Privacy overeenkomst

DE ONDERGETEKENDEN:

Technische Universiteit Eindhoven, gevestigd aan Groene Loper 3, 5612 AE Eindhoven, Kamer van Koophandel nummer 51278871, en rechtsgeldig vertegenwoordigd door [VERTEGENWOORDIGER] (hierna: "**TU/e** ")

en

[**NAAM LEVERANCIER/VERWERKER**], gevestigd aan [ADRES] te [PLAATS], Kamer van Koophandel nummer [NUMMER], en rechtsgeldig vertegenwoordigd door [VERTEGENWOORDIGER] (hierna: "**Leverancier**");

hierna gezamenlijk: "**Partijen**" en individueel ook: "**Partij**";

OVERWEGENDE DAT:

- TU/e en Leverancier op [datum] een overeenkomst hebben gesloten voor de levering van (vaste en mobiele) elektronische communicatiediensten (hierna: de "Communicatiediensten") (hierna: de "Overeenkomst");
- Als onderdeel van de Overeenkomst neemt TU/e tevens de online serviceportal van Leverancier, (hierna: het "Serviceportal"), af;
- Met betrekking tot de Communicatiediensten bestaat tussen Partijen een relatie van zelfstandige verwerkingsverantwoordelijken in de zin van de Algemene Verordening Gegevensbescherming ("AVG"). Ten aanzien van een beperkt deel van de dienstverlening via het Serviceportaal bestaat echter een relatie van verwerkingsverantwoordelijke en verwerker, waarbij TU/e de doeleinden van en de middelen voor de verwerking vaststelt en derhalve optreedt als Verwerkingsverantwoordelijke in de zin van de AVG, terwijl Leverancier in het kader van het aanbieden van het Serviceportaal Persoonsgegevens verwerkt en derhalve optreedt als Verwerker in de zin van de AVG;
- Privacywetgeving, waaronder de AVG, vereist dat een dergelijke verwerking wordt geregeld in een overeenkomst of andere rechtshandeling tussen TU/e en Leverancier;
- Partijen komen overeen hun nadere afspraken dienaangaande vast te leggen in deze overeenkomst (hierna: de "Privacy overeenkomst").

Onderdeel 1 – Algemene bepalingen

ARTIKEL 1 DEFINITIES EN VARIA

1.1 In deze Privacy overeenkomst betekenen de met hoofdletter geschreven termen hetzelfde als in artikel 4 AVG, tenzij anders gedefinieerd.

1.2 De in dit document genoemde bijlagen en de latere aanpassingen en aanvullingen daarvan zijn een onderdeel van deze Privacy overeenkomst.

1.3 Deze Privacy overeenkomst gaat in als Partijen deze Privacy overeenkomst hebben ondertekend. Als de Verwerking van de Persoonsgegevens al is begonnen voordat deze Privacy overeenkomst is ondertekend, geldt deze Privacy overeenkomst met terugwerkende kracht met ingang van de datum waarop de Verwerking is gestart. Deze Privacy overeenkomst is niet los van de Overeenkomst te beëindigen.

1.4 Op deze Privacy overeenkomst is hetzelfde recht van toepassing als dat van de Overeenkomst. Geschillen over deze Privacy overeenkomst worden voorgelegd aan de bevoegde rechter van de Overeenkomst.

1.5 Als er tegenstrijdigheden zijn tussen deze Privacy overeenkomst en de Overeenkomst voor wat betreft de Verwerking van Persoonsgegevens, gelden de bepalingen van deze Privacy overeenkomst.

ARTIKEL 2 ROLVERDELING

2.1 Iedere Partij treedt op als zelfstandige Verwerkingsverantwoordelijke ten aanzien van de Persoonsgegevens waarvoor zij zelfstandig de Doeleinden en middelen voor de verwerking vaststelt.

