SURF JURIDISCH NORMEN-KADER (CLOUD)SERVICES

Mr. Tatjana Landzaat
Mr. Olga Scholcz
SURF Cloud Event, 11 oktober 2018

JURIDISCHE COMMISSIE SURF

- Tegelijk met vaststellen JNK in 2014, introductie Juridische Commissie (“JC”);
- Komt 4 keer per jaar bijeen;
- JC adviseert de Directieraad van SURF over inhoud en toepassing JNK;
- Maar ook over: aanpassing en aansluiting van JNK bij ontwikkelingen op gebied wet- en regelgeving;
- Directieraad besluit over eventuele aanpassingen;
- Directieraad legt verantwoording af aan de Ledenraad.

JURIDISCHE COMMISSIE & SURF MODEL VERWERKERSOVEREENKOMST

- SURF model verwerkersovereenkomst wordt jaarlijks geëvalueerd in de JC;

- SURF verwerkersovereenkomst voor “eigen” SURF dienstverlening; dichtbij de SURF model verwerkersovereenkomst gebleven en voor de verschillende werkmaatschappijen bijna identiek. Deze wordt binnenkort verstuurd aan de instellingen.

SURF Juridisch Normenkader (Cloud)services (JNK)

SURFmarket Cloudcontracten

Doel: rechtmatige inkoop waarbij het JNK wordt meegenomen, onder andere door middel van de SURF model verwerkers-overeenkomst.

COMPLIANCE STATEMENTS

- Model Compliance Statements (NL/EN);
- Gebaseerd op de SURF model verwerkersovereenkomst;
- Te vinden (indien gemaakt) bij de betreffende overeenkomst op de leverancier informatie pagina;

Voorbeelden Compliance Statements

ARTIKEL	MODEL VERWERKERSOVEREENKOMST	ARTIKEL LETTERLIJK OVERGENOMEN?	OPMERKINGEN / AFWIJKINGEN MODEL VERWERKERSOVEREENKOMST
	maar niet beperkt tot Medewerkers en/of Sub-verwerkers. Verwerker draagt er zorg voor dat de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, de in de Verwerkersovereenkomst opgenomen verplichtingen naleven door middel van een Schriftelijke overeenkomst.		
5.8	Verwerker brengt Verwerkingsverantwoordelijke onverwijld op de hoogte indien Verwerker en/of door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, in strijd handelen met de Verwerkersovereenkomst en/of de met Verwerker gesloten Schriftelijke overeenkomst zoals bedoeld in artikel 5.7.	JA	
5.9	Verwerker verstrekt op verzoek van Verwerkingsverantwoordelijke een afschrift van de Schriftelijke overeenkomst tussen Verwerker en de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers.	NEE	Deze bepaling is als volgt aangevuld: “Verwerker verstrekt op verzoek van Verwerkingsverantwoordelijke een afschrift van relevante delen van de Schriftelijke overeenkomst tussen Verwerker en de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers.”
5.10	Verwerker blijft ten aanzien van de Verwerkingsverantwoordelijke volledig verantwoordelijk en volledig aansprakelijk	NEE	Deze bepaling is als volgt aangepast: “Verwerker blijft ten aanzien van de Verwerkingsverantwoordelijke volledig

