**Toetsingskader**

**Privacy (Pluscluster 7)**

**versie 3.1 – oktober 2020**

****

**IBPDOC7**

Verantwoording

**Bronnen:**

**SURFaudit toetsingskader**

*Stichting SURF*

*Februari 2015*

**Opdracht verstrekking door:**

Kennisnet / saMBO-ICT

**Auteurs**

Leo Bakker (Kennisnet)

Ludo Cuijpers (Kennisnet)

Axel Eissens (Kennisnet)

Job Vos (Kennisnet)

Peter Vermeijs (MBORaad)

**Met dank aan:**

Ingeborg van der Molen (ROC Midden Nederland)

Sylvia Liem (Mondriaan College)

Janine Kloosterman (Nordwin College)

Maarten Velthuis (Rijn IJssel)

Niels Dutij (cibap)

Martijn Bijleveld (saMBO-ICT)

Leo Bakker (Kennisnet)

***Versie 3.1 oktober 2020***

Bij deze update zijn wijzigingen in het gemeenschappelijk normenkader verwerkt. Er zijn twee statements uit het IB-kader toegevoegd en de beschrijving van de privacy-impact is bij alle statements gewijzigd.

**Sommige rechten voorbehouden**

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgever van Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.

**Creative commons**

Naamsvermelding 3.0 Nederland

(CC BY 3.0)

**De gebruiker mag:**

* Het werk kopiëren, verspreiden en doorgeven
* Remixen – afgeleide werken maken

**Onder de volgende voorwaarde:**

* Naamsvermelding – De gebruiker dient bij het werk de naam van Kennisnet te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

*In dit document worden de beginselen en principes beschreven die een onderwijsinstelling moet aanhouden als hij gegevens verzamelt over studenten en docenten. wet- en regelgeving is eveneens afkomstig van deze beginselen. Dit document is bedoeld om de wet eenvoudiger te kunnen begrijpen. De tekst is geschreven voor niet-juristen. Daarbij is er voor gekozen om niet altijd de letterlijke juridische bewoordingen aan te houden. Met deze vertaalslag gaan soms juridische finesses en details verloren. Voor de volledigheid wordt u altijd aangeraden om bij twijfel de wettekst te raadplegen en zo nodig een deskundige in te schakelen.*

Inhoudsopgave

[Verantwoording 2](#_Toc53387268)

[1. Inleiding 5](#_Toc53387269)

[1.1 Uitgangspunt is het Privacy Compliance kader 5](#_Toc53387270)

[1.2 Update Toetsingskader Privacy, augustus 2019 6](#_Toc53387271)

[1.3 Informatiebeveiliging en privacy 6](#_Toc53387272)

[1.4 Samenhang tussen informatiebeveiliging en privacy 8](#_Toc53387273)

[1.5 Concrete beheersmaatregelen in het toetsingskader 8](#_Toc53387274)

[1.6 Toelichting op de hoofdstukken 9](#_Toc53387275)

[2. Toepassing Toetsingskader Informatiebeveiliging (cluster 1 t/m 6) bij privacy 10](#_Toc53387276)

[2.1 Toelichting toetsingskader 10](#_Toc53387277)

[2.2 Clustering naar thema’s 10](#_Toc53387278)

[2.3 Generieke statements (informatiebeveiliging) met een specifiek belang voor de privacy: 11](#_Toc53387279)

[3. Toetsingskader Privacy 15](#_Toc53387280)

[3.1 Aanvullende statements privacy 15](#_Toc53387281)

[3.2 Uitwerking aanvullende statements privacy 19](#_Toc53387282)

[P.1: Privacybeleid 19](#_Toc53387283)

[P.2: Functionaris Gegevensbescherming 21](#_Toc53387284)

[P.3: Rechtmatige verwerking van persoonsgegevens 23](#_Toc53387285)

[P.4: Register van verwerkingsactiviteiten (dataregister) 25](#_Toc53387286)

[P.5: Bewaartermijnen 27](#_Toc53387287)

[P.6: Verwerking t.b.v. onderzoek 29](#_Toc53387288)

[P.7: Verwerking van bijzondere persoonsgegevens 31](#_Toc53387289)

[P.8: Geautomatiseerde besluitvorming 33](#_Toc53387290)

[P.9: Informatiebeveiliging 35](#_Toc53387291)

[P.10: Verwerkersovereenkomsten 37](#_Toc53387292)

[P.11: Transparant over privacy 39](#_Toc53387293)

[P.12: Informeren over verwerkingen 41](#_Toc53387294)

[P.13: Procedures rechten van de betrokkenen 43](#_Toc53387295)

[P.14: Geheimhouding 45](#_Toc53387296)

[P.15: Bewustzijn, opleiding en training ten aanzien van privacy 47](#_Toc53387297)

[P.16: Bewijs van vernietiging persoonsgegevens 49](#_Toc53387298)

[P.17: Dataclassificatie 51](#_Toc53387299)

[P.18: Datalekken en beveiligingsincidenten 53](#_Toc53387300)

[P.19: Bijzondere persoonsgegevens 55](#_Toc53387301)

[P.20: Privacy by design en privacy by default 56](#_Toc53387302)

[P.21: Data Protection Impact Assessment (DPIA) 58](#_Toc53387303)

[P.22: Controle naleving beleid 60](#_Toc53387304)

[P.23: Rapportage van privacy gebeurtenissen 62](#_Toc53387305)

[P.24: Gebeurtenissen registreren 63](#_Toc53387306)

[Bijlage 1: Framework 2.0 informatiebeveiliging en privacy in het mbo 64](#_Toc53387307)

# Inleiding

## Uitgangspunt is het Privacy Compliance kader[[1]](#footnote-2)

Privacy is een thema dat door de digitalisering van de maatschappij, de populariteit van sociale media en niet te vergeten de nieuwe Europese wetgeving in deze, meer leeft dan ooit. Er wordt steeds meer informatie met elkaar gedeeld en dit roept vragen op over wat wel of niet verstandig is. Ook in het onderwijs is te merken dat ICT steeds vaker wordt ingezet in het onderwijs, zowel bij het leren als bij de analyse van resultaten bijvoorbeeld. Maar ook in de secundaire processen zoals bij de deelnemersadministratie of onderwijslogistiek. Het toenemend opslaan en verzamelen van informatie over deelnemers, maakt dat er ook meer aandacht moet zijn voor privacy en informatiebeveiliging.

Willen onderwijsinstellingen[[2]](#footnote-3) in de toekomst gebruik blijven maken van gegevens, én willen deelnemers (en docenten) ook nog gegevens met instellingen blijven delen, dan moet er een goed samenspel zijn tussen:

1. de interactie met deelnemers en docenten;

2. de interactie met de betrokken partijen (zoals instellingen en hun leveranciers);

3. de gebruikte middelen (de gegevens).

Dit noemen we samen het digitale ecosysteem: partijen en middelen zijn van elkaar afhankelijk om in balans te komen. Bij een datalek, is er - spreekwoordelijk - sprake van vervuiling en een verstoring van die balans. Het lek moet worden gedicht, de vervuiling wordt zo veel mogelijk verwijderd, maatregelen worden genomen om herhaling te voorkomen en met betrokkenen wordt gebouwd aan het vertrouwen om te voorkomen dat een nieuw lek opnieuw plaatsvindt.

Het zorgvuldig omgaan met gegevens is (wettelijk) de verantwoordelijkheid van onderwijsinstellingen zelf. Zij kunnen dit niet afwentelen op bijvoorbeeld hun leveranciers. Door het toegenomen gebruik van ICT in het onderwijs, en de toenemende mogelijkheden daarvan, komt de noodzaak voor informatiebeveiligingsbeleid en privacy steeds vaker in beeld. De bescherming van privacy en daarmee samenhangende gegevens wordt steeds belangrijker voor mbo-instellingen.

In de publicatie [“Privacy compliance kader” (IBPDOC2B)](https://www.sambo-ict.nl/netwerken/informatiebeveiliging/framework-ibp/) worden de uitgangspunten en principes van privacy beschreven. De principes zijn daarin vertaald naar normen voor een juiste handhaving van de privacy, het privacy normenkader. Daarin staat het doel van privacy centraal (het ‘wat’ en ‘waarom’). De manier om dat doel te bereiken (het ‘hoe’) wordt in dit document beschreven. Hierbij worden de normen vertaald naar concrete maatregelen, statement genoemd, die voor de instellingen handvatten zijn om de privacy voor deelnemers en medewerkers te kunnen garanderen. De privacy statements zijn op dezelfde wijze vormgegeven als de statements uit het normenkader informatiebeveiliging. In dit toetsingskader staat bij ieder statement genoemd aan welk bovenliggend basis privacy principe wordt voldaan.

Een onderwijsinstelling kan op verschillende manieren voldoen aan de statements. Om dat op uniforme wijze meetbaar te maken, wordt er een evidence (bewijslast) gekoppeld aan ieder statement. Deze evidence bestaat uit maatregelen die een instelling in meer- of mindere mate genomen moet hebben om aan het statement te voldoen. In dit toetsingskader worden de maatregelen beheersmaatregelen genoemd. De niveaus waarop voldaan kan worden aan de maatregelen worden volwassenheidsniveaus (maturity levels) genoemd.

## Update Toetsingskader Privacy, augustus 2019

Dit toetsingskader gaat uit van de vastgestelde Nederlandse vertaling van de AVG zoals opgenomen in het Publicatieblad van de Europese Unie van 4 mei 2016. De officiële benaming is “*Verordening EU 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)*[[3]](#footnote-4). In de periode tussen 25 mei 2016 en 25 mei 2018 hebben organisaties de tijd en gelegenheid gekregen om te voldoen aan de AVG. In de praktijk is gebleken dat veel mbo-instellingen in het voorjaar van 2018 hard aan de slag zijn gegaan met de AVG.

Het Toetsingskader Privacy is drie keer gebruikt voor een Benchmark (2016, 2017 en 2018). In 2018 is de AVG volledig in werking getreden. Er is sinds de eerste versie van het toetsingskader privacy veel ervaring opgedaan met de AVG, dit kader en met diverse praktijkvoorbeelden en casuïstiek. Het bleek nuttig en zinvol om het toetsingskader daaraan aan te passen. Dat is versie 3.0 geworden die voor u ligt. Daarbij is als uitgangspunt gehanteerd dat er zoveel mogelijk wordt aangesloten bij het bestaande toetsingskader en de gehanteerde systematiek, waarbij wijzigingen alleen worden doorgevoerd indien deze noodzakelijk zijn. Dat is gelukt.

Vanuit het oogpunt dat onderwijsinstellingen privacy bewustere organisaties moeten worden, betekent de AVG op hoofdlijnen dat de baseline voor privacy beheersmaatregelen gemiddeld *boven* de 2 zou moeten liggen. Bij de benchmark 2018 bleek de gemiddelde waarde voor het mbo (nog) op 2.3 te liggen. Het ambitieniveau voor de benchmark 2019 ligt op 3.

