gemeente roerdalen

GEMEENTEBLAD

Officiële uitgave van de gemeente Roerdalen

Nr. 187102

21 juli

2020

Beleidsregel van het college van burgemeester en wethouders van de gemeente Roerdalen houdende regels omtrent de privacy 2020

Vastgesteld op: 30 juni 2020 door het college van burgemeester en wethouders van gemeente Roerdalen

1. Inleiding en aanleiding

We hebben als samenleving bepaald dat privacy een grondrecht is. In de Nederlandse Grondwet, het Handvest van de Grondrechten van de Europese Unie en het Europees Verdrag voor de Rechten van de Mens noemen we het 'eerbiediging van de persoonlijke levenssfeer'. Daarbij is een bijzondere plaats ingeruimd voor de bescherming van persoonsgegevens.

Met persoonsgegevens bedoelen we alle gegevens die herleidbaar zijn naar een geïdentificeerd of identificeerbaar natuurlijk persoon. Alles wat we met die persoonsgegevens doen, noemen we verwerken, zoals: opslaan, kopiëren, publiceren, aanpassen, raadplegen en delen. We kunnen persoonsgegevens zinvol verwerken om als samenleving beter te kunnen functioneren. Denk aan het verstrekken van passende zorg, onderwijs of financiële ondersteuning. Maar de verwerking van persoonsgegevens maakt ons ook kwetsbaar. Bijvoorbeeld voor discriminatie, uitbuiting of chantage. Denk aan de verwerking van gegevens over onze gezondheid, geloofsovertuiging of seksuele geaardheid. Daarom moeten we de persoonlijke levenssfeer, en persoonsgegevens in het bijzonder, beschermen.

Om persoonsgegevens te beschermen is het verwerken ervan bij wet beperkt. De bescherming van persoonsgegevens is in Europa sinds 2016 geregeld met de Algemene Verordening Gegevensbescherming. In Nederland is dit nader uitgewerkt in de Uitvoeringswet Algemene Verordening Gegevensbescherming. Voor een aantal situaties zijn er extra eisen óf vrijheden geregeld in materiewetgeving zoals de Wet maatschappelijke ondersteuning, de Participatiewet, de Jeugdwet, de Wet op het primair onderwijs of de Wet politiegegevens.

Roerdalen is verwerkingsverantwoordelijk voor verwerkingen van persoonsgegevens waarvan zij zelf doel en middelen bepaalt. Dus waarvan Roerdalen bepaalt waarom, wanneer, welke persoonsgegevens op welke manier verwerkt worden. Het maakt daarbij niet uit of dat door de medewerkers of systemen van de organisatie zelf worden verwerkt óf dat een andere organisatie de gegevens verwerkt voor Roerdalen.

De Gemeente Roerdalen (hierna 'Roerdalen') is soms betrokken bij de verwerking van persoonsgegevens van andere organisaties. Daarbij bepalen die organisaties de voorwaarden waaronder deze verwerkingen plaats vinden.

Zorgvuldig omgaan met de persoonsgegevens is essentieel voor het vertrouwen in de overheid. Roerdalen werkt steeds meer samen met inwoners, bedrijven en instellingen, met andere overheden, met landelijke of regionale organisaties die zorgen voor zorg, onderwijs, huisvesting, veiligheid en met internationale of lokale bedrijven. Het is belangrijk dat iedereen die op deze manier betrokken is bij de gemeentelijke taken goed omgaat met de persoonsgegevens die daarbij verwerkt worden.

Iedereen mag er daarom op vertrouwen dat ook Roerdalen persoonsgegevens op een behoorlijke en zorgvuldige wijze verwerkt: rechtvaardig, veilig en transparant. Dat is de verantwoordelijkheid van Roerdalen als geheel én van iedere medewerker afzonderlijk.

Dit privacybeleid beschrijft wat deze verantwoordelijkheid in de praktijk betekent voor Roerdalen. Roerdalen is transparant over de manier waarop de organisatie met persoonsgegevens omgaat. Daarom vertalen wij dit beleidsdocument tevens naar een voor het publiek begrijpelijke tekst: een privacyverklaring.

1.1. Reikwijdte

Dit privacybeleid geeft voor onze organisatie invulling aan de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). Op enkele werkterreinen zijn de AVG en de UAVG (deels) niet van toepassing. Zo is er bijvoorbeeld een separate Richtlijn gegevensbescherming opsporing en vervolging. Dit privacybeleid is op deze werkterreinen niet van toepassing.