Voorbeelden Compliance Statements

CLAUSE	MODEL PROCESSOR AGREEMENT	ARTIKEL LETTERLIJK OVERGENOMEN?	OPMERKINGEN / AFWIJKINGEN MODEL PROCESSOR AGREEMENT
	Processor to simultaneously provide all of the information from Annex C, the information may be provided to the Controller step-by-step without unreasonable delay and no later than within 24 hours after the discovery.		'Notwithstanding the provisions of Clause 8.1, if and in so far as it is not possible for the Processor to simultaneously provide all of the information from Annex C, the information may be provided to the Controller step-by-step.'
8.3	The Processor has organised adequate policy and adequate procedures to detect Personal Data Breaches at the earliest possible stage, to notify the Controller of this no later than within 24 hours, to adequately and immediately respond to this, to prevent or limit (further) unauthorised disclosure, alteration and provision or otherwise unlawful Processing, and to prevent repetition of the same. At the Controller's request, the Processor shall provide information about and allow inspection of this policy organised by the Processor and these procedures organised by the Processor.	NEE	Deze bepaling is vervangen door: 'The Processor has organised adequate policy and adequate procedures to detect Personal Data Breaches at the earliest possible stage, to notify the Controller of this in accordance with Clause 8.1, to adequately and immediately respond to this, to use best endeavours to prevent or limit (further) unauthorised disclosure, alteration and provision or otherwise unlawful Processing, and to use best endeavours to prevent repetition of the same. At the Controller's request, the Processor shall provide evidence of this policy and procedures.'
8.4	The Processor shall maintain a register In Writing of all Personal Data Breaches that relate to or are connected with the (performance of the) Agreement, including the facts regarding the Personal Data Breach, its consequences and the corrective measures taken. At the Controller's request, the Processor shall provide the Controller with a copy of this register.	NEE	Deze bepaling is zodanig aangepast dat leverancier niet een kopie van het gehele register hoeft te overleggen, maar alleen de voor verwerkingsverantwoordelijke relevante informatie.
9.	**TRANSFER OF PERSONAL DATA**		
9.1	Personal Data may be transferred to third	NEE	Deze bepaling is vervangen door de volgende

Doel JNK: stevige basis voor contracten met (cloud)leveranciers, goede privacy waarborgen

Notitie JNK

Standaard bepalingen

Bijlage A

Standaard bepalingen

Bijlage B

Instructie

Bijlage C

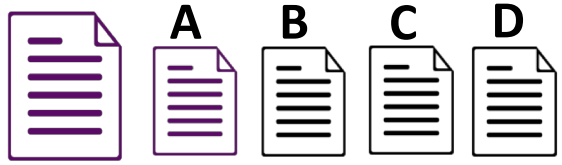
Instructie

Bijlage D

Instructie

SURF JNK modelverwerkersovereenkomst

JNK



Notitie JNK

Op te nemen in de hoofdovereenkomst

(losse) overeenkomst horend bij hoofdovereenkomst

Bijlage A: Model verwerkersovereenkomst

Standaard bepalingen omtrent:

- Intellectueel eigendom
- Vertrouwelijkheid
- Beschikbaarheid
- Privacy

Standaard bepalingen omtrent:

- Verwerking persoonsgegevens

SURF JNK model verwerkersovereenkomst

Overeenkomst:

- Omgang met persoonsgegevens
- Inzet van hulpleveranciers
- Verlenen van bijstand en medewerking
- Meldplicht inbreuk ivm Persoonsgegevens (hierna genoemd: datalek)
- Beveiliging
- Audit
- Internationaal verkeer
- Opsporingsverzoeken
- Informeren van betrokkenen
- Vrijwaring
- Dataportabiliteit

Bijlage A

Specificatie verwerking, beveiliging etc.

Deze bijlage dient door verwerker en verwerkingsverantwoordelijke gezamenlijk te worden ingevuld en zo nodig te worden geactualiseerd

Bijlage B

Beveiligingsmaatregelen

Bijlage C

Informatieverplichting bij een inbreuk in verband met persoonsgegevens (datalek)

SURF JNK: normen verwerkersovereenkomst (1)

Omgang met persoonsgegevens

1. Enkel verwerken in opdracht op instructie van verwerkingsverantwoordelijke
2. Niet verwerken voor eigen of andere doeleinden
3. Enkel Persoonsgegevens verwerken voor zover noodzakelijk
4. Persoonsgegevens niet langer bewaren dan noodzakelijk

Inzet van Hulpleveranciers

1. Enkel inschakelen Hulpleveranciers met toestemming van verwerkingsverantwoordelijke
2. Zelfde afspraken maken met Hulpleveranciers over verwerking persoonsgegevens
3. Inzicht in afspraken met hulpleveranciers

SURF JNK: normen verwerkersovereenkomst (2)

Bijstand en medewerking

1. Beveiliging van persoonsgegevens
2. Uitvoeren van controles en audits
3. Uitvoeren van PIA’s
4. Voorafgaande raadpleging Toezichthoudende autoriteit
5. Voldoen aan verzoeken van de Toezichthoudende autoriteit
6. Voldoen aan verzoeken van Betrokkenen
7. Melden van Inbreuken in verband met Persoonsgegevens

