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	2.0 Onderwijs
Auteur	Eddy Brunekreef.
Opsteldatum	15 mei 2023

Versie geschiedenis:

Versie	Status	Datum	Auteur	Omschrijving
001	**Ontwerp**	**07-06-2022**	**BRR**	**Conceptversie**
002	**Controle**	**29-06-2022**	**BRR**	**Goedgekeurd door Hoofd ICT.**
003	**Controle FG**	**30-06-2022**	**BRR**	**Goedgekeurd door de Lumen Group.**
004	**Aanbieden GMR**	**24-11-2022**	**BRR**	**Aangeboden voor goedkeuring GMR.**
005	**Goedgekeurd**	**24-11-2022**	**BRR**	**Goedgekeurd GMR.**

Vastgesteld door OGMF:

Versie	Datum	Naam	Functie
001	09-02-2023	**Drs. M. Sprenger**	**Voorzitter College van Bestuur**

Inhoud

Bewaar- en vernietigingsbeleid OGMF.

1. Inleiding

1.1 Waarom een bewaar- en vernietigingsbeleid?

OGMF is een openbare scholengemeenschap. OGMF heeft werknemers in dienst en richt zich onder andere op leerlingen in het Vo segment. Dit betekent dat OGMF omgaat met veel persoonsgegevens van zowel medewerkers als leerlingen en andere betrokkenen. OGMF 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 OGMF 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.

OGMF 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 OGMF persoonsgegevens niet langer bewaart dan noodzakelijk is voor het doel waarvoor de persoonsgegevens zijn verzameld. Het beperkt bewaren van persoonsgegevens verkleint de risico op datalekken. In het bewaar- en vernietigingsbeleid worden de kaders voor het bewaren en vernietigen van persoonsgegevens vastgelegd

1.2 Reikwijdte

OGMF gebruikt gegevens van medewerkers en leerlingen voor het uitvoeren van onder andere de primaire taakstelling binnen het onderwijssegment van het VO. Hiervoor worden persoonsgegevens opgeslagen en bewaard. Het opslaan of bewaren van persoonsgegevens is een vorm van verwerking van deze gegevens. Voor het bewaren van elk gegeven dient een specifiek doel aanwezig te zijn. Het vaststellen van een doel draagt bij aan de tenuitvoerlegging van dit bewaar- en vernietigingsbeleid. Wanneer de persoonsgegevens niet meer noodzakelijk zijn voor het vastgestelde doel, dan zullen deze persoonsgegevens vernietigd worden.

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 OGMF verantwoordelijk voor is. Bij de invoering van het beleid zullen de proceseigenaren, systeemeigenaren en gegevenseigenaren worden betrokken. Vanuit informatiebeveiliging is het belangrijk dat uiteindelijk passende maatregelen zijn genomen om te voldoen aan wet- en regelgeving.

Bewaarde persoonsgegevens
Dit bewaar- en vernietigingsbeleid heeft betrekking op de categorieën persoonsgegevens zoals deze in het privacy beleid van OGMF is opgenomen. In bijlage E staan de bewaartermijnen die binnen OGMF 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 weergeeft de ingangsdatum van de bewaartermijn, 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. OGMF 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 eisen toegestaan. Binnen OGMF wordt ook bijzondere persoonsgegevens bewaard van werknemers en leerlingen. OGMF ziet extra toe op een juiste naleving van dit beleid met betrekking tot bijzondere persoonsgegevens. Dit doet zij 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 OGMF 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 aan, 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 zodat de risico op datalekken beperkt blijft.

Voor het bewaren van persoonsgegevens binnen OGMF 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 OGMF relevant zijn, zijn ook regels met betrekking tot het bewaren en/of archiveren van (persoons)gegevens opgenomen. Voorbeelden hiervan zijn onder andere de Wet register onderwijsdeelnemers, Archiefwet, belastingwetgeving, regelgeving voor jaarverslaglegging, etc. 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 welke bijzondere wetgeving een rol speelt en hoe aan de daarin neergelegde eisen ten aanzien van de bewaartermijnen tegemoet kan worden gekomen.

