Privacyreglement
Stichting Basisschool De Ridderslag
mei 2018

1. Toepasselijkheid

Dit reglement geldt voor de gehele organisatie die deel uitmaakt van Stichting Basisschool de Ridderslag, gevestigd aan de Ridder van Catsweg 256a te Gouda.

2. Definities

Persoonsgegevens

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'), zoals bijvoorbeeld naam, adres, geboortedatum, titel(s), geslacht, adres, telefoonnummer, e-mailadres, functie, personeelsnummer, medische rapportages, inhoud van e-mails, prestaties/cijfers, brieven, klachten, foto's, video's, IP-adressen, tracking cookies, loginnamen en wachtwoorden.

Verwerking van persoonsgegevens

Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, geautomatiseerd of handmatig, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Bijzondere persoonsgegevens

Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, genetische gegevens (DNA/RNA) of biometrische gegevens (bijv. foto's) met het oog op de unieke identificatie van een persoon, en gegevens over gezondheid, of iemands seksueel gedrag of seksuele gerichtheid.

Betrokkene

Degene op wie een persoonsgegeven betrekking heeft, en die al dan niet wordt vertegenwoordigd door een wettelijk vertegenwoordiger. Betrokkenen kunnen bijvoorbeeld zijn: leerlingen, ouders, medewerkers en bezoekers.

Wettelijk vertegenwoordiger

Degene die het ouderlijk gezag over een minderjarige uitoefent. Meestal zal dit een ouder zijn, maar het kan ook gaan om een voogd. Als een leerling 16 jaar of ouder is, beslist hij in voorkomende gevallen zelf over zijn privacy.

Verwerkingsverantwoordelijke

De entiteit die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit reglement is het bevoegd gezag, te weten het bestuur van Stichting Basisschool De Ridderslag, vertegenwoordigd door de schoolleider, de verwerkingsverantwoordelijke.

Verwerker	De natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zoals bijvoorbeeld de leverancier van een leerlingvolgsysteem of leerling-administratiesysteem. Een verwerker heeft een uitvoerende taak, ten behoeve van de activiteiten van de verwerkingsverantwoordelijke.
Derde	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, de verwerkingsverantwoordelijke, de verwerker, of de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om persoonsgegevens te verwerken.
Stichting Basisschool de Ridderslag	De verwerkingsverantwoordelijke in de zin van dit reglement, hierna kortweg aangeduid als 'De Ridderslag'.

3. Reikwijdte en doelstelling

1. Dit reglement stelt regels over de verwerking van persoonsgegevens van alle betrokkenen bij de organisatie, waaronder leerlingen en hun wettelijk vertegenwoordigers, medewerkers, bezoekers en externe relaties (bijv. leveranciers en opdrachtnemers).
2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door De Ridderslag worden verwerkt. Het reglement heeft tot doel:
a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens;
b. vast te stellen met welk doel en op welke (juridische) grondslag persoonsgegevens binnen De Ridderslag worden verwerkt;
c. ook overigens te borgen dat persoonsgegevens binnen De Ridderslag rechtmatig, transparant en behoorlijk worden verwerkt;
d. de rechten van betrokkenen vast te leggen en te borgen dat deze rechten door De Ridderslag worden gerespecteerd.

4. Doelen van de verwerking van persoonsgegevens

Bij de verwerking van persoonsgegevens houdt De Ridderslag zich aan de relevante wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG), de uitvoeringswet AVG en de onderwijswetgeving.

Doelen

1. De verwerking van persoonsgegevens vindt plaatst voor:
a. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, het voorzien in hun (extra) ondersteuningsbehoefte, dan wel het geven van schooladviezen;
b. het verstrekken en/of ter beschikking stellen van leermiddelen;
c. het bewaken van de veiligheid binnen de scholen en het beschermen van eigendommen van medewerkers, leerlingen en bezoekers;
d. het bekend maken van informatie over de organisatie en leermiddelen als bedoeld onder a en b;
e. het bekend maken van de activiteiten van de organisatie, bijvoorbeeld op de website van De Ridderslag, in nieuwsbrieven, brochures of de schoolgids of via *social media*;

f. het berekenen, vastleggen en innen van bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen, alsmede het verzoeken om vrijwillige bijdragen;
g. het aanvragen van bekostiging, het behandelen van geschillen daarover en het doen uitoefenen van accountantscontrole;
h. het onderhouden van contacten met oud-leerlingen;
i. het aangaan en uitvoeren van arbeidsovereenkomsten, samenwerkingsrelaties met opdrachtnemers en contracten met leveranciers;
j. de uitvoering of toepassing van wet- en regelgeving;
k. juridische procedures waarbij De Ridderslag betrokken is.
2. De verwerking van persoonsgegevens mag ook plaatsvinden voor doelen die verenigbaar zijn met de doelen zoals beschreven in lid 1.