SURF JNK: normen verwerkersovereenkomst (3)

Beveiliging

1. Passende technische en organisatorische maatregelen
2. Maatregelen ter voorkoming van onrechtmatige verwerking en verlies
3. Maatregelen ter voorkoming van onnodige verzameling
4. Schriftelijk vastleggen van maatregelen
5. Toepasselijke maatregelen opnemen in bijlage verwerkersovereenkomst
6. Op verzoek informatie verstrekken over beveiliging aan verwerkingsverantwoordelijke

SURF JNK: normen verwerkersovereenkomst (4)

Meldplicht datalekken

1. Mogelijke datalekken binnen 24 uur kunnen melden aan verwerkingsverantwoordelijke: AVG: binnen 72 uur.
2. Hulpleveranciers onverwijld mogelijke datalekken laten melden
3. Maatregelen kunnen treffen bij een datalek
4. Op verzoek meewerken aan informeren toezichthouder en betrokkenen
5. Register bijhouden

Wanneer moet een datalek worden gemeld?

Aan de Toezichthoudende Autoriteit:
Als het leidt tot risico's voor de rechten en vrijheden van betrokkenen. Zie Guidelines van Werkgroep 29:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf

U hoeft de betrokkenen (de personen van wie u gegevens verwerkt) alleen te informeren als een datalek waarschijnlijk een hoog risico voor hun rechten en vrijheden oplevert.
Hiervoor moet u onder andere kijken of het datalek kan leiden tot fysieke, materiële of immateriële schade voor de betrokkenen. Zoals: discriminatie, (identiteits-)fraude, financiële schade en reputatieschade (bron: autoriteit persoonsgegevens)

SURF JNK: normen verwerkersovereenkomst (5)

Audit

1. Stel de risicoklasse van de te verwerken persoonsgegevens vast
2. Doe een periodiek onderzoek naar de bescherming van persoonsgegevens
3. Stel de audit in de vorm van een TPM ter beschikking
4. Verzorg maandelijks een rapportage over beveiligingsbeheer
5. Neem indien nodig maatregelen n.a.v. de audit

Internationaal verkeer

1. Verwerk in principe geen persoonsgegevens buiten de EER
2. Verwerk alleen persoonsgegevens buiten de EER met toestemming verwerkingsverantwoordelijke
3. Zorg voor voldoende waarborgen om zorgvuldige verwerking te garanderen
4. Laat indien nodig de gegevens encrypted versturen

SURF JNK: normen verwerkersovereenkomst (6)

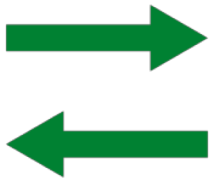
Opsporingsverzoeken

1. Informeer verwerkingsverantwoordelijke bij een opsporingsverzoek
2. Handel het verzoek af op instructie van verwerkingsverantwoordelijke
3. Behartig de belangen van de verwerkingsverantwoordelijke bij niet mogen informeren

Informeren betrokkenen

1. Verleen medewerking aan verwerkingsverantwoordelijke bij uitoefening rechten door betrokkene
2. Stuur verzoeken van betrokkenen door naar verwerkingsverantwoordelijke
3. Handel bij verzoeken naar instructie van de verwerkingsverantwoordelijke
4. Publiceer bij aanbieden van een eindgebruikersdienst op verzoek een privacy policy

SURF JNK: normen verwerkersovereenkomst (7)



Dataportabiliteit

1. Op verzoek data overdragen aan verwerkingsverantwoordelijke
2. Op verzoek van verwerkingsverantwoordelijke data vernietigen
3. Op verzoek aan betrokkene (in gestructureerd, gangbare en machine leesbare vorm) en op diens verzoek aan andere verwerkingsverantwoordelijke

Specificatie verwerkingen

1. Beschrijf de (categorieën) betrokkenen
2. Beschrijf de (categorieën) persoonsgegevens
3. Beschrijf de groepen medewerkers en hun rechten
4. Beschrijf de risicoklasse van de persoonsgegevens
5. Specificeer de bewaartermijnen
6. Beschrijf de beveiligingsmaatregelen
7. Benoem de hulpleveranciers

Link naar documentatie JNK

- https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html

Samen aanjagen van vernieuwing