In bijlage D wordt meer informatie gegeven over de Archiefwet, omdat binnen het VO de Archiefwet een grote rol speelt in het bewaren en vernietigen van persoonsgegevens binnen OGMF. 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 het OGMF persoonsgegevens per computer worden bewaard, de AVG van toepassing is. Maar de AVG is ook van toepassing in situaties waarin handmatig persoonsgegevens worden bewaard, en er dus geen geautomatiseerde verwerking aan de orde is. Als er bijvoorbeeld sprake is van geschreven gespreksnotities van een leidinggevende met een werknemer in een functioneringsgesprek, dan is de AVG ook 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 aan 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 OGMF 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 staan 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 goede tip: als het kennelijk alleen maar 'handig' is om bepaalde persoonsgegevens te vragen aan bijvoorbeeld ouders of sportverenigingen, 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 documenten wetten waarin concrete bewaartermijnen gesteld. Deze termijnen kunnen gelden als minimale of maximale bewaartermijnen. OGMF 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. Hierom 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.

4. 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 OGMF worden verschillende rollen met bijbehorende taken en verantwoordelijkheden onderkend. Uiteindelijk is het zorgvuldig omgaan met persoonsgegevens een verantwoordelijkheid voor iedereen in de organisatie.

4.1 Rollen en verantwoordelijkheden

4.1.1 De bestuurder (eindverantwoordelijke)

De bestuurder is eindverantwoordelijk voor het bewaar- en vernietigingsbeleid en stelt het beleid en de basismaatregelen op het gebied van bewaren en vernietigen van persoonsgegevens vast.
De inhoudelijke verantwoordelijkheid voor het bewaar- en vernietigingsbeleid is gemandateerd aan Eddy Brunekreef, Privacy Officer.

De verantwoordelijke voor ICT adviseert samen met Eddy Brunekreef, Privacy Officer, de bestuurder en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen OGMF.

Alle werknemers hebben verantwoordelijkheid met betrekking tot privacy en informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven o.a. op de website en in het regelement ICT-middelen. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.
Medewerkers wordt 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 (G)MR.

De bestuurder 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 bestuurder en niet van de Functionaris Gegevensbescherming.

4.1.2 Overige privacy gerelateerde taken

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

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

4.2 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 bepaald methodiek vereist.

4.2.1 Bewaren van persoonsgegevens

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

- Data wordt enkel opgeslagen in de daarvoor bestemde en ingerichte systemen;
- De systemen waarop data worden 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 leerlingen worden alleen opgeslagen in het leerlingvolgsysteem.
    - Alle persoonsgegevens van medewerkers worden opgeslagen in het personeelsdossier in Afas Insite;
    - Voor het opslaan van eigen bestanden en/of mappen wordt uitsluitend gebruik gemaakt van Office 365;
    - Voor het opslaan van gemeenschappelijke bestanden en/of mappen wordt uitsluitend gebruik gemaakt van Office 365 en interne server-opslagmedia.
- Mailboxen van medewerkers moeten conform wettelijke bewaartermijnen, opgeruimd worden na de gestelde termijn bij beëindiging van de aanstelling;
- Gevoelige of bijzondere persoonsgegevens op papier moeten altijd in opgesloten kasten bewaard te worden. 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), geldt binnen OGMF-gedragsregels en bepaalde uitgangspunten. Deze gedragsregels en uitgangspunten zijn uitgewerkt in bijlage E van dit beleid.

4.2.2 Vernietigen van persoonsgegevens

OGMF 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 OGMF. Dit protocol is opgenomen in bijlage B van dit beleid.

4.2.3 Bijzondere persoonsgegevens

OGMF verwerkt ook bijzondere persoonsgegevens van leerlingen en medewerker. 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 welk doel dit gedaan wordt. In alle situaties is er overleg met de Privacy Officer als zich nieuwe ontwikkelingen voordoet t.a.v. bijzondere persoonsgegevens.

Bijlage A: Definities

Om de gebruikte begrippen in dit bewaar- en vernietigingsbeleid voldoende inzichtelijk en duidelijk te maken, worden de begrippen hieronder kort toegelicht.