5. Doelbinding

Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. De Ridderslag verwerkt niet meer gegevens dan noodzakelijk is om de betreffende doelen te bereiken.

6. Soorten persoonsgegevens

De categorieën van persoonsgegevens zoals deze binnen De Ridderslag worden verwerkt, worden geregistreerd in een verwerkingsregister.

7. Grondslag verwerking

Verwerking van persoonsgegevens gebeurt alleen indien aan een van de onderstaande voorwaarden is voldaan:

a. 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 De Ridderslag is opgedragen.

b. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op De Ridderslag rust.

c. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (bijvoorbeeld de arbeidsovereenkomst) of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.

d. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van Stichting Basisschool de Ridderslag of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen, met name wanneer de betrokkene een kind is; in het kader van deze grondslag zal dus een belangenafweging moeten plaatsvinden.

e. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen (levensbelang).

f. De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.

9. Bewaartermijnen

Stichting Basisschool de Ridderslag bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor deze worden verwerkt, tenzij het langer bewaren van de persoonsgegevens op grond van wet- of regelgeving verplicht is.

10. Toegang

Binnen de organisatie van De Ridderslag geldt dat personen slechts toegang hebben tot persoonsgegevens voor zover dat daadwerkelijk nodig is. De toegang van medewerkers tot persoonsgegevens is dan ook beperkt tot de gegevens die noodzakelijk zijn voor de goede uitoefening van hun functie en (dus) hun werkzaamheden. Verder wordt slechts toegang verschaft tot de in de administratie en systemen van de school opgenomen persoonsgegevens aan:
a. de verwerker die van De Ridderslag de opdracht heeft gekregen om persoonsgegevens te verwerken, maar alleen voor zover dat noodzakelijk is in het licht van de gemaakte afspraken;
b. derden voor zover uit de wet voortvloeit dat De Ridderslag verplicht is om toegang te geven of sprake is van een (andere) grondslag voor deze verwerking, bijvoorbeeld de vervulling van een taak van algemeen belang.

11. Beveiliging en geheimhouding

1. De Ridderslag neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. Deze maatregelen zijn er mede op gericht om niet noodzakelijke verzameling en verdere (niet noodzakelijke) verwerking van persoonsgegevens te voorkomen.
2. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen.
3. Een ieder die betrokken is bij de verwerking van persoonsgegevens binnen De Ridderslag is verplicht tot geheimhouding van de betreffende persoonsgegevens, en zal deze gegevens slechts verwerken voor zover dat noodzakelijk is voor de uitoefening van de betreffende functie, werkzaamheden of taak.

12. Verstrekken gegevens aan derden

De Ridderslag kan persoonsgegevens aan derden verstrekken als daarvoor een grondslag bestaat in de zin van artikel 7 van dit reglement.

13. Sociale media

Voor het eventuele gebruik van persoonsgegevens in sociale media door De Ridderslag, worden aparte afspraken gemaakt in een sociale-mediaprotocol van De Ridderslag, dat dan onderdeel uitmaakt van de veiligheidsplannen van de school.

14. Rechten betrokkenen

1. De Ridderslag erkent de rechten van betrokkenen, handelt daarmee in overeenstemming en bewerkstelligt dat betrokkenen deze rechten daadwerkelijk kunnen uitoefenen. Het betreft in het bijzonder de volgende rechten:

Inzage

a. Een betrokkene heeft recht op inzage van de door De Ridderslag verwerkte persoonsgegevens die op hem betrekking hebben, behalve voor

zover het gaat om werkdocumenten, interne notities en andere documenten die uitsluitend bedoeld zijn voor intern overleg en beraad. Indien en voor zover dit recht op inzage ook de rechten en vrijheden van anderen raakt, bijvoorbeeld als in de documenten ook persoonsgegevens van anderen dan de betrokkene zijn vermeld, kan De Ridderslag het recht op inzage beperken.

