High-level vergelijking verwerkersovereenkomst Framework ibp in het mbo en SURF

Inleiding
Dit document biedt een high-level vergelijking tussen de Generiek model Verwerkersovereenkomst 3.0 Framework ibp in het mbo uit maart 2018 (hierna: Framework ibp-model) en de SURF Model Verwerkersovereenkomst uit oktober 2017 (hierna: SURF-model).

Vergelijking per onderwerp

- **Beveiliging**

Artikelen SURF-model	**Artikelen Framework ibp-model**
Artikel 6, Bijlage B	Artikel 6, Bijlage 2

Algemeen
In beide modellen kunnen partijen de beveiligingsmaatregelen die verwerker dient te treffen (verder) uitwerken in de bijlagen. In het Framework ibp-model wordt specifiek verwezen naar het 'Certificeringsschema informatiebeveiliging en privacy ROSA' om aan te tonen dat voldaan is aan de beveiligingseisen. Daarnaast is in het Framework ibo-model standaard al een lijst opgenomen met maatregelen die de verwerker minimaal dient te treffen.

Toelichting
In beide modellen staat dat verwerker passende technische en organisatorische maatregelen moet treffen in overeenstemming met de AVG. Deze maatregelen kunnen in beide modellen in de bijlagen worden uitgewerkt. In het Framework ibp-model is al een lijst met beveiligingsmaatregelen opgenomen die de verwerker minimaal dient te treffen. In het SURF-model staat geen lijst met beveiligingsmaatregelen. Het is aan partijen zelf om dit in de bijlage te specificeren. Bovendien wordt in het ibp-model specifiek verwezen naar het 'Certificeringsschema informatiebeveiliging en privacy ROSA', als mogelijkheid om aan te tonen dat de verwerker voldoet aan de technische maatregelen.

- **Aansprakelijkheid**

Artikelen SURF-model	**Artikelen Framework ibp-model**
Artikel 11	Artikel 12

Algemeen
In het Framework ibp-model wordt grotendeels aangesloten bij de aansprakelijkheidsbepaling zoals overeengekomen tussen partijen in de hoofdovereenkomst. Bij het SURF-model wordt niet aangesloten bij de hoofdovereenkomst, maar is een nieuwe bepaling opgenomen.

Toelichting
In het Framework ibp-model wordt in principe aangesloten bij de aansprakelijkheidsbepaling uit de hoofdovereenkomst, met enkele beperkingen. Een eventuele beperking in de hoofdovereenkomst ten aanzien van aansprakelijkheid voor schade door een geldboete van een toezichthouder of een verhaalsactie op grond van artikel 82, is niet geldig.

In het SURF-model wordt niet aangesloten bij het aansprakelijkheidsartikel uit de hoofdovereenkomst. In het SURF-model staat dat de verwerker volledig aansprakelijk is voor tekortkomingen en geeft hij een vrijwaring aan de instelling.

- **Datalek**

Artikelen SURF-model	**Artikelen Framework ibp-model**
Artikel 8	Artikel 7

Algemeen
In het Framework ibp-model is meer geregeld omtrent beveiligingsincidenten. Er staat echter geen concrete termijn in waarbinnen de verwerker een datalek dient te melden aan de instelling. Dit staat wel in het SURF-model.

Toelichting
In het SURF-model staat een termijn van 24 uur vermeld waarbinnen verwerkers een datalek dienen te melden aan de instelling. In het Framework ibp-model staat geen termijn waarbinnen de verwerker het datalek dient te melden aan de instelling. Er staat alleen dat dit *onverwijld* dient te gebeuren. Daarnaast staat in het Framework ibp-model dat de instelling ook een melding aan de verwerker zal maken in geval van een datalek bij de instelling zelf. Dit staat niet in het SURF-model.

- **Inschakelen sub-verwerkers**

Artikelen SURF-model	**Artikelen Framework ibp-model**
Artikel 5	Artikel 10

Algemeen
In het Framework ibp-model is een algemene toestemming opgenomen voor het inschakelen van sub-verwerkers, in het SURF-model is het aan de instelling om te kiezen tussen algemene of specifieke toestemming.

Toelichting
In het Framework ibp-model is een algemene toestemming opgenomen voor verwerkers voor het inschakelen van sub-verwerkers, met de mogelijkheid voor de instelling om bezwaar te maken. In het SURF-model kan de instelling in de bijlage kiezen voor algemene of specifieke toestemming. Als er voor algemene toestemming wordt gekozen, stelt het SURF-model strengere eisen aan deze toestemming. Het voordeel van specifieke toestemming is dat je als instelling meer controle houdt op de sub-verwerkers die worden ingeschakeld. Het levert echter wel meer werk op voor de verwerkingsverantwoordelijke.