Het privacybeleid is van toepassing op alle activiteiten waarbij Roerdalen persoonsgegevens verwerkt, door een ander laat verwerken, samen met andere partijen verwerkt, of uitwisselt met andere partijen.

De Algemene Verordening Gegevensbescherming stelt de verwerkingsverantwoordelijke verantwoordelijk voor de kwaliteit van de verwerking van persoonsgegevens en de naleving van de wettelijke eisen. Bovendien moet de verantwoordelijke de naleving van de wettelijke eisen kunnen aantonen.

Dit privacybeleid beschrijft wat de verantwoordelijkheid voor de bescherming van persoonsgegevens in de praktijk betekent voor Roerdalen. Het beleid beschrijft:
- De manier waarop Roerdalen met persoonsgegevens omgaat;
- De manier waarop we de verwerking van persoonsgegevens beheersen: het privacy management systeem;
- De manier waarop we aantonen dat we de verwerking van persoonsgegevens beheersen;
- De beheerorganisatie die we daarvoor inrichten (rollen, taken en verantwoordelijkheden).

1.2. Voor wie is dit beleid bedoeld?

Alle medewerkers houden zich aan het privacybeleid. Iedere medewerker draagt daarbij verantwoordelijkheid die past bij zijn niveau en rol. We verwachten van elke medewerker bijvoorbeeld dat deze werkinstructies en – procedures volgt, privacyrisico's in zijn werk signaleert, en signalen van datalekken intern meldt volgens de daarvoor geldende procedure. Van ICT-beheerders verwachten we daarnaast bijvoorbeeld dat deze beveiligingslekken ook opspoort en dicht. Van beleidsmakers en beslissers verwachten we dat ze rekening houden met het privacybeleid als ze beleids- of organisatorische keuzes maken of nieuwe diensten willen ontwikkelen. Van inkopers en ICT-medewerkers verwachten we dat ze rekening houden met het privacybeleid als bij het ontwerpen en aanbesteden van nieuwe systemen ontwerpen

Het privacybeleid is ook het vertrekpunt voor (interne) controles, audits en periodieke onderzoeken, en om aan de interne toezichthouder (de Functionaris Gegevensbescherming) en de nationale toezichthouder (de Autoriteit Persoonsgegevens) aan te tonen dat we de privacywet- en regelgeving naleven.

2. Uitgangspunten

Iedereen mag er op vertrouwen dat Roerdalen persoonsgegevens verwerkt conform de geldende wet- en regelgeving en op een behoorlijke en zorgvuldige wijze: rechtvaardig, veilig en transparant. Dat is de verantwoordelijkheid van Roerdalen als geheel én van iedere medewerker afzonderlijk. Daarbij gelden de volgende uitgangspunten.
- We verwerken persoonsgegevens alleen als we hiervoor een wettelijke grondslag hebben.
- We verwerken persoonsgegevens alleen voor heldere en specifiek beschreven doelen.
- We verwerken persoonsgegevens alleen als dit noodzakelijk is voor een goede uitvoering deze doelen.
- We beperken de inbreuk op de persoonlijke levenssfeer door het verwerken van persoonsgegevens zoveel mogelijk. Zo nodig passen we ons beleid of onze werkprocessen aan voor zover deze aanpassingen het realiseren van beleidsdoelen niet onevenredig schaadt. In alle gevallen zorgen we er voor dat de inbreuk op de persoonlijke levenssfeer niet onevenredig groot is in verhouding tot het doel dat we nastreven.
- We verwerken persoonsgegevens alleen voor andere doelen dan waarvoor de gegevens zijn verworven als deze doelen verenigbaar zijn met het oorspronkelijke doel en/óf als de wet de verdere verwerking toestaat.
- We stellen persoonsgegevens alleen beschikbaar aan andere organisaties voor verwerking voor hun eigen doelen als de wet dit toestaat.
- We zorgen er voor dat de beschikbaarheid, integriteit en vertrouwelijkheid van de persoonsgegevens past bij het doel dat we nastreven en bij de gevoeligheid van de gegevens die we verwerken: we verwerken persoonsgegevens alleen als deze juist, nauwkeurig, feitelijk en actueel zijn.
- We vernietigen of anonimiseren persoonsgegevens wanneer deze niet langer noodzakelijk zijn voor het doel waarvoor we ze verwerken of wanneer de wettelijke bewaartermijn is verstreken.
- We communiceren transparant over hoe we met persoonsgegevens omgaan en hoe we de persoonsgegevens die we verwerken beschermen.
- We informeren betrokkenen (diegenen waarvan de persoonsgegevens zijn) zo mogelijk vóórdat we starten met het verwerken van persoonsgegevens over de kaders van de verwerking en hun rechten ten aanzien van de persoonsgegevens die we verwerken.
- We voorkomen inbreuken op de bescherming van de persoonsgegevens (datalekken) door adequate beschermingsmaatregelen te nemen.