Bij het verstrekken van de betreffende gegevens verschaft De Ridderslag voorts informatie over:

- de verwerkingsdoeleinden;
- de categorieën van persoonsgegevens die worden verwerkt;
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- (indien van toepassing) ontvangers in derde landen of internationale organisaties;
- (indien mogelijk) hoe lang de gegevens worden bewaard;
- dat de betrokkene het recht heeft om te verzoeken dat de persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van de persoonsgegevens wordt beperkt, alsmede dat hij het recht heeft om bezwaar te maken tegen de verwerking van de persoonsgegevens;
- het feit dat de betrokkene een klacht kan indienen bij de Autoriteit Persoonsgegevens;
- de bron van de persoonsgegevens, indien de persoonsgegevens niet van de betrokkene zelf zijn verkregen;
- het eventueel toepassen van geautomatiseerde besluitvorming en de betreffende onderliggende logica en het belang en de gevolgen voor de betrokkene;
- de passende waarborgen indien de persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie.

Verbetering, aanvulling, verwijdering

b. De Ridderslag verbetert de persoonsgegevens van een betrokkene in het geval de betrokkene terecht heeft aangegeven dat de gegevens onjuist zijn, en De Ridderslag vult de persoonsgegevens van een betrokkene aan indien de betrokkene terecht om aanvulling heeft verzocht. Voorts kan de betrokkene verzoeken om verwijdering van zijn persoonsgegevens. De Ridderslag gaat daartoe over indien is voldaan aan een wettelijke grondslag voor het verzoek, tenzij het onmogelijk is om aan het verzoek te voldoen of dit een onredelijke inspanning zou vergen.

Bezwaar

c. Indien De Ridderslag persoonsgegevens verwerkt op de grondslag van artikel 7 onder a of artikel 7 onder d van dit reglement, kan de betrokkene bezwaar maken tegen de verwerking van zijn persoonsgegevens. In dat geval staakt De Ridderslag de verwerking van de betreffende per-

soonsgegevens, behalve als naar het oordeel van De Ridderslag het belang van De Ridderslag, het belang van derden of het algemeen belang in het betreffende concrete geval zwaarder weegt.

Beperken verwerking

d. De betrokkene kan voorts verzoeken om de verwerking van zijn persoonsgegevens te beperken, namelijk indien hij een verzoek tot verbetering heeft gedaan, indien hij bezwaar heeft gemaakt tegen de verwerking, als de persoonsgegevens niet meer nodig zijn voor het doel van de verwerking of als de gegevensverwerking onrechtmatig is. De Ridderslag staakt dan de verwerking, tenzij de betrokkene toestemming heeft gegeven voor de verwerking, De Ridderslag de gegevens nodig heeft voor een rechtszaak of de verwerking nodig is ter bescherming van de rechten van een andere persoon of vanwege gewichtige redenen.

Kennisgevingsplicht

e. Als De Ridderslag op verzoek van een betrokkene een verbetering of verwijdering van persoonsgegevens heeft uitgevoerd, of de verwerking van persoonsgegevens heeft beperkt, zal De Ridderslag eventuele ontvangers van de betreffende persoonsgegevens daarover informeren.

Procedure

2. De Ridderslag handelt een verzoek van een betrokkene zo spoedig mogelijk, maar uiterlijk binnen een maand na ontvangst van het verzoek, af. Afhankelijk van de complexiteit en van het aantal verzoeken kan die termijn indien nodig met twee maanden worden verlengd. Als deze verlenging plaatsvindt, wordt de betrokkene daarover binnen een maand na de ontvangst van het verzoek geïnformeerd. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt. Wanneer De Ridderslag geen gevolg geeft aan het verzoek van de betrokkene, deelt De Ridderslag onverwijld en uiterlijk binnen een maand na ontvangst mede waarom het verzoek niet wordt ingewilligd en informeert hij de betrokkene over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens of beroep bij de rechter in te stellen.

Intrekken toestemming

3. Indien voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming te allen tijden door de betrokkene of zijn wettelijk vertegenwoordiger worden ingetrokken. Als de toestemming wordt ingetrokken, staakt De Ridderslag de verwerking van persoonsgegevens, behalve als er een andere grondslag (zoals bedoeld in artikel 7) voor de gegevensverwerking is. Het intrekken van de toestemming tast de rechtmatigheid van verwerkingen die reeds hebben plaatsgevonden niet aan.

