

Verwerkingsovereenkomst (versie 14 augustus 2025)

1 Algemeen

- 1.1 Bij de uitvoering van het Contract, kan Telenet - op verzoek en in opdracht van de Klant – bepaalde persoonsgegevens ontvangen, raadplegen of op andere wijze verwerken in de hoedanigheid van verwerker van de Klant. De Partijen komen overeen dat de Klant de verwerkingsverantwoordelijke en Telenet de verwerker van zulke persoonsgegevens is.
- 1.2 De Partijen wensen de van toepassing zijnde Wetgeving inzake Gegevensbescherming na te leven, en door middel van deze Verwerkingsovereenkomst, die samen moet worden gelezen met de Bijlagen, afspraken te maken met betrekking tot de verwerking van persoonsgegevens door Telenet ten behoeve van de Klant bij de uitvoering van het Contract.

2 Definities

Ter aanvulling van de begrippen die reeds elders in het Contract en de Wetgeving inzake Gegevensbescherming gedefinieerd zijn zullen alle met een hoofdletter beginnende woorden en uitdrukkingen die gebruikt worden, in het enkelvoud en het meervoud, onderstaande betekenissen hebben:

“Betrokkene”	een geïdentificeerde of identificeerbare natuurlijke persoon van wie de persoonsgegevens zich onder het beheer van de Klant bevinden en het voorwerp uitmaken van de verwerking door Telenet in de context van het Contract;
“Bijlage”	elke bijlage bij deze Verwerkingsovereenkomst die integraal onderdeel uitmaakt van de Verwerkingsovereenkomst;
“Subverwerker”	elke derde partij waarop door de verwerker een beroep gedaan wordt om persoonsgegevens te verwerken namens de verwerkingsverantwoordelijke;
“Verwerkingsovereenkomst”	deze verwerkingsovereenkomst tussen de Partijen, inclusief alle Bijlagen, die integraal onderdeel uitmaakt van het Contract afgesloten tussen de Partijen en zoals van tijd tot tijd gewijzigd door de Partijen;
“Vertrouwelijke Informatie”	zoals gedefinieerd in het Contract;
“Wetgeving Gegevensbescherming”	inzake alle Toepasselijke Wetgeving zoals gedefinieerd in het Contract met betrekking tot de verwerking van persoonsgegevens en privacy, met inbegrip van Verordening (EU) 2016/679 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (de "Algemene Verordening Gegevensbescherming" of "AVG"). De termen "persoonsgegevens", "verwerkingsverantwoordelijke", "verwerker", "verwerking", "inbreuk in verband met persoonsgegevens" enz. hebben de betekenis die er in de Wetgeving inzake Gegevensbescherming aan wordt gegeven.

3 Verplichtingen van de Partijen

- 3.1 De Klant en Telenet zullen de Wetgeving inzake Gegevensbescherming naleven met betrekking tot de verwerking van persoonsgegevens in het kader van de dienstverlening.
- 3.2 De Klant is verantwoordelijk voor:
- (i) de naleving van alle toepasselijke verplichtingen en taken van de verwerkingsverantwoordelijke;
 - (ii) de opvolging van door Betrokkenen uitgeoefende rechten;
 - (iii) het voorzien van de nodige verwerkingsgronden (m.i.v. het verkrijgen van alle vereiste toestemmingen van de Betrokkenen);
 - (iv) de naleving van de toepasselijke informatieverplichtingen tegenover de Betrokkenen.