- Wanneer onverhoopt toch een datalek optreedt, nemen we tijdig adequate herstelmaatregelen om herhaling te voorkomen en schade voor de betrokkenen zo veel mogelijk te voorkomen of te beperken.
- Wanneer dat vereist is informeren we de nationale toezichthouder (de Autoriteit Persoonsgegevens) over een datalek en de oorzaken en herstelmaatregelen die we hebben ondernomen.
- Als dat vereist en/ of passend is, informeren we betrokkenen over een datalek waarbij hun persoonsgegevens betrokken zijn en over de herstelmaatregelen die we hebben genomen.
- Als dat vereist en/ of passend is, informeren we betrokkenen bij een datalek waarbij hun persoonsgegevens betrokken zijn over aanvullende maatregelen die de betrokkenen zelf kunnen nemen om schade te voorkomen of zoveel mogelijk te beperken.
- Wanneer het nodig is om de rechtmatigheid, veiligheid en transparantie van de verwerking te garanderen, leggen we voor een verwerking van persoonsgegevens nader beleid, procesbeschrijvingen, werkwijzen en passende beschermingsmaatregelen vast en passen deze consequent toe.
- We beveiligen informatiesystemen tegen het optreden van risico's die de vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens aantasten.
- Bij het ontwerpen en ontwikkelen van nieuwe systemen, processen en diensten houden we rekening met de bescherming van persoonsgegevens en passen we privacy by design en privacy by default toe.
- We controleren en evalueren de effectieve werking van beleid, procesbeschrijvingen, werkwijzen, protocollen en beschermingsmaatregelen en stellen deze zo nodig bij.
- We handelen klachten van betrokkenen over de manier waarop we omgaan met persoonsgegevens tijdig op een toegankelijke en transparante manier af en volgens de daarvoor geldende procedure.
- We handelen verzoeken van betrokkenen ten aanzien van onze verwerking van hun persoonsgegevens tijdig op een toegankelijke en transparante manier af en volgens de daarvoor geldende procedure.
- Wanneer wij samenwerken met andere partijen en daarbij sprake is van verwerking van persoonsgegevens, dan maken we heldere afspraken over de kaders en verantwoordelijkheden voor de verwerking van persoonsgegevens, en de beschermingsmaatregelen die we daarbij treffen,. We leggen deze afspraken vast in een (verwerkers)overeenkomst, controleren en evalueren de effectieve werking ervan en stellen ze zo nodig bij.

3. Privacybeheersysteem en beheerorganisatie

Bij veranderingen in bijvoorbeeld wet- en regelgeving, jurisprudentie en richtlijnen beoordeelt Roerdalen of haar activiteiten nog steeds voldoen aan de privacywetgeving. Dat is ook het geval als zich interne wijzigingen voordoen, bijvoorbeeld bij veranderingen in beleid, bedrijfsprocessen of (informatie)systemen. Als blijkt dat de wijzigingen (nieuwe) privacyrisico's met zich meebrengen, neemt Roerdalen passende maatregelen om het optreden van deze risico's te voorkomen. Om dit continue verbeterproces te borgen richten we een privacybeheersysteem in.

Het privacybeheersysteem bevat het beleid, de rollen, de taken, de verantwoordelijkheden, de procedures en de maatregelen die samen zorg dragen voor een geborgde rechtmatige, veilige en transparante verwerking van persoonsgegevens. De verwerkingsverantwoordelijke is verantwoordelijk voor het inrichten en onderhouden van het privacybeheersysteem.

Dit privacybeleid beschrijft de inrichting van het privacybeheersysteem en de privacybeheerorganisatie: de verdeling van rollen, taken en verantwoordelijkheden die nodig zijn voor de werking van het privacybeheersysteem.

