Bewaar- en vernietigingsbeleid

Beleidsmodel aangeleverd door Lumen Group inclusief bijlagen ter ondersteuning in de naleving van de wettelijke verplichting uit de AVG (Artikel 5 en 30 AVG).

Classificatie	Vertrouwelijk
Versie	1.0 Onderwijs
Auteurs	Lumen Group
Opsteldatum	30 juni 2020

Voorwoord Lumen Group

Voor organisaties vormt het verwerken van persoonsgegevens een substantieel onderdeel van de bedrijfsvoering. Onder verwerking van persoonsgegevens valt onder andere het verzamelen, vastleggen, bewaren, raadplegen, gebruiken en zelfs het vernietigen of wissen van deze persoonsgegevens. Iedere organisatie is door de Algemene Verordening Gegevensbescherming (AVG) verplicht om beleid op te stellen en uit te voeren dat gericht is op de vaststelling van bewaartermijnen van persoonsgegevens en de vernietiging ervan na het verstrijken van de bewaartermijnen. Hierbij moet rekening gehouden worden met de aard, omvang, context en het doel van de verwerkingen binnen de organisatie. Ook contractuele bepalingen hebben hier in sommige gevallen invloed op. Wanneer er geen wettelijke bewaartermijn van toepassing is, dan geldt **de hoofdregel volgens de AVG** dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk.

Met het oog op de verplichtingen rondom bewaren en vernietigen van persoonsgegevens en de complexiteit hiervan in verband met specifieke wetten (zoals de Archiefwet) die gelden, heeft Lumen Group dit template opgesteld. Lumen Group beoogt hiermee bij te dragen aan de naleving van wettelijke verplichtingen door haar klanten in het onderwijs, zodat er op een correcte manier met de verwerking van persoonsgegevens wordt omgegaan.

Let op: naast het beschikken over een goed beleid en het uitvoeren hiervan, is het belangrijk om het beleid actueel te houden. Dit gebeurt door processen van actualisatie (versiebeheer, periodieke evaluaties, etc.) in te bedden in de PDCA-cyclus en toe te zien op de naleving hiervan. Een proces van actualisatie maakt aantoonbaar dat <ORGANISATIE> invulling geeft aan haar verplichtingen en verantwoordelijkheden.

Toelichting template

Dit template bevat de wettelijke vereisten die gesteld zijn in de AVG ten opzichte van een bewaar- en vernietigingsbeleid. Ook hebben wij de tips en adviezen van de Autoriteit Persoonsgegevens meegenomen in het opstellen van dit template. Het template is gedeeltelijk gebruiksklaar, echter de passages zijn organisatie-neutraal geformuleerd. In geel is gearceerd waar aanvulling vereist is, om het bewaar- en vernietigingsbeleid te specificeren naar de eigen organisatie.

Daarnaast zijn er vijf bijlages, die ook door de organisatie ingevuld moeten worden. Deze zijn dus nog **niet** volledig, maar bieden de juiste opzet en kaders.

In gevallen waarin bestaande templates of beleidsstukken blijven bestaan, dan kan dit template gebruikt worden als inspiratiebron voor de verdere uitwerking van bestaande documenten.

Vanuit Lumen Group bieden wij ook de mogelijkheid om tegen een gereduceerd uurtarief de aangeboden templates te implementeren binnen de organisatie. Als dit gewenst is (doordat er onvoldoende capaciteit binnen de organisatie bestaat bijvoorbeeld), neem dan contact met ons op om deze mogelijkheid te bespreken.

Template Bewaar- en vernietigingsbeleid

Versiebeheer

Datum	Auteur	Versie	Status	Aanpassing

Goedgekeurd

Datum	Goedgekeurd door	Functie	Handtekening	Geplande revisie

Inhoudsopgave

Bewaar- en vernietigingsbeleid <ORGANISATIE>

1. Inleiding

1.1 Waarom een bewaar- en vernietigingsbeleid?

<ORGANISATIE> is een <omschrijving bedrijf/organisatie>. <ORGANISATIE> heeft werknemers in dienst en richt zich onder andere op <deelnemers in de organisatie, bijvoorbeeld: leerlingen>. Dit betekent dat <ORGANISATIE> omgaat met veel persoonsgegevens van zowel medewerkers als <deelnemers in de organisatie, bijvoorbeeld: leerlingen> en andere betrokkenen. <ORGANISATIE> vindt het belangrijk dat met deze persoonsgegevens zorgvuldig wordt omgegaan. Het verwerken van persoonsgegevens brengt namelijk een grote verantwoordelijkheid met zich mee. Zo mogen persoonsgegevens niet onbeperkt bewaard blijven en moeten van een bewaartermijn voorzien zijn. In dit bewaar- en vernietigingsbeleid wordt beschreven hoelang <ORGANISATIE> persoonsgegevens bewaart ten behoeve van een vooraf bepaald doel of op basis van een wettelijke verplichting. Na het verstrijken van de bewaartermijn moeten de persoonsgegevens worden vernietigd.

<ORGANISATIE> houdt zich hierbij aan de van toepassing zijnde wet- en regelgeving (*Algemene Verordening Gegevensbescherming*) en richtlijnen van de Autoriteit Persoonsgegevens. Dit beleid beoogt dus dat <ORGANISATIE> persoonsgegevens niet langer bewaart dan noodzakelijk is voor het doel waarvoor de persoonsgegevens zijn verzameld. Het beperkt bewaren van persoonsgegevens verkleint de risico's op datalekken of -incidenten. In dit bewaar- en vernietigingsbeleid worden de kaders voor het bewaren en vernietigen van persoonsgegevens vastgelegd.
Het is belangrijk dat het beleid binnen de hele organisatie bekend is en nageleefd wordt. Hiertoe worden medewerkers erover geïnformeerd en is het beleid door iedereen te raadplegen op <Sharepoint bijvoorbeeld>

1.2 Reikwijdte

De wet maakt bij het bewaren van persoonsgegevens geen onderscheid tussen digitale of analoge persoonsgegevens; is de bewaartermijn verstreken dan moeten de gegevens digitaal of op papier vernietigd worden. Dit strekt zich ook uit tot de verwerkingen die zijn uitbesteed en techniek mag hierbij geen belemmering vormen.

Het bewaar- en vernietigingsbeleid is van toepassing op de hele organisatie, alle taken en processen, objecten, gegevensverzamelingen en onderliggende informatiesystemen waar <ORGANISATIE> verantwoordelijk voor is. Bij de invoering van het beleid zijn de proceseigenaren, systeemeigenaren en gegevenseigenaren betrokken. Ook zijn vanuit informatiebeveiligingsoogpunt passende maatregelen genomen om te voldoen aan wet- en regelgeving.