2.2 Op de verwerkingsactiviteiten genoemd in Tabel 1: Rolverdeling, waarvoor Partijen zich identificeren als zelfstandige Verwerkingsverantwoordelijken, is Deel 2 – Verwerking tussen Verwerkingsverantwoordelijken van toepassing. Op de verwerkingsactiviteiten waarvoor Leverancier optreedt als Verwerker, is Deel 3 – Verwerkersbepalingen van toepassing.

Verwerking	Rol TU/e	Rol Leverancier
Levering van telecommunicatiediensten	Zelfstandig verwerkingsverantwoordelijke	Zelfstandig verwerkingsverantwoordelijke
Klantadministratie	Zelfstandig verwerkingsverantwoordelijke	Zelfstandig verwerkingsverantwoordelijke
Fraude preventie	Zelfstandig verwerkingsverantwoordelijke	Zelfstandig verwerkingsverantwoordelijke
Facturatie- en betalingsadministratie	Zelfstandig verwerkingsverantwoordelijke	Zelfstandig verwerkingsverantwoordelijke
Naleving van telecommunicatierechtelijke en wettelijke verplichtingen	Zelfstandig verwerkingsverantwoordelijke	Zelfstandig verwerkingsverantwoordelijke
Klantenondersteuning met betrekking tot telecommunicatiediensten	Zelfstandig verwerkingsverantwoordelijke	Zelfstandig verwerkingsverantwoordelijke
Gebruikersbeheer in de Serviceportal	Verwerkingsverantwoordelijke	Verwerker
Aanmaken van accounts in de Serviceportal	Verwerkingsverantwoordelijke	Verwerker
Onderhoud van accounts in de Serviceportal	Verwerkingsverantwoordelijke	Verwerker

Tabel 1: Rolverdeling

a) contactgegevens voor meer informatie over het datalek;
b) (aanbevolen) mitigeringsmaatregelen;
c) mogelijke gevolgen en risico's voor de privacy van betrokkenen.

Part 2 – Verwerking tussen zelfstandig Verantwoordelijken

ARTIKEL 3 VERANTWOORDELIJKHEDEN VAN DE ZELFSTANDIGE VERWERKINGSVERANTWOORDELIJKEN

3.1 Iedere Partij zal:

a) voldoen aan de AVG
b) beschikken over een eigen grondslag voor de verwerking;
c) betrokkenen voorzien van de vereiste privacy- en transparantie-informatie;
d) zelfstandig voldoen aan de verplichtingen die op een verwerkingsverantwoordelijke rusten.

ARTIKEL 4 BEVEILIGING, INCIDENTEN & DATALEKKEN

4.1 Elke partij zal passende technische en organisatorische maatregelen treffen overeenkomstig art. 32 AVG om een beveiligingsniveau te waarborgen dat passend is bij de risico's van de verwerking, gericht op het voorkomen van accidentele of onwettige vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking van of toegang tot verzonden, opgeslagen of anderszins verwerkte persoonsgegevens.

4.2 Elke partij voert interne beveiligingsincidenten- en datalekprocedures uit die gericht zijn op het detecteren en handelen naar beveiligingsincidenten en datalekken, inclusief maatregelen om te handelen bij ontdekking.

4.3 Bij het vernemen van een (mogelijke) datalek of beveiligingsincident met betrekking tot de persoonsgegevens en/of diensten die onder de Overeenkomst worden geleverd en die de andere Partij kunnen treffen, moet de getroffen Partij de andere Partij onverwijld (of binnen 24 uur)hiervan op de hoogte stellen. De kennisgeving moet, voor zover beschikbaar en relevant, ten minste het volgende bevatten:

a) de aard van het datalek of beveiligingsincident;
b) categorieën van de betreffende persoonsgegevens

ARTIKEL 5 VERZOEKEN VAN BETROKKENEN

5.1 Iedere Partij is verantwoordelijk voor de afhandeling van verzoeken die zij rechtstreeks ontvangt van betrokkenen met betrekking tot haar eigen verwerkingsactiviteiten. Indien daarvoor redelijkerwijs medewerking van de andere Partij vereist is, zullen Partijen elkaar in redelijkheid bijstand verlenen.

