Persoonsgegevens van Betrokkene op een wijze die in overeenstemming is met de rechten van Betrokkene."*