Deze update is vooral een aanpassing op de formulering van de statements en de bijbehorende bewijslast (evidence) met als doel die helderder en eenduidiger te maken. Dat komt de kwaliteit van privacy binnen onderwijsinstellingen ten goede, wat terug te zien zal zijn in de benchmark – zo is de verwachting.

De volgende concrete wijzigingen zijn doorgevoerd:

* De terminologie sluit aan bij de teksten, toepassing en interpretaties van de AVG.
* Waar mogelijk wordt de gehanteerde systematiek van de update van het Toetsingskader Informatiebeveiliging versie 4.0 overgenomen.
* Dat betekent onder andere dat bij de bewijslast alleen de niveaus 2 en 3 zijn uitgewerkt. Niveau 1 is ad hoc en behoeft geen nadere omschrijving (er is niet of ad hoc geregeld). Niveau 4 gaat uit van de evidence op niveau 3, maar dan opgenomen in een pdca-cyclus. En niveau 5 gaat dan uit van niveau 4 met een goedkeurende verklaring van een externe deskundige.
* Er zijn drie statements geschrapt. Deze hadden te veel overlap met informatiebeveiligings-statements; in de praktijk bleken deze andere statements voldoende om privacy te regelen.
* Naast de beschrijvingen van de statements en bewijslast in dit document is ook een spreadsheet ontwikkeld met alle statements en bewijslast. Dat blijkt voor velen een handiger manier om met de statements te werken dan de Word versie. Het spreadsheet is opgenomen in het Framework 2.0

## Informatiebeveiliging en privacy

Privacy is het topje van de, juridische, ijsberg. Er is veel samenhang tussen de handhaving van privacy en het informatiebeveiligingsbeleid. Sterker nog, geen privacy zonder informatiebeveiliging en andersom. In de statements van IB staat expliciet dat aan privacy moet worden gewerkt (statement 1.20) en andersom staat in het privacy normenkader expliciet dat de informatiebeveiliging op orde moet zijn (statement P9).

De normen en statements voor informatiebeveiliging zijn in zes clusters ondergebracht, voor privacy zijn aanvullende statement in een cluster 7 opgenomen. Het bijgaande plaatje is daarom wel illustratief voor de samenhang tussen privacy en informatiebeveiliging.



**Voorbeeld:**

Om de samenhang tussen informatiebeveiliging en privacy weer te geven is een voorbeeld wellicht handig:

*Het College van Bestuur van een mbo-instelling wil graag de mogelijkheid laten onderzoeken om tijdens ziekte van een medewerker zijn/haar onderwijs gerelateerde mail te mogen gebruiken. De mail omgeving is eigendom van de mbo-instelling*.

Vanuit de privacywetgeving is dit niet toegestaan. Een oplossing is om aan de OR een voorstel voor te leggen waarbij gegarandeerd wordt dat binnen de e-mail omgeving door de medewerker een map “Privé” wordt aangemaakt. Deze map zal nooit bekeken worden, ook niet tijdens langdurige ziekte van een medewerker. De overige e-mails mogen wel - onder strikte voorwaarden - bekeken worden. Als de OR (op basis van WOR, artikel 27, lid k) hiermee akkoord gaat, dan kan dit beleid worden geeffectueerd. Vervolgens moeten er vanuit informatiebeveiligingsaspecten enkele dingen geregeld worden:

Beleid: Er moet een beleid “e-mail inzage” worden voorgelegd aan de OR en na instemming is dit een aanvulling op de arbeidsovereenkomst.

Personeel: Personeel en externen moeten worden geïnformeerde en eventueel getraind.

Toegang: De fysieke toegang tot de exchange server (e-mail) moet goed geregeld zijn om de privacy te waarborgen.

Continuïteit: Tijdens grote verstoringen moet de e-mail omgeving veilig opgeslagen zijn en eventueel d.m.v. een back up teruggeplaatst worden.

Applicaties: De toegang tot de e-mail omgeving (applicatie toegang) is alleen voorbehouden aan de eigenaar en in een noodsituatie aan de applicatie beheerder die toegang heeft en kan verschaffen tot de e-mail van een medewerker (behalve de Privé-map).

Logging: De eigenaar van de e-mail moet te allen tijde kunnen controleren wie er toegang heeft gehad tot zijn e-mails. Ook moet hij kunnen controleren dat de Privé-map niet is bekeken.

En los van deze punten, moet de mailomgeving uiteraard ook voldoen aan overige wet- en regelgeving en informatiebeveiliging.

## Samenhang tussen informatiebeveiliging en privacy

Uitgangspunt voor de informatiebeveiliging is het ISO-normenkader 27001/27002. Dat is de basis voor het kader dat in het onderwijs wordt gebruikt. Bij de update van het mbo-toetsingskader IB is besloten om het gehele ISO-kader te hanteren wat een set van ***108*** normen en statements oplevert. Dit is geheel uitgewerkt in het betreffende [Toetsingskader Informatiebeveiliging IBPDOC3.](https://www.sambo-ict.nl/netwerken/informatiebeveiliging/framework-ibp/#actueel) In principe geldt dat de gehele informatiebeveiliging op orde moet zijn om de privacy ook te kunnen garanderen. Er zijn daarin echter wel specifieke aandachtpunten te benoemen. Zo is er een subset uit het toetsingskader informatiebeveiliging gehaald die vooral aandacht behoeven als het gaat om de privacy.

Deze subset van ***36*** statements is uit het algemene normenkader IB gelicht en in dit document in hoofdstuk 2 weergegeven. De statements zijn voorzien van een toelichting over de samenhang met privacy. Het spreekt voor zich dat bij de monitoring van de privacy in een instelling met name ook naar deze IB-statements gekeken moet worden en dat het ambitieniveau voor deze statements wellicht ook wat hoger moet worden gezet op bijvoorbeeld een niveau 3 of zelfs 4 in het komende jaar.

**Informatiebeveiliging**

**ISO 27002 (114 normen)**

**IB mbo/ho**

**Normenkader: 108 statements**

**Privacy**

**AVG (99 artikelen)**

**Privacy in het mbo**

**Compliance kader: 21 statements**

**Gemeenschappelijk**

**Normenkader: 36 statements**

Maar naast deze statements op basis van het generieke informatiebeveiligingskader (gemeenschappelijk, zie afbeelding) was er ook de noodzaak om een set van aanvullende statements voor privacy op te stellen op basis van de betreffende wet- en regelgeving. Dit heeft aanleiding gegeven tot het opstellen van een compleet compliance kader privacy voor het mbo-onderwijs. Dit is een veelomvattende en uitgebreide set geworden met ***21*** specifieke privacy statements die hierin zijn opgenomen. Dat waren er dus 24 in de eerste versie van het normen- en toetsingskader privacy. Deze statements zijn opgenomen in een apart document: IBPDOC2b Compliance kader privacy voor het mbo. Dit juridisch normenkader, wat het in feite is, ligt ten grondslag aan het toetsingskader privacy IBPDOC7 dat in dit document wordt uitgewerkt. De aanvullende statements voor privacy zijn weergegeven in hoofdstuk 3.

## Concrete beheersmaatregelen in het toetsingskader

Het compliance kader privacy is de basis voor het inrichten van de informatiebeveiliging omtrent de privacy en het is tevens de basis voor het voorliggende toetsingskader privacy. Door aan de statements uit het compliance kader privacy een korte beschrijving, alsmede de evidence toe te voegen is het toetsingskader privacy mbo ontstaan. De evidence wordt op vijf verschillende volwassenheidsniveau ’s weergegeven, net als bij het generieke toetsingskader Informatiebeveiliging. De bewijslast is alleen voor de niveaus 2 en 3 beschreven. Voor niveau 1 is dat niet nodig (ad-hoc, er is geen bewijslast voor dit laagste niveau). Voor niveau 4 geldt dat dit hetzelfde is als niveau 3 maar dan geborgd in een jaarlijkse pdca-cyclus. Niveau 5 is gelijk aan niveau 4 maar dan voorzien van een externe verklaring. Die laatste twee behoeven dus geen beschrijving op statement niveau.

Het toetsingskader privacy mbo is bedoeld om onderwijsinstellingen een kader en handvatten te bieden om de informatiebeveiliging rondom privacy te regelen. Door het hanteren van de verschillende niveaus kan er een beeld van de reële situatie gemaakt worden (het bereikte niveau), als mede een streef- of ambitieniveau waaraan de instelling in de (nabije) toekomst wil gaan voldoen. Het toetsingskader wordt ook gebruikt om de Benchmark IBP in het mbo op te stellen. Dit laat sector breed goed zien wat de ontwikkelingen zijn.

## Toelichting op de hoofdstukken

Hoofdstuk 1 geeft een algemene inleiding op het privacy cluster en gaat in op de samenhang tussen informatiebeveiliging en privacy.

Hoofdstuk 2 geeft een opsomming, per cluster (1 t/m 6), van statements uit het toetsingskader Informatiebeveiliging (IBPDOC3) die relevant zijn in het kader van privacy compliance. Dit zijn dus beheersmaatregelen gericht op informatiebeveiliging, die ook relevant zijn om privacy goed te regelen.

Hoofdstuk 3 geeft een opsomming van de aanvullende privacy statements (cluster 7).

# Toepassing Toetsingskader Informatiebeveiliging (cluster 1 t/m 6) bij privacy

## Toelichting toetsingskader

De statements in het normen- en toetsingskader privacy bestaan uit statements vanuit het toetsingskader ibp mbo en statements vanuit het compliance kader privacy. In dit hoofdstuk zijn de statements weergegeven uit het generieke ibp toetsingskader met die aantekening dat die dus in het kader van de privacy extra aandacht behoeven.

## Clustering naar thema’s

De update van het Toetsingskader Informatiebeveiliging mbo bevat ***101*** statements, waarvan ***36* heel direct** gerelateerd zijn aan privacy, verdeeld over 6 clusters. De clustering is gebaseerd op een logische indeling die goed bruikbaar is voor het mbo-onderwijs. De clustering is tevens toegepast op de statements afkomstig van de wet en regelgeving privacy.