"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 lokale opslag bevinden, maar er kan bijvoorbeeld ook sprake zijn van een cloudopslag. Denk bij die laatste aan bijvoorbeeld het LVS of Afas Insite.
"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 gegeven 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 start pas te lopen 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 OGMF wordt voor het opslaan van (persoons)gegevens/data gebruik gemaakt van zowel elektronische gegevensdragers, zoals (interne en externe) harde schijven en servers, als conventionele gegevensdragers, zoals papier en plaknotities. 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 OGMF voor het veilig vernietigen van data op zowel elektronische als conventionele gegevensdragers. De vernietiging van data is belegd bij de betreffende applicatiebeheerders en/of de afd. ICT van OGMF of een leverancier van ICT-middelen indien hiervoor goede afspraken en controlemaatregelen bestaan in bijvoorbeeld in een verwerkersovereenkomst. Afspraken over het vernietigen van data moeten afgedwongen en gecontroleerd kunnen worden zodat OGMF de regie hierop kan houden.

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 OGMF opdat de risico op datalekken hierdoor beperkt blijft. Gegevensdragers kunnen immers vertrouwelijke informatie bevatten die binnen de organisatie moeten blijven zodat de privacy van medewerkers en betrokkenen gewaarborgd blijven. Hiervoor zijn de volgende uitgangspunten voor zowel elektronische gegevensdragers als voor conventionele gegevensdragers die gelden binnen OGMF:

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 dient op éénzelfde standaard werkwijze te worden uitgevoerd;
- De fysieke opslag van elektronische gegevensdragers dient op een veilige wijze plaats te vinden totdat de gegevens veilig vernietigd kunnen worden. De opslag vindt daarom plaats in de afgesloten ruimte bij de afd. ICT. De toegang tot deze ruimte komt uitsluitend toe tot personeel van de afd. ICT of onder toezicht van dit personeel;
- Vernietiging van programmatuur en gegevens op de gegevensdrager(s) van elektronische gegevensdragers, vindt plaats door middel van het overschrijven van de gegevensdrager met een willekeurig bit-patroon;
- Alle activiteiten rondom het vernietigen van, en verkrijgen van toegang, tot data op elektronische gegevensdragers wordt geregistreerd in een daartoe bestemde log bestanden of middels certificaten van vernietiging door een specialistisch bedrijf.
- Indien vernietiging van data op een elektronische gegevensdrager niet mogelijk is, dan dient de gegevensdrager fysiek te worden vernietigd door een goedgekeurde derde partij;
- Indien de vernietiging van data wordt uitgevoerd door een derde partij, dan moet daaraan voorafgaand een verwerkersovereenkomst worden 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 OGMF is opgeslagen.

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

- Er dient een onderscheid gemaakt te worden 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 dient uitsluitend bewaard te worden voor zover dit noodzakelijk is;
- Bij het bewaren van conventionele gegevensdragers met gevoelige informatie of informatie die (in)direct herleidbaar is naar een individu, dient gebruik te worden gemaakt van afgesloten opslagplaatsen zoals een bureaulade met een slot of een afgesloten dossierkamer met beperkte toegang;
- De toegang tot dossierkamer waar conventionele gegevensdragers bewaard kunnen worden komt uitsluitend toe tot functioneel rechthebbende binnen OGMF;
- Alle activiteiten rondom het vernietigen van, en verkrijgen van toegang, tot data op conventionele gegevensdragers wordt geregistreerd in een daartoe bestemde logbestanden;
- 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 alvorens deze wordt afgevoerd bij oud papier*.

Verantwoordelijkheid vernietiging data op gegevensdragers

De verantwoordelijkheid om data op elektronische gegevensdragers te vernietigen ligt bij Privacy Officer. Deze 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.

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 ten aanzien van bestaande data. Wanneer er een calamiteit is waardoor de data van de back-up teruggeplaatst moeten 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.

De afd. ICT van OGMF 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 kan te maken hebben met het formaat waarin data opgeslagen wordt op de back-up. Het is niet herkenbaar als persoonsgegeven. Mogelijk wordt een back-up onbruikbaar voor recovery wanneer er onderdelen uit verwijderd zijn.