Bewaarde persoonsgegevens

Dit bewaar- en vernietigingsbeleid heeft betrekking op de categorieën persoonsgegevens zoals deze in het privacybeleid van <ORGANISATIE> zijn opgenomen. Het verwerkingsregister geeft weer welke persoonsgegevens binnen <ORGANISATIE> verwerkt worden. In <bijlage E> staan de bewaartermijnen die binnen <ORGANISATIE> gehanteerd worden. De bewaartermijnen zijn per categorie

persoonsgegevens uitgewerkt in tabellen. In kolom 2 van deze tabellen staat de soort persoonsgegeven vermeld. Bij bijzondere persoonsgegevens is het verwerkingsdoel expliciet opgenomen in kolom 2. Kolom 3 van de tabellen geeft de ingangsdatum van de bewaartermijn weer, zodat duidelijk is vanaf welke periode een bewaartermijn ingaat. In kolom 4 van de tabellen staan de richtlijnen vermeld voor het bewaren van de persoonsgegevens. Deze richtlijnen betreffen doorgaans maximale bewaartermijnen, maar in sommige gevallen wordt er een minimale bewaartermijn voorgeschreven in de wet. <ORGANISATIE> geeft in kolom 5 aan wat de bepaalde bewaartermijn is voor de betreffende persoonsgegevens. Hierbij wordt bij niet-wettelijke bewaartermijnen (bijv. bewaren van (portret)foto's) een onderbouwing vermeld.

Bijzondere persoonsgegevens

Het bewaren van bijzondere persoonsgegevens, zoals gezondheidsgegevens of gegevens over religieuze of levensbeschouwelijke overtuigingen van een betrokkene is volgens de AVG uitsluitend onder strenge voorwaarden toegestaan. Binnen <ORGANSATIE> worden ook bijzondere persoonsgegevens bewaard. <ORGANSATIE> ziet extra toe op een juiste naleving van dit beleid met betrekking tot bijzondere persoonsgegevens. Dit doen wij door de in hoofdstuk 4 beschreven methodiek.

Wettelijke bewaartermijnen

Het bewaren van persoonsgegevens voor een vastgestelde termijn, kan op basis van de wet verplicht zijn. Deze wettelijke bewaartermijnen gelden ook binnen <ORGANSATIE> ten aanzien van bepaalde persoonsgegevens en zijn vastgesteld onder de kolom "Richtlijn bewaartermijn" in <bijlage E>.

2. Juridisch kader

2.1 Bewaartermijnen en de Algemene Verordening Gegevensbescherming

Ten aanzien van het bewaren van persoonsgegevens schrijft de AVG geen concrete bewaartermijnen voor. De AVG biedt wel enkele wettelijke kaders, zodat bepaald kan worden hoe lang gegevens bewaard moeten worden. In het algemeen geldt dat persoonsgegevens niet langer bewaard mogen worden dan de termijn die noodzakelijk is voor het doel waarvoor de persoonsgegevens zijn verzameld of worden gebruikt. Het uitgangspunt is dat het bewaren van persoonsgegevens een uitzondering is en niet de regel. Dit uitgangspunt draagt bij aan het beperkt bewaren van persoonsgegevens en het voorkomen dat de persoonsgegevens onnodig bewaard worden. Uiteindelijk blijft hierdoor het risico op datalekken beperkt.

Voor het bewaren van persoonsgegevens binnen <ORGANISATIE> geldt daarom het uitgangspunt dat persoonsgegevens bewaard worden indien dit noodzakelijk is voor het doel waarvoor de gegevens worden gebruikt. Wanneer de persoonsgegevens niet meer noodzakelijk zijn voor het bestemde doel, dan worden deze vernietigd.

2.2 Overige wetgeving

In diverse bijzondere wetten die ook voor <ORGANISATIE> relevant zijn, zijn ook regels met betrekking tot het bewaren en/of archiveren van (persoons)gegevens opgenomen. Voorbeelden hiervan zijn

onder andere de Archiefwet, belastingwetgeving, regelgeving voor jaarverslaglegging, <ZELF AANVULLEN>. Deze wetten dienen in onderlinge samenhang met de AVG te worden bezien.

Door het in kaart brengen van de verwerkingen van persoonsgegevens per verwerking, wordt beoordeeld of, en zo ja welke bijzondere wetgeving een rol speelt en hoe aan de daarin neergelegde eisen ten aanzien van de bewaartermijnen tegemoet wordt gekomen.

In bijlage D wordt meer informatie gegeven over de Archiefwet, omdat binnen het onderwijs de Archiefwet een grote rol speelt in het bewaren en vernietigen van persoonsgegevens binnen <ORGANISATIE>. Ook heeft de Autoriteit Persoonsgegevens richtlijnen voorgeschreven rondom bewaartermijnen binnen het onderwijs. In bijlage C is meer informatie uitgewerkt hierover.

3. Uitgangspunten en normen voor het bewaren van persoonsgegevens

3.1 Kernbegrippen van de AVG

Voor een goed begrip van dit beleid is het noodzakelijk om een aantal begrippen nader te omschrijven. Bij de begripsbepaling wordt zoveel mogelijk uitgegaan van de definities opgenomen in de AVG. Een overzicht van de begrippen is opgenomen in bijlage A.

3.2 Toepasselijkheid AVG

De AVG is van toepassing op *'de geheel of gedeeltelijke geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen'* (Artikel 2 AVG).

Dit betekent dat wanneer <ORGANISATIE> persoonsgegevens digitaal bewaart, de AVG van toepassing is. Maar de AVG is ook van toepassing in situaties waarin persoonsgegevens niet-digitaal worden bewaard, en er dus geen geautomatiseerde verwerking aan de orde is. Als er bijvoorbeeld sprake is van handgeschreven gespreksnotities van een leidinggevende met een werknemer in een functioneringsgesprek, dan is de AVG ook daarop van toepassing.

Voor een structurele implementatie en regelmatige actualisatie van dit beleid, is het noodzakelijk om de kaders voor het bepalen van bewaartermijnen voor persoonsgegevens vast te stellen. Naast de reeds vastgestelde bewaartermijnen in bijlage E, schrijft de AVG enkele uitgangspunten voor die gebruikt kunnen worden om nieuwe bewaartermijnen vast te stellen of bestaande bewaartermijnen te wijzigen. De onderstaande richtlijnen bieden handvatten voor het bepalen van de noodzakelijke bewaartermijnen wanneer bestaande termijnen aan herziening toe zijn, of wanneer er nieuwe categorieën persoonsgegevens bewaard worden.

3.2.1 Noodzakelijkheid

De noodzakelijkheid om persoonsgegevens te verwerken, door deze onder andere te bewaren, is afhankelijk van het gestelde doel van verwerking. Dus voor het bewaren van persoonsgegevens moet volgens de AVG vastgesteld worden welke termijn noodzakelijk is om het doel van de verwerking te bereiken. Dit geldt als hoofdregel. In beginsel is het dus de taak van <ORGANISATIE> om aan de hand van het doel van de verwerking van persoonsgegevens, te bepalen hoelang persoonsgegevens noodzakelijk bewaard moeten worden.