**Schematische samenvatting clustering:**

|  |  |  |  |
| --- | --- | --- | --- |
| Cluster | Onderwerpen (o.a.) | Kwaliteitsaspecten | Betrokkenen |
| Beleid en OrganisatiePrivacy maakt gebruik van 10 van de 24 statements. | InformatiebeveiligingsbeleidClassificatieInrichten beheerCryptografie | BeschikbaarheidIntegriteitVertrouwelijkheidControleerbaarheid | College van bestuurDirecteuren |
| Personeel, deelnemers en gastenPrivacy maakt gebruik van 5 van de 10 statements. | InformatiebeveiligingsbeleidAanvullingen arbeidsovereenkomstScholing en bewustwording | VertrouwelijkheidIntegriteit | College van bestuurDienst HROndernemingsraad |
| Ruimte en ApparatuurPrivacy maakt gebruik van 1 van de 20 statements. | Beveiligen van hardware, devices en bekabeling | BeschikbaarheidVertrouwelijkheid | College van bestuurDienst ICT of afdeling |
| ContinuïteitPrivacy maakt gebruik van 3 van de 17 statements. | Anti-virussen, back up, bedrijfscontinuïteit planning | Beschikbaarheid | College van bestuurDienst ICT of afdelingfunctioneel beheer |
| Toegangsbeveiliging en IntegriteitPrivacy maakt gebruik van 13 van de 19 statements. | Gebruikersbeheer, wachtwoorden, online transacties, cryptografisch sleutelbeheer, validatie | IntegriteitVertrouwelijkheid | College van bestuurDienst ICT of afdeling functioneel beheer |
| Controle en loggingPrivacy maakt gebruik van 4 van de 11 statements. | Systeemacceptatie, loggen van gegevens, registreren van storingen, toetsen beleid | Controleerbaarheid | College van bestuurStafmedewerker informatiebeveiligingKwaliteitszorg  |

Voor een afdoende risicobeheersing t.a.v. informatiebeveiliging en privacy binnen een onderwijsinstelling moeten alle ***101*** statements op orde zijn. Daarbij zou dan uitgegaan moeten worden van een minimum volwassenheidsniveau 2 voor de maatregelen om aan het statement te voldoen. Dat wil zeggen opzet, bestaan en gedeeltelijke werking (een aantal collega’s werkt volgens de afspraak maar nog niet de gehele organisatie. Voor een aantal van de privacy gelieerde statements zou niveau 3 of 4 van toepassing zijn om de privacy risico’s voldoende te mitigeren. Deze statements zijn hieronder weergegeven.

## Generieke statements (informatiebeveiliging) met een specifiek belang voor de privacy:

**Cluster beleid en organisatie**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **1.1** | **5.1.1** | **Beleidsregels voor informatiebeveiliging**: Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur |
| Informatiebeveiliging is een belangrijke randvoorwaarde voor bescherming van de privacy van betrokkenen. Een en ander moet tot uitdrukking komen in de doelstellingen, verantwoordelijkheden en processen die de organisatie daarvoor heeft ingericht. Een compleet en actueel informatiebeveiligings- en privacybeleid (IBP) is daarvoor een belangrijke voorwaarde. |
| **1.5** | **6.1.5** | **Informatiebeveiliging in projectbeheer:** Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project. |
| Privacy by design is een belangrijk uitgangspunt van de AVG en het is daarom belangrijk om bij de initiatie van projecten de check op privacyaspecten mee te nemen. |
| **1.6** | **6.2.1** | **Beleid voor mobiele apparatuur**: Er dient beleid te worden vastgesteld om de risico’s die het gebruik van mobiele apparatuur met zich meebrengt te beheren. |
| Er worden veel persoonsgegevens verwerkt op mobiele apparatuur, ook in de thuissituatie. In het beleid moet de beveiliging van deze toepassingen en devices speciale aandacht krijgen. |
| **1.7** | **8.2.1** | **Classificatie van informatie**: Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging. |
| De AVG eist dat de organisatie in control is op het gebied van de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens. De (BIV-)classificatie is belangrijk voor het bepalen van de te nemen maatregelen om de privacy van betrokkenen te beschermen. |
| **1.8** | **8.2.2** | **Informatie labelen**: Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie. |
| Voor een adequate bescherming van (bijzondere) persoonsgegevens is het belangrijk om deze goed als zodanig te kunnen identificeren. Goed bijgewerkte dataregisters spelen een belangrijke rol daarbij. |
| **1.9** | **10.1.1** | **Beleid inzake het gebruik van crypto grafische beheersmaatregelen:** Ter bescherming van informatie behoort een beleid voor het gebruik van crypto grafische beheersmaatregelen te worden ontwikkeld. |
| Om in een open omgeving als een onderwijsorganisatie op een veilige manier met persoonsgegevens te kunnen werken, is encryptie van deze gegevens een belangrijke voorwaarde. |
| **1.15** | **15.1.2** | **Opnemen van beveiligingsaspecten in leveranciersovereenkomsten:** Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt. |
| Voor de bescherming van de privacy van betrokkenen is het belangrijk dat externe partijen zich bewust zijn van hun verantwoordelijkheid/aansprakelijkheid en dat zij daaraan gehouden kunnen worden. |
| **1.18** | **16.1.2** | **Rapportage van informatiebeveiligingsgebeurtenissen:** Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. |
| De impact kan aanzienlijk worden beperkt door een tijdige reactie. Een belangrijk privacy-aspect is de tijdige beoordeling/reactie op datalekken. |
| **1.19** | **18.1.3** | **Beschermen van registraties**: Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave. |
| Het classificeren van informatie is een belangrijke voorwaarde om passende beschermingsniveaus en bewaartermijnen te kunnen inregelen. |
| **1.20** | **18.1.4** | **Privacy en bescherming van persoonsgegevens**: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.**Dit statement is de verbindende schakel tussen informatiebeveiliging en privacy. IB is een wettelijke eis om zorgvuldig met persoonsgegevens om te gaan.** |
| Bescherming van privacy wordt in samenhang met het informatiebeveiligingsbeleid geregeld, bij voorkeur in de vorm van een IBP-beleid. |

**Personeel, studenten en gasten**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **2.1** | **7.1.2** | **Arbeidsvoorwaarden**: De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden. |
| Bovenstaande geldt ook ten aanzien van de bescherming van de privacy van betrokkenen. |
| **2.2** | **7.2.2** | **Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging:** Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. |
| Goede training is van groot belang voor de correcte omgang met persoonsgegevens. |
| **2.3** | **9.2.6** | **Toegangsrechten intrekken of aanpassen:** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast. |
| Aandachtspunt in relatie tot privacy (AVG) is dat medewerkers uitsluitend toegang behoren te hebben tot persoonsgegevens die uit hoofde van hun functie/rol strikt noodzakelijk zijn. Actuele en fijnmazige autorisatie is daarvoor een voorwaarde. |
| **2.4** | **11.2.9** | **‘Clear desk’- en ‘clear screen’-beleid**: Er behoort een ‘clear desk’-beleid voor papieren documenten en verwijderbare opslagmedia en een ‘clear screen’-beleid voor informatie verwerkende faciliteiten te worden ingesteld. |
| Vanwege het open karakter van een schoolorganisatie in combinatie met de vertrouwelijkheid van persoonsgegevens is naleving van het ‘clear desk’- en ‘clear screen’-beleid een belangrijk aandachtspunt. |
| **2.5** | **13.2.4** | **Vertrouwelijkheids- of geheimhoudingsovereenkomst:** Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd. |
| Voor geheimhouding kan verwezen worden naar de cao. Daarnaast kan er gebruik worden gemaakt van pre-screening, VOG en/of functioneringsgesprekken. Let op dat voor externe medewerkers en gasten aparte overeenkomsten gemaakt dienen te worden. |

**Ruimtes en apparatuur**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **3.14** | **11.2.7** | **Veilig verwijderen of hergebruiken van apparatuur:** Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven. |
| Opslagmedia kunnen bestanden met (gevoelige/bijzondere) persoonsgegevens bevatten, vanuit privacy-oogpunt is de controle hierop van groot belang. |

**Continuïteit**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **4.5** | **12.3.1** | **Back-up van informatie:** Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt.  |
| Uit oogpunt van beschikbaarheid, integriteit verdient het regelmatig back-uppen van informatie speciale aandacht. In verband met vertrouwelijkheid dient daarbij gezorgd te worden voor beveiligde opslag. |
| **4.13** | **16.1.5** | **Respons op informatiebeveiligingsincidenten:** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures. |
| Informatiebeveiligingsincidenten kunnen grote gevolgen hebben voor de bescherming van de privacy van gebruikers binnen de organisatie. Als er bij ernstige incidenten persoonsgegevens in het geding zijn moet er worden gehandeld naar de procedure datalekken. |
| **4.14** | **17.1.2** | **Informatiebeveiligingscontinuïteit implementeren:** De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen. |
| Tijdens een crisis (waaronder een cybercrisis) verdient de bescherming van persoonsgegevens extra aandacht. |

**Vertrouwelijkheid en integriteit**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **5.1** | **9.1.1** | **Beleid voor toegangsbeveiliging:** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. |
| De principes van de AVG vereisen een strikte toegangsbeveiliging op basis van het ‘need to know’-principe. |
| **5.2** | **9.1.2** | **Toegang tot netwerken en netwerkdiensten:** Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. |
| Ongeautoriseerde en onveilige verbindingen met netwerkdiensten vormen een bedreiging voor de privacy van betrokkenen. |
| **5.3** | **9.2.1** | **Registratie en afmelden van gebruikers:** Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. |
| Ongeautoriseerde toegang vormt een bedreiging voor de privacy van betrokkenen. Een goed functionerend proces voor het beheren van gebruikersaccounts/toegangsrechten is daarvoor cruciaal. |
| **5.4** | **9.2.2** | **Gebruikers toegang verlenen:** Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. |
| Ongeautoriseerde toegang vormt een bedreiging voor de privacy van betrokkenen. Een goed functionerend proces voor het beheren van gebruikersaccounts/toegangsrechten is daarvoor cruciaal. |
| **5.5** | **9.2.3** | **Beheren van speciale toegangsrechten:** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst. |
| **Privacy toets:** het betreft hier de super users / administrators rechten. |
| **5.6** | **9.2.4** | **Beheer van geheime authenticatie-informatie van gebruikers:** Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces. |
| Als accounts met speciale toegangsrechten worden misbruikt, door de gebruiker van het account, of iemand die onbevoegd toegang heeft verkregen, dan kan dit grote gevolgen hebben voor de privacy van betrokkenen. |
| **5.7** | **9.3.1** | **Geheime authenticatie-informatie gebruiken:** Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie informatie houden aan de praktijk van de organisatie. |
| Als een kwaadwillende gebruiker onbevoegd toegang krijgt door het compromitteren van een gebruikersaccount dan kan dit grote gevolgen hebben voor de privacy van betrokkenen. |
| **5.8** | **9.4.1** | **Beperking toegang tot informatie:** Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging. |
| De principes van de AVG schrijven voor dat er niet meer informatie mag worden gedeeld dan strikt noodzakelijk voor het uitvoeren van de werkzaamheden. |
| **5.9** | **9.4.2** | **Beveiligde inlogprocedures:** Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure. |
| Als een kwaadwillende gebruiker onbevoegd toegang krijgt door het compromitteren van een gebruikersaccount dan kan dit grote gevolgen hebben voor de privacy van betrokkenen. |
| **5.10** | **10.1.2.1** | **Sleutelbeheer:** Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld. |
| Door gebruik te maken van versleuteling van gegevens worden zowel de kans als de impact van een incident waarbij persoonsgegevens worden gelekt beperkt. |
| **5.12** | **12.4.2** | **Beschermen van informatie in logbestanden:** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. |
| In het geval van een datalek is het belangrijk dat er logbestanden aanwezig zijn om de oorzaak, achtergronden en impact van het incident te kunnen onderzoeken en daarover verantwoording af te kunnen leggen. |
| **5.16** | **13.2.3** | **Elektronische berichten**: Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd |
| Als gevoelige informatie wordt verstuurd via (bijvoorbeeld) e-mail dan moeten deze berichten beschermd worden tegen onbevoegde toegang. |
| **5.27** | **13.2.3** | **Bescherming van testgegevens:** Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd. |
| Bij het testen van systemen waarbinnen persoonsgegevens worden verwerkt moet extra aandacht zijn voor het beschermen van deze gegevens. |