15. Transparantie

De Ridderslag informeert de betrokkene(n) actief over de verwerking van hun persoonsgegevens, in ieder geval door middel van een laagdrempelige privacyverklaring. In de privacyverklaring wordt in ieder geval de volgende informatie vermeld:
a) de contactgegevens van De Ridderslag;

b) de contactgegevens van de functionaris voor gegevensbescherming van De Ridderslag;
c) de doeleinden van de gegevensverwerking en de grondslagen voor de verwerking;
d) een omschrijving van de belangen van De Ridderslag indien de verwerking wordt gebaseerd op het gerechtvaardigd belang van De Ridderslag;
e) de (categorieën) ontvangers van de persoonsgegevens, zoals verwerkers of derden;
f) in voorkomend geval: of de persoonsgegevens worden verzonden aan landen buiten de Europese Economische Ruimte (EER);

g) hoe lang de persoonsgegevens zullen worden bewaard;
h) dat de betrokkene het recht heeft om De Ridderslag te verzoeken om inzage, verbetering of verwijdering van persoonsgegevens, en dat hij het recht heeft om te verzoeken om beperking van de verwerking, om bezwaar te maken of om een beroep te doen op het recht van gegevensoverdraagbaarheid;
i) dat de betrokkene het recht heeft om zijn toestemming in te trekken, als de gegevensverwerking is gebaseerd op toestemming;
j) dat de betrokkene het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
k) of de verstrekking van de persoonsgegevens een wettelijke of contractuele verplichting is, dan wel een noodzakelijke voorwaarde is om een overeenkomst te kunnen sluiten, en of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de gevolgen zijn indien hij de persoonsgegevens niet verstrekt;
l) het bestaan van geautomatiseerde besluitvorming, vergezeld van nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

16. Meldplicht datalekken

Een ieder die betrokken is bij een verwerking van persoonsgegevens is verplicht om een datalek per ommegaande te melden bij De Ridderslag conform het protocol beveiligingsincidenten en datalekken (bijlage 1) van De Ridderslag. Een datalek is elke inbreuk waarbij persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk zijn gemaakt.

17. Klachten

1. Wanneer een betrokkene van mening is dat het doen of nalaten van De Ridderslag niet in overeenstemming is met de AVG, dit reglement of (andere) toepasselijke wet- of regelgeving, dan kan een klacht worden ingediend overeenkomstig de binnen De Ridderslag geldende klachtenregeling. Een betrokkene kan zich eveneens wenden tot de functionaris voor gegevensbescherming van De Ridderslag.
2. Als een klacht naar de mening van betrokkene door De Ridderslag niet correct is afgewikkeld, kan hij zich wenden tot de rechter of de Autoriteit Persoonsgegevens.

18. Onvoorziene situatie

Indien zich een situatie voordoet die niet beschreven is in dit reglement, neemt het Bestuur van De Ridderslag de benodigde maatregelen, en wordt beoordeeld of dit reglement dientengevolge moet worden aangevuld of aangepast.

19. Wijzigingen reglement

1. Dit reglement is na instemming van de medezeggenschapsraad (MR) vastgesteld door de schoolleider en goedgekeurd door het bestuur van De Ridderslag. Het reglement wordt gepubliceerd op de website van De Ridderslag. Het reglement wordt verder actief onder de aandacht gebracht, bijvoorbeeld door middel van verwijzing in de schoolgids.
2. Dit reglement kans slechts worden gewijzigd na instemming van de MR.

20. Slotbepaling

Dit reglement wordt aangehaald als het privacyreglement van De Ridderslag en treedt in werking op 25 mei 2018.

Bijlage 1

Protocol informatiebeveiligingsincidenten en datalekken
Stichting Basisschool De Ridderslag

Ridder van Catsweg 256a info@ridderslag.nl
2805 BC Gouda www.ridderslag.nl

Inhoud

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van Basisschool De Ridderslag.

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen van beveiligingsincidenten en datalekken.

Dit protocol is van toepassing op de gehele organisatie van Basisschool De Ridderslag zoals vermeld in het IBP beleid en al haar medewerkers.

