Reglement gegevensbescherming en privacy medewerkers

Naam	**SIKO**
Van	College van bestuur
Aan	Gemeenschappelijke Medezeggenschapsraad (GMR)
Document	Reglement gegevensbescherming en privacy medewerkers
Documentversie	januari 2020

Inleiding

Iedere schoolorganisatie verwerkt persoonsgegevens van zijn medewerkers. Dit is onvermijdelijk, immers zouden zonder deze verwerkingen zaken als het uitbetalen van salaris en het voeren van een basisadministratie voor de Belastingdienst onmogelijk zijn.

De organisatie dient de persoonlijke levenssfeer van de medewerkers zo goed mogelijk te beschermen en daarbij de verplichte maatregelen zoals omschreven in de Algemene verordening gegevensbescherming (AVG) in acht te nemen.

Dit privacyreglement is onderdeel van deze maatregelen. Hierin legt SIKO afspraken met betrokkenen (in dit geval medewerkers) vast omtrent de verwerking van hun persoonsgegevens.

Met dit privacyreglement wil SIKO duidelijkheid geven over het beleid en de regels van onze organisatie over de omgang met privacy en de verwerking van persoonsgegevens van medewerkers.

Voor algemene informatie over de verwerking van persoonsgegevens verwijzen we in Nederland onder meer naar de website van de Autoriteit Persoonsgegevens. De tekst van de Algemene verordening gegevensbescherming (AVG) en de daarop gebaseerde regelgeving is eveneens op deze website terug te vinden.

1. Definities

In dit privacyreglement wordt verstaan onder:

Persoonsgegevens
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

> *Uitleg: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon is een persoonsgegeven. Denk hierbij aan naam, adresgegeven. Er zijn vele soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Echter, ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens.*

Daarnaast kunnen er nog vele andere persoonsgegevens zijn. Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden ook wel bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd.

Verwerking van persoonsgegevens
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Uitleg: in het kort gaat bij het bij verwerking dus om alle handelingen die een organisatie kan uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen. In het kader van dit reglement gaat het voornamelijk om gegevens die omwille van sociale regelgeving in het personeelsdossier worden bijgehouden.

Bestand
Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen

Verwerkingsverantwoordelijke
De natuurlijke persoon, rechtspersoon of ieder ander die, of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Wanneer er in dit reglement gesproken wordt over de verwerkingsverantwoordelijke dan wordt daarmee SIKO bedoeld.

Functionaris voor de Gegevensbescherming (FG)
Degene die onder verantwoordelijkheid van de verwerkingsverantwoordelijke is belast met de (dagelijkse) zorg voor de verwerking van persoonsgegevens en toezicht houdt op de naleving van de privacyregels binnen de organisatie.

Verwerker
Degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Uitleg: de verwerker is degene die in opdracht van SIKO persoonsgegevens verwerkt.

Betrokkene
Degene op wie een persoonsgegeven betrekking heeft.

2. De reikwijdte en het doel van dit reglement

2.1. Dit reglement stelt regels over de verwerking van persoonsgegevens van medewerkers door SIKO

2.2. Dit reglement is van toepassing op alle persoonsgegevens van medewerkers die door SIKO worden verwerkt. Het doel van dit reglement is:

a. de persoonlijke levenssfeer van medewerkers van wie persoonsgegevens worden verwerkt te beschermen tegen misbruik van die gegevens en tegen het verwerken van onjuiste gegevens;
b. te voorkomen dat persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze verzameld zijn;
c. de rechten van de medewerkers zoals die onder meer voortvloeien uit de AVG te waarborgen.

3. Het doel van de verwerking van persoonsgegevens

3.1. Slechts die persoonsgegevens worden verwerkt, die rechtmatig verkregen zijn, zoals bedoeld in artikel 6 AVG. SIKOverwerkt uitsluitend persoonsgegevens voor onder meer de navolgende doeleinden:
a. Het voeren van sollicitatieprocedures;
b. Het voeren van een personeelsadministratie;
c. Het voeren van een salarisadministratie;
d. Het voeren van een pensioenadministratie;
e. Het kunnen verstrekken van uitkeringen bij ontslag;
f. Het maken van een roosterindeling.