De noodzakelijkheid wordt getoetst aan de hand van twee criteria:

a. ***Proportionaliteit***: het type persoonsgegevens dat verwerkt wordt, moet redelijkerwijs noodzakelijk zijn om het doel (van het verwerken) te bereiken, en de gebruikte persoonsgegevens in verhouding staan tot dat doel.

b. ***Subsidiariteit***: het doel (van de verwerking van persoonsgegevens) is niet met minder, alternatieve of andere gegevens te bereiken. Een tip: als het kennelijk alleen maar 'handig' is om bepaalde persoonsgegevens te vragen aan bijvoorbeeld <relevante doelgroep zoals ouders>, dan is het gebruik van die persoonsgegevens dus niet 'noodzakelijk'.

Naast de bovengenoemde hoofdregel bestaat er in de nationale wetgeving voor enkele specifieke gegevens en documentenwetten waarin concrete bewaartermijnen zijn gesteld. Deze termijnen kunnen gelden als minimale of maximale bewaartermijnen. <ORGANISATIE> is daarom naast haar eigen beoordeling over de noodzakelijke bewaartermijn, óók gebonden aan de minimale en maximale termijnen volgens de wet. Deze termijnen worden wettelijke bewaartermijnen genoemd.

3.2.2 Bepalen bewaartermijnen

Om de bewaartermijnen voor een categorie persoonsgegevens te bepalen, is het dus van belang om eerst de noodzakelijkheid voor het bewaren van deze persoonsgegevens vast te stellen. Zoals hierboven beschreven, wordt de noodzakelijkheid bepaald aan de hand van het doel van de verwerking óf aan de hand van een wettelijke verplichting om bepaalde (persoons)gegevens te bewaren.

Wanneer er geen wettelijke bewaartermijn van toepassing is, dan geldt **de hoofdregel volgens de AVG** dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk. Het is vereist dat niet-wettelijke bewaartermijnen (bijv. bewaren van (portret)foto's) worden onderbouwd.

Bestaat er wel een wettelijke bewaartermijn, dan zullen persoonsgegevens langer bewaard moeten worden dan dat dit noodzakelijk is voor het doel. Er zal vastgesteld moeten worden wat de ingang van een bewaartermijn is, zodat voldaan kan worden aan wettelijke vereisten. Bovendien kan uit de wet volgen dat na een verlopen bewaartermijn de persoonsgegevens vernietigd óf gearchiveerd moeten worden. Om deze reden moet ook vastgesteld worden wat de opvolging is na het verstrijken van een wettelijke bewaartermijn. Moeten de persoonsgegevens worden vernietigd of gearchiveerd? In bijlage D staat beschreven wanneer persoonsgegevens op basis van de Archiefwet gearchiveerd moeten worden.

5. Organisatorisch kader

Het waarborgen van de privacy ligt niet bij één persoon. Een veelheid van personen binnen de organisatie is betrokken om aan de vereisten van de wet- en regelgeving te kunnen voldoen. Het is daarom van belang om binnen de organisatie duidelijk aan te geven wie waarvoor verantwoordelijkheid draagt.

Het doel van een heldere verdeling van taken en bevoegdheden, van middelen en rapportagelijnen is het waarborgen dat op de juiste wijze invulling wordt gegeven aan de eisen van het bewaar- en vernietigingsbeleid in lijn met de AVG en andere geldende wet- en regelgeving.
Binnen <ORGANISATIE> worden verschillende rollen met bijbehorende taken en verantwoordelijkheden onderkend. Uiteindelijk is het zorgvuldig omgaan met persoonsgegevens een verantwoordelijkheid voor iedereen in de organisatie.

5.1 Rollen en verantwoordelijkheden

5.1.1 De directie of bestuur (eindverantwoordelijke)

De directie is eindverantwoordelijk voor het bewaar- en vernietigingsbeleid en stelt het beleid en de basismaatregelen vast.
De inhoudelijke verantwoordelijkheid voor het bewaar- en vernietigingsbeleid is gemandateerd aan <INVULLEN NAAM EN FUNCTIE>

De verantwoordelijke voor ICT adviseert samen met <INVULLEN NAAM EN FUNCTIE> de directie en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen <ORGANISATIE>.

Alle werknemers hebben verantwoordelijkheid met betrekking tot privacy en informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het personeelshandboek en de <BIJVOORBEELD GEDRAGSCODE ICT EN GEBRUIK DIGITALE BEDRIJFSMIDDELEN>. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.
Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van datalekken- en beveiligingsincidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de OR).
<evt. andere taken en verantwoordelijkheden vastleggen>

De directie bevordert de beschikbaarheid van voldoende middelen om uitvoering van het bewaar- en vernietigingsbeleid te waarborgen. Naleving van de privacywetgeving is de uitdrukkelijke verantwoordelijkheid van de directie en niet van de Functionaris Gegevensbescherming.

5.1.2 Overige privacygerelateerde taken

Teamleiders (uitvoeringsverantwoordelijke):
De teamleiders zijn verantwoordelijk voor de verwerkingen en het beheer van persoonsgegevens binnen hun team op de betreffende afdeling. De teamleiders zijn medeverantwoordelijk voor het creëren van bewustwording en de naleving van het bewaar- en vernietigingsbeleid binnen de werkprocessen van de eigen afdeling.

Systeemeigenaar /functioneel beheerder:
Iedere systeemeigenaar of functioneel beheerder is verantwoordelijk voor zijn/haar applicatie en bijbehorende ICT-faciliteiten. De systeemeigenaar of functioneel beheerder moet er voor zorgen dat de applicatie blijft beantwoorden aan de eisen van de wet- en regelgeving, waaronder de privacywetgeving.

<OVERIGE ROLLEN BINNEN ORGANISATIE TOEVOEGEN>

5.2 Methodiek

Tot zover zijn de wettelijke kaders, uitgangspunten, rollen en verantwoordelijkheden die aan dit beleid ten grondslag liggen, uiteengezet. Om dit beleid integraal uit te voeren op organisatieniveau, is een bepaalde methodiek vereist.

5.2.1 Bewaren van persoonsgegevens

In het kader van dataminimalisatie is het van belang om data, het digitaal bewaren van (persoons)gegevens, zo centraal en enkelvoudig mogelijk op te slaan. Zo wordt voorkomen dat er geen overzicht is rondom het bewaren en vernietigen van persoonsgegevens. De volgende uitgangspunten gelden voor het opslaan van data:

- Data wordt enkel opgeslagen in de daarvoor bestemde en ingerichte systemen;
- De systemen waarop data wordt opgeslagen zijn enkel toegankelijk voor geautoriseerde personen;
- Er wordt niet meer data opgeslagen dan noodzakelijk (“bewaren is de uitzondering, vernietigen de regel”);
- Data wordt opgeslagen in overeenstemming met de (wettelijke) bewaartermijnen.