4 Verplichtingen Telenet

4.1 Instructies

- 4.1.1 Telenet zal de persoonsgegevens uitsluitend verwerken in overeenstemming met deze Verwerkingsovereenkomst, volgens de schriftelijke instructies van de Klant, indien redelijkerwijs nodig is om de dienstverlening te kunnen verstrekken in overeenstemming met het Contract of zoals vereist door de dwingende Toepasselijke Wetgeving en voor de doeleinden zoals bepaald in de Bijlage bij deze Verwerkingsovereenkomst. De Partijen komen overeen dat het Contract alle instructies van de Klant met betrekking tot de verwerking van de persoonsgegevens bevat. Bijkomende of alternatieve instructies moeten schriftelijk worden opgesteld en voorafgaandelijk door beide Partijen worden overeengekomen.
- 4.1.2 Telenet zal de Klant zo snel mogelijk in kennis stellen als een instructie van de Klant naar het oordeel van Telenet inbreuk maakt op de Wetgeving inzake Gegevensbescherming.
- 4.1.3 Telenet is gerechtigd om de persoonsgegevens zonder instructies van de Klant te verwerken indien een op haar van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling haar tot verwerking verplicht. In dergelijk geval stelt Telenet

de Klant in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

4.2 Vertrouwelijkheid

4.2.1 Telenet verbindt zich ertoe de vertrouwelijkheid van de persoonsgegevens te vrijwaren in overeenstemming met de toepasselijke Wetgeving inzake Gegevensbescherming en alle redelijke maatregelen te nemen om ervoor te zorgen dat:

- (i) de toegang tot de persoonsgegevens wordt beperkt tot die medewerkers die de persoonsgegevens moeten kunnen raadplegen en alleen voor zover dat nodig voor de dienstverlening aan de Klant;
- (ii) deze medewerkers onderworpen zijn aan passende verplichtingen inzake de vertrouwelijkheid en de geheimhouding van de gegevens, conform de toepasselijke Wetgeving inzake Gegevensbescherming; en
- (iii) deze medewerkers zich houden aan deze Verwerkingsovereenkomst en de Wetgeving inzake Gegevensbescherming (hierna samen de "**Verplichtingen inzake Gegevensbescherming**").

4.3 Derden en Subverwerkers

4.3.1 Telenet verbindt zich ertoe de persoonsgegevens niet over te dragen of mee te delen aan derden zonder de voorafgaande schriftelijke toestemming van de Klant.

4.3.2 Door het sluiten van het Contract, machtigt de Klant Telenet evenwel om een beroep te doen op Subverwerkers voor de verwerking van de persoonsgegevens. Wanneer het een beroep doet op Subverwerkers zal Telenet:

- (i) met elke Subverwerker een schriftelijke overeenkomst afsluiten die verplichtingen bevat in verband met de verwerking van de persoonsgegevens die gelijkwaardig aan en niet minder streng zijn dan de Verplichtingen inzake Gegevensbescherming; en
- (ii) tegenover de Klant aansprakelijk blijven voor elke inbreuk door een Subverwerker op de Verplichtingen inzake Gegevensbescherming.

4.3.3 De Klant machtigt Telenet bovendien om op elk ogenblik bijkomende of andere Subverwerkers aan te stellen. Telenet zal de Klant van zulke aanstelling in kennis stellen. De Klant aanvaardt en erkent dat hij binnen de dertig (30) dagen na zulke kennisgeving het recht zal hebben om bezwaar te maken tegen de aanstelling door het Contract te beëindigen, doch enkel op voorwaarde dat:

- (i) het bezwaar gesteund is op een objectieve, dwingende en onderbouwde rechtvaardiging met betrekking tot de reden waarom de nieuwe Subverwerker niet aan de verplichtingen krachtens het Contract en de Wetgeving inzake Gegevensbescherming kan voldoen; en
- (ii) Telenet het bezwaar niet redelijkerwijs kan weerleggen of wegnemen.

4.3.4 De Klant begrijpt en erkent dat alle informatie met betrekking tot de door Telenet aangestelde Subverwerkers als Vertrouwelijke Informatie wordt beschouwd.

4.4 Internationale doorgiften

De Klant machtigt Telenet om de persoonsgegevens te verwerken in een derde land buiten de Europese Economische Ruimte dat niet door de Europese Commissie wordt erkend als een land dat een passend beschermingsniveau waarborgt volgens artikel 45 van de AVG, op voorwaarde dat passende waarborgen worden geboden conform de Wetgeving inzake Gegevensbescherming (zoals bijvoorbeeld de ondertekening van de standaardcontractbepalingen voor de doorgifte van persoonsgegevens aan in derde landen gevestigde verwerkers, goedgekeurde bindende bedrijfsvoorschriften, of de aansluiting bij een goedgekeurde gedragscode).