Het is niet nodig om alle back-ups te vernietigen of te schonen van alle persoonsgegevens, indien 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 speciaal gemaakte 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 gedurende het recovery proces vindt een check op de selectielijsten plaats. Reeds vernietigde data worden na recovery wederom vernietigd. Hiervan wordt een registratie bijgehouden;
- Bij de terugplaatsing van data gedurende het recovery proces, houdt de afd. ICT van OGMF rekening met eventueel verwijderde of gecorrigeerde gegevens in het kader van de rechten van de betrokkene;
- In de autorisatiematrix is vastgelegd wie toegangsrechten heeft tot back-ups en de daarmee samenhangende werkzaamheden;
- Er wordt gebruik gemaakt van een opslagplaats van 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 gemaakt wordt wie op welk moment toegang heeft geprobeerd te krijgen of heeft gekregen tot bepaalde systemen;
- Bij het overschrijven van back-ups wordt de kortst mogelijke bewaartermijn gehanteerd.

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

Verzameling elektronische gegevensdragers

1. Er wordt een aanvraag gedaan door een medewerker bij de Service desk om één of meerdere elektronische gegevensdragers af te laten voeren voor de vernietiging van data;
2. Door Service desk medewerker wordt geïnventariseerd welke aangemelde gegevensdragers in aanmerking komen voor data vernietiging en dient vastgesteld te worden of (zeer) gevoelige data (potentieel) aanwezig is op de gegevensdrager;
3. De elektronische gegevensdrager wordt medewerker van de afd. ICT verzameld voor vernietiging.
4. De opgehaalde elektronische gegevensdragers worden geregistreerd door een medewerker van de afd. ICT;
5. De afleverende medewerker ontvangt een bewijs van aflevering van de elektronische gegevensdrager;
6. De elektronische gegevensdrager wordt beveiligd opgeslagen in een afgesloten ruimte bij de afd. ICT.

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 moeten worden door een medewerker van de afd. ICT.

De vernietiging van data vindt plaats door de elektronische gegevensdrager te overschrijven met een willekeurige patroon. Hierbij moet onderscheid gemaakt te worden 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 moet de medium meervoudig overschreven te worden. Wanneer dit niet mogelijk is of indien de aard van de data zéér gevoelig of bijzonder is, dan moet de gegevensdrager fysiek vernietigd te worden door een medewerker van de afd. ICT of een gecertificeerd bedrijf.

Controle na vernietiging data op elektronische gegevensdragers

Nadat data is vernietigd op elektronische gegevensdragers moet gecontroleerd worden of de vernietiging van data succesvol heeft plaatsgevonden. Deze controle dient vastgelegd te worden in Topdesk door een medewerker van de afd. ICT.

Dit protocol "*Vernietigen data op gegevensdragers"* is voor het laatst gewijzigd op: 10-06-2022
Goedgekeurd op 24-11-2022 door GMR.
Vastgesteld op 09-02-2023 door het CvB.

Bijlage C: Bewaartermijnen voor 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 om gaan met de persoonsgegevens van leerlingen. De persoonsgegevens van leerlingen moeten na verloop van twee jaar vernietigd worden (voor het speciaal onderwijs is dat drie jaar), wanneer zij van school vertrekken. 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);
- Adresgegevens van (oud-)leerlingen voor het organiseren van reünies.

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.

Met betrekking tot het digitaal leermateriaal, zijn de volgende bewaartermijnen van toepassing:

- 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 leermaterialen geven vuistregels voor het bewaren van gegevens voor digitaal leermateriaal, 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 kunnen 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. Dit wordt geregeld in de verwerkersovereenkomst.

Bedacht moet worden dat na beëindigen van de licentie op een digitaal leermiddel, persoonsgegevens altijd vernietigd moeten worden, of worden overgedragen (teruggegeven) aan de school. Ook hierover kunnen extra afspraken worden gemaakt.

Bijlage D: Archiefwet

Hieronder is de Archiefwet die eventueel van toepassing is op OGMF, toegelicht vanuit het perspectief van het onderwijs.

De AVG stelt archivering in het algemeen belang, voor wetenschappelijk of historisch onderzoek en archivering voor statische 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 toepassing van de Archiefwet strekt zich enkel uit over overheidsgegevens. Dit betekent dat de Archiefwet van toepassing is voor organisaties die in stand worden gehouden door de overheid (gemeente of openbaar lichaam) of (gedeeltelijk) taken van openbaar gezag uitoefenen. Gegevens die dergelijke organisaties verwerken vallen hiermee onder de Archiefwet. De gemeente bepaalt dan – doorgaans – de bewaartermijnen en archiefregels.