Rollen van partijen
Een goede verdeling van verantwoordelijkheden is noodzakelijk voor een goede toepassing van de Algemene Verordening Gegevensbescherming (AVG). Bij de verdeling van die verantwoordelijken zijn de volgende definities uit de wet bepalend:

Verwerkingsverantwoordelijk
In de AVG wordt de nadruk gelegd op de verantwoordelijkheid van organisaties en instanties (in de AVG aangeduid als 'verwerkingsverantwoordelijken') om te kunnen aantonen dat zij zich aan de wet houden (accountability). De verwerkingsverantwoordelijke is de natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, die alleen of samen met anderen het doel van en de middelen voor de verwerking vaststelt. Bij de gemeente is dat het bestuursorgaan in het kader van wiens taken of bevoegdheden de verwerking van persoonsgegevens plaats vindt. Bijvoorbeeld de burgemeester, het college, de gemeenteraad, de heffings- en invorderingsambtenaar of de leerplichtambtenaar. Daar waar in dit stuk gesproken wordt van verwerkingsverantwoordelijke, wordt telkens gedoeld op het bestuursorgaan in het kader van wiens taken of bevoegdheden de verwerking van persoonsgegevens plaats vindt.

De verwerkingsverantwoordelijke is verantwoordelijk voor:
- De naleving van de beginselen voor de verwerking van persoonsgegevens.
- De maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd.

Verwerker
Een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt zonder aan diens rechtstreekse gezag onderworpen te zijn. Een voorbeeld van een verwerker die ten behoeve van Roerdalen persoonsgegevens verwerkt is de Gemeenschappelijke Regeling MER.

Andere verwerker ('sub verwerker')
Van een subverwerker is sprake wanneer een verwerker andere verwerkers inschakelt. Hierdoor kan een ketenverantwoordelijkheid tussen verschillende partijen ontstaan.

Gezamenlijke verwerkingsverantwoordelijken
Door de manier waarop Roerdalen haar taken organiseert kan sprake zijn van de betrokkenheid van verschillende verwerkingsverantwoordelijken. Bijvoorbeeld wanneer Roerdalen zijn taken uitvoert in samenspraak met maatschappelijke organisaties of overheden. Er kan dan ook sprake zijn van gezamenlijke verantwoordelijkheden, bijvoorbeeld als er geen duidelijke scheiding meer aan te brengen is tussen de verantwoordelijkheden van de verschillende verwerkingsverantwoordelijken. Of als de partijen het voor de betrokkenen niet wenselijk vinden dat er onderscheid wordt gemaakt tussen de verantwoordelijkheden van de verschillende verwerkingsverantwoordelijken.

Ontvangers
Een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, waaraan persoonsgegevens worden verstrekt.

3.1. Privacybeheerorganisatie
Het inrichten van de privacybeheerorganisatie heeft als doel de rollen, de taken, de verantwoordelijkheden die nodig zijn voor het borgen van de bescherming van persoonsgegevens structureel te verdelen.

Vaststelling van privacybeleid
Het college stelt het privacybeleid vast. Het neemt daarbij de aanbevelingen van de functionaris voor de gegevensbescherming (FG) in acht en bevordert de beschikbaarheid van voldoende middelen om het privacybeheer passend te waarborgen.

Verantwoordelijkheid voor de uitvoering van het privacybeleid
De verwerkingsverantwoordelijke is verantwoordelijk voor de uitvoering van het privacybeleid en voor de controle op de naleving wet- en regelgeving en het privacybeleid. De feitelijke uitvoering volgt de lijnen van de interne organisatie, waarbij iedere leidinggevende verantwoordelijkheden heeft op zijn eigen niveau.

Toezicht op en advies over de uitvoering van het privacybeleid en de naleving van privacywet- en regelgeving
Voor onafhankelijk toezicht op en advies over de uitvoering van het privacybeleid en de naleving van privacy wet- en regelgeving wijst de verwerkingsverantwoordelijke een Functionaris voor de Gegevensbescherming (FG) aan. De functionaris voor de gegevensbescherming (FG) brengt verslag uit over de voortgang en kwaliteit van de uitvoering van het privacybeleid en doet aanbevelingen voor verdere optimalisering.

De functionaris voor de gegevensbescherming (FG) treedt tevens op als privacy-ombudsman en is in voorkomende gevallen de liaison met de landelijke ombudsman en de autoriteit persoonsgegevens (AP). Zijn positie en taakuitoefening worden nader geregeld in een statuut dat de verwerkingsverantwoordelijke vaststelt.

Beheer van het privacybeleid en de privacybeheersysteem
De privacycoördinator (PC) is de beheerder van het privacybeleid en het privacybeheersysteem.

Coördinatie van de uitvoering van het privacybeleid
De privacycoördinator is verantwoordelijk voor de coördinatie van de uitvoering van organisatiebrede privacyprocessen zoals het opstellen van handreikingen en standaarden, het bijhouden van registers, bewustwording en training van medewerkers en het afhandelen van verzoeken van betrokkenen en datalekken.