- **Verzoeken van toezichthoudende autoriteit**

Artikelen SURF-model	**Artikelen Framework ibp-model**
Artikel 4.3	Artikel 5.3

Algemeen
In het SURF-model is meer geregeld over hoe de verwerker dient te handelen in geval van een verzoek van een toezichthoudende autoriteit.

- **Toegang tot persoonsgegevens**

Artikelen SURF-model	**Artikelen Framework ibp-model**
Artikel 5, Bijlage A	Artikel 5.4 en artikel 6.2

Algemeen
Voor toegang tot persoonsgegevens is in het SURF-model meer geregeld. Zo moeten bijvoorbeeld de categorieën medewerkers die toegang krijgen tot de gegevens, worden gespecificeerd in de bijlage.

- **Vertrouwelijkheid**

Artikelen SURF-model	**Artikelen Framework ibp-model**
Artikel 10	Artikel 5

Algemeen
De bepaling in het SURF-model omtrent vertrouwelijkheid is wederzijds opgesteld, terwijl de bepaling uit het Framework ibp-model alleen voor de verwerker geldt.

- **Einde overeenkomst**

Artikelen SURF-model	**Artikelen Framework ibp-model**
Artikel 13	Artikel 11

Algemeen
Uit het SURF-model volgt dat de verwerker na afloop van de overeenkomst de gegevens dient te vernietigen, te retourneren dan wel naar een andere partij dient te sturen, al naar gelang de keuze van de instelling. In het Framework ibp-model staat enkel dat de verwerker de gegevens zal vernietigen of bewaren na afloop van de overeenkomst.

- **Doorgifte van persoonsgegevens**

Artikelen SURF-model	**Artikelen Framework ibp-model**
Artikel 9	Artikel 9

Algemeen
Beide modellen bieden dezelfde bescherming voor internationale doorgifte van persoonsgegevens.

Toelichting
Volgens beide modellen mag de verwerker alleen persoonsgegevens doorgeven naar internationale organisaties, als hier specifieke Schriftelijke toestemming voor is verleend door de instelling. Het SURF-model specificeert de mogelijkheden voor doorgifte naar landen buiten de EER (de drie doorgeefmechanismen uit de AVG). Het Framework ibp-model stelt in het algemeen dat doorgifte alleen mag gebeuren als aan ‘alle wettelijke voorschriften’ voor doorgifte is voldaan. Feitelijk worden in beide modellen dezelfde eisen gesteld aan doorgifte. Deze zijn in het SURF-model alleen gespecificeerd.

- **Audit**

Artikelen SURF-model	Artikelen Framework ibp-model
Artikel 7, Bijlage B	Artikel 6, Bijlage 2

Algemeen
Het SURF-model stelt de verwerker verplicht om periodiek en op eigen kosten een externe audit te laten verrichten en een TPM-verklaring te overleggen, *tenzij* er volgens de verwerkingsverantwoordelijke sprake is van een verwerking met risiconiveau 'Laag'. In het ibp-model staat enkel dat verwerker periodiek verklaart te voldoen aan passende technische maatregelen voor de beveiliging van de Verwerking van de Persoonsgegevens.

Toelichting
In beide modellen is opgenomen dat de instelling op eigen initiatief een audit mag laten verrichten op eigen kosten (wat ook een verplichting uit de AVG is). Aan deze mogelijkheid worden in het Framework ibp-model wel nadere eisen gesteld.

Uit het SURF-model volgt daarnaast dat de verwerker in principe periodiek en op eigen kosten een audit zal laten verrichten door een externe deskundige. Hoe vaak deze periodieke audit dient plaats te vinden, is afhankelijk van het risiconiveau van de verwerking. In het Framework ibp-model staat daarentegen alleen dat de verwerker periodiek verklaart dat voldaan wordt aan passende technische maatregelen voor de beveiliging van de Verwerking van de Persoonsgegevens. De inhoud, werkwijze en vorm van deze verklaring kunnen partijen onderling afspreken. Er staat niet vermeld dat dit een verklaring van een derde partij dient te zijn (TPM-verklaring). In het SURF-model is dus in principe een periodieke auditverplichting voor de verwerker opgenomen, welke in het idp-model niet staat.