**Controle en logging**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **6.1** | **9.2.5** | **Beoordeling van toegangsrechten van gebruikers:** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. |
| Het correct toekennen van autorisaties is een belangrijke voorwaarde voor goede bescherming van vertrouwelijke gegevens, zeker als het gaat om speciale toegangsrechten. |
| **6.2** | **12.4.1** | **Gebeurtenissen registreren:** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. |
| Goede logbestanden zijn een voorwaarde om onderzoek te kunnen doen naar de aanleiding, achtergronden en de impact van informatiebeveiligingsgebeurtenissen zoals datalekken. |
| **6.9** | **18.2.2** | **Naleving van beveiligingsbeleid en –normen:** Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging. |
| Voor een goede bescherming van de privacy is de controle op naleving cruciaal en dit dient daarom belegd te zijn op managementniveau. |
| **6.10** | **18.2.3** | **Beoordeling van technische naleving:** Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging. |
| Voor een goede bescherming van de privacy moet de beveiliging van de informatiesystemen op orde zijn en regelmatig worden beoordeeld. |

# Toetsingskader Privacy

ISO 27001 en 27002, de Code voor Informatiebeveiliging, beschrijft weliswaar alle voorkomende risico’s op het gebied van informatiebeveiliging, maar alleen op een generieke manier. De Code is niet opgesteld om alle risico’s die samenhangen met privacy te verminderen. Weliswaar wordt een flink deel van de risico’s afgedekt maar niet alle. In dit hoofdstuk benoemen we alle *aanvullende* statements die vanuit het complete compliance kader privacy zijn geselecteerd. Zoals aangegeven zijn die op dezelfde wijze gerangschikt als de generieke statements.

In de rechter kolom wordt vermeld van welk privacy principe het statement is afgeleid.

Bij de update van het toetsingskader privacy in augustus 2019 zijn drie statements van de oorspronkelijke 24 statements vervallen (P.19, P.23 en P.24). Er zijn nog ***21*** statements over.

## Aanvullende statements privacy

**Beleid en organisatie**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Statement** | **Principe** |
| **P.1** | [**Privacybeleid:**](#_P.1:__Privacy-beleid)De instelling moet een voor de organisatie passend niveau van privacy en gegevensbescherming bereiken en houden. Hiertoe wordt een passend privacy- en gegevensbeschermingsbeleid opgesteld, goedgekeurd en beheerd. Hierin zijn de taken, bevoegdheden en verantwoordelijkheden eenduidig belegd. | 5) TransparantieAVG art: 5, 25 |
| **P.2** | [**Functionaris Gegevensbescherming:**](#_P.2:__Functionaris)De instelling benoemt een functionaris voor gegevensbescherming (FG) die is belast met toezicht op de verwerkingen van persoonsgegevens binnen de instelling. De instelling zorgt er voor dat alle andere werkzaamheden van de FG verenigbaar zijn met zijn taken en verplichtingen als FG en dat die niet tot een belangenconflict leiden. De aangewezen FG wordt intern en extern bekend gemaakt. | 9) VerantwoordelijkheidAVG art: 24, 37 |
| **P.3** | [**Rechtmatige verwerking van persoonsgegevens**](#_P.3:_Rechtmatige_verwerking)De instelling draagt er zorg voor dat bij verwerking van persoonsgegevens de volgende uitgangspunten worden gehanteerd: P.3a Doelbepaling en doelbinding: voor iedere categorie van verwerkingen wordt – voorafgaand aan die verwerking - een specifiek doeleinde vastgesteld, en dit doeleinde is gecommuniceerd bij de gegevensverzameling. De instelling zorgt er voor dat persoonsgegevens alleen worden verwerkt voor het doeleinde waarvoor die gegevens verkregen zijn.P.3b Grondslag (rechtmatigheid): de instelling zorgt er voor dat persoonsgegevens altijd op basis van een in de AVG genoemde grondslag worden verwerkt. Indien toestemming noodzakelijk is voor verwerkingen van persoonsgegevens van deelnemers jonger dan 16 jaar, dan wordt toestemming altijd afgestemd met de wettelijke vertegenwoordigers. Verkregen toestemming wordt vastgelegd en is reproduceerbaar. P.3c Dataminimalisatie: het verwerken van persoonsgegevens moet noodzakelijk voor het behalen van het onder P.3a benoemde doel. De inbreuk op de privacy van betrokkene moet te rechtvaardigen zijn om het doeleinde te bereiken (proportionaliteit), de te verzamelen persoonsgegevens blijven beperkt tot datgene wat minimaal nodig is om de doeleinde(n) te bereiken (subsidiariteit). P.3d Transparantie: de instelling informeert de gebruikers (of hun wettelijke vertegenwoordigers) en medewerkers van wie persoonsgegevens worden verwerkt, beknopt, transparant, eenvoudig toegankelijk en in begrijpelijke taal over het beleid alsmede over alle gegevensverwerkingen. P.3e Data-integriteit: de verantwoordelijke gaat zorgvuldig om met de verwerkte persoonsgegevens en waarborgt het behoud en bescherming van de juistheid en de consistentie van die gegevens. | 2) Doel en doelbinding3) Grondslag4) Dataminimalisatie 5) Transparantie8) Data-integriteitAVG art: 5, 6, 12 |
| **P.4** | [**Register van verwerkingsactiviteiten (dataregister):**](#_P.4:_Register_van)Alle verwerkingen van persoonsgegevens binnen of door de instelling zijn opgenomen in een of meerdere dataregisters.  | 9) VerantwoordelijkheidAVG art: 30, 39 |
| **P.5** | [**Bewaartermijnen:**](#_P.5:_Bewaartermijnen)Er is een actief beleid omtrent het bewaren, archiveren en vernietigen van persoonsgegevens. Persoonsgegevens worden niet langer verwerkt dan nodig voor het gestelde doeleinde. De instelling stelt op basis van de Archiefwet (waaronder het BSD valt) de vernietigings- en bewaartermijnen vast van de verwerkte persoonsgegevens en neemt deze termijnen op in het dataregister**.** | 4) DataminimalisatieAVG art: 5, 30 |

|  |  |  |
| --- | --- | --- |
| **P.6** | [**Verwerking t.b.v. onderzoek**](#_P.6:_Verwerking_t.b.v.)Persoonsgegevens mogen worden verwerkt ten behoeve van: a) archivering in het algemeen belang (Archiefwet);b) wetenschappelijk of historisch onderzoek; of c) statistische doeleindenindien passende technische en organisatorische maatregelen zijn genomen om de privacy van de betrokken deelnemers te garanderen. Onder deze maatregelen wordt in ieder geval verstaan dat er niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk is. Hierbij valt te denken aan pseudonimisering (in geval de data herleidbaar moet zijn tot individuen) of anonimisering (in geval data niet herleidbaar hoeft te zijn). Bij historische, statistische of wetenschappelijke doeleinden is verwerking alleen mogelijk op basis van strikte voorwaarden vergelijkbaar met de ‘Gedagscode voor Onderzoek & Statistiek’ en het bevoegd gezag voorafgaand toestemming heeft verleend. | 2) Doel en doelbindingAVG art: 89 |
| **P.7** | [**Verwerking van bijzondere persoonsgegevens:**](#_P.7:_Verwerking_van)De instelling verwerkt geen bijzondere persoonsgegevens, uitgezonderd:• iemands religieuze of levensbeschouwelijke overtuigingen voor zover dit nodig is gelet op het doel van de instelling en voor de verwezenlijking van haar grondslag strikt noodzakelijk is,• ras of etnische afkomst, voor zover de instelling daartoe op grond van een wet verplicht is, of alleen in met het doel om personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen om feitelijke nadelen verband houdende met de grond ras op te heffen of te verminderen,• biometrische gegevens (zoals vingerafdruk of irisscan) voor zover deze gebruikt worden met het oog op authenticatie of beveiligingsdoeleinden.• gezondheid of iemands seksueel gedrag of seksuele gerichtheid, voor zover dat met het oog op de speciale begeleiding van deelnemers of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is, tenzij de deelnemer voor het gebruik van deze categorieën persoonsgegevens zelf toestemming heeft gegeven voor het verwerken van de hiervoor genoemde categorieën persoonsgegevens.  | 2) DataminimalisatieAVG art: 9 |
| **P.8** | [**Geautomatiseerde besluitvorming:**](#_P.8:__Geautomatiseerde)Bij verwerkingen van persoonsgegevens mogen geen volledig geautomatiseerde besluiten worden genomen (waaronder profilering) die voor de betrokkene rechtsgevolgen hebben of hem in aanmerkelijke mate treffen. | 2) Doel en doelbindingAVG art: 21, 22 |

|  |  |  |
| --- | --- | --- |
| **P.9** | [**Informatiebeveiliging**:](#_P.9:__Informatiebeveiliging) De instelling neemt organisatorische en technische beheersmaatregelen om een passend beveiligingsniveau te waarborgen van alle verwerkingen van persoonsgegevens. Hierbij let de instelling op de risico’s die de verwerking(en) met zich meebrengen, en met de aard en classificatie van de te beschermen persoonsgegevens. Bij de maatregelen wordt rekening gehouden met de stand van de techniek en de kosten van de uitvoering van de beheersmaatregelen. | 7) BeveiligingAVG art: 5, 32 |
| **P.10** | [**Verwerkersovereenkomsten**:](#_P.10:__Verwerkersovereenkomsten) De instelling schakelt voor de verwerking van persoonsgegevens voor of namens de instelling, uitsluitend leveranciers in als verwerker. Deze verwerker moet de onderwijsinstelling afdoende garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen, zodat de verwerking door verwerker aan de wet voldoet. De instelling legt afspraken met alle verwerkers vast in een verwerkersovereenkomst waarin aan alle relevante wettelijk vereiste onderdelen wordt voldaan. | 9) VerantwoordelijkheidAVG art: 28 |