Uitvoering van het privacybeleid

Elke leidinggevende is proceseigenaar van een of meerdere bedrijfsprocessen. De leidinggevende is verantwoordelijk voor de feitelijke uitvoering van het privacybeleid in de bedrijfsprocessen waar hij eigenaar van is.

Ondersteuning bij de uitvoering van het privacybeleid
De proceseigenaren krijgen bij de uitvoering van het privacybeleid ondersteuning van een kernteam privacy bestaand uit een juridisch medewerker, de privacycoördinator (PC), de informatieveiligheidsbeheerder (ISM) en advies van de functionaris gegevensbescherming (FG) en de informatieveiligheidsadviseur (CISO).

Evalueren van het privacybeleid
Zowel wet- en regelgeving, jurisprudentie als de organisatie zelf zijn steeds aan verandering onderhevig. Het privacybeleid zal steeds op deze veranderingen moeten aan blijven sluiten. De privacycoördinator (PC) evalueert het privacybeleid daarom uiterlijk 3 jaar na vaststellen of eerder als de veranderde omstandigheden daarom vragen en rapporteert zijn bevindingen aan het college.

Rapportage van de voortgang van de uitvoering
De proceseigenaren rapporteren de voortgang van de uitvoering periodiek aan de directie. De bestuurlijke verantwoording sluit aan bij de bestaande kaders voor risicomanagement en de planning- en controlcyclus. Daardoor wordt een bredere compliance-verantwoording automatisch onderdeel van de verantwoording van de individuele afdelingen.

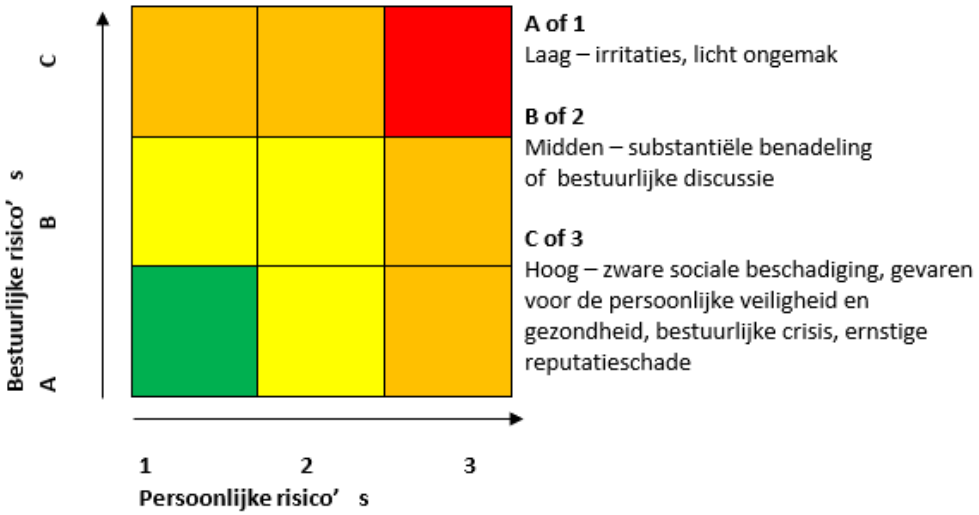
4. Het register van verwerkingsactiviteiten

Om aantoonbaar rechtvaardig, veilig en transparant persoonsgegevens te verwerken, is het noodzakelijk dat Roerdalen zicht en inzicht krijgt in de verwerkingen van persoonsgegevens die er plaats vinden. Roerdalen houdt daartoe een wettelijk verplicht register van verwerkingen bij.

5. Beheersen van risico's van verwerkingen

De AVG verwacht van de verwerkingsverantwoordelijke dat deze de verschillende belangen die gemoeid zijn met een verwerking goed tegen elkaar afweegt. Daarnaast wordt van de verwerkingsverantwoordelijke verwacht dat deze passende maatregelen neemt om de risico's van een verwerking te voorkomen.

De uitvoering van het privacybeleid is evenwichtig. Een risicoanalyse brengt de persoonlijk risico's voor de betrokkenen en het bestuurlijk risico voor de organisatie in kaart. De risico's worden door praktische, organisatorische en technische maatregelen beheerst. De methode die daarbij wordt gebruikt sluit aan bij het risicobeleid.



5.1. De data protection impact assessment

Een data protection impact assessment (DPIA) , ook wel privacy impact assessment (PIA) of gegevensbeschermingseffectbeoordeling (GEB), genoemd, is een instrument waarmee het effect van verwerkingsactiviteiten op de bescherming van persoonsgegevens op een gestructureerde en heldere manier in beeld in kaart wordt gebracht om vervolgens passende maatregelen te kunnen nemen om de risico's te verkleinen.