4.5 Technische en organisatorische maatregelen

Telenet treft passende technische en organisatorische maatregelen om in overeenstemming met de toepasselijke Wetgeving inzake Gegevensbescherming een beschermingsniveau te verzekeren dat passend is voor het risico van de verwerking van de persoonsgegevens (met inbegrip van het risico van toevallige of ongeoorloofde toegang, wijziging, vernietiging, beschadiging, aantasting of verlies, en elke andere ongeoorloofde of onwettige verwerking of mededeling). Technische en organisatorische maatregelen worden alleen genomen voor zover en in de mate dat ze rechtstreeks of onrechtstreeks bijdragen tot de bescherming van de persoonsgegevens. Aangezien alle technische en organisatorische maatregelen het voorwerp zijn van technische vooruitgang en ontwikkeling, heeft Telenet op elk moment het recht om andere passende maatregelen te treffen. Een overzicht van de genomen technische en organisatorische maatregelen voor de verwerking van persoonsgegevens op de systemen en netwerken van Telenet ten behoeve van de Klant worden uiteengezet in artikel 11 van deze Verwerkingsovereenkomst.

4.6 Inbreuk in verband met persoonsgegevens

Telenet zal de Klant zo snel mogelijk waarschuwen als het een inbreuk in verband met persoonsgegevens vaststelt met betrekking tot persoonsgegevens die door Telenet ten behoeve van de Klant op de systemen en netwerken van Telenet worden verwerkt, en zal de Klant, zo snel mogelijk, informatie over de inbreuk in verband met persoonsgegevens verschaffen, rekening houdend met de aard van de verwerking en de informatie waarover Telenet beschikt. Indien de

inbreuk met betrekking tot persoonsgegevens te wijten is aan een handeling of nalatigheid van Telenet, zal Telenet alle redelijke maatregelen nemen om alle als gevolg van de inbreuk in verband met persoonsgegevens verloren, beschadigde, vernietigde, gewijzigde of aangetaste persoonsgegevens binnen een redelijk tijdsbestek te herstellen, opnieuw samen te stellen en/of te reconstrueren.

4.7 Bijstand

4.7.1 Telenet zal de Klant de bijstand en/of medewerking verstrekken die de Klant redelijkerwijs kan verzoeken om aan zijn verplichtingen volgens de Wetgeving inzake Gegevensbescherming te voldoen (met betrekking tot de persoonsgegevens die Telenet in het kader van het Contract ten behoeve van de Klant verwerkt), met inbegrip van:

- (i) het op verzoek van de Klant verstrekken van informatie over de technische en organisatorische maatregelen die Telenet heeft getroffen om de persoonsgegevens te beschermen;
- (ii) indien en voor zover dit wettelijk toegestaan is, de Klant op de hoogte brengen van elk toegangsverzoek voor de mededeling van de persoonsgegevens dat van eender welke toezichthoudende autoriteit, rechtbank of andere instantie uit een bevoegd rechtsgebied zou uitgaan. Om alle twijfel ter zake weg te nemen en voor zover bij wet is toegestaan, zal Telenet geen persoonsgegevens meedelen of vrijgeven na ontvangst van een dergelijk verzoek, zonder eerst overleg gepleegd te hebben met de Klant;
- (iii) de Klant op de hoogte brengen van verzoeken van Betrokkenen die gebruik maken van hun rechten als Betrokkenen volgens de Wetgeving inzake Gegevensbescherming en, in voorkomend geval, de nodige bijstand verlenen bij de uitvoering van deze verzoeken;
- (iv) meewerken aan de gegevensbeschermingseffectbeoordeling die de Klant volgens de wet verplicht is uit te voeren met betrekking tot de verwerkingsactiviteit uitgevoerd in het kader van het Contract en de verplichting om de bevoegde toezichthoudende autoriteit voorafgaand de verwerking te raadplegen wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien de Klant geen maatregelen neemt om dat risico te beperken;
- (v) het melden van inbreuken in verband met persoonsgegevens die voortvloeien uit de verwerking van persoonsgegevens door Telenet ten behoeve van de Klant aan de toezichthoudende autoriteit overeenkomstig artikel 33 AVG en, indien van toepassing, de mededeling aan de Betrokkene overeenkomstig artikel 34 AVG.