ARTIKEL 6 INTERNATIONALE DOORGIFTE

6.1 Iedere Partij blijft zelfstandig verantwoordelijk voor het waarborgen van een rechtmatig doorgiftemechanisme overeenkomstig Hoofdstuk V van de AVG.

Part 3 – Verwerkersbepalingen

ARTIKEL 7 INSTRUCTIES

7.1 Leverancier verwerkt Persoonsgegevens uitsluitend op basis van de gedocumenteerde instructies van TU/e en uitsluitend voor zover noodzakelijk voor de uitvoering van de Overeenkomst, met

inbegrip van het aanbieden van het Serviceportaal en daarmee redelijkerwijs samenhangende activiteiten, tenzij Partijen schriftelijk anders zijn overeengekomen. Leverancier zal de Persoonsgegevens niet voor enig ander doel verwerken.

7.2 Leverancier verricht alle verwerkingen van Persoonsgegevens in overeenstemming met de AVG en overige toepasselijke wet- en regelgeving op het gebied van gegevensbescherming, waaronder de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) en de Telecommunicatiewet (hierna: 'Toepasselijke Wetgeving').

7.3 Verwerker informeert Verwerkingsverantwoordelijke onmiddellijk als:
a) een instructie van Verwerkingsverantwoordelijke in strijd is met de AVG en/of Toepasselijke Wetgeving;
b) Verwerker niet langer aan deze Privacy overeenkomst kan voldoen;
c) Verwerker op grond van een wettelijke verplichting de Persoonsgegevens moet verwerken, tenzij deze informatieverstrekking op basis van de wet verboden is.

ARTIKEL 8 VERLENEN VAN MEDEWERKING

8.1 Op verzoek van TU/e werkt Leverancier direct mee aan het nakomen van de verplichtingen die Verwerkingsverantwoordelijke ter zake van de Persoonsgegevens heeft op grond van de AVG en Toepasselijke Wetgeving. Die medewerking, in deze Privacy overeenkomst op een aantal onderwerpen nader uitgewerkt, heeft betrekking op onder meer:
a) voldoen aan verzoeken van Betrokkenen;
b) uitvoeren van Data Protection Impact Assessments (DPIA's) en voorafgaande raadpleging bij Toezichthoudende autoriteiten;
c) uitvoeren van Data Transfer Impact Assessments (DTIA's);
d) voldoen aan verzoeken van (inter)nationale (overheids-)instanties.

3.2 Als Leverancier een verzoek krijgt van een (inter)nationale (overheids-) instantie over de Persoonsgegevens, dan:
a) neemt Leverancier direct contact op met TU/e, en
b) volgt Leverancier de instructies van TU/e op.

ARTIKEL 9 GEHEIMHOUDING

9.1 Leverancier is verplicht tot geheimhouding van de Persoonsgegevens. Personen die voor Leverancier werken hebben een geheimhoudingsverklaring getekend, of zijn op een andere manier gebonden aan geheimhouding. TU/e kan hiervan bewijs vragen.

5.2 De geheimhouding kan worden doorbroken als dit noodzakelijk is voor de uitvoering van de Overeenkomst of deze Privacy overeenkomst, door Toepasselijke Wetgeving, een uitspraak van een Nederlandse rechter of een rechter in een andere EU-lidstaat. In geval van een rechterlijke uitspraak uit een derde land, treedt Leverancier eerst in overleg met Verwerkingsverantwoordelijke alvorens de Persoonsgegevens te verstrekken.

ARTIKEL 10 BEVEILIGING

10.1 Leverancier neemt passende technische en organisatorische maatregelen in de zin van artikel 32 AVG om de Persoonsgegevens te beveiligen. De maatregelen die Leverancier heeft geïmplementeerd, zijn opgenomen in Bijlage B.