- De privacycoördinator stelt de DPIA-standaard, -afwegingskader en -procedure op.
- Het college stelt de DPIA-standaard, -afwegingskader en –procedure vast,
- De proceseigenaar voert in ieder geval een DPIA uit voor alle nieuwe of wijzigende verwerkingen met een hoog risicoprofiel volgens het DPIA-afwegingskader en in alle gevallen vóórdat een dergelijke (gewijzigde) verwerking start.
- De proceseigenaar vraagt de functionaris voor de gegevensbescherming (FG) bij de uitvoering van een DPIA om advies ten aanzien van de rechtmatigheid, veiligheid en transparantie van de verwerking.

Overgangsregeling
- Voor verwerkingen met een hoog privacyrisico die voor 25 mei 2018 al bestonden voert de proceseigenaar na deze datum een DPIA uit wanneer:
- De verwerking verandert, bijvoorbeeld door nieuwe technologie of wijziging van doel;
- Het risico verandert;
- De omgeving verandert, bijvoorbeeld door maatschappelijke veranderingen.

Deze overgangstermijn eindigt op 25 mei 2021. Voor alle verwerkingen met een hoog privacyrisico is op dat moment een DPIA uitgevoerd.

Evalueren van de DPIA
Omdat zowel de verwerkingen zelf als de omstandigheden waaronder de verwerkingen plaats vinden constant veranderen, betekent dit dat de proceseigenaar de kansen, risico's en maatregelen moet evalueren. De proceseigenaar evalueert een DPIA daarom uiterlijk 3 jaar na vaststellen van de DPIA.

5.2. Passende maatregelen om risico's te beperken

Technische, procesmatige, juridische en organisatorische maatregelen zorgen voor een op het risico afgestemd beveiligingsniveau. Hierbij wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, en de aard, omvang, context en doeleinden van de verwerkingen. Ook wordt rekening gehouden met de, qua waarschijnlijkheid en ernst, uiteenlopende risico's voor de rechten en vrijheden van personen.

Wanneer Roerdalen persoonsgegevens verwerkt of laat verwerken door een derde, zorgt Roerdalen ervoor dat ook deze derde passende beveiligingsmaatregelen treft om de persoonsgegevens te beschermen.

Als uitgangspunt kiest Roerdalen voor technische maatregelen om de veiligheid te waarborgen. Daar waar de technische mogelijkheden ontbreken of disproportioneel hoge kosten met zich meebrengen, zoekt Roerdalen naar organisatorische en of procesmatige maatregelen als alternatief voor of als aanvulling op de technische maatregelen.

6. Samenwerking met andere partijen

6.1 Inschakeling verwerkers, verwerkersovereenkomst
Roerdalen schakelt enkel verwerkers in die afdoende garanties bieden met betrekking tot het toepassen van passende technische, procesmatige, communicatieve en organisatorische maatregelen. De afspraken omtrent de verwerking door de verwerker worden schriftelijk vastgelegd in een verwerkersovereenkomst. Het college stelt daartoe een model-verwerkersovereenkomst vast. Een verwerkersovereenkomst stellen we vast voordat de dienstverlening aanvangt. Het naleven van de verwerkersovereenkomst toetsen we periodiek of steekproefsgewijs. De uitgangspunten voor dergelijke controles stellen we vast in auditbeleid.

6.2. Roerdalen als verwerker

Soms treedt Roerdalen zelf op als verwerker voor derden. Hierbij zijn deze derden de Verwerkingsverantwoordelijke. Roerdalen biedt daarbij aan de Verwerkingsverantwoordelijke voldoende garanties voor het zorgvuldig verwerken van gegevens door het toepassen van passende technische en organisatorische maatregelen. De afspraken omtrent de verwerking worden schriftelijk vastgelegd in een verwerkersovereenkomst, voordat de dienstverlening door Roerdalen aanvangt.

6.3. Gelijkwaardige samenwerking

Het kan voorkomen dat Roerdalen een andere partij inschakelt, of met een andere partij samenwerkt, die geen verwerker is, maar waarmee wel persoonsgegevens worden uitgewisseld. Bijvoorbeeld in een ketensamenwerking. Roerdalen zorgt ervoor dat samenwerkingen voldoen aan het privacybeleid

en dat er passende afspraken worden gemaakt om de bescherming van persoonsgegevens te waarborgen.