4.7.2 Indien Telenet in zijn hoedanigheid als verwerker een verzoek van een Betrokkene met betrekking tot een verwerking van persoonsgegevens in het kader van het Contract aan de Klant ontvangt, zal hij in geen enkel geval zelf reageren op dit verzoek van de Betrokkene en dit verzoek onverwijld overmaken aan de Klant.

4.7.3 Telenet behoudt zich het recht voor om alle redelijke kosten met betrekking tot zijn verplichtingen om deze bijstand en/of medewerking te verlenen aan te rekenen aan de Klant.

4.8 Audit

4.8.1 De Klant heeft het recht om redelijkerwijs na te gaan of Telenet deze Verwerkingsovereenkomst naleeft. Telenet stelt de Klant tijdens de duur van de Verwerkingsovereenkomst alle informatie ter beschikking die nodig is om aan te tonen dat is voldaan aan de verplichtingen van de Verwerkingsovereenkomst en de verplichtingen die rechtstreeks voortvloeien uit de Toepasselijke Wetgeving inzake Gegevensbescherming.

4.8.2 Telenet zal toestemmen met en meewerken aan redelijke verzoeken om audits die worden uitgevoerd door een erkende onafhankelijke auditor die door de Klant wordt aangesteld en die geen concurrentiële activiteit uitoefent, op kosten van de Klant, na een voorafgaand schriftelijk verzoek van de Klant met een voorafgaande kennisgeving van dertig (30) kalenderdagen. De Partijen komen overeen het aantal en de reikwijdte van de audits te beperken tot wat nodig is om de naleving door Telenet van de Verwerkingsovereenkomst te verifiëren, met een maximum van eenmaal per kalenderjaar.

4.8.3 Telenet zal tijdens de audit alle redelijke ondersteuning en bijstand verlenen. De Klant zal Telenet een kopie van het ontwerp van het auditrapport bezorgen en zal Telenet toelaten om opmerkingen te maken en wijzigingen voor te stellen vooraleer de definitieve versie van het auditrapport wordt opgesteld. De Partijen komen overeen dat elk auditrapport vertrouwelijk is en niet mag worden gepubliceerd of anderszins met derde partijen mag worden gedeeld.

4.9 Verwijdering

4.9.1 Na de beëindiging van het Contract zal Telenet zonder onnodige vertraging elk gebruik van de onderliggende persoonsgegevens die ten behoeve van de Klant worden verwerkt, stopzetten en – tenzij de wet de verdere bewaring van de persoonsgegevens voorschrijft – de persoonsgegevens en de kopieën die het ervan bezit vernietigen of anonimiseren.

5 Aansprakelijkheid

Zonder afbreuk te doen aan de aansprakelijkheidsuitsluitingen en -beperkingen van het Contract, kan Telenet alleen aansprakelijk worden gesteld voor de schade die door de verwerking van persoonsgegevens wordt veroorzaakt als gevolg van de niet-naleving van deze Verwerkingsovereenkomst, als Telenet de wettige instructies van de Klant niet heeft nageleefd of voor een overtreding van de verplichtingen van de Wetgeving inzake Gegevensbescherming die specifiek op verwerkers zijn gericht. Telenet zal echter niet aansprakelijk zijn jegens de Klant indien en voor zover de Klant rechtstreeks of onrechtstreeks aansprakelijk is voor de schade (bv. indien de schade het gevolg is van het niet nakomen door de Klant

van een van zijn verplichtingen of verantwoordelijkheden uit hoofde van het Contract of het niet naleven van de toepasselijke wetgeving). In dit verband vrijwaart de Klant Telenet tegen vorderingen van derden.