Om de bovenstaande uitgangspunten te realiseren, gelden de volgende regels:

- Data wordt zoveel mogelijk centraal en enkelvoudig opgeslagen op één locatie op de daarvoor bestemde en ingerichte systemen
    - Alle persoonsgegevens van <betrokkenen> worden alleen opgeslagen in <programma/informatiebeheersysteem applicatie>;
    - Alle persoonsgegevens van medewerkers worden opgeslagen in het personeelsdossier in <programma/informatiebeheersysteem applicatie>;
    - Voor het opslaan van eigen bestanden en/of mappen wordt uitsluitend gebruik gemaakt van <applicatie>;
    - Voor het opslaan van gemeenschappelijke bestanden en/of mappen wordt uitsluitend gebruik gemaakt van <applicatie>.
- Mailboxen van medewerkers worden na elk <school/kalender> jaar opgeruimd ;
- Gevoelige of bijzondere persoonsgegevens op papier worden altijd in afgesloten kasten bewaard. De autorisatie van toegang is vastgelegd via sleutelbeheer.

Ten aanzien van processen waarbij back-ups worden gemaakt van persoonsgegevens of persoonsgegevens worden teruggeplaatst uit een bestaand back-up (recovery), gelden binnen <ORGANISATIE> bepaalde gedragsregels en uitgangspunten. Deze zijn uitgewerkt in bijlage E van dit beleid.

5.2.2 Vernietigen van persoonsgegevens

<ORGANISATIE> vernietigt of archiveert persoonsgegevens zodra deze niet meer noodzakelijk zijn voor het bestemde doel of wanneer een wettelijke bewaartermijn is verstreken, zoals in dit beleid is vastgesteld. Het vernietigen van deze persoonsgegevens wordt verricht aan de hand van het vernietigingsprotocol van <ORGANISATIE>. Dit protocol is opgenomen in bijlage B van dit beleid.

5.2.3 Bijzondere persoonsgegevens

<ORGANISATIE> verwerkt ook bijzondere persoonsgegevens van <betrokkenen>. De bijzondere persoonsgegevens worden bewaard onder strenge eisen. Zo wordt bij het bewaren van bijzondere persoonsgegevens expliciet in het verwerkingsregister en in het overzicht van vastgestelde bewaartermijn, onderbouwd voor wel doel dit gedaan wordt. <evt. andere genomen maatregelen t.a.v. het verwerken van bijzondere persoonsgegevens>

Bijlage A: Definities

"AVG": De Algemene Verordening Gegevensbescherming (AVG) betreft de Verordening (EU) 2016/679 van het Europees Parlement en de Raad 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.
"Archiefwet": De Archiefwet is een Nederlandse wet uit 1995 die het beheer en de toegang van overheidsarchieven regelt.
"Archiveren": Met ***archiveren*** wordt bedoeld het bewaren van gegevens op een gespecialiseerde bewaarplaats, ingericht voor de opslag van documenten zoals bijvoorbeeld een archief. Het archief kan zich in een [relevante locatie] bevinden, maar er kan bijvoorbeeld ook sprake zijn van een regionaal of provinciaal archief.
"Bewaartermijn (AVG)":[1] Een ***bewaartermijn*** volgens de AVG houdt de periode in dat persoonsgegevens ten minste bewaard moeten blijven voor hetgeen waar ze nodig voor zijn, daarna moeten ze worden vernietigd. Een bewaartermijn die met privacy of de AVG te maken heeft, is dus tegelijk een minimale én maximale bewaartermijn.
"Bewaartermijn (Archiefwet)": In de ***Archiefwet***[2] betekent bewaren dat de (persoons)gegevens ongelimiteerd moeten worden bewaard. Een bewaartermijn in de Archiefwet betekent dat de gegevens na afloop van die termijn naar een aangewezen archief moeten worden overgebracht (dus uit het eigen archief naar een provinciaal of landelijk archief). De gegevens worden dus niet vernietigd. Als gegevens volgens de Archiefwet na een bepaalde vastgestelde periode vernietigd moeten worden, dan wordt dit een ***vernietigingstermijn*** genoemd. Een bewaartermijn gaat pas in nadat het gebruik van de persoonsgegevens is beëindigd.
"Dataminimalisatie":[3] Een van de vijf vuistregels voor het omgaan met persoonsgegevens is dataminimalisatie. Dit betekent dat alleen die persoonsgegevens gebruikt worden die noodzakelijk zijn en dat goed nagedacht wordt over welke persoonsgegevens gevraagd, opslagen en bewaard worden.
"Verwerken":[4] Onder verwerken wordt verstaan: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
"Vernietigen": Gegevens op papier kunnen eenvoudig worden vernietigd, door het papier en de kopieën te vernietigen. Bij digitale gegevensdragers wordt informatie gewist, maar gemakshalve noemen we het wissen van digitale gegevens óók vernietigen.
"Persoonsgegevens":[5] Persoonsgegevens zijn gegevens die direct of indirect te herleiden zijn tot mensen. Op het verwerken van deze gegevens is de AVG van toepassing. Als we spreken over gegevens, data of informatie dan gaat dat niet alleen over persoonsgegevens, het kan ook over de jaarcijfers gaan. Belangrijk is om te onthouden dat als informatie (in)direct tot mensen herleidbaar is, de AVG van toepassing is.

[1] Artikel 5 lid 1 sub c AVG; overweging 39 AVG.
[2] Zie hoofdstuk 7 voor een uitleg wanneer deze van toepassing is.
[3] Artikel 5 lid 1 sub c AVG.
[4] Artikel 4 sub 2 AVG.
[5] Artikel 4 sub 1 AVG.

Bijlage B: Vernietigingsprotocol

Inleiding

Binnen [ORGANISATIE] wordt voor het opslaan van data, het digitaal bewaren van (persoons)gegevens, gebruik gemaakt van zowel elektronische gegevensdragers, zoals (interne en externe) harde schijven en servers, als conventionele gegevensdragers, zoals papier en (plak)notities. Persoonsgegevens die op deze gegevensdragers zijn opgeslagen moeten vernietigd worden zodra deze niet meer noodzakelijk zijn. De noodzakelijkheid is onder meer afhankelijk van (wettelijke) bewaartermijnen, en in- en uitdiensttreding van personeel dat gebruik maakt van gegevensdragers.