10.2 Leverancier zal deze maatregelen periodiek evalueren en actualiseren om de blijvende doeltreffendheid ervan en de aansluiting bij technologische ontwikkelingen te waarborgen. Wijzigingen in deze maatregelen mogen niet leiden tot een lager beschermingsniveau dan tussen Partijen is overeengekomen. Leverancier zal TU/e informeren over materiële wijzigingen in Bijlage B en zal op verzoek redelijke bewijsstukken verstrekken waaruit blijkt welke beveiligingsmaatregelen zijn geïmplementeerd.

ARTIKEL 11 DATALEKKEN

11.1 Leverancier informeert TU/e onverwijld, en uiterlijk binnen 24 uur na ontdekking, over iedere Inbreuk in verband met Persoonsgegevens of een redelijk vermoeden daarvan. Indien niet alle informatie direct beschikbaar is, verstrekt Leverancier deze gefaseerd zodra deze beschikbaar komt.

11.2 Leverancier meldt een Inbreuk niet aan een Toezichthoudende Autoriteit of Betrokkenen, tenzij TU/e hiervoor voorafgaande schriftelijke instructie heeft gegeven.

11.3 Leverancier neemt zo snel mogelijk maatregelen om de oorzaken van de Inbreuk weg te nemen en de mogelijke nadelige gevolgen van de Inbreuk zoveel mogelijk te verminderen of ongedaan te maken.

11.4 Leverancier beschikt over passende procedures voor het opsporen, melden, beheersen en afhandelen van Inbreuken en verstrekt hierover op verzoek informatie aan TU/e.

11.5 Leverancier houdt een register bij van alle Inbreuken die verband houden met de verwerking van Persoonsgegevens, inclusief de gevolgen en getroffen maatregelen, en verstrekt hiervan op verzoek een afschrift aan TU/e.

ARTIKEL 12 SUB-VERWERKERS

12.1 TU/e verleent Leverancier hierbij toestemming om gebruik te maken van de in Bijlage A opgenomen Subverwerkers. Leverancier zal geen aanvullende Subverwerker inschakelen en geen bestaande Subverwerker vervangen zonder de voorafgaande specifieke schriftelijke toestemming van TU/e.

12.2 Leverancier draagt er zorg voor dat iedere Subverwerker contractueel wordt gebonden aan verplichtingen die ten minste gelijkwaardig zijn aan de verplichtingen die op grond van deze Privacy overeenkomst op Leverancier rusten. Op verzoek van TU/e verstrekt Leverancier een kopie van de relevante contractuele bepalingen die met een Subverwerker zijn overeengekomen. Leverancier is gerechtigd daarbij commercieel gevoelige of vertrouwelijke informatie weg te laten.

12.3 Leverancier blijft het primaire aanspreekpunt voor TU/e en blijft volledig aansprakelijk voor de nakoming van de verplichtingen van de door hem ingeschakelde Subverwerkers en voor alle verwerkingen die door deze Subverwerkers worden uitgevoerd, alsof deze door Leverancier zelf worden verricht.

ARTIKEL 13 AUDITS

13.1 Leverancier is verplicht om periodiek een onafhankelijke, externe deskundige een audit te laten uitvoeren ten aanzien van de organisatie en processen van Leverancier, teneinde aan te tonen dat Leverancier aan het bepaalde in de Privacy overeenkomst, de AVG en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet. Het auditrapport wordt op verzoek verstrekt.

13.2 De frequentie van de reguliere audit die door de Leverancier moet worden uitgevoerd, is vastgelegd in Bijlage A. Reguliere audits moeten ten minste eens per twee jaar worden uitgevoerd. Echter, indien er sprake is van verwerking van bijzondere categorieën van Persoonsgegevens of indien de Verwerking een hoog risico inhoudt voor de rechten en vrijheden van de Betrokkenen, moet de Leverancier de audits ten minste jaarlijks uitvoeren.