**Personeel, studenten en gasten**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Statement** | **Principe** |
| **P.11** | [**Transparant over privacy:**](#_P.11:_Transparant_over)De instelling informeert de (ouders van) deelnemers en medewerkers van wie persoonsgegevens worden verwerkt, beknopt, transparant, eenvoudig toegankelijk en in begrijpelijke, duidelijke en eenvoudige taal over het privacy beleid en de rechten en verplichtingen van betrokkenen. | 5) TransparantieAVG art: 5, 12 |
| **P.12** | [**Informeren over verwerkingen:**](#_P.12:_Informeren_over)De instelling informeert deelnemers, hun ouders en medewerkers actief over de verwerking van hun persoonsgegevens, en wat de rechten van de betrokkenen en hoe die uitgeoefend kunnen worden. De informatie bevat ten minste de in de wet opgesomde informatie. | 5) TransparantieAVG art: 5, 13 |
| **P.13** | [**Procedures rechten van de betrokkenen:**](#_P.13:_Procedures_rechten) De instelling stelt procedures vast ten behoeve van de uitoefening van de rechten van betrokkenen.  | 6) Rechten betrokkeneAVG art: 12, 13, 15, 16, 17, 20 |
| **P.14** | [**Geheimhouding:**](#_P.14:_Geheimhouding)De instelling moet een geheimhoudingsplicht aan de medewerkers opleggen en erop toezien dat de medewerkers de geheimhoudingsplicht naleven. Met de functionarissen die uit hoofde van hun functie toegang hebben tot grote verzamelingen van bijzondere persoonsgegevens (van medewerkers en/of deelnemers) en/ of beschikken over verhoogde (beheer-)rechten ten aanzien van systemen waarin persoonsgegevens van medewerkers en deelnemers worden verwerkt, sluit de instelling een separate integriteits- en geheimhoudingsverklaring af. | 9) VerantwoordelijkheidAVG art: 9, 38, 90 |
| **P.15** | [**Bewustzijn, opleiding en training ten aanzien van privacy:**](#_P.15:_Bewustzijn,_opleiding) De instelling stimuleert het privacy bewustzijn van de medewerkers door training en scholing te bieden aan alle medewerkers, en door gebruik te maken van andere vormen van communicatie over privacy. | 5) TransparantieAVG art: 39 |

**Ruimte en apparatuur**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Statement** | **Principe** |
| **P.16** | [**Bewijs van vernietiging persoonsgegevens:**](#_P.16:_Bewijs_van)Van apparatuur die niet langer wordt gebruikt, worden de op het apparaat aanwezige persoonsgegevens op een betrouwbare en veilige wijze vernietigd. Van deze vernietiging en de wijze waarop, wordt een verklaring opgemaakt, of afgegeven door een derde die verantwoordelijk is voor de vernietiging. | 4) Dataminimalisatie7) BeveiligingAVG art: 5 |

**Vertrouwelijkheid en integriteit**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Statement** | **Principe** |
| **P.17** | [**Dataclassificatie:**](#_P.17:_Dataclassificatie)De instelling moet de kwaliteit van de gegevens (gegevenskwaliteit) borgen. Hiertoe heeft de instelling inzicht in de classificatie van persoonsgegevens. | 8) DatakwaliteitAVG art: 5, 32 |
| **P.18** | [**Datalekken en beveiligingsincidenten:**](#_P.18:_Datalekken_en)De instelling stelt een procedure vast voor het melden en afhandelen van datalekken en beveiligingsincidenten. In dit beleid is opgenomen dat een datalek zo snel mogelijk na ontdekking aan de toezichthouder en eventueel de betrokkene(n) wordt gemeld. Datalekken en beveiligingsincidenten worden opgenomen in een incidentenregister.  | 5) TransparantieAVG art: 33, 34 |
| **P.19** | [**Bijzondere persoonsgegevens:**](#_P.19:_Bijzondere_persoonsgegevens)**Vervallen**, maatregelen zijn vervat in P.7, P.9 en P.17. | 4) Beveiliging |

**Controle en Logging**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Statement** | **Principe** |
| **P.20** | [**Privacy by design en privacy by default:**](#_P.20:_Privacy_by)De instelling moet beleid opstellen en goedkeuren dat toeziet op de beginselen van privacy by design en privacy by default. | 4) Dataminimalisatie8) DatakwaliteitAVG art: 25 |
| **P.21** | [**Data Protection Impact Assessment (DPIA):**](#_P.21:_Data_Protection)De instelling voert Data protection Impact Assessments (GegevensBeschermingsEffectBeoordeling) uit om inzicht te krijgen in de privacyrisico's en om deze risico's zo veel mogelijk te mitigeren. Een DPIA wordt uitgevoerd in geval van: - nieuwe verwerkingen; - grote of ingrijpende wijzigingen in de bestaande verwerking van persoonsgegevens die specifiek de risico’s wijzigt voor de privacy van de betrokken deelnemers en medewerkers;- verwerking van grote hoeveelheden persoonsgegevens of bijzondere persoonsgegevens. | 2) Doel en doelbinding7) Doel en doelbinding8) DatakwaliteitAVG art: 25 |
| **P.22** | [**Controle naleving beleid:**](#_P.22:_Controle_naleving)De instelling moet de naleving van IBP beleid en - maatregelen intern en extern monitoren, beoordelen en evalueren. | 9) VerantwoordelijkheidAVG art: 5, 24, 32, 35, 39 |
| **P.23** | [**Rapportage van privacy gebeurtenissen**:](#_P.23:_Rapportage_van) **Vervallen**, deze maatregel is vervat in P.2, P.11, P.12, P.18 en cluster 1 statement 18. | 7) Beveiliging |
| **P.24** | [**Gebeurtenissen registreren:**](#_P.24:_Gebeurtenissen_registreren) **Vervallen**, deze maatregel is vervat in cluster 6 statement 2. | 5) Transparantie 9) Verantwoordelijkheid |

## Uitwerking aanvullende statements privacy

## P.1: Privacybeleid

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.1** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 5, 25** |
| **Controledoelstelling: Privacybeleid:**De instelling moet een voor de organisatie passend niveau van privacy en gegevensbescherming bereiken en houden. Hiertoe wordt een passend privacy- en gegevensbeschermingsbeleid opgesteld, goedgekeurd en beheerd. Hierin zijn de taken, bevoegdheden en verantwoordelijkheden eenduidig belegd. |
| **Toelichting:**De AVG verplicht de instelling om een passend gegevensbeschermingsbeleid te voeren en dat regelmatig te evalueren. Passend betekent dat er rekening wordt gehouden met de aard en omvang van de verwerkingen van persoonsgegevens binnen de instelling. Dit beleid moet leiden tot een passend niveau van privacy- en gegevensbescherming. Maak gebruik van het model-beleid als basis of referentie. |
| **Bewijsvoering:**Inhoudsopgave IBP-beleid: 1. Richtlijnen, 2. Governance, 3. Compliance, 4. Incidentenbeheer, 5. Bijlagen. |
| ❷Overleg het IBP-beleid, voorzien van versiebeheer, dat goedgekeurd is door het bevoegd gezag en de OR/studentenraad en/of (G)MR |
| ❸Overleg een printscreen van een internet-/intranetpagina waar (een link naar) het IBP-beleid staat. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.2: Functionaris Gegevensbescherming

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.2** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 24, 37** |
| **Controledoelstelling: Functionaris Gegevensbescherming**De instelling benoemt een functionaris voor gegevensbescherming (FG) die is belast met toezicht op de verwerkingen van persoonsgegevens binnen de instelling. De instelling zorgt er voor dat alle andere werkzaamheden van de FG verenigbaar zijn met zijn taken en verplichtingen als FG en dat die niet tot een belangenconflict leiden. De aangewezen FG wordt intern en extern bekend gemaakt. |
| **Toelichting:**De instelling moet een FG aanwijzen. De FG moet onafhankelijk kunnen handelen waartoe een reglement voor de FG wordt vastgesteld door het bevoegd gezag. Voor het overige: zie Handreiking FG. |
| **Bewijsvoering:**Er moet een FG aangewezen zijn die aan de wettelijke voorschriften voldoet. |
| ❷ Overleg het bestuursbesluit en de bevestiging van de aanmelding van de FG bij de AP waaruit blijkt dat een FG is aangewezen.❷ Overleg het door het bevoegd gezag vastgestelde reglement FG waaruit ten minste blijkt dat de FG onafhankelijk is, het bevoegd gezag adviseert en controleert op naleving van wet- en regelgeving rondom privacy. |
| ❸ Overleg een agenda, notulen of adviezen waaruit blijkt dat de FG overleg heeft gevoerd met het bevoegd gezag. ❸ Overleg een afschrift van het incidentenregister waaruit blijkt dat de FG betrokken is geweest bij beveiligingsincidenten.❸ Overleg bewijs van communicatie over hoe deelnemers en medewerkers de FG kunnen bereiken (denk bijvoorbeeld aan informatie op de website). |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.3: Rechtmatige verwerking van persoonsgegevens

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.3** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 5, 6, 12** |
| **Controledoelstelling: Rechtmatige verwerking van persoonsgegevens** De instelling draagt er zorg voor dat bij verwerking van persoonsgegevens de volgende uitgangspunten worden gehanteerd: 1. P.3a Doelbepaling en doelbinding: voor iedere categorie van verwerkingen wordt – voorafgaand aan die verwerking - een specifiek doeleinde vastgesteld, en dit doeleinde is gecommuniceerd bij de gegevensverzameling. De instelling zorgt er voor dat persoonsgegevens alleen worden verwerkt voor het doeleinde waarvoor die gegevens verkregen zijn.
2. P.3b Grondslag (rechtmatigheid): de instelling zorgt er voor dat persoonsgegevens altijd op basis van een in de AVG genoemde grondslag worden verwerkt. Indien toestemming noodzakelijk is voor verwerkingen van persoonsgegevens van deelnemers jonger dan 16 jaar, dan wordt toestemming altijd afgestemd met de wettelijke vertegenwoordigers. Verkregen toestemming wordt vastgelegd en is reproduceerbaar.
3. P.3c Dataminimalisatie: het verwerken van persoonsgegevens moet noodzakelijk voor het behalen van het onder P.3a benoemde doel. De inbreuk op de privacy van betrokkene moet te rechtvaardigen zijn om het doeleinde te bereiken (proportionaliteit), de te verzamelen persoonsgegevens blijven beperkt tot datgene wat minimaal nodig is om de doeleinde(n) te bereiken (subsidiariteit).
4. P.3d Transparantie: de instelling informeert de gebruikers (of hun wettelijke vertegenwoordigers) en medewerkers van wie persoonsgegevens worden verwerkt, beknopt, transparant, eenvoudig toegankelijk en in begrijpelijke taal over het beleid alsmede over alle gegevensverwerkingen.
5. P.3e Data-integriteit: de verantwoordelijke gaat zorgvuldig om met de verwerkte persoonsgegevens en waarborgt het behoud en bescherming van de juistheid en de consistentie van die gegevens.
 |
| **Toelichting:**Alle verwerkingen van persoonsgegevens binnen de instelling voldoen aan de vijf (herziene) vuistregels voor privacy. Deze basis privacy principes, die afgeleid zijn van de AVG zijn: 1. doelbepaling en doelbinding,
2. grondslag,
3. dataminimalisatie en
4. transparantie (over de rechten, maar ook over de verschillende verwerkingen van persoonsgegevens) en
5. data-integriteit.