6 Duur en beëindiging

- 6.1 Deze Verwerkingsovereenkomst zal gelden vanaf de aanvaarding ervan door beide Partijen en zal na afloop of beëindiging van het Contract van kracht blijven, zolang Telenet toegang heeft tot de persoonsgegevens die het voorwerp van deze Verwerkingsovereenkomst uitmaken.
- 6.2 Deze Verwerkingsovereenkomst mag tijdens de duur van de verwerking van persoonsgegevens door Telenet slechts beëindigd worden na wederzijdse overeenstemming tussen de Partijen.

7 Volledige overeenkomst

Deze Verwerkingsovereenkomst vervangt alle andere schriftelijke of mondelinge onderhandelingen, overeenkomsten, afspraken of verklaringen tussen de Partijen met betrekking tot privacy en de bescherming van de persoonsgegevens die onder het Contract door Telenet ten behoeve van de Klant worden verwerkt.

8 Wijzigingen

Deze Verwerkingsovereenkomst kan alleen met wederzijdse instemming van de Partijen worden aangevuld, gewijzigd of aangepast. Geen enkele aanvulling, wijziging of aanpassing van deze Verwerkingsovereenkomst is bindend tenzij deze schriftelijk is en door beide Partijen is ondertekend.

9 Toepasselijk recht en bevoegde rechtbank

- 9.1 Deze Verwerkingsovereenkomst en alle (buiten)contractuele verbintenissen die eruit voortvloeien of ermee verband houden, worden beheerst door en geïnterpreteerd volgens Belgisch recht.
- 9.2 Elk geschil met betrekking tot het afsluiten, de geldigheid, de interpretatie en/of de uitvoering van deze Verwerkingsovereenkomst of van latere contractuele afspraken of verplichtingen die eruit voortvloeien, evenals elk ander geschil met betrekking tot of in verband met deze Verwerkingsovereenkomst, zal worden onderworpen aan de exclusieve bevoegdheid van rechtbanken en hoven van Antwerpen (afdeling Mechelen).

10 Vertaling

In geval van twijfel of tegenstrijdigheid tussen de verschillende taalversies heeft de Nederlandstalige versie van de Verwerkingsovereenkomst voorrang.

11 Overzicht van technische en organisatorische maatregelen

11.1 Vooraf

Telenet zal de maatregelen implementeren die in dit artikel beschreven worden, op voorwaarde dat de maatregelen rechtstreeks of onrechtstreeks bijdragen of kunnen bijdragen tot de bescherming van de persoonsgegevens die Telenet verwerkt in het kader van de dienstverlening aan de Klant.

De technische en organisatorische maatregelen zijn van toepassing op de verwerking van persoonsgegevens ten behoeve van de Klant op de systemen en netwerken van Telenet en/of in de vestigingen/gebouwen van Telenet.

De technische en organisatorische maatregelen zijn onderhevig aan technische vooruitgang en ontwikkeling. In die optiek is het Telenet toegestaan om alternatieve gepaste maatregelen te implementeren op voorwaarde dat het beveiligingsniveau van zulke maatregelen niet minder is dan de van de maatregelen die in dit artikel worden uiteengezet.

De Klant kan te allen tijde, op zijn kosten, om aanpassingen van de technische en operationele maatregelen die in dit artikel beschreven worden, verzoeken, als zulke aanpassingen naar zijn mening nodig zijn om aan de wettelijke eisen op het vlak van gegevensbescherming en aanverwante veiligheidskwesties met betrekking tot de door Telenet krachtens het Contract geleverde dienstverlening te voldoen. Alle wijzigingen zullen in onderling overleg overeengekomen worden.