In lijn met het beleid over bewaar- en vernietigingstermijnen, en wet- en regelgeving op het domein van privacy en informatiebeveiliging, is dit protocol opgesteld om richtlijnen te bieden aan medewerkers van [ORGANISATIE] voor het veilig vernietigen van data op zowel elektronische als conventionele gegevensdragers. Dit protocol ziet toe op de vernietiging van data in het algemeen en beperkt zich daarom niet uitsluitend tot het vernietigen van *persoons*gegevens. De vernietiging van data is belegd bij de afdeling [ICT/andere afdeling] van [ORGANISATIE] of een leverancier van ICT-middelen als hiervoor goede afspraken en controlemaatregelen bestaan in bijvoorbeeld in een verwerkersovereenkomst. Afspraken over het vernietigen van data wordt afgedwongen en gecontroleerd zodat [ORGANISATIE] de regie hierop houdt.

Uitgangspunten van het veilig vernietigen van data op gegevensdragers

Een standaard proces van veilige vernietiging van data op gegevensdragers draagt bij aan het minimaliseren van het data-gebruik door [ORGANISATIE] zodat het risico op datalekken beperkt blijft. Gegevensdragers kunnen immers vertrouwelijke informatie bevatten die binnen de organisatie moet blijven om de privacy van medewerkers en betrokkenen te waarborgen . Hiervoor gelden de volgende uitgangspunten voor zowel elektronische gegevensdragers als voor conventionele gegevensdragers binnen [ORGANISATIE]:

Elektronische gegevensdragers (i.e.: USB-sticks, harde schijven, servers, laptops, computers, smartphones, opslaglocaties van data voor bepaalde applicaties)

- De vernietiging van data op alle elektronische gegevensdragers wordt op eenzelfde standaard werkwijze uitgevoerd, namelijk door middel van het overschrijven van de gegevensdrager met een willekeurig bitpatroon;
- De fysieke opslag van elektronische gegevensdragers gebeurt op een veilige wijze totdat de gegevens vernietigd worden. De opslag vindt daarom plaats in de afgesloten ruimte [vindplaats ruimte]. [Persoon] heeft uitsluitend toegang tot deze ruimte OPTIONEEL: *zoals staat vermeld in de autorisatiematrix van [ORGANISATIE]*;
- Alle activiteiten rondom het vernietigen van, en verkrijgen van toegang tot data opgeslagen op beheerde elektronische gegevensdragers, wordt geregistreerd in een daartoe bestemde [register/ander document];
- Indien vernietiging van data op een elektronische gegevensdrager niet mogelijk is, dan wordt de gegevensdrager fysiek vernietigd door [persoon] of door een goedgekeurde derde partij;
- Indien de vernietiging van data wordt uitgevoerd door een derde partij, dan wordt daaraan voorafgaand een verwerkersovereenkomst afgesloten met deze partij.

De bovengenoemde uitgangspunten zijn voor zover mogelijk ook van toepassing op elektronische gegevensdragers van derde partijen waar informatie met betrekking tot [ORGANISATIE] is opgeslagen.

Conventionele gegevensdragers (i.e.: plaknotities, papier, boeken, fysieke dossiers)

- Er wordt een onderscheid gemaakt tussen gevoelige informatie of informatie die (in)direct herleidbaar is naar een individu en informatie van algemene aard;
- Gevoelige informatie of informatie die (in)direct herleidbaar is naar een individu wordt uitsluitend bewaard voor zover dit noodzakelijk is;
- Bij het bewaren van conventionele gegevensdragers met gevoelige informatie of informatie die (in)direct herleidbaar is naar een individu, wordt gebruik gemaakt van afgesloten opslagplaatsen zoals een bureaulade met een slot of een afgesloten dossierkamer met beperkte toegang;
- [Persoon] heeft uitsluitend toegang tot dossierkamer waar conventionele gegevensdragers bewaard worden
- Alle activiteiten rondom het vernietigen van, en verkrijgen van toegang, tot data op beheerde conventionele gegevensdragers (zoals opgeslagen dossiers) wordt geregistreerd in een daartoe bestemde [register/ander document];
- Bij het vernietigen van conventionele gegevensdragers wordt gebruik gemaakt van *een (afsluitbare) papierbak voor gevoelige informatie* EN/OF *een versnippermachine voor papieren documenten bij zeer gevoelige informatie voordat deze wordt afgevoerd bij oud papier*.

Verantwoordelijkheid vernietiging data op gegevensdragers

De verantwoordelijkheid om data op elektronische gegevensdragers te vernietigen ligt bij [persoon]. [Persoon] is verantwoordelijk voor het actueel houden van de procedure vernietigen van data op gegevensdragers. Van alle stappen in het proces wordt een logboek bijgehouden door de uitvoerenden. Dit logboek dient ter controle van de uitgevoerde activiteiten en om de wettelijke plicht rondom bewaren en vernietigen aantoonbaar te maken.

OPTIONEEL: Jaarlijkse inventarisatie van data

In het kader van dataminimalisatie maakt [afdeling] ieder jaar op [datum] een overzicht van data die vernietigd moet (laten) worden. Hiervan wordt verslag gemaakt door [afdeling/persoon]. Dit verslag wordt gecommuniceerd met de directie.

Back-ups en recovery

De back-up van data betreft het proces waarbij een identieke kopie van data op het actieve systeem gemaakt wordt op een ander systeem als een beveiligingsmaatregel. Wanneer er een calamiteit is waardoor de data van de back-up teruggeplaatst moet worden op het actieve systeem, spreken we van recovery. Daarbij kunnen ook persoonsgegevens teruggeplaatst zijn. Na een recovery moet altijd geverifieerd worden of er persoonsgegevens teruggeplaatst zijn die op een (recente) selectielijst hebben gestaan. Selectielijsten geven weer welke (categorie) persoonsgegevens relevant zijn voor het van toepassing zijnde doel. Zie bijlage D voor meer informatie over selectielijsten.

[De centrale ICT afdeling/of een andere afdeling] is verantwoordelijk voor het maken van back-ups en het eventueel terugplaatsen van gegevens.

Met de huidige back-uptechnieken is het over het algemeen niet mogelijk op een specifiek persoonsgegeven uit de back-up te vernietigen. Dit heeft te maken met het formaat waarin data opgeslagen wordt op de back-up. Het is niet herkenbaar als persoonsgegeven. Mogelijk wordt een back-up zelfs onbruikbaar voor recovery wanneer er onderdelen uit verwijderd zijn.