Uit het dataregister blijkt welke categorieën persoonsgegevens van welke betrokkenen voor welke doeleinden en met welke grondslag worden gebruikt. De FG controleert het dataregister. |
| **Bewijsvoering:**Medewerkers worden geïnstrueerd over de 5 vuistregels en uit het dataregister blijkt of de verwerkingen van de instelling voldoen aan de vuistregels. |
| ❷Overleg documentatie of werkinstructies waaruit blijkt dat medewerkers zijn geïnformeerd over het rechtmatige verwerken van persoonsgegevens❷ Overleg de dataregisters |
| ❸Overleg een notitie, werkinstructie, presentatie of voorlichtingsmateriaal van een nieuwe verwerking, waaruit blijkt dat voor aanvang van de verwerking een toetsing op de 5 vuistregels heeft plaatsgevonden. ❸ Overleg een recent ingevuld dataregister waaruit ten minste blijkt wat het doel, grondslag van de verwerking is, en of daarbij getoetst is welke categorieën persoonsgegevens verwerkt worden.❸ Overleg bewijs dat de FG het dataregister heeft gecontroleerd/getoetst. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.4: Register van verwerkingsactiviteiten (dataregister)

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.4** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 30, 39** |
| **Controledoelstelling: Register van verwerkingsactiviteiten (dataregister):**Alle verwerkingen van persoonsgegevens binnen of door de instelling zijn opgenomen in een of meerdere dataregisters.  |
| **Toelichting:**De instelling heeft een of meerdere dataregisters waarin alle verwerkingen van persoonsgegevens door of namens de instelling zijn opgenomen. Het dataregister wordt gecontroleerd door de FG. |
| **Bewijsvoering:**Er is een dataregister |
| ❷Overleg een dataregister waarin de verwerkingen van persoonsgegevens zijn opgenomen. |
| ❸Overleg een bijgewerkte versie van het dataregister (niet ouder dan een jaar). ❸ Overleg documentatie waaruit blijkt dat de FG het dataregister heeft gecontroleerd/ getoetst. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.5: Bewaartermijnen

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.5** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 5, 30** |
| **Controledoelstelling: Bewaartermijnen**Er is een actief beleid omtrent het bewaren, archiveren en vernietigen van persoonsgegevens. Persoonsgegevens worden niet langer verwerkt dan nodig voor het gestelde doeleinde. De instelling stelt op basis van de Archiefwet (waaronder het BSD valt) de vernietigings- en bewaartermijnen vast van de verwerkte persoonsgegevens en neemt deze termijnen op in het dataregister. |
| **Toelichting:**De leiding van de organisatie moet beleid opstellen en goedkeuren inzake het bewaren van persoonsgegevens. Hierin moet minimaal worden opgenomen: 1. op welke wijze de (minimale en) maximale bewaartermijnen worden vastgesteld;
2. welke manieren van voorkomen van de persoonsgegevens moeten worden verwijderd of gekenmerkt als verwijderd;
3. op welke wijze het verwijderen na het verstrijken van de bewaartermijn plaats vindt;
4. de wijze waarop persoonsgegevens worden geanonimiseerd zodat de gegevens niet herleidbaar zijn tot de betrokkene(n);
5. de vereisten aan het protocol dat wordt opgesteld van het verwijderen van de persoonsgegevens;
6. de taken, bevoegdheden en verantwoordelijkheden ten aanzien van het bewaren van persoonsgegevens.
 |
| **Bewijsvoering:**Het IBP-beleid bevat bepalingen over bewaartermijnen, of er is een separaat bewaartermijnenbeleid. Hierbij wordt uitgegaan van het DSP (Documentair Structuur Plan) van de MBO-Raad. |
| ❷Overleg het beleid rondom bewaartermijnen waaruit blijkt hoe de instelling omgaat met bewaartermijnen, of overleg het bewaartermijnenbeleid van de instelling |
| ❸ Overleg de Dataregisters: Medewerker, Student en Relatie, waarin de bewaartermijnen zijn opgenomen afgeleid van het IBP beleid of separaat bewaartermijnenbeleid van de instelling. ❸ Overleg een bewijs van uitvoering van het bewaartermijnenbeleid, waaronder bijvoorbeeld verstaan wordt het anonimiseren of verwijderen van persoonsgegevens conform de vastgestelde bewaartermijnen. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.6: Verwerking t.b.v. onderzoek

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.6** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 89** |
| **Controledoelstelling: Verwerking t.b.v. onderzoek**Persoonsgegevens mogen worden verwerkt ten behoeve van: * archivering in het algemeen belang (Archiefwet);
* wetenschappelijk of historisch onderzoek; of
* statistische doeleinden

indien passende technische en organisatorische maatregelen zijn genomen om de privacy van de betrokken deelnemers te garanderen. Onder deze maatregelen wordt in ieder geval verstaan dat er niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk is. Hierbij valt te denken aan pseudonimisering (in geval de data herleidbaar moet zijn tot individuen) of anonimisering (in geval data niet herleidbaar hoeft te zijn). Bij historische, statistische of wetenschappelijke doeleinden is verwerking alleen mogelijk op basis van strikte voorwaarden vergelijkbaar met de ‘Gedagscode voor Onderzoek & Statistiek’ en het bevoegd gezag voorafgaand toestemming heeft verleend. |
| **Toelichting:**Bij het verwerken van persoonsgegevens voor archivering, wetenschappelijk, historisch of statistische doeleinden, gelden specifieke regels. |
| **Bewijsvoering:**Er zijn in het beleid instructies opgenomen voor verwerking van persoonsgegevens in het kader van "historische, statistische of wetenschappelijke doeleinden". |
| ❷Overleg een beleidsdocument dat is vastgesteld aangaande verwerking van persoonsgegevens in het kader van "historische, statistische of wetenschappelijke doeleinden" waarbij gebruik wordt gemaakt van een in de sector gebruikte gedragscode. |
| ❸Overleg een printscreen van het intranet waaruit blijkt dat medewerkers kennis hebben kunnen nemen van het vastgestelde beleid op het gebied van gebruik van persoonsgegevens in het kader van "historische, statistische of wetenschappelijke doeleinden" en/of overleg documentatie waaruit blijkt dat de instelling betrokken is/was bij onderzoek voor historische, statistische of wetenschappelijke doeleinden en welke maatregelen hierbij genomen zijn. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.7: Verwerking van bijzondere persoonsgegevens

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.7** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 9** |
| **Controledoelstelling: Verwerking van bijzondere persoonsgegevens**De instelling verwerkt geen bijzondere persoonsgegevens, uitgezonderd:* iemands religieuze of levensbeschouwelijke overtuigingen voor zover dit nodig is gelet op het doel van de instelling en voor de verwezenlijking van haar grondslag strikt noodzakelijk is
* ras of etnische afkomst, voor zover de instelling daartoe op grond van een wet verplicht is, of alleen in met het doel om personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen om feitelijke nadelen verband houdende met de grond ras op te heffen of te verminderen
* biometrische gegevens (zoals vingerafdruk of irisscan) voor zover deze gebruikt worden met het oog op authenticatie of beveiligingsdoeleinden
* gezondheid of iemands seksueel gedrag of seksuele gerichtheid, voor zover dat met het oog op de speciale begeleiding van deelnemers of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is, tenzij de deelnemer voor het gebruik van deze categorieën persoonsgegevens zelf toestemming heeft gegeven voor het verwerken van de hiervoor genoemde categorieën persoonsgegevens.
 |
| **Toelichting:**Het verbod op het verwerken van bijzondere persoonsgegevens wordt slechts onder specifieke omstandigheden opgeheven. Denk bij het vragen van toestemming aan de specifieke vereisten rondom de leeftijdgrenzen, is de betrokkene onder curatele gesteld, etc. |
| **Bewijsvoering:**De bijzondere persoonsgegevens worden geïmplementeerd in de Registers voor Verwerkingsactiviteiten. De dataregisters bestaan uit Register voor Verwerkingsactiviteiten, globale autorisatie en BIV classificatie. De Bijzondere persoonsgegevens zijn geclassificeerd in de kolom BIV, vertrouwelijkheid hoog (rood), van het Dataregister. |
| ❷Overleg een document waarin de dataregisters Medewerker, Leerling/Student en Relatie zijn goedgekeurd door het CvB. |
| ❸Overleg de actuele versies (jaarlijkse toetsing) van de dataregisters: Medewerker, Leerling/Student en Relatie❸ Overleg werkinstructies voor medewerkers die in hun praktijk dagelijks werken met bijzondere persoonsgegevens |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.8: Geautomatiseerde besluitvorming

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.8** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 21, 22** |
| **Controledoelstelling: Geautomatiseerde besluitvorming** Bij verwerkingen van persoonsgegevens mogen geen volledig geautomatiseerde besluiten worden genomen (waaronder profilering) die voor de betrokkene rechtsgevolgen hebben of hem in aanmerkelijke mate treffen. |
| **Toelichting:**Er dient altijd een menselijke toets uitgevoerd te worden bij geautomatiseerde besluitvorming. Uitzonderingen: als de geautomatiseerde verwerking berust op nadrukkelijke toestemming van de betrokkene of de totstandkoming of uitvoering van een overeenkomst of op basis is van een wettelijke regeling. |
| **Bewijsvoering:**De onderwijsinstellingen maken geen gebruik van profilering. Learning analytics, big data, Google analytics, etc. worden alleen aanvullend gebruikt bij het onderwijsproces en nooit solitair. |
| ❷Overleg instructies rondom geautomatiseerde besluitvorming en profilering. |
| ❸Overleg een document waarin medewerkers in kennis worden gesteld over geautomatiseerde besluitvorming en profilering. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.9: Informatiebeveiliging