11.2 Beschrijving van de technische en organisatorische maatregelen

A. Fysieke toegangscontrole tot vestigingen/gebouwen

Telenet zal de volgende fysieke toegangscontrolemaatregelen treffen, voor zover er in de vestigingen/gebouwen van Telenet persoonsgegevens verwerkt worden:

1. Beperking van de toegangsrechten voor kantoorgebouwen, datacentra en serverlokalen tot het benodigde minimum op basis van een voorafgaande veiligheidsscreening van alle werknemers die toegang (willen) verkrijgen tot de datacentra. Toegang door externe personen wordt voorafgaand aangevraagd mits motivering.
2. Doeltreffende controle van de toegangsrechten door middel van een geschikt vergrendelingssysteem (bv. veiligheidssleutel met gedocumenteerd sleutelbeheer, elektronische vergrendelingssystemen met gedocumenteerd beheer van bevoegdheden).
3. Voor het verkrijgen, aanpassen en intrekken van toegangsbevoegdheden moet er een uitgebreid en volledig gedocumenteerd proces geïmplementeerd zijn.
4. Regelmatige en gedocumenteerde herziening van toegangsbevoegdheden die op dat moment zijn toegekend.
5. Maatregelen om ongeoorloofde toegang en toegangspogingen te voorkomen en te detecteren (bv. regelmatige herziening van de inbraakbeveiliging van deuren, poorten en ramen, alarmsystemen, videobewaking, bewakingsagenten en veiligheidspatrouille).
6. Schriftelijke instructies voor werknemers en bezoekers voor de omgang met technische toegangsbeveiligingsmaatregelen.
7. Het op regelmatige basis aanbieden van opleidingen aan werknemers over fysieke toegangsbeveiliging van vestigingen/gebouwen van Telenet.

B. Controle van de logische toegang tot systemen

Telenet zal de volgende maatregelen treffen om de toegang tot systemen en netwerken te controleren, waarin persoonsgegevens ten behoeve van de Klant verwerkt worden of via welke toegang verleend kan worden tot persoonsgegevens van de Klant, voor zover deze persoonsgegevens worden verwerkt op de systemen en netwerken van Telenet:

1. Beperking van toegangsrechten tot IT-systemen en (niet-)openbare netwerken tot het benodigde minimum.
2. Regelmatige controle van authenticatie, autorisatie en accounting via geïndividualiseerde en unieke gebruikersidentificaties en veilige authenticatieprocessen.
3. Bij gebruik van wachtwoorden voor authenticatie zullen de nodige regels vastgesteld worden ter verzekering van de kwaliteit van de wachtwoorden op het vlak van lengte, complexiteit en regelmaat van wijziging. Er zullen technische testmethoden geïmplementeerd worden ter verzekering van de wachtwoordkwaliteit.
4. Bij het gebruik van asymmetrische sleutelmethoden (bv. certificaten, private-publieke-sleutelmethoden) voor authenticatie, zal erop toegezien worden dat geheime (persoonlijke) sleutels altijd beschermd worden met een wachtwoord (wachtwoordzin). De eisen die in overeenstemming met paragraaf 3 hierboven gesteld worden, dienen nageleefd te worden.
5. Alle accounts moeten regelmatig doorgelicht worden en, als een account niet regelmatig over een bepaalde toegang dient te beschikken, moeten de rechten ter zake afgenomen worden.

6. Regelmatige en gedocumenteerde herziening van de logische toegangsbevoegdheden die op dat moment zijn toegekend.
7. Er moeten gepaste maatregelen getroffen worden ter beveiliging van de netwerkinfrastructuur (bv. netwerkpoortbeveiliging IEEE 802.1X, inbraakdetectiesystemen, gebruik van 2-factor authenticatie voor toegang vanop afstand, scheiding van netwerken, content filtering, versleutelde netwerkprotocollen, enz.).
8. Schriftelijke instructies en opleidingen op regelmatige basis voor werknemers bij omgang met bovenstaande beveiligingsmaatregelen en veilig gebruik van wachtwoorden.
9. De installatie van kritieke of belangrijke beveiligingsupdates/-patches moet verzekerd zijn binnen een redelijke tijdsspanne, afhankelijk van de criticaliteit, het risico en de testing vereisten:
 - a. in controller besturingssystemen;
 - b. in serverbesturingssystemen die via publieke netwerken toegankelijk zijn (bv. webserver);
 - c. in applicatieprogramma's;
 - d. in beveiligingsinfrastructuur (virusscanners, firewalls, IDS-systemen, content filters, routers, enz.); alsook
 - e. in serverbesturingssystemen van interne servers.