De partijen sluiten dan een overeenkomst omtrent de verwerking van persoonsgegevens waarin de respectieve verantwoordelijkheden worden vastgelegd, zoals:
- Benoemen van gezamenlijke doel(en) en middelen.
- Beschrijven van hoe ze omgaan met verzoeken van betrokkene om hun rechten uit te oefenen.
- Regelen van de inrichting, kaders en voorwaarden van de onderlinge relatie.
- Maken van afspraken over informatiebeveiliging.

7. Omgaan met datalekken

Voor elke verwerking van persoonsgegevens neemt Roerdalen passende beschermingsmaatregelen. Deze maatregelen moeten er voor zorgen dat veiligheid van deze gegevens is gewaarborgd. Dat wil zeggen dat de beschikbaarheid, integriteit, vertrouwelijkheid van de persoonsgegevens en de rechtmatigheid en transparantie van de verwerking van die persoonsgegevens afdoende is verzekerd. Desondanks kan zich een situatie voordoen waarbij de veiligheid van de persoonsgegevens wordt doorbroken.

Het gaat bij een datalek om situaties waarbij een onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden of kan plaatsvinden doordat beveiligingsmaatregelen (on)bewust zijn omzeild of doorbroken of dat geen of onvoldoende beveiligingsmaatregelen zijn genomen. Het gaat ook om situaties waarbij persoonsgegevens verloren zijn gegaan, waardoor ze niet meer beschikbaar zijn, en om situaties waarin gegevens in handen kunnen komen of zijn gekomen van derden die geen toegang tot die gegevens mogen hebben. Wanneer zich een dergelijk informatiebeveiligingsincident voordoet, waarbij persoonsgegevens betrokken zijn, handelt Roerdalen in overeenstemming met de vastgestelde procedure datalekken.

Dit protocol bevat een vastgesteld proces van te doorlopen stappen en rollen, taken en verantwoordelijkheden om:
- Te bepalen of er sprake is van een datalek.
- Te bepalen of het datalek gemeld moet worden aan de Autoriteit Persoonsgegevens.
- Te bepalen of het datalek gemeld moet worden aan de betrokkenen.
- De eventuele schade of de kans hierop, bij een datalek te beperken en de getroffen perso(o)n(en) te beschermen.
- De noodzakelijke documentatie van een datalek

Wanneer aan de orde, meldt Roerdalen het datalek zonder onredelijke vertraging, maar uiterlijk binnen 72 uur nadat er kennis van het datalek is genomen aan de Autoriteit Persoonsgegevens en indien nodig aan de betrokkenen.

Wanneer Roerdalen zelf niet de verwerkingsverantwoordelijke is, maar als verwerker optreedt namens een andere verwerkingsverantwoordelijke, dan meldt Roerdalen een datalek terstond aan de verwerkingsverantwoordelijke conform de verwerkersovereenkomst die aan de samenwerking ten grondslag ligt.

Wanneer Roerdalen samenwerkt met andere verwerkingsverantwoordelijken, zoals ketenpartners, dan stelt Roerdalen deze andere partner terstond op de hoogte van een datalek conform de privacyafspraken die aan de samenwerking ten grondslag liggen.

De proceseigenaar van de verwerking waarin het datalek is opgetreden is verantwoordelijk voor de afhandeling van het datalek conform de vastgestelde procedure datalekken. Roerdalen houdt een register bij van alle datalekken die optreden. De privacycoördinator beheert het register.

8. Omgaan met gegevensverstrekkingen

In sommige gevallen kan Roerdalen persoonsgegevens verstrekken aan andere partijen, zoals andere overheidsorganisaties. Structurele verstrekkingen van persoonsgegevens worden vastgelegd in het register van verwerkingen en gewaarborgd met passende privacy-afspraken. Daarnaast kan het voorkomen dat er incidenteel persoonsgegevens worden verstrekt aan andere partijen. De proceseigenaar van de verwerking waaruit de persoonsgegevens worden verstrekt is er verantwoordelijk voor dat dergelijke verstrekkingen rechtmatig, veilig en transparant plaats vinden conform de vastgestelde procedure voor gegevensverstrekkingen. Roerdalen registreert alle incidentele verstrekkingen van persoonsgegevens. In de procedure voor gegevensverstrekkingen is vastgelegd op welke wijze de registratie plaats vindt.

9. Rechten van betrokkenen

Roerdalen borgt de onderstaande rechten van betrokkenen. Bij Roerdalen hechten we er belang aan om dit op een eenduidige wijze te doen. Hiertoe richt de privacycoördinator adequate heldere en laagdrempelige procedures in.