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.9** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 5, 32** |
| **Controledoelstelling: Informatiebeveiliging**De instelling neemt organisatorische en technische beheersmaatregelen om een passend beveiligingsniveau te waarborgen van alle verwerkingen van persoonsgegevens. Hierbij let de instelling op de risico’s die de verwerking(en) met zich meebrengen, en met de aard en classificatie van de te beschermen persoonsgegevens. Bij de maatregelen wordt rekening gehouden met de stand van de techniek en de kosten van de uitvoering van de beheersmaatregelen. |
| **Toelichting:**De organisatie moet kunnen aantonen hoe het passende niveau wordt bereikt en behouden. Het doel van de beheersmaatregelen is de integriteit en vertrouwelijkheid van de persoonsgegevens te garanderen, en om de gegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze bepaling is de schakelbepaling naar cluster 1 tot en met 6. Bij het beveiligen van persoonsgegevens wordt rekening gehouden met de classificatie van die gegevens. Zo zullen bijzondere persoonsgegevens met een hogere BIV-classificatie beter beveiligd moeten worden.  |
| **Bewijsvoering:**De technische beveiliging is onderdeel van het Toetsingskader Informatiebeveiliging, waardoor de risico's afdoende in kaart zijn gebracht. Dit statement gaat dieper in op de Privacy risico's, zoals bijvoorbeeld datalekken, die in een jaarplan gemitigeerd dienen te worden. |
| ❷Overleg aan de hand van de risicoanalyse een plan waarin de maatregelen benoemd zijn om de actuele en technische risico's in het kader van Privacy te mitigeren. |
| ❸Overleg een opleveringsdocument waaruit de uitvoering van het plan blijkt. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.10: Verwerkersovereenkomsten

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.10** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 28** |
| **Controledoelstelling: Verwerkersovereenkomsten**De instelling schakelt voor de verwerking van persoonsgegevens voor of namens de instelling, uitsluitend leveranciers in als verwerker. Deze verwerker moet de onderwijsinstelling afdoende garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen, zodat de verwerking door verwerker aan de wet voldoet. De instelling legt afspraken met alle verwerkers vast in een verwerkersovereenkomst waarin aan alle relevante wettelijk vereiste onderdelen wordt voldaan. |
| **Toelichting:**De instelling heeft met iedere verwerker een verwerkersovereenkomst. Een verwerkersovereenkomst bevat ten minste het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven. Bij voorkeur wordt gebruik gemaakt van het model van het privacy convenant, of de generieke model verwerkersovereenkomst behorend bij het Framework IBP mbo. |
| **Bewijsvoering:**Het aanwezig zijn van verwerkersovereenkomsten is niet voldoende. Er dient gecontroleerd te worden of alle verwerkers in beeld zijn, en of met al deze partijen een verwerkersovereenkomst is afgesloten.  |
| ❷Toon een aantal verwerkersovereenkomsten die ten minste de wettelijk vereiste onderdelen bevatten. |
| ❸Toon aan de hand van het dataregister aan dat met alle verwerkers een verwerkersovereenkomst is afgesloten. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.11: Transparant over privacy

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.11** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 5, 12** |
| **Controledoelstelling: Transparant over privacy**De instelling informeert de (ouders van) deelnemers en medewerkers van wie persoonsgegevens worden verwerkt, beknopt, transparant, eenvoudig toegankelijk en in begrijpelijke, duidelijke en eenvoudige taal over het privacy beleid en de rechten en verplichtingen van betrokkenen. |
| **Toelichting:**Betrokkenen moeten goed en helder geïnformeerd worden over wat de onderwijsinstelling doet met hun persoonsgegevens. Hierbij kan gebruik worden gemaakt van de toelichting bij het dataregister (privacyverklaring of -statement). Het gaat hier niet om alleen het privacyreglement (wat een beschrijving geeft van de rechten van de betrokkenen) maar dit statement is gericht op informeren van betrokkenen.  |
| **Bewijsvoering:**Het informeren van betrokkenen is een wezenlijk onderdeel van de AVG. Naast het vaststellen van een beleid en privacyreglement, moet dat beleid ook begrijpelijk worden uitgelegd. Dit statement ziet op het transparant zijn over de verwerking van persoonsgegevens door onderwijsinstelling. |
| ❷Overleg bewijs (bijvoorbeeld screenprint website) over hoe de instelling deelnemers, hun ouders en medewerkers informeert over het beleid en rechten en verplichtingen van betrokkenen. Ten minste het beleid en het privacyreglement moeten beschikbaar zijn voor deelnemers en medewerkers |
| ❸Toets (gedeeltelijk) of de uitleg begrijpelijk genoeg is, hierbij is het Europese referentiekader voor talen taalniveau niet hoger dan B2; B1 het uitgangspunt. Er zijn verschillende online tools beschikbaar om het taalniveau te controleren. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.12: Informeren over verwerkingen

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.12** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 5, 13** |
| **Controledoelstelling: Informeren over verwerkingen**De instelling informeert deelnemers, hun ouders en medewerkers actief over de verwerking van hun persoonsgegevens, en wat de rechten van de betrokkenen en hoe die uitgeoefend kunnen worden. De informatie bevat ten minste de in de wet opgesomde informatie. |
| **Toelichting:**Naast het op hoofdlijnen informeren van de medewerkers en studenten over het algemene privacy beleid en reglement (zie P.11), moeten betrokkenen ook concreet worden geïnformeerd over iedere verwerking van hun gegevens. Denk hierbij aan het inschrijfformulier waar een toelichting is bijgevoegd over wat er met de persoonsgegevens wordt gedaan (de doeleinden en bijvoorbeeld met wie de gegevens binnen de instelling worden gedeeld).Het informeren van deelnemers en medewerkers kan per verwerking, maar ook middels een privacyreglement waarin alle verwerkingen en categorieën persoonsgegevens zijn samengevoegd. Hiernaast bevat het reglement informatie over de rechten en verplichten van onderwijsinstelling en betrokkenen.  |
| **Bewijsvoering:**Controleer of betrokkenen worden geïnformeerd over de verwerkingen van hun persoonsgegevens en of hierbij de wettelijk vereiste informatie wordt gegeven. Controleer of een privacyreglement is vastgesteld en gepubliceerd. |
| ❷Overleg het privacyreglement inclusief bewijs dat dit gepubliceerd is. |
| ❸ Overleg bewijs (kopie, screenshot) dat betrokkenen actief geïnformeerd worden over hun rechten en verplichtingen op het moment dat er - voor het eerst - persoonsgegevens van hen worden verwerkt door de onderwijsinstelling. Denk hierbij bijvoorbeeld aan een verwijzing naar het privacyreglement bij het toezenden van de OOK of arbeidsovereenkomst. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.13: Procedures rechten van de betrokkenen

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.13** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 12, 13, 15, 16, 17, 20** |
| **Controledoelstelling: Procedures rechten van de betrokkenen**De instelling stelt procedures vast ten behoeve van de uitoefening van de rechten van betrokkenen. |
| **Toelichting:**Dit statement ziet op het organiseren van de nodige procedures rondom de rechten van betrokkenen. Het informeren van betrokkenen over hun rechten is opgenomen in P12, het informeren van betrokkenen over het beleid staat in P11. Het betreft hier de rechten: Recht op informatie (P.12)* Recht op inzage: deelnemers, ouders en medewerkers mogen hun eigen persoonsgegevens inzien.
* Recht op rectificatie en correctie: deelnemers, ouders en medewerkers mogen een school vragen onjuiste persoonsgegevens aan te passen.
* Recht op vergetelheid: ouders, deelnemers en medewerkers mogen persoonsgegevens laten verwijderen indien aan een aantal criteria is voldaan.
* Recht op beperking van de verwerking: als deelnemers en de onderwijsinstelling bijvoorbeeld onenigheid hebben over het verwerken van de persoonsgegevens, dan mogen betrokkenen vragen om persoonsgegevens – tijdelijk – niet meer te gebruiken.
* Recht op dataportabiliteit: dataportabiliteit betekent dat data in een aantal gevallen overdraagbaar moet zijn aan een andere verwerkingsverantwoordelijke in een gestructureerde, gangbare en machine-leesbare vorm.
* Recht van bezwaar: ouders, deelnemers en medewerkers mogen – in een aantal gevallen – bezwaar maken tegen het gebruiken van persoonsgegevens.
* Recht met betrekking tot geautomatiseerde besluitvorming en profilering: zie P.8

\* Het is ook mogelijk om één procedure voor meerdere verwerkingen te hanteren.\* De procedures kunnen eventueel worden ondersteund met frequently asked questions (FAQ) |
| **Bewijsvoering:**Het beleid voor "Rechten van de betrokkenen" dat is gebaseerd op de documenten van SURF, saMBO-ICT of Kennisnet. |
| ❷Overleg het document "Rechten van de betrokkenen" en toon waar dit document eenvoudig te raadplegen is. |
| ❸ Overleg een printscreen waaruit blijkt waar betrokkenen zich toe kunnen wenden om de hun toekomende rechten uit te oefenen. ❸ Toon afschriften van de uitleg of instructies aan medewerkers van personeelszaken, de administratie, het loket voor deelnemers of studenteninformatie over de uitoefening van de rechten van de betrokkenen. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.14: Geheimhouding

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.14** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 9, 38, 90** |
| **Controledoelstelling: Geheimhouding**De instelling moet een geheimhoudingsplicht aan de medewerkers opleggen en erop toezien dat de medewerkers de geheimhoudingsplicht naleven. Met de functionarissen die uit hoofde van hun functie toegang hebben tot grote verzamelingen van bijzondere persoonsgegevens (van medewerkers en/of deelnemers) en/ of beschikken over verhoogde (beheer-)rechten ten aanzien van systemen waarin persoonsgegevens van medewerkers en deelnemers worden verwerkt, sluit de instelling een separate integriteits- en geheimhoudingsverklaring af. |
| **Toelichting:**In de cao of arbeidsovereenkomsten met medewerkers zijn bepalingen over geheimhouding opgenomen. De separate integriteits- en geheimhoudingsverklaring voor de beperkte groep functionarissen is bedoeld om deze medewerkers te informeren en bewust te maken van hun verantwoordelijkheid om op een verantwoordelijke en bevoegde manier om te gaan met deze gegevens en dientengevolge de informatie van de organisatie te beschermen. |
| **Bewijsvoering:**Er is beleid ten aanzien van geheimhouding. |
| ❷ Overleg een document dat vastgesteld is door het bevoegd gezag waarin het beleid ten aanzien van geheimhoudingsplicht voor medewerkers is opgenomen. |
| ❸ Overleg een document waaruit blijkt dat medewerkers gehouden zijn aan een geheimhoudingsplicht.❸ Overleg een document waaruit blijkt voor wie aparte geheimhoudingsverklaringen worden gebruikt en/ of met welke medewerkers, die uit hoofde van hun functie toegang hebben tot omvangrijke verzamelingen bijzondere persoonsgegevens en/ of beschikken over verhoogde (beheer-)rechten ten aanzien van de kritische systemen van de instelling, separate integriteits- en geheimhoudingsovereenkomsten worden afgesloten. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.15: Bewustzijn, opleiding en training ten aanzien van privacy