Gegevens en archiefbescheiden mogen volgens de Archiefwet alleen vernietigd worden als ze in een geldige selectielijst staan vermeld en daarin als vernietigbaar zijn aangemerkt, en de archiefbescheiden naar een overheidsarchief moeten.

Openbare scholen worden in stand gehouden door een openbaar lichaam, gemeente of openbare rechtspersoon (al dan niet via een gemeenschappelijke regeling). Hiermee vallen scholen onder de taak van een gemeente. Daarmee vallen deze openbare scholen 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, diploma's en (eindexamen)cijferlijsten.

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. OGMF houdt zich ten minste aan de gestelde minimale of 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 die nu door OGMF gemaakt moet worden. De wettelijk vervallen termijnen kunnen daarom 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 5 jaar (art. 20 Wet register onderwijsdeelnemers)	[5]	[…]	[Applicatie beheerder]
2	Gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen (Dit is afhankelijk van of deze gegevens kwalificeren als	datum van uitschrijving	minimaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp oud) tot maximaal 5 jaar (art. 20 Wet register onderwijsdeelnemers)	[2]	[…]	[Applicatie beheerder]

	basisgegevens van de leerling)[6]					
3	Gegevens over leerprestaties van de leerling	datum van uitschrijving	maximaal 5 jaar (art. 20 Wet register onderwijsdeelnemers)	[5]	[…]	[Applicatie beheerder]
4	Werk (cijfers) van het centraal examen en de re-kentoets	na vaststelling van de uitslag	maximaal 5 jaar (art. 20 Wet register onderwijsdeelnemers)	[5]	[…]	[Applicatie beheerder]
5	Verslagen van gesprekken met de ouders	datum van uitschrijving	maximaal 5 jaar (art. 20 Wet register onderwijsdeelnemers)	[5]	[…]	[Applicatie beheerder]
6	Psychologisch rapport (Dit is afhankelijk van of het psychologisch rapport kwalificeert als basisgegeven van de leerling)	datum van uitschrijving	minimaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp oud) tot maximaal 5 jaar (art. 20 Wet register onderwijsdeelnemers)	[2]	[…]	[Applicatie beheerder]
7	Adresgegevens	datum van uitschrijving	maximaal 5 jaar (art. 20 Wet register onderwijsdeelnemers)	[5]	[…]	[Applicatie beheerder]
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)	[1 maand]	[…]	[Systeem beheerder]
9	[…]	[…]	[…]	[…]	[…]	[…]
10	[…]	[…]	[…]	[…]	[…]	[…]

[6] In artikel 11 van de Wet register onderwijsdeelnemers wordt aangegeven dat ook gegevens over gezondheid deel uit kunnen maken van de basisgegevens. Indien dit het geval is, geldt er een bewaartermijn van maximaal 5 jaar.

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 betrekking heeft	minimaal 7 jaar (art. 103a lid 3 Wvo) Let op: verplichte wettelijke termijn!	[7]	[…]	[Applicatie beheerder]
2	Gegevens over in– en uitschrijving	datum van uitschrijving	maximaal 5 jaar (art. 20 Wet register onderwijsdeelnemers)	[5]	[…]	[Applicatie beheerder]
3	Gegevens over verzuim en afwezigheid	datum van uitschrijving	maximaal 5 jaar (art. 20 Wet register onderwijsdeelnemers)	[5]	[…]	[Applicatie beheerder]
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)	[2]	[…]	[Applicatie beheerder]
5	Communicatiegegevens oud-leerlingen	datum van uitschrijving	Verwijderen op verzoek van de leerling of bij diens overlijden (art. 41 lid 5 Vrijstellingsbesluit Wbp oud)	[Datum uitschrijving]	[…]	[Applicatie beheerder]
6	[…]	[…]	[…]	[…]	[…]	[…]

7	[…]	[…]	[…]	[…]	[…]	[…]
8	[…]	[…]	[…]	[…]	[…]	[…]

Het overzicht van bewaartermijnen inzake persoonsgegevens van leerlingen/oud-leerlingen is voor het laatst gewijzigd op: 10-06-2022
Goedgekeurd op 24-11-2022 door GMR.
Vastgesteld op 09-02-2023 door het CvB.