3.2. SIKO verwerkt niet meer gegevens dan noodzakelijk is om de hiervoor beschreven doelen te bereiken.

4. De grondslag voor de verwerking

4.1. Verwerking van persoonsgegevens gebeurt alleen op grond van:
a. Toestemming: als de medewerker voor de verwerking zijn toestemming heeft verleend.
b. Overeenkomst: als de gegevensverwerking noodzakelijk is voor het sluiten of de uitvoering van een (arbeids)overeenkomst.
c. Wettelijke verplichting: als de gegevensverwerking noodzakelijk is op grond van een wet waaraan SIKO zich moet houden.
d. Vitaal belang: als het over een belang gaat dat essentieel is voor iemands leven of gezondheid en die persoon niet om toestemming kan worden gevraagd.
e. Algemeen belang: de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan SIKO is opgedragen.
f. Gerechtvaardigd belang: als SIKO een gerechtvaardigd belang heeft om de persoonsgegevens te verwerken, tenzij het recht op privacy van de medewerker voor gaat.

5. De soorten gegevens die verwerkt worden

5.1 Onder meer de navolgende persoonsgegevens worden verwerkt:
a. Naam, voornamen, voorletters, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer;
b. Het burgerservicenummer (BSN) van de medewerker;

c. Nationaliteit van de medewerker;
d. Persoonsgegevens ten aanzien van de personeelsadministratie, zoals bank en-betaalgegevens, gegevens omtrent de opleiding en ervaring van de medewerker, ziekteverzuim en beoordelingssystemen.

5.2 Een gedetailleerde opgave van verwerkte privacy- en persoonsgevoelige informatie is beschikbaar via document: **Opgave verwerkte privacy- en persoonsgevoelige informatie medewerkers**

5.3 Persoonsgegevens worden door SIKO op naam van de medewerker verzameld. De verzameling van persoonsgegevens van de medewerker vormt ten dele het personeelsdossier.

6. Verstrekking van en toegang tot persoonsgegevens

6.1. Persoonsgegevens worden slechts verstrekt aan degenen die worden genoemd in het register van verwerkingsactiviteiten. Een gedetailleerde opgave is beschikbaar via document: **Register van verwerkingsactiviteiten**

6.2. Behoudens daartoe strekkende wettelijke voorschriften in wet- en regelgeving hebben slechts toegang tot de persoonsgegevens, degenen, waaronder begrepen derden, die zijn belast met of leiding geven aan de activiteiten die in verband staan met de verwerking van de gegevens of die daarbij noodzakelijk zijn betrokken.

6.3. De verwerker en eenieder die onder het gezag van de verwerkingsverantwoordelijke of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt deze uitsluitend in opdracht van de verwerkingsverantwoordelijke, tenzij hij Unierechtelijk of lidstaatrechtelijk tot de verwerking gehouden is.

7. Monitoren van gebruik ICT en internet op school

7.1 Voor het gebruik van ICT-systemen en internet op school wordt gebruik gemaakt van software waarmee ICT- en internetgebruik door medewerkers gecontroleerd kan worden.

7.2 SIKO slaat gegevens over het gebruik van ICT en internet door medewerkers op voor de volgende doelen:

a. Het verbeteren van de ICT-systemen;
b. Het opsporen van medewerkers die schade aan de ICT-systemen hebben veroorzaakt;
c. Het blokkeren van usb-poorten, bepaalde software en sociale media wanneer dit ongewenst is (bijvoorbeeld in bepaalde lessen).