9.1. Recht op informatie
Roerdalen verzamelt gegevens om haar taken te kunnen uitvoeren. Indien dit persoonsgegevens betreffen, heeft Roerdalen de plicht om betrokkenen, voor zover deze daar niet reeds van op de hoogte zijn, te informeren over verwerkingen van hun persoonsgegevens. Roerdalen verstrekt dan aan betrokkenen informatie over de verwerking, zoals het doel daarvan, welke persoonsgegevens worden verwerkt en of de gegevens aan anderen worden verstrekt. Dit met inachtneming van de voorwaarden en beperkingen zoals die neergelegd zijn in wet- en regelgeving.

9.2. Recht op inzage
Betrokkenen hebben de mogelijkheid om te controleren of en op welke manier hun gegevens worden verzameld en verwerkt. Dit met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving.

9.3. Recht op rectificatie
Als Roerdalen persoonsgegevens van betrokkenen verwerkt die naar hun oordeel onjuist of onvolledig zijn, kunnen zij een verzoek indienen bij Roerdalen om deze persoonsgegevens te rectificeren of aan te vullen. Dit met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving.

9.4. Recht op gegevenswissing
Betrokkenen hebben het recht persoonsgegevens te laten wissen indien Roerdalen niet langer een goede grond heeft voor het verwerken hiervan. Bijvoorbeeld als betrokkenen een gegeven toestemming intrekken, als de persoonsgegevens onrechtmatig zijn verwerkt, onjuist zijn of de gegevens niet langer nodig zijn.

9.5. Recht van bezwaar tegen verwerking
Betrokkenen hebben het recht aan Roerdalen te vragen hun persoonsgegevens niet meer te verwerken en bezwaar te maken tegen de verwerking van hun persoonsgegevens. Roerdalen moet hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

9.6. Recht op beperking van de verwerking
Het recht op beperking houdt in dat Roerdalen de persoonsgegevens (tijdelijk en onder voorwaarden) niet mag verwerken en niet mag wijzigen, bijvoorbeeld wanneer betrokkenen de juistheid van de gegevens ter discussie stellen.

9.7. Recht op overdraagbaarheid van gegevens (dataportabiliteit)
Roerdalen is vanuit de AVG niet verplicht invulling te geven aan overdraagbaarheid van gegevens voor zover het werkzaamheden betreft in het kader van algemeen belang, de uitoefening van een openbaar gezag, wanneer deze zijn openbare taken uitoefent of aan een wettelijke verplichting voldoet.
In alle andere gevallen treft de proceseigenaar passende voorzieningen om dataportabiliteit mogelijk te maken.

9.8. Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / profiling
Uitgangspunt in de AVG is dat er geen geautomatiseerde besluitvorming op basis van profilering mag plaatsvinden, als daaraan rechtsgevolgen voor de betrokkene (degene wiens persoonsgegevens het betreft) zijn verbonden of het besluit hem in aanmerkelijke mate treft. Daarbij kan gedacht worden aan bijvoorbeeld de kredietwaardigheid van een persoon. Een ander voorbeeld is het verwerken van sollicitaties via internet zonder menselijke tussenkomst.

9.9. Uitoefening van rechten
Om gebruik te maken van de bovenstaande rechten kunnen betrokkenen bij Roerdalen een verzoek indienen t.a.v. verwerkingen waarvoor Roerdalen verwerkingsverantwoordelijke is. Binnen vier weken beoordeelt Roerdalen of het verzoek gerechtvaardigd is. Roerdalen laat binnen die termijn weten wat er met het verzoek gaat gebeuren, waaronder of Roerdalen de behandeling van het verzoek met maximaal twee maanden verlengt en waarom dat noodzakelijk is.

Roerdalen behandelt het verzoek volgens de daarvoor door haar vastgestelde procedure.

De verwerkingsverantwoordelijke neemt naar aanleiding van een verzoek een besluit in het kader van de Algemene wet bestuursrecht.

Verzoeken t.a.v. verwerkingen waarvoor een van de bestuursorganen van Roerdalen verwerkingsverantwoordelijke is, dienen betrokkenen in beginsel bij de gemeente in, tenzij daarover specifieke andere afspraken gemaakt worden tussen de gemeente en een verwerker of samenwerkingspartner.

9.10. Vragen en klachten

Een betrokkenen kan over de verwerking van persoonsgegevens door Roerdalen contact op nemen met de functionaris voor de gegevensbescherming (FG). Elke betrokkene heeft daarnaast het recht om een klacht of een verzoek tot bemiddeling in te dienen bij de Autoriteit Persoonsgegevens.