Gebruikte termen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die er voor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **Informatievoorziening**; het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- **Datalek**; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplichting melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een fikse boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in je leerlingadministratie of digitale leermiddelen. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moet de school met deze verwerkers aanvullende afspraken over het melden van datalekken.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten valt dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie ‘gelekt’. Een voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van (bijvoorbeeld) klas 3b, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een verwerker voor de school. Er kan worden afgesproken dat een verwerker **namens** de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het schoolbestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

Afspraken met leveranciers

Het schoolbestuur moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Spreek af:

- Hoe informeer je elkaar over datalekken, en zorg ook voor bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Wie doet de melding bij de Autoriteit Persoonsgegevens.
- Welke informatie/gegevens de verwerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding, en dat je elkaar informeert over de melding (maak afspraken dat je een kopie van de melding krijgt of doorstuurt).
- De tijd waarbinnen de verwerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

Maak schriftelijke afspraken met uw verwerker(s) over datalekken. Hiervoor kan gebruik worden gemaakt van de model verwerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl).

Werkwijze

Uitgangssituatie

- Er is een informatiebeveiligings- en privacy-reglement;

De vier rollen

Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

1. **Ontdekker (medewerker)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt (servicedesk)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder (functionaris gegevensbescherming** of **privacy officer)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (security officer/ict coördinator)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De zeven stappen

1. **Ontdekken**
   De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij de school.
2. **Inventariseren**
   De school bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd:
   - Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
   - Datum/periode van het beveiligingsincident
   - Aard van het beveiligingsincident
   - Wanneer van toepassing (bij een datalek):
     - Omschrijving van de groep betrokkenen
     - Aantal betrokkenen

- Type persoonsgegevens in kwestie
- Worden de gegevens binnen een keten gedeeld

3. **Beoordelen**

Wanneer de school voldoende informatie heeft verzameld, en een datalek vermoed, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.

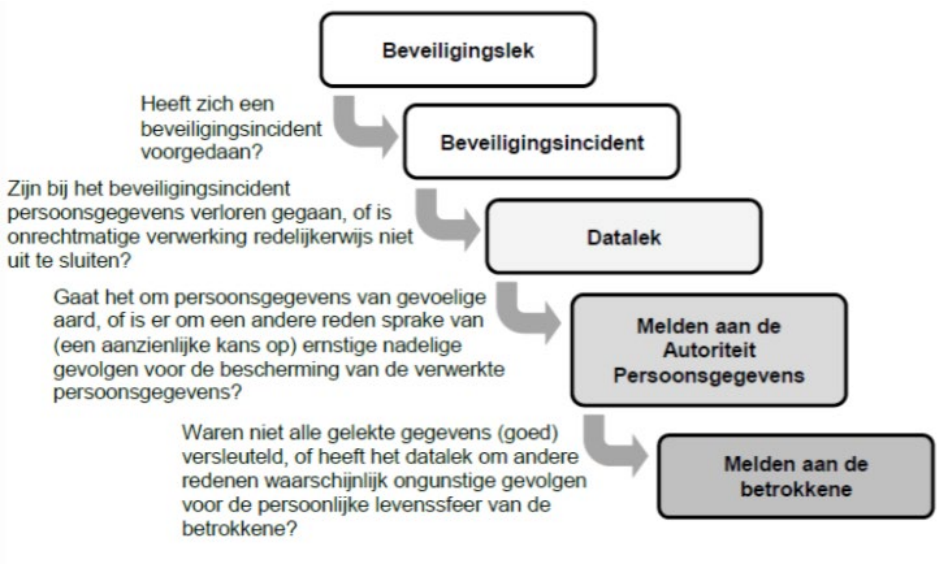
De volgende informatie wordt vastgelegd door de Melder:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkenen gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', hou je rekening met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, moet er gemeld worden.

Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar ook wanneer de gelekte gegevens "gevoelig" zijn zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

De onderstaande beslisboom kan gebruikt worden



4. **Repareren**

De school wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De school legt onderstaande vast:

- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.

- Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

5. **Melden**
   Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Melder dit binnen twee werkdagen doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0. Het meldingsformulier is openbaar en neem eens een kijkje welke informatie er eigenlijk nodig is om een datalek te melden. Dan ben je voorbereid als dat ooit nodig mocht zijn.
6. **Vastleggen**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de school waarmee het incident is afgesloten. De school verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.
7. **Informeren betrokkene: leerling en/of zijn ouders**
   Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan er van worden uitgaan dat het lekken van gevoelige aard gelekt gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

Monitoring beveiligingsincidenten en datalekken

Wanneer er meldingen zijn van beveiligingsincidenten en datalekken maakt de school een analyse in samenwerking met de functionaris gegevensbescherming.

In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

Het schoolbestuur wordt geïnformeerd over de uitkomsten van de analyse.