8. Beveiliging en geheimhouding

8.1 Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke (en de verwerker) passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

8.2 Indien sprake is van elektronische verwerking van persoonsgegevens zal de beheerder via een coderingsbeveiliging de verschillende personen, als bedoeld in artikel 5, toegang geven tot bepaalde gedeelten van de persoonsgegevens of tot alle persoonsgegevens al naar gelang hun werkzaamheden dit vereisen.

8.3 Eenieder die betrokken is bij de uitvoering van dit reglement en daarbij de beschikking krijgt over persoonsgegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs kan vermoeden en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift ter zake van de persoonsgegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding daarvan. Dit geldt niet indien enig wettelijk voorschrift hem tot bekendmaking verplicht of uit zijn taak bij de uitvoering van dit reglement de noodzaak tot bekendmaking voortvloeit.

8.4 De verwerkingsverantwoordelijke zal conform artikel 34 van de AVG een inbreuk onverwijld aan betrokkene mededelen, indien de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

8.5 Eenieder die betrokken is bij de uitvoering van dit reglement en op de hoogte raakt van een (mogelijk) inbreuk op de beveiliging zoals bedoeld in art. 6.4 is verplicht, zo spoedig mogelijk, doch in ieder geval binnen 24 uur na kennisneming, hiervan onverwijld melding te maken bij de verwerkingsverantwoordelijke of Veiligheidsfunctionaris.

9. Informatieverstrekking

9.1 De verwerkingsverantwoordelijke informeert betrokkene over het verwerken van diens persoonsgegevens, voorafgaand aan de verzameling van de persoonsgegevens of, indien de gegevens van derden afkomstig zijn, voorafgaand aan het moment van vastlegging.

9.2 De verwerkingsverantwoordelijke informeert betrokkene over de categorieën persoonsgegevens die worden verwerkt, met welk doel dat gebeurt, aan wie de gegevens worden verstrekt. In voorkomend geval worden de contactgegevens van de FG verstrekt en wordt de betrokkene geïnformeerd in het geval dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een derde land of een internationale organisatie; tevens geeft de verwerkingsverantwoordelijke in dat geval aan of er al dan niet een adequaatheidsbesluit van de Europese Commissie bestaat en in het geval van in artikel 46, artikel 47 of artikel 49, lid 1, tweede alinea AVG, bedoelde doorgiften, welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd.

9.3 Wanneer de gegevens bij de betrokkene worden verzameld, verstrekt de verwerkingsverantwoordelijke tevens de informatie zoals genoemd in artikel 13 lid 2 AVG.

9.4 Wanneer de gegevens niet van de betrokkene zijn verkregen, verstrekt de verwerkingsverantwoordelijke tevens de informatie zoals genoemd in artikel 14 lid 2 AVG.

9.5 Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld, verstrekt de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in lid 2.

9.6 Voornoemde informatie hoeft niet te worden verstrekt, wanneer de betrokkene reeds over de informatie beschikt.

9.7 Indien de informatie niet van de betrokkene zelf is verkregen, behoeft de informatie tevens niet te worden verstrekt indien het verstrekken van die informatie onmogelijk blijkt of

onevenredig veel inspanning zou vergen, het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven bij Unie- of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen, of de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van Unierecht of lidstatelijke recht, waaronder een statutaire geheimhoudingsplicht.

9.8 Indien de informatie niet van de betrokkene zelf is verkregen, verstrekt de verwerkingsverantwoordelijke de in deze bepaling bedoelde informatie binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens. Indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, wordt de informatie uiterlijk op het moment van het eerste contact met de betrokkene verstrekt. Indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, wordt de informatie verstrekt uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.

10. Het melden van datalekken

10.1. Wanneer er een inbreuk op de beveiliging van SIKO plaatsvindt die waarschijnlijk ongunstige gevolgen zal hebben voor privacy een medewerker, dan brengt SIKO de medewerker zo spoedig mogelijk op de hoogte van de betreffende inbreuk op de beveiliging.

10.2. SIKO hoeft geen melding te maken indien zij passende technische en organisatorische beschermingsmaatregelen heeft genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling.