Het is daarom niet nodig om alle back-ups te vernietigen of te schonen van alle persoonsgegevens, als de volgende uitgangspunten worden nageleefd;

- Enkel noodzakelijke informatie wordt opgeslagen in een back-up en niet standaard “alles”;
- Voor het maken van back-ups wordt uitsluitend gebruik gemaakt van speciale programmatuur voor het maken van back-ups op specifieke apparatuur geschikt voor het maken van back-ups (opslaan van data op USB-sticks volstaat niet als een back-up oplossing);
- Na terugplaatsing van data vanwege een recoveryproces vindt een check op de selectielijsten plaats. Reeds vernietigde data wordt na recovery wederom vernietigd. Hiervan wordt een registratie bijgehouden;
- Bij de terugplaatsing van data gedurende het recoveryproces, houdt [de centrale ICT afdeling/of een andere afdeling] rekening met eventueel verwijderde of gecorrigeerde gegevens in het kader van de rechten van de betrokkene. Dit wordt gedaan door de herstelde data na te lopen op persoonsgegevens die verwijderd of aangepast zijn naar aanleiding van een uitoefeningsverzoek, en de verwijdering of aanpassing te handhaven. Hiervoor wordt het register van uitoefeningsverzoeken geraadpleegd;
- In de autorisatiematrix is vastgelegd wie toegangsrechten heeft tot back-ups en de daarmee samenhangende werkzaamheden;
- Er wordt gebruik gemaakt van een opslagplaats van de back-ups met een beperkte toegang;
- Bij de processen van het maken van back-ups en de toepassing van een recovery wordt gebruik gemaakt van logging zodat inzichtelijk is wie op welk moment toegang heeft geprobeerd te krijgen of heeft gekregen tot bepaalde systemen;
- Back-ups worden zo snel mogelijk overschreven.

Bovenstaande regels gelden ook als er een back-up wordt teruggezet bij of door de leverancier van bijvoorbeeld het administratiesysteem.

Inzameling elektronische gegevensdragers

1. Er wordt een aanvraag gedaan door een medewerker bij [persoon] om één of meerdere elektronische gegevensdragers af te laten voeren voor de vernietiging van data;
2. Door [persoon] wordt geïnventariseerd welke aangemelde gegevensdragers in aanmerking komen voor datavernietiging en wordt vastgesteld of er (zeer) gevoelige data (potentieel) aanwezig is op de gegevensdrager;

3. De elektronische gegevensdrager wordt *door de medewerker zelf aangeleverd bij [afdeling]* OF *wordt door [persoon] afgehaald*. [MAAK HIERIN EEN KEUZE];
4. *De aanlevering* OF *afname* van de elektronische gegevensdrager wordt geregistreerd door [persoon];
5. De afleverende medewerker ontvangt een bewijs van aflevering van de elektronische gegevensdrager;
6. De elektronische gegevensdrager wordt beveiligd opgeslagen in [ruimte].

Vernietiging van data op elektronische gegevensdragers

De data op de elektronische gegevensdrager wordt vernietigd. Indien vernietiging van de data niet mogelijk is, dan zal de gegevensdrager fysiek vernietigd worden door [persoon/instantie].

De vernietiging van data vindt plaats door de elektronische gegevensdrager te overschrijven met een willekeurige patroon. Hierbij wordt onderscheid gemaakt tussen 'reguliere' data en (zeer) gevoelige of bijzondere data. Voor het vernietigen van (zeer) gevoelige data is het enkelvoudig overschrijven van de gegevensdrager niet voldoende en wordt het medium meervoudig overschreven. Wanneer dit niet mogelijk is of indien de aard van de data zéér gevoelig of bijzonder is, dan wordt de gegevensdrager fysiek vernietigd door [persoon/instantie].

OPTIONEEL: Toezicht op vernietiging

Het vernietigen van elektronische gegevensdragers vindt plaats door twee personen zodat een adequaat toezicht op de vernietiging gewaarborgd is. [Persoon 1] houdt toezicht op de uitvoering van de vernietiging van data door [persoon 2]. [Persoon 1] brengt verslag uit van de vernietiging met de vermelding van de benodigde informatie (zoals serienummer van de gegevensdrager, betrokken personen en omschrijving van de vernietiging). Het verslag wordt ondertekend door [persoon 1 (en persoon 2)].

Controle na vernietiging data op elektronische gegevensdragers

Nadat data is vernietigd op elektronische gegevensdragers wordt gecontroleerd of de vernietiging van data succesvol heeft plaatsgevonden. Deze controle wordt vastgelegd in [het register/ander document] door [persoon].

Dit protocol "*Vernietigen data op gegevensdragers"* is voor het laatst gewijzigd op: (<datum>)
Vastgesteld op (<datum>) door (<…>)
Goedgekeurd op (<datum>) door (<…>

Bijlage C: Bewaartermijnen in het onderwijs

De Autoriteit Persoonsgegevens (AP) heeft voor onderwijsorganisaties een bewaartermijn van twee jaar genoemd als richtlijn voor het bewaren van persoonsgegevens van leerlingen. De AP merkt kinderen aan als extra kwetsbaar en daardoor moeten onderwijsinstellingen zorgvuldig omgaan met de persoonsgegevens van leerlingen. De persoonsgegevens van leerlingen worden na vertrek van school na twee jaar vernietigd (voor het speciaal onderwijs is dat drie jaar). Dit is anders wanneer specifieke wetgeving een andere bewaartermijn aangeeft.

Onderwijswetten

In de onderwijswetten zijn specifieke regels opgenomen voor het bewaren van (persoons)gegevens. Hierbij is meestal per wet en per bewaartermijn een aparte afweging opgenomen waarom die informatie persé bewaard moet worden.

Er gelden onder andere (langere) wettelijke bewaartermijnen voor:

- Gegevens van een oud-leerling in de leerlingenadministratie (5 jaar);
- Gegevens over verzuim en in- en uitschrijving (5 jaar na vertrek);
- Gegevens over een leerling die naar een school voor speciaal onderwijs is verwezen (3 jaar na vertrek).

Digitaal leermateriaal en toetsen

Voor gegevens met betrekking tot digitaal leermateriaal, gelden er geen specifieke wettelijke bewaartermijnen. Scholen hebben meestal gedurende een heel schooljaar de informatie nodig van het digitaal leermiddel dat ze gebruiken, plus gegevens van het jaar daarvoor. Dit om ontwikkelingen en trends te kunnen zien, maar ook als een leerling blijft zitten kunnen gegevens worden vergeleken en (her)gebruikt. Voor het VO geldt daarbij dat leerlingen doorgaans examens afleggen in de laatste twee schooljaren. Zo wordt er bijvoorbeeld in de 3e klas van het vmbo al examen gedaan in maatschappijleer of wordt de rekentoets afgelegd. Dat betekent dat in het kader van examinering en het Examenbesluit, deze 6 maanden na het verlaten van de school door de leerlingen, bewaard moeten blijven. In het geval dat een leerling in de bovenbouw blijft zitten, heeft dit dus ook gevolgen voor het langer bewaren van zijn gegevens in het digitaal leermateriaal.

Uit de Tijdelijke handreiking bewaartermijnen van Kennisnet wordt met betrekking tot het digitaal leermateriaal, de volgende bewaartermijnen van toepassing verklaard:

- VO onderbouw (en PO): gegevens huidige schooljaar, plus het schooljaar voorafgaand aan lopende schooljaar;
- VO bovenbouw: gegevens huidige schooljaar, plus twee schooljaren voorafgaand aan lopende schooljaar.