C. Controle van de toegang tot gegevens

Telenet zal de volgende maatregelen treffen op het vlak van toegangscontrole, voor zover Telenet zelf verantwoordelijk is voor de toegangsbevoegdheden tot de persoonsgegevens die worden verwerkt ten behoeve van de Klant:

1. Beperking van toegangsbevoegdheden tot persoonsgegevens tot het absolute vereiste minimum.
2. Doeltreffende controle van de toegangsbevoegdheden via een gepast concept van rechten en rollen.
3. De implementatie van een uitgebreid en volledig gedocumenteerd proces inzake het verlenen van toegang tot, en het wijzigen, kopiëren en verwijderen van persoonsgegevens.
4. Redelijke maatregelen ter bescherming van terminalapparatuur, servers en andere infrastructuurelementen tegen ongeoorloofde toegang (bv. concept ter bescherming tegen virussen met meerdere niveaus, content filtering, applicatiefirewall, inbraakdetectiesystemen, desktopfirewall, systeem hardening, content versleuteling).
5. Technische beveiligingsmaatregelen voor export- en importinterfaces (hardware- en applicatie gerelateerd).

Telenet heeft de volgende verplichtingen tot samenwerking met de toegangscontrole, tenzij hij de toegangsbevoegdheden tot de persoonsgegevens beheert:

1. Een uitgebreid proces voor het aanvragen, aanpassen en intrekken van toegangsbevoegdheden binnen zijn verantwoordelijkheidsgebied.
2. Regelmatige en gedocumenteerde herziening van de toegangsbevoegdheden die op dat moment zijn toegewezen, voor zover mogelijk.
3. Kennisgeving aan de Klant indien de bestaande toegangsbevoegdheden niet langer nodig zijn.

D. Controle inzake gegevenstransmissie

Telenet zal de volgende maatregelen inzake transmissiecontrole treffen, voor zover er persoonsgegevens door Telenet ten behoeve van de Klant ontvangen, overgedragen of vervoerd worden:

1. Er moeten gepaste maatregelen getroffen worden ter beveiliging van de netwerkinfrastructuur (bv. netwerkpoortbeveiliging IEEE 802.1X, inbraakdetectiesystemen, gebruik van 2-factor authenticatie voor toegang vanop afstand, scheiding van netwerken, content filtering, versleutelde netwerkprotocollen, enz.).
2. Versleuteling van informatiedragers.
3. Gebruik van versleutelde communicatieprotocollen (zoals op TLS gebaseerde protocollen).
4. Inspectiemechanismen ter identificatie van elders gesitueerde terminals tijdens overdrachten.
5. Controletellingen met ontvangen persoonsgegevens
6. Schriftelijke instructies en verplichte jaarlijkse opleidingen voor werknemers inzake de omgang met en beveiliging van mobiele toestellen en informatiedragers.

E. Controle inzake gegevensinvoer

Opdat achteraf gecontroleerd en nagegaan kan worden of en door wie de persoonsgegevens geraadpleegd, gewijzigd en verwijderd kunnen worden van de gegevensverwerkingssystemen, zal Telenet de volgende maatregelen treffen om de invoer te controleren in zijn systemen die voor de verwerking van persoonsgegevens ten behoeve van de Klant worden gebruikt of die toegang tot zulke systemen mogelijk te maken of voorzien, voor zover Telenet verantwoordelijk is voor gegevensinvoer:

1. Creatie en beveiligde opslag van verwerkingsprotocollen.
2. Beveiliging van back-uplogbestanden tegen manipulatie.

F. Controle inzake gegevensverwerking

Opdat kan verzekerd worden dat de persoonsgegevens enkel verwerkt kunnen worden in overeenstemming met de bepalingen van deze Verwerkingsovereenkomst zal Telenet processen en documentatie voorzien inzake:

1. het selecteren van Subverwerkers volgens Wetgeving inzake Gegevensbescherming en technische aspecten.
2. het verzekeren van de voorgeschreven voorafgaande doorlichting van Subverwerkers in overeenstemming met de bepalingen van de Toepasselijke Wetgeving.
3. het verzekeren van de tijdige instructie van de operationele Data Protection Officers bij de introductie van nieuwe of de wijziging van bestaande procedures voor de verwerking van de persoonsgegevens.
4. de verplichtingen van iedereen die verantwoordelijk is voor het verwerken van de persoonsgegevens met het oog op de handhaving van de vertrouwelijkheid van de gegevens in overeenstemming met de toepasselijke wettelijke bepalingen.
5. het verzekeren van de vertrouwelijkheid van de personen aan wie de verwerking van de persoonsgegevens wordt toevertrouwd met de relevante gegevensbeschermingsvoorschriften en de specifieke instructies van de Klant.
6. het behoud van de erkenning van de operationele Data Protection Officer.
7. het verzekeren van de onmiddellijke verwittiging van de Klant bij een onwettige verwerving van kennis over persoonsgegevens of andere beschermde informatie.

G. Beschikbaarheidscontrole

Opdat de persoonsgegevens beschermd worden tegen onbedoelde vernietiging of verlies, zal Telenet de volgende maatregelen implementeren om beschikbaarheid te controleren, op voorwaarde dat de verwerking van de persoonsgegevens noodzakelijk is om productieve dienstverlening ten behoeve van de Klant te kunnen handhaven:

1. Werking en regelmatig onderhoud van brandalarmsystemen in serverruimten, datacentra en kritieke infrastructuurruimten.
2. Aanmaken van regelmatige back-ups en erop toezien dat er voor een sterk en veerkrachtig 'disaster recovery'-systeem gezorgd werd.
3. Regelmatig controleren en testen van de back-upintegriteit.
4. Processen en documentatie voor de recuperatie van systemen en gegevens.
5. Alle persoonsgegevens op papier moeten opgeslagen, verwerkt en vernietigd worden in overeenstemming met de ter zake geldende goede beveiligingspraktijken.

H. Toeëigeningscontrole

Opdat persoonsgegevens die voor verschillende doeleinden verzameld werden ook apart verwerkt kunnen worden, zal Telenet de volgende maatregelen treffen om de persoonsgegevens ten behoeve van de Klant gescheiden te verwerken:

1. Logische en/of fysieke scheiding van test-, ontwikkelings- en productiesystemen.
2. Scheiding op controllerniveau binnen verwerkingssystemen en bij interfaces.
3. Verzekering van de onafgebroken identificeerbaarheid van de persoonsgegevens.

I. Bewaring en verwijdering van gegevens

Opdat de persoonsgegevens alleen zo lang als nodig bewaard worden en verwijderd worden na hun volledige verwerking, zal Telenet de volgende maatregelen treffen om het verwijderen van de persoonsgegevens te verzekeren, op voorwaarde dat deze persoonsgegevens ten behoeve van de Klant worden verwerkt:

1. Ervoor zorgen dat de persoonsgegevens altijd gewist of geanonimiseerd kunnen worden op verzoek van de Klant.
2. Processen, hulpmiddelen en documentatie voor een veilige verwijdering op een zodanige manier dat de betrokken persoonsgegevens middels de huidige stand van de technologie niet gerecupereerd kunnen worden.
3. Richtlijnen voor werknemers over hoe en wanneer welke gegevens verwijderd moeten worden.

Bijlage(n): Specifieke details van de verwerking van persoonsgegevens

Te raadplegen op de webpagina's van de betreffende oplossingen.