13.3 Indien de Leverancier periodiek een verklaring of certificaat (bijv. een ISO 27001-certificaat) van een onafhankelijke deskundige overlegt waaruit blijkt dat de Leverancier voldoet aan de verplichtingen uit de Privacy overeenkomst, de AVG en de toepasselijke wetgeving, en er geen aanwijzingen zijn van niet-naleving, is een reguliere audit niet vereist. Deze verklaring of certificaat moet bij het verlopen van de geldigheidsduur worden vernieuwd en opnieuw worden aangeleverd.

13.4 Indien concrete omstandigheden naar het oordeel van TU/e daartoe aanleiding geven of indien TU/e vermoedt dat Leverancier zijn verplichtingen niet nakomt, kan TU/e alsnog een eigen audit (laten) uitvoeren. Leverancier zal daar zijn medewerking aan verlenen, onder meer door het verlenen van toegang tot systemen en documenten. De kosten van een eigen audit zijn voor rekening van TU/e, tenzij uit de audit blijkt dat Leverancier tekort is geschoten in de nakoming van zijn verplichtingen uit deze Privacy overeenkomst. Indien dit het geval is, neemt Leverancier direct en op eigen kosten alle redelijke maatregelen om te zorgen dat Leverancier alsnog aan deze verplichtingen voldoet. TU/e meldt de audit minstens veertien (14) dagen van tevoren. De audit zal de normale bedrijfsactiviteiten van Leverancier niet onredelijk verstoren

13.5 TU/e behandelt de uit de (reguliere) audit verkregen informatie vertrouwelijk en deelt deze alleen met die samenwerkingspartners voor wie kennisname van de informatie redelijkerwijs noodzakelijk is. TU/e noch de hiervoor bedoelde samenwerkingspartners zullen de auditresultaten openbaar maken of met derden delen, tenzij dit wettelijk vereist is.

ARTIKEL 14 RETOURNEREN EN VERWIJDERING VAN PERSOONSGEGEVENS

14.1 Binnen een (1) maand nadat de Overeenkomst op welke grond dan ook eindigt, vernietigt of retourneert Leverancier alle Persoonsgegeven (en eventueel kopieën bij Subverwerkers). Kiest TU/e voor teruggave, dan draagt Leverancier deze in een gangbaar format over aan TU/e of aan een andere partij die TU/e aanwijst. Indien in Bijlage A een afwijkende bewaartermijn is opgenomen in relatie tot specifieke Verwerkingen van de Persoonsgegevens, prevaleert die termijn boven de termijn uit dit artikel.

14.2 De verplichtingen voor Leverancier uit deze Privacy overeenkomst blijven gelden tot het moment dat Leverancier geen Verwerkingen van de Persoonsgegevens meer verricht.

14.3 Leverancier bevestigt schriftelijk aan TU/e dat hij aan alle verplichtingen uit lid 1 heeft voldaan als daarom wordt gevraagd.

ARTIKEL 15 AANSPRAKELIJKHEID EN VRIJWARING

15.1 De bepalingen over vrijwaringen, aansprakelijkheid en schadevergoeding in de Overeenkomst zijn onverkort van toepassing op deze Privacy overeenkomst.

ALDUS OVEREENGEKOMEN DOOR PARTIJEN:

Technische Universiteit Eindhoven	**[NAAM LEVERANCIER]**
Datum:	*Datum:*
_____	_____
Naam *Functie*	Naam *Functie*

Bijlage A: Specificatie van de Verwerking van de Persoonsgegevens

Versienummer XX, datum: [datum]

Omschrijving verwerking ('wat ga je doen')	Doel van de verwerking ('waarom ga je dit doen')	Betrokkenen	Persoons-gegevens	Bewaartermijn(en) van de Persoonsgegevens
1 ….				
2 ….				
3 ….				