Deze bewaartermijnen voor digitaal leermateriaal zijn richtlijnen, waarbij afhankelijk van het type dienst of product afwijkingen mogelijk zijn. Zo is het mogelijk dat bij adaptief leermateriaal gegevens langer bewaard moeten worden om trends of leergedrag in beeld te brengen, afhankelijk van de wijze van analyse van die data. Belangrijk is dat het schoolbestuur afspraken maakt met de leverancier over het bewaren en vernietigen van de persoonsgegevens. Na beëindigen van de licentie op een digitaal leermiddel, moeten persoonsgegevens altijd vernietigd worden, of worden overgedragen (teruggegeven) aan de school. Hierover moeten expliciete afspraken worden gemaakt. Dit wordt meestal geregeld in een verwerkersovereenkomst.

Bijlage D: Archiefwet

Hieronder is de Archiefwet toegelicht vanuit het perspectief van het onderwijs.

De AVG stelt archivering in het algemeen belang, voor wetenschappelijk of historisch onderzoek en archivering voor statistische doeleinden buiten het toepassingsbereik van de algemene regel dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk . Zo laat de AVG ruimte om in nationale wetgeving nadere regels te stellen ten aanzien van archivering van persoonsgegevens. In Nederland is dit gebeurd door middel van de Archiefwet. Op basis van de Archiefwet mogen persoonsgegevens langer bewaard worden als dit voorgeschreven wordt.

De Archiefwet heeft alleen betrekking op overheidsgegevens. Dit betekent dat de Archiefwet van toepassing is op overheidsorganisaties (gemeenten en openbare lichamen) die (gedeeltelijk) taken van openbaar gezag uitoefenen. Gegevens die dergelijke organisaties verwerken vallen onder de Archiefwet. De gemeente bepaalt– doorgaans – de bewaartermijnen en archiefregels.

Openbare scholen worden in stand gehouden door een openbaar lichaam, gemeente of openbare rechtspersoon (al dan niet via een gemeenschappelijke regeling). Hierdoor vallen openbare scholen onder de taak van een gemeente en dus onder de Archiefwet. Zo geeft de gemeente invulling aan wat er bewaard moet worden. Het schoolbestuur valt onder de gemeentelijke archiefinspectie. Scholen met een publiekrechtelijke rechtsvorm vallen, omdat ze onderdeel zijn van de overheid, voor hun gehele archiefbeheer onder de Archiefwet.

Het bijzonder onderwijs valt alleen onder de Archiefwet voor zover het bestuur overheidstaken uitvoert (openbaar gezag).

Het gaat hierbij om:

- Het afgeven van getuigschriften door het bevoegd gezag op grond van onderwijswetgeving;
- Besluiten tot het verlenen van vrijstelling op grond van de Leerplichtwet.

Archiefbescheiden waarop de Archiefwet van toepassing is, mogen alleen vernietigd worden als ze in een geldige selectielijst staan vermeld en daarin als vernietigbaar zijn aangemerkt. In een selectielijst is ook aangegeven of - en welke - archiefbescheiden naar een gemeentearchief of regionaal historisch centrum (RHC) overgebracht moeten worden. Dit noemen we archiefbewaarplaatsen.

De PO-Raad en VO-raad zijn in overleg met o.a. het ministerie van OCW en het Nationaal Archief over het opstellen van een sectorale selectielijst (basisselectiedocument). Daarmee komt er meer duidelijkheid over de precieze bewaartermijnen.

Er wordt, tot er een basisselectiedocument is, <u>géén</u> informatie en documentatie vernietigd rondom vrijstellingen van de Leerplichtwet, ook diploma's en (eindexamen)cijferlijsten worden níet vernietigd.

Bijlage E: Bewaartermijnen

Hieronder is een overzicht opgenomen met diverse categorieën van persoonsgegevens en de daarbij behorende bewaartermijnen en wettelijke grondslag. In kolom 3 van de tabellen staan richtlijnen vermeld voor de te hanteren bewaartermijn. Deze richtlijnen betreffen doorgaans maximale bewaartermijnen, maar in sommige gevallen wordt er een minimale bewaartermijn voorgeschreven in de wet. <ORGANISATIE> houdt zich aan de gestelde maximale termijn uit de wet.

Ook wordt in kolom 3 vaak verwezen naar de Wet bescherming persoonsgegevens (Wbp) die reeds vervallen is, samen met het daarbij horende Vrijstellingsbesluit. De concrete bewaartermijnen die bij deze vervallen wet zijn vastgesteld blijven relevant vanwege de afweging die de wetgever destijds heeft gemaakt en die nu door <ORGANISATIE> is gemaakt. De wettelijk vervallen termijnen dienen als richtlijn om de bewaartermijn vast te stellen.

Tabel bewaartermijnen persoonsgegevens leerlingen/oud-leerlingen (onderwijskundig)

	Brongegevens en grondslag	**Ingangsdatum bewaartermijn**	**Richtlijn bewaartermijn (wet/AVG)**	**Bepaalde bewaartermijn**	**Verantwoording langere bewaartermijn**	**Vernietigen/wissen volgens protocol door**
1	Het onderwijskundig rapport	datum van uitschrijving	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
2	Gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen	datum van uitschrijving	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
3	Gegevens over leerprestaties van de leerling	datum van uitschrijving	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
4	Werk van het centraal examen en de re-kentoets	na vaststelling	6 maanden (art. 57 Examenbesluit) Let op: verplichte wettelijke termijn!	[…]	[…]	[…]

		van de uitslag				
5	Verslagen van gesprekken met de ouders	datum van uitschrijving	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
6	Psychologisch rapport	datum van uitschrijving	maximaal 2 jaar Wanneer het rapport wordt opgevraagd bij een school voor po in het kader van toelating tot een school voor vo 3 en maximaal 5 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
7	Adresgegevens	datum van uitschrijving	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
8	Gegevens over het gebruik van ICT-middelen en het schoolnetwerk	moment van opname	maximaal 6 maanden (art. 32 lid 6 en art. 34 lid 5 Vrijstellings-besluit Wbp oud)	[…]	[…]	[…]
9	[…]	[…]	[…]	[…]	[…]	[…]
10	[…]	[…]	[…]	[…]	[…]	[…]

Tabel bewaartermijnen persoonsgegevens leerlingen/oud-leerlingen (administratief)