10.3. SIKO hoeft evenmin melding te maken als dit onevenredige inspanning zou vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

11. Rechten betrokkene

11.1 Elke betrokkene komen de rechten toe zoals omschreven in de artikelen 15 tot en met 22 van de AVG.

11.2 Indien de verwerkingsverantwoordelijke twijfelt aan de identiteit van de verzoeker, vraagt hij zo spoedig mogelijk aan de verzoeker schriftelijk nadere gegevens inzake zijn identiteit te verstrekken of een geldig identiteitsbewijs te overleggen. Door dit verzoek wordt de termijn opgeschort tot het tijdstip dat het gevraagde bewijs is geleverd

11.3 Een verzoek zoals bedoeld in artikel 13 tot en met 22 AVG dient te worden gedaan aan de verwerkingsverantwoordelijke, die binnen een redelijke termijn, doch in ieder geval binnen één maand aan dit verzoek gehoor geeft. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

12. Bewaartermijn

12.1. SIKO bewaart de persoonsgegevens niet langer dan noodzakelijk is voor het vervullen van het doel waarvoor zij zijn verkregen. SIKO zal persoonsgegevens niet langer bewaren dan op grond van de AVG en de daarop gebaseerde regelgeving is toegestaan.

13. Klachten of geschillen

13.1. Indien de betrokkene van mening is dat de bepalingen van de AVG en de daarop gebaseerde regelgeving niet of niet op juiste wijze door SIKO worden nageleefd, dan kan betrokkene zich wenden tot de verwerkingsverantwoordelijke of de FG.

14. Inwerkingtreding en duur

14.1. Dit reglement kan aangehaald worden als “Privacyreglement medewerkers” en treedt in werking op 22 april 2020.

14.2. Dit reglement zal, na inwerkingtreding, in beginsel iedere twee jaar worden herzien.

14.3. SIKO is bevoegd om evidente verschrijvingen in het reglement te corrigeren, dan wel tekstuele aanpassingen te doen, indien en voor zover dit de inhoud, aard en strekking van dit reglement en de daarin opgenomen bepalingen niet doen wijzigen. Daadwerkelijke inhoudelijke wijzigingen in dit privacyreglement zullen, indien van toepassing, ter instemming worden voorgelegd aan Gemeenschappelijke Medezeggenschapsraad.

15. Slotbepaling

15.1. De Gemeenschappelijke Medezeggenschapsraad van SIKO heeft haar instemming gegeven voor de inhoud van dit document.

15.2. In het geval van onvoorziene omstandigheden, is SIKO gerechtigd van dit reglement af te wijken, een en ander slechts indien er sprake is van een direct en zwaarwegend belang voor SIKO of de medewerker.

16. Contact

16.1. Bij vragen kunnen medewerkers contact opnemen met de verwerkingsverantwoordelijke, diens gevolmachtigde FG of Veiligheidsfunctionaris.

Gebruik van dit privacyreglement

Het geheel of gedeeltelijk gebruik van dit privacyreglement is uitsluitend toegestaan door de rechtmatige licentienemer van YourSafetynet school+. De inhoud van dit privacyreglement is beschermd door copyright © waardoor het niet is toegestaan om dit privacyreglement:

- Te vermenigvuldigen en/of openbaar te maken door middel van druk, fotokopie, microfilm of op enigerlei wijze zonder nadrukkelijke schriftelijke toestemming van Media Security Networks BV
- Te gebruiken indien de huidige licentieovereenkomst van YourSafetynet school+ is vervallen

Dit privacyreglement is zorgvuldig en naar beste weten samengesteld. Regel- en wetgeving zijn voortdurend aan verandering onderhevig waardoor Media Security Networks BV niet kan instaan voor de juistheid of volledigheid hiervan. Media Security Networks BV aanvaardt geen enkele aansprakelijkheid voor schade, van welke aard dan ook, als gevolg van handelingen en/of beslissingen die op basis van dit privacyreglement zijn genomen.