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.15** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 39** |
| **Controledoelstelling: Bewustzijn, opleiding en training ten aanzien van privacy**De instelling stimuleert het privacy bewustzijn van de medewerkers door training en scholing te bieden aan alle medewerkers, en door gebruik te maken van andere vormen van communicatie over privacy. |
| **Toelichting:**Hiervoor kan gebruik worden gemaakt van een diversiteit van methoden en materialen. Bijvoorbeeld een privacy gedragscode, online trainingen, introductiebijeenkomsten voor nieuwe medewerkers, nieuwsberichten of een awareness-programma. De FG is niet per definitie eindverantwoordelijk voor het geven van trainingen of voorlichting. Bij het geven van voorlichting wordt gekozen voor een geïntegreerde aanpak waarbij informatiebeveiliging en privacy worden gecombineerd. Uitgangspunt is dat alle medewerkers relevante scholing hebben gevolgd. |
| **Bewijsvoering:**Er is een awareness campagne en/of introductie-/scholingsprogramma opgesteld voor de huidige en de toekomstige medewerkers. Dit plan kan worden bijgesteld als gevolg van actuele ontwikkelingen op het IBP-gebied. Hierbij is een planning opgenomen op welke termijn alle medewerkers IBP-scholing hebben gekregen. |
| ❷ Overleg een document waar de awareness (algemeen) en de scholing (doelgroepen) in het kader van IBP is beschreven en vastgesteld. |
| ❸ Overleg een begroting in het kader van bewustzijn, opleiding en training rondom IBP en geef een overzicht van de financiële realisatie hiervan. ❸ Overleg een lijst waaruit aangetoond wordt dat een ruime meerderheid van de medewerkers IBP-scholing heeft gevolgd. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.16: Bewijs van vernietiging persoonsgegevens

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.16** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 5** |
| **Controledoelstelling: Bewijs van vernietiging persoonsgegevens**Van apparatuur die niet langer wordt gebruikt, worden de op het apparaat aanwezige persoonsgegevens op een betrouwbare en veilige wijze vernietigd. Van deze vernietiging en de wijze waarop, wordt een verklaring opgemaakt, of afgegeven door een derde die verantwoordelijk is voor de vernietiging. |
| **Toelichting:**In geval van afvoer van apparatuur moet in het kader van accountability worden vastgelegd of en hoe de persoonsgegevens zijn verwijderd. |
| **Bewijsvoering:** Er zijn heldere afspraken gemaakt met derden over de vernietiging van persoonsgegevens wanneer apparatuur niet langer wordt gebruikt, daar wordt ook een verklaring van verstrekt. |
| ❷Overleg het beleid waaruit blijkt dat persoonsgegevens op een betrouwbare en veilige wijze worden vernietigd in geval apparatuur niet langer wordt gebruikt. |
| ❸ Overleg een of meerdere verklaringen waaruit blijkt of en hoe de op de afgevoerde apparatuur aanwezige persoonsgegevens zijn vernietigd. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.17: Dataclassificatie

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.17** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 5, 32** |
| **Controledoelstelling: Dataclassificatie**De instelling moet de kwaliteit van de gegevens (gegevenskwaliteit) borgen. Hiertoe heeft de instelling inzicht in de classificatie van persoonsgegevens. |
| **Toelichting:**Om zorgvuldig en integer met persoonsgegevens om te kunnen gaan, is het noodzakelijk om vast te stellen welke categorie en classificatie van persoonsgegevens verwerkt worden. |
| **Bewijsvoering:**De data integriteit van de verwerking wordt geïmplementeerd in de Registers voor Verwerkingsactiviteiten. De dataregisters bestaan uit Register voor Verwerkingsactiviteiten, globale autorisatie en BIV classificatie. Toelichting: de classificatie is terug te vinden in het Dataregister als BIV-classificatie. |
| ❷ Overleg bewijs waaruit het beleid en criteria rondom classificatie blijken.  |
| ❸ Overleg de actuele BIV-classificatie, dit kan zijn opgenomen in de dataregisters. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.18: Datalekken en beveiligingsincidenten

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.18** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 33, 34** |
| **Controledoelstelling: Datalekken en beveiligingsincidenten**De instelling stelt een procedure vast voor het melden en afhandelen van datalekken en beveiligingsincidenten. In dit beleid is opgenomen dat een datalek zo snel mogelijk na ontdekking aan de toezichthouder en eventueel de betrokkene(n) wordt gemeld. Datalekken en beveiligingsincidenten worden opgenomen in een incidentenregister.  |
| **Toelichting:**Een datalek is een inbreuk waarbij persoonsgegevens zijn betrokken. De definitie in de AVG: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. |
| **Bewijsvoering:**Het model beleidsplan schrijft voor dat een procedure voor datalekken en beveiligingsincidenten wordt vastgesteld.  |
| ❷ Overleg het beleid of de procedure datalekken. |
| ❸ Overleg een printscreen waaruit blijkt dat het beleid en procedure rondom datalekken eenvoudig te raadplegen is.❸ Toon het incidentenregister met daarin (ruimte voor) meldingen van datalekken en beveiligingsincidenten. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.19: Bijzondere persoonsgegevens

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.19** | [**Terug naar index**](#_Aanvullende_statements_privacy) |
| **Controledoelstelling: Bijzondere persoonsgegevens** |
| **Toelichting:** **Vervallen**, maatregelen zijn vervat in P.7, P.9 en P.17.  |
| **Bewijsvoering:**  |
| ❷  |
| ❸  |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

## P.20: Privacy by design en privacy by default

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.20** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 25** |
| **Controledoelstelling: Privacy by design en privacy by default**De instelling moet beleid opstellen en goedkeuren dat toeziet op de beginselen van privacy by design en privacy by default. |
| **Toelichting:**Dit statement gaat er van uit dat privacy standaard een uitgangspunt is voor de instelling. In het beleid wordt dit als uitgangspunt genomen. Hierbij moet rekening worden gehouden met de stand van de techniek. Gezien de snelheid waarmee de techniek zich ontwikkelt moet dit beleid regelmatig worden beoordeeld en zo nodig worden aangepast.Hierbij valt te denken aan privacy by default: standaard staat delen uit op nieuwe accounts, en privacy by design: autorisaties moeten per medewerkers/groep worden aangevraagd en geverifieerd, dit gaat niet automatisch of voor iedereen hetzelfde, pseudonimisering (ECK-ID). |
| **Bewijsvoering:**De instelling heeft beleid dat er op gericht is dat privacy als uitgangspunt telt, bijvoorbeeld bij ontwikkelingen rond nieuwe softwaresystemen (inkoop en bouw). |
| ❷ Overleg het beleid waaruit volgt of en hoe invulling wordt gegeven aan beginselen van privacy by default en privacy by design. |
| ❸ Overleg bewijs dat bij de inkoop of ontwikkeling van software rekening gehouden is met privacy by design en privacy by default. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.21: Data Protection Impact Assessment (DPIA)

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.21** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 25** |
| **Controledoelstelling: Data Protection Impact Assessment (DPIA)**De instelling voert Data Protection Impact Assessments (GegevensBeschermingsEffectBeoordeling) uit om inzicht te krijgen in de privacy risico’s en om deze risico's zo veel mogelijk te mitigeren. Een DPIA wordt uitgevoerd in geval van: - nieuwe verwerkingen; - grote of ingrijpende wijzigingen in de bestaande verwerking van persoonsgegevens die specifiek de risico’s wijzigt voor de privacy van de betrokken deelnemers en medewerkers;- verwerking van grote hoeveelheden persoonsgegevens of bijzondere persoonsgegevens. |
| **Toelichting:**Een DPIA (GBEB) moet in geval de AVG dit voorschrijft worden uitgevoerd. |
| **Bewijsvoering:**In het IBP-beleid is omschreven of en wanneer een DPIA wordt uitgevoerd, dit wordt overgenomen voor zover noodzakelijk in ander relevant beleid (inkoop, aanbestedingen). |
| ❷Overleg het gehanteerde format DPIA. |
| ❸ Overleg een overzicht van uitgevoerde DPIA's.❸ Overleg een overzicht van niet uitgevoerde DPIA's, met toelichting van reden. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.22: Controle naleving beleid

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.22** | [**Terug naar index**](#_Aanvullende_statements_privacy) | **AVG art: 5, 24, 32, 35, 39** |
| **Controledoelstelling: Controle naleving beleid**De instelling moet de naleving van IBP-beleid en -maatregelen intern en extern monitoren, beoordelen en evalueren. |
| **Toelichting:**De aantoonbare certificering kan door middel van een peer review en een externe audit worden verkregen. De frequentie van de externe audit is ten minste éénmaal in de 4 jaar. |
| **Bewijsvoering:**Er is audit uitgevoerd door een deskundige die niet het self-assessment heeft uitgevoerd. |
| ❷ Overleg informatie waaruit blijkt dat de instelling de naleving van het beleid en normen controleert (selfassessment). Het deelnemen aan de benchmark IBP mbo is een voorbeeld van een uitwerking hiervan. |
| ❸ Overleg een rapport van peer review of auditor die de naleving van het beleid en normen van de instelling toetst. Hierbij is het Framework IBP mbo de kritische ondergrens. |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

**Bevindingen en aanbevelingen**

|  |
| --- |
| **Bevindingen opzet en bestaan (niveau 2)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingenwerking (niveau 3)** |
| **Bevinding:** **Aanbeveling:** |
| **Bevindingen PDCA (niveau 4)** |
| **Bevinding:** **Aanbeveling:** |
| **Risico:** |
| **Conclusie:**  | **Volwassenheids-niveau****X** |

## P.23: Rapportage van privacy gebeurtenissen

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.23** | [**Terug naar index**](#_Aanvullende_statements_privacy) |
| **Controledoelstelling: Rapportage van privacy gebeurtenissen** |
| **Toelichting:** **Vervallen**, deze maatregel is opgenomen in P.2, P.11, P.12, P.18 en cluster 1 statement 18. |
| **Bewijsvoering:**  |
| ❷  |
| ❸  |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

## P.24: Gebeurtenissen registreren

|  |  |
| --- | --- |
| **Self****assessment** |  |
| **Cluster:**  | **7 Privacy** |
| **Privacy toetsingskader****nummer:** **P.24** | [**Terug naar index**](#_Aanvullende_statements_privacy) |
| **Controledoelstelling: Gebeurtenissen registreren** |
| **Toelichting: Vervallen,** deze maatregel is opgenomen in cluster 6 statement 2.  |
| **Bewijsvoering:**  |
| ❷  |
| ❸  |
| **Auditor(s):**  |
| **Methode van beoordeling:**  |
| **Documentatie:** |  |  |
| **Interview:** |  |  |
| **Waarneming ter plaatse:** |  |  |
| **Re-performance** |  |  |
| **Goedkeuring van de beoordeling** (naam en datum)**:** |
| **Referenties:** |

Bijlage 1: Framework 2.0 informatiebeveiliging en privacy in het mbo



1. Bron: Privacy Compliance kader (IBPDOC2B) [↑](#footnote-ref-2)
2. Met instelling wordt de rechtspersoon bedoeld, concreet wordt deze vertegenwoordigd door de verantwoordelijke. Binnen het mbo zal dit de voorzitter van het College van Bestuur zijn. [↑](#footnote-ref-3)
3. Officiële Nederlandse vertaling:

<http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=NL> [↑](#footnote-ref-4)