	Brongegevens en grondslag	**Ingangsdatum bewaartermijn**	**Richtlijn bewaartermijn (wet/AVG)**	**Bepaalde bewaartermijn**	**Verantwoording langere bewaartermijn**	**Vernietigen/wissen volgens protocol door**
1	Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school ontvangt	na afloop van het schooljaar waarop de bekostiging	7 jaar (art. 103a lid 3 Wvo) Let op: verplichte wettelijke termijn!	[…]	[…]	[…]

		betrekking heeft				
2	Gegevens over in– en uitschrijving	datum van uitschrijving	5 jaar (art. 6 Bekostigingsbesluit Wvo) Let op: verplichte wettelijke termijn!	[…]	[…]	[…]
3	Gegevens over verzuim en afwezigheid	datum van uitschrijving	5 jaar (art. 6 Bekostigingsbesluit Wvo) Let op: verplichte wettelijke termijn!	[…]	[…]	[…]
4	Gegevens met betrekking tot de vergoeding van de kosten verbonden aan leerlingvervoer	na afloop van het schooljaar waarop de verstrekking van de vergoeding betrekking heeft	maximaal 2 jaar (art. 21 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
5	Communicatiegegevens oud-leerlingen	datum van uitschrijving	Verwijderen op verzoek van de leerling of bij diens overlijden (art. 41 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
6	[…]	[…]	[…]	[…]	[…]	[…]
7	[…]	[…]	[…]	[…]	[…]	[…]
8	[…]	[…]	[…]	[…]	[…]	[…]

Het overzicht van bewaartermijnen inzake persoonsgegevens van leerlingen/oud-leerlingen is voor het laatst gewijzigd op: (<datum>)
Vastgesteld op (<datum>) door (<…>)
Goedgekeurd op (<datum>) door (<…>)

Tabel bewaartermijnen persoonsgegevens personeel

	Brongegevens en grondslag	Ingangsdatum bewaartermijn	Richtlijn bewaartermijn (wet/AVG)	Bepaalde bewaartermijn	Verantwoording langere bewaartermijn	Vernietigen/wissen volgens protocol door
1	Akte van aanstelling/ arbeidsovereenkomst	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
2	Wijzigingen arbeidsovereenkomst	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
3	Correspondentie inzake benoemingen, promotie, demotie	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
4	Aanspraken in verband met de beëindiging van het dienstverband	datum waarop aanspraken zijn geëindigd	maximaal 2 jaar (art. 9 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
5	Afspraken inzake werk MR	einde lidmaatschap	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
6	Burgerlijke staat werknemer	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
7	Kopie getuigschrift	einde dienstverband	maximaal 2 jaar (art. 9 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
8	Afspraken inzake opleidingen	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]

9	Aanvraag opleiding door werknemer	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
10	Afspraken omtrent loopbaan	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
11	Verslagen functionerings- en beoordelings-gesprekken	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
12	Correspondentie UWV en bedrijfsarts	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
13	Verslaglegging inzake Wet Verbetering Poortwachter	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
14	Verzuimregistratie als werkgever eigenrisi-codrager Ziektewet is	einde dienstverband	5 jaar De bedrijfsarts moet de gegevens 10 jaar bewaren. In verband met eigenrisicodragerschap WGA mogen de gegevens voor de duur van het WGA-traject bewaard blijven (10 jaar). (art. 3 lid 2 Regeling werkzaamheden, administratieve voorschriften en kosten eigenrisicodragen ZW) Let op: verplichte wettelijke termijn!	[…]	[…]	[…]
15	Verslaglegging van correspondentie met betrekking tot problematische	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]

	(financiële) privé-situatie					
16	Loonbeslagen	-	tot opheffing (art. 9 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
17	Correspondentie met betrekking tot jubilea	-	tot einde dienstverband (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
18	Correspondentie directie/PZ/direct leidinggevende	-	afhankelijk van ontslagsituatie bij einde dienstverband of tot maximaal 2 jaar daarna (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
19	Identiteitspapieren van derden ingeleende vreemdelingen waarvoor een tewerkstellingsvergunning is verleend	einde dienstverband	5 jaar (art. 15 lid 4 Wet arbeid vreemdelingen) Let op: verplichte wettelijke termijn!	[…]	[…]	[…]

Tabel bewaartermijnen persoonsgegevens sollicitanten

	Brongegevens en grondslag	Ingangsdatum bewaartermijn	Richtlijn bewaartermijn (wet/AVG)	Bepaalde bewaartermijn	Verantwoording langere bewaartermijn	Vernietigen/wissen volgens protocol door
1	Sollicitatiebrief, -formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek	na beëindiging sollicitatieprocedure of einde dienstverband/benoemings-termijn	maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant (art. 5 lid 6 en art. 7 lid 5 Vrijstellingsbesluit Wbp oud)			
2	[…]	[…]	[…]	[…]	[…]	[…]

Het overzicht van bewaartermijnen inzake persoonsgegevens van personeel en sollicitanten is voor het laatst gewijzigd op: (<datum>)
Vastgesteld op (<datum>) door (<…>)
Goedgekeurd op (<datum>) door (<…>)

Tabel bewaartermijnen persoonsgegevens leveranciers

	Brongegevens en grondslag	**Ingangsdatum bewaartermijn**	**Richtlijn bewaartermijn (wet/AVG)**	**Bepaalde bewaartermijn**	**Verantwoording langere bewaartermijn**	**Vernietigen/wissen volgens protocol door**
1	Persoonsgegevens van (vertegenwoordigers van) leveranciers	nadat de desbetreffende transactie is afgewikkeld	maximaal 2 jaar (art. 13 lid 5 Vrijstellingsbesluit Wbp *oud*)			
2	[…]	[…]	[…]	[…]	[…]	[…]

Tabel bewaartermijnen persoonsgegevens huurders

	Brongegevens en grondslag	**Ingangsdatum bewaartermijn**	**Richtlijn bewaartermijn (wet/AVG)**	**Bepaalde bewaartermijn**	**Verantwoording langere bewaartermijn**	**Vernietigen/wissen volgens protocol door**
1	Persoonsgegevens van huurders	maximaal 2 jaar nadat de huur is beëindigd	maximaal 2 jaar (art. 14 lid 5 Vrijstellingsbesluit Wbp oud)			
2	[…]	[…]	[…]	[…]	[…]	[…]

Tabel bewaartermijnen persoonsgegevens alle bovengenoemde categorieën en bezoekers

	Brongegevens en grondslag	**Ingangsdatum bewaartermijn**	**Richtlijn bewaartermijn (wet/AVG)**	**Bepaalde bewaartermijn**	**Verantwoording langere bewaartermijn**	**Vernietigen/wissen volgens protocol door**
1	Camera en videobeelden	moment van opname	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten (art. 38 lid 6 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
2	Gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de video-opnamen zijn gemaakt.	moment van opname	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten (art. 38 lid 6 Vrijstellingsbesluit Wbp oud)	[…]	[…]	[…]
3	Registratielijsten bezoekers	moment van registratie	niet langer dan nodig (art. 5 lid 1e AVG)			
4	[…]	[…]	[…]	[…]	[…]	[…]

Het overzicht van bewaartermijnen inzake persoonsgegevens van overige betrokkenen is voor het laatst gewijzigd op: (<datum>)
Vastgesteld op (<datum>) door (<…>)
Goedgekeurd op (<datum>) door (<…>)