Frequentie van de uit te voeren reguliere audit: [SELECTEER ÉÉN OPTIE EN VERWIJDER DE REST. INDIEN 'NIET VAN TOEPASSING' WORDT GEKOZEN, SPECIFICEER HET CERTIFICAAT OF DE VERKLARING]

o Eens per 2 jaar

o Jaarlijks

o Niet van toepassing, aangezien de Verwerker periodiek een [naam verklaring of certificaat, bijv. ISO 27001-certificaat] overlegt van een onafhankelijke deskundige waaruit blijkt dat de Verwerker voldoet aan de verplichtingen uit de Verwerkersovereenkomst, de AVG en de toepasselijke wetgeving

De door Verwerker ingeschakelde Subverwerkers zijn:

Subverwerker (naam en adres)	Persoonsgegevens die Subverwerker verwerkt	Omschrijving van de reden voor de subverwerking	Land van verwerking

De doorgiften naar derde landen bij de Verwerking zijn:

Doorgifte naar derde landen (naam en adres partij die Persoonsgegevens ontvangt)	Doel doorgifte (kostenbesparingen, schaalvoordelen of beveiligingsverbeteringen)	Doorgifte-mechanisme (bijv. Standard Contractual Clauses)	Aanvullende maatregelen naar aanleiding van een doorgifte aan een derde land (indien van toepassing)

Contactgegevens:

Algemene contactgegevens	Naam	Functie	E-mailadres	Telefoonnummer

Leverancier				
TU/e				

Contactgegevens bij Inbreuk	**Naam**	**Functie**	**E-mailadres**	**Telefoonnummer**
TU/e	1: 2: Computer Emergency Response Team (CERT) 3: TU/e Privacy	1: 2: CERT 3: Privacy Team	1: 2: cert@tue.nl 3: privacy@tue.nl	1: 2: +31 (0) 40 – 247 5678 3: N/A
Leverancier				

Bijlage B: Beveiligingsmaatregelen

Versienummer XX, datum: [datum]

SELECTEER ÉÉN OPTIE EN VERWIJDER DE ANDERE

OPTIE 1: Als Verwerker beschikt over certificaten die afdoende zijn

Leverancier beschikt over de volgende geldige certificaten of verklaringen van een deskundige derde waaruit blijkt dat Verwerker voldoet aan zijn verplichting de Persoonsgegevens die hij ten behoeve van TU/e verwerkt adequaat te beveiligen:

Naam of nummer	**Toepassingsgebied**	**Geldigheidsduur**
bijv. ISO 27001, NEN 7510, SOC 2		

Leverancier draagt ervoor zorg dat hij gedurende deze Verwerkersovereenkomst blijft beschikken over bovenstaande certificaten of een gelijkwaardige opvolger daarvan met een nieuwe geldigheidsduur.

OPTIE 2: Als Verwerker niet beschikt over certificaten die afdoende zijn

In de hieronder opgenomen tabel zijn de door Verwerker genomen beveiligingsmaatregelen om (ook) de Persoonsgegevens die hij ten behoeve van Verwerkingsverantwoordelijke verwerkt adequaat te beveiligen, beschreven.

Voor zover Verwerker een bepaalde maatregel niet of niet geheel heeft genomen, is dit vermeld in de kolom 'Toelichting'.

#	**Onderwerp**	**Maatregel**	**Toelichting** **Geef aan of en hoe de maatregel is geïmplementeerd. Indien niet volledig geïmplementeerd, leg dan uit waarom.**
1	Informatie-beveiligings- en privacybeleid	Verwerker heeft een informatiebeveiligings- en privacybeleid dat voldoet aan de AVG en eventuele richtsnoeren van de Autoriteit Persoonsgegevens en aansluit op algemene standaarden zoals ISO 27001/2/18, NOREA of CoBIT. Verwerker heeft dit beleid intern gecommuniceerd en concreet geïmplementeerd door middel van gedocumenteerde procedures.	Verwerker kan in deze tabel ook steeds verwijzen naar de specifieke plaats in een document waaruit blijkt dat en hoe de maatregel is geïmplementeerd (zoals een hoofdstuk of paragraaf in een intern beleidsdocument).
2	Versleutelde opslag en verzending gegevens	Verwerker past actuele en algemeen als veilig beschouwde vormen van versleuteling (encryptie) toe op gegevens voor opslag ('at rest') en verzending ('in transit') om het risico te minimaliseren dat de inhoud van de gegevens kan worden ingezien door personen die daar niet toe bevoegd zijn.	