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]	[…]	[Applicatie beheerder/P&O]
2	Wijzigingen arbeidsovereenkomst	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[2]	[…]	[Applicatie beheerder/P&O]
3	Correspondentie inzake benoemingen, promotie, demotie	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[2]	[…]	[Applicatie beheerder/P&O]
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)	[2]	[…]	[Applicatie beheerder/P&O]
5	Afspraken inzake werk MR	einde lidmaatschap	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[2]	[…]	[Applicatie beheerder/P&O]
6	Burgerlijke staat werknemer	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[2]	[…]	[Applicatie beheerder/P&O]
7	Kopie getuigschrift	einde dienstverband	maximaal 2 jaar (art. 9 lid 5 Vrijstellingsbesluit Wbp oud)	[2]	[…]	[Applicatie beheerder/P&O]
8	Afspraken inzake opleidingen	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[2]	[…]	[Applicatie beheerder/P&O]

9	Aanvraag opleiding door werknemer	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[2]	[…]	[Applicatie beheerder/P&O]
10	Afspraken omtrent loopbaan	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[2]	[…]	[Applicatie beheerder/P&O]
11	Verslagen functionerings- en beoordelings-gesprekken	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[2]	[…]	[Applicatie beheerder/P&O]
12	Correspondentie UWV en bedrijfsarts	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[2]	[…]	[Applicatie beheerder/P&O]
13	Verslaglegging inzake Wet Verbetering Poortwachter	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[2]	[…]	[Applicatie beheerder/P&O]
14	Verzuimregistratie als werkgever eigenrisicodrager Ziektewet is	einde dienstverband	minimaal 5 jaar De bedrijfsarts moet de gegevens minimaal 10 jaar bewaren. In verband met eigenrisicodrager-schap 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!	[5]	[…]	[Applicatie beheerder/P&O]
15	Verslaglegging van correspondentie met betrekking tot problematische	einde dienstverband	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[2]	[…]	[Applicatie beheerder/P&O]

	(financiële) privé-situatie					
16	Loonbeslagen	-	tot opheffing (art. 9 lid 5 Vrijstellingsbesluit Wbp oud)	[tot opheffing]	[…]	[Applicatie beheerder/P&O]
17	Correspondentie met betrekking tot jubilea	-	tot einde dienstverband (art. 7 lid 5 Vrijstellingsbesluit Wbp oud)	[tot einde dienstverband]	[…]	[Applicatie beheerder/P&O]
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)	[2]	[…]	[Applicatie beheerder/P&O]
19	Identiteitspapieren van derden ingeleende vreemdelingen waarvoor een tewerkstellings-vergunning is verleend	einde dienstverband	minimaal 5 jaar (art. 15 lid 4 Wet arbeid vreemdelingen) Let op: verplichte wettelijke termijn!	[5]	[…]	[Applicatie beheerder/P&O]

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)	[maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant]		[Applicatie beheerder/P&O]
2	[…]	[…]	[…]	[…]	[…]	[…]

Het overzicht van bewaartermijnen inzake persoonsgegevens van personeel en sollicitanten is voor het laatst gewijzigd op: 10-06-2022
Goedgekeurd op 24-11-2022 door GMR.
Vastgesteld op 09-02-2023 door het CvB.

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]		[Applicatie beheerder/PSA]
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]		[Applicatie beheerder/PSA]
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)	[maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten]	[…]	[Geautomatiseerd/Privacy Officer]
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)	[maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten]	[…]	[Geautomatiseerd/Privacy Officer]
3	Registratielijsten bezoekers	moment van registratie	niet langer dan nodig (art. 5 lid 1e AVG)	[niet langer dan nodig]		[Conciërge locaties]
4	[…]	[…]	[…]	[…]	[…]	[…]

Het overzicht van bewaartermijnen inzake persoonsgegevens van overige betrokkenen is voor het laatst gewijzigd op: 10-06-2022
Goedgekeurd op 24-11-2022 door GMR.
Vastgesteld op 09-02-2023 door het CvB.