3	Access management	Verwerker past de principes van 'least privilege' en 'need-to-know' toe op zijn medewerkers en toegestane Subverwerkers. Verwerker zal tijdig gebruikerstoegang intrekken of wijzigen bij enige verandering in de status van zijn of Subverwerkers' medewerkers Verwerker maakt gebruik van actuele en algemeen als veilig beschouwde vormen van versleuteling (encryptie) ten behoeve van identificatie, authenticatie en autorisatie.	
4	Medewerkers	Verwerker informeert zijn medewerkers over hun verantwoordelijkheden m.b.t. informatiebeveiliging en ziet erop toe dat medewerkers hun verplichtingen nakomen.	
5	Contract-management subverwerkers	Verwerker sluit met iedere toegestane Subverwerker een schriftelijke overeenkomst die de Subverwerker contractueel verplicht tot nakoming van dezelfde verplichtingen in verband met de Verwerking als die waar Verwerker op grond van deze Verwerkersovereenkomst aan is gebonden. Verwerker ziet er nauwlettend op toe dat Subverwerkers hun verplichtingen nakomen.	
6	Security incident detection & response	Verwerker heeft gedocumenteerd beleid dat geschikt is om Inbreuken te detecteren, op te lossen en te melden.	
7	Vulnerability / patch management	Verwerker zoekt regelmatig of doorlopend naar kwetsbaarheden binnen de gebruikte en aangeboden applicaties, systemen en netwerken. Verwerker installeert, implementeert security patches direct of zo snel mogelijk na het verschijnen daarvan.	
8	Netwerk- en systeem-beveiliging	Verwerker heeft maatregelen getroffen om misbruik van en malware op het netwerk en de systemen van Verwerker tegen te gaan en te detecteren (zoals firewalls en antivirussoftware van betrouwbare leveranciers).	
9	Fysieke toegangs-beveiliging	Verwerker neemt passende maatregelen (zoals sloten, camera's, alarmsystemen) om de ruimtes waarin gegevens kunnen worden verwerkt, te beveiligen tegen onbevoegde toegang.	

10	Logging en monitoring	Door logging en monitoring wordt aangetoond dat slechts legitieme gebruikers en/of toepassingen de gegevens gebruiken. Bij signalering van niet-legitieme gebruikers en/of toepassingen wordt passende actie ondernomen.	
11	Locatie aantonen	Verwerker kan de fysieke locatie/geografie van opgeslagen gegevens aantonen.	
12	Business continuity & disaster recovery	Verwerker heeft beleid, procedures en processen geïmplementeerd om te waarborgen dat de geleverde diensten of producten en de verwerkte gegevens beschikbaar blijven in geval van onvoorziene omstandigheden en rampen, dan wel zo snel mogelijk volledig worden hersteld.	
13	Veilige applicatie-ontwikkeling	Verwerker gebruikt industriestandaarden (bv. OWASP, BSIMM, ACS, NIST) om beveiliging in applicatieontwikkeling te integreren.	
14	Onafhankelijke controle	Verwerker staat toe dat een externe partij audits, kwetsbaarheidsscans en periodieke penetratietests op zijn applicaties en netwerken uitvoert in opdracht van Verwerkingsverantwoordelijke, in overleg met Verwerker. Bij voorkeur geeft Verwerker zelf ook regelmatig opdracht aan deskundige externe partijen om audits, kwetsbaarheidsscans en periodieke penetratietests op zijn applicaties en netwerken uit te voeren. Bij voorkeur heeft Verwerker ook beleid en procedures voor het vinden en melden van beveiligingsproblemen door onafhankelijke beveiligingsonderzoekers (zoals responsible disclosure policy en/of bug bounty programma). Het toekennen van beloningen aan partijen die substantiële beveiligingsproblemen op een verantwoorde manier hebben gemeld, wordt hierbij als positief beschouwd.	