



- Handreiking anonimiseren bij aanvraag vergunning

Versie 2

UBR | voor een
ambitieuze
overheid



WIJZIGING BEKENDMAKINGS WET

1. Inleiding

1.1 Doelgroep van deze handreiking

Deze handreiking is bedoeld voor partijen die – vaak namens een opdrachtgever – documenten opstellen voor een vergunningaanvraag bij een overheidsorganisatie (gemeente, provincie, waterschap, omgevingsdienst etc.). Het gaat dan bijvoorbeeld om een architect, aannemer, raadgevende ingenieursbureaus, stedenbouwkundige, installatietechnische bureau, archeologen, landbouwkundige of andere professional.

1.2 Doel van de handreiking

Een vergunningaanvraag die is ingediend bij een overheidsorganisatie moet door die overheidsorganisatie ter inzage worden gelegd voor geïnteresseerden. Dit geldt niet alleen voor de aanvraag zelf, maar ook voor alle documenten die de aanvraag ondersteunen (zoals rapporten en bouwtekeningen).

In de aangeleverde documenten kunnen gevoelige gegevens staan. Bijvoorbeeld namen van uw opdrachtgever, van uw eigen medewerkers of van ambtenaren die u gesproken heeft. In rapporten en ontwerpen kunnen bedrijfsgegevens staan die vertrouwelijk zijn en waarvan openbaarmaking moet worden voorkomen, zoals kosten of beveiligingsmaatregelen. Terinzagelegging van die informatie kan leiden tot een risico voor uw opdrachtgever of voor uw eigen organisatie. U mag immers niet zomaar gegevens over een persoon (een medewerker of een opdrachtgever) of over een bedrijf (uw eigen bedrijf of een opdrachtgever) met derden delen. Maar deze informatie moet wel gedeeld worden met de overheidsorganisatie, omdat anders beoordeling van de vergunningaanvraag niet mogelijk is.

Met deze handreiking helpen wij u om keuzes te maken in het aanleveren van de documenten bij de overheidsorganisatie, zodat u niet voor verrassingen komt te staan. Het volgen van deze handreiking voorkomt eventuele problemen met persoonsgegevens van uw eigen personeel en problemen met opdrachtgevers rond bedrijfsgegevens en privacy. Bovendien geeft het volgen van de handreiking blijk van professionaliteit.

1.3 De overheidsorganisatie

Overheidsorganisaties zijn verplicht om een vergunningaanvraag en de documenten die de aanvraag onderbouwen, ter inzage te leggen. Dit gebeurt nu meestal nog in een publiek gebouw (zoals een gemeente- of provinciehuis), maar de terinzagelegging zal steeds vaker plaatsvinden door de documenten op internet te plaatsen. Daarmee worden deze documenten steeds toegankelijker.

Overheidsorganisaties hebben een eigen verantwoordelijkheid om te voorkomen dat persoonsgegevens en bedrijfsgeheimen ten onrechte openbaar worden gemaakt. Deze verantwoordelijkheid kan de overheidsorganisatie alleen waarmaken door samenwerking met de aanleverende partijen. Daarom wordt van die partijen die documenten opstellen voor een vergunningaanvraag en de aanvraag indienen gevraagd om in de documenten zorgvuldig met persoonsgegevens om te gaan, duidelijk te maken met welke gegevens vertrouwelijk moet worden omgegaan en documenten zo op te maken dat deze eenvoudig geanonimiseerd¹ kunnen worden.

1.4 Aanbevelingen

Het bovenstaande leidt tot de volgende aanbevelingen:

1. Neem geen onnodige persoonsgegevens of vertrouwelijke bedrijfsgegevens op in documenten die bestemd zijn om ter inzage te worden gelegd.
2. Vermeld noodzakelijke persoonsgegevens maar één keer (noem de naam van een opdrachtgever bijvoorbeeld slechts eenmaal en spreek verder over 'de opdrachtgever');
3. Zorg dat persoonsgegevens en vertrouwelijke bedrijfsgegevens gemakkelijk gevonden en verwijderd kunnen worden (ook bijvoorbeeld door anonimiseringssoftware). Neem geen persoonsgegevens op in een tekening, maak geen handgeschreven aantekeningen met persoonsgegevens erin en zet persoonsgegevens en vertrouwelijke bedrijfsgegevens zoveel mogelijk op een makkelijk herkenbare plaats, bijvoorbeeld in een speciale bijlage.
4. Ideaal: maak twee versies van een document. Eén versie voor de overheidsorganisatie dat de aanvraag behandelt en één openbare versie voor de terinzagelegging.

In de volgende hoofdstukken zal dieper op deze aanbevelingen worden ingegaan.

¹ In het dagelijkse taalgebruik wordt de term 'anonimiseren' gebruikt voor verwijderen van persoonsgegevens uit een openbaar te maken versie van documenten door deze zwart te maken of te vervangen door aanduidingen als 'aanvrager' of 'A'. Ook in deze handreiking gebruiken we 'anonimiseren' in deze betekenis. De Algemene verordening gegevensbescherming (AVG) gebruikt hiervoor een afwijkende juridische terminologie en spreekt in dit geval van 'pseudonimiseren' (ook als er geen sprake is van het gebruik van een pseudoniem). Van 'anonimiseren' is volgens de AVG sprake als op geen enkele manier meer kan worden achterhaald over welke persoon het gaat. Bij de in de handreiking besproken documenten is anonimiseren in deze betekenis onmogelijk, omdat de overheid altijd een origineel behoud waarin de persoonsgegevens leesbaar blijven en het ook overigens met de nodige moeite meestal mogelijk blijft om aan de inhoud van het document te ontlezen over wie het gaat.

2. Welke documenten worden digitaal ter inzage gelegd?

Voorbeelden van documenten die (digitaal) ter inzage moeten worden gelegd zijn aanvragen of verleningen van bekendmakingen, verlening van een vergunning na toepassing van de uniforme, openbare voorbereidingsprocedure, vaststelling van een verkeersbesluit, besluit tot onteigening of een voornemen tot vervreemding van cultureel erfgoed. De overheidsorganisatie waar u mee te maken heeft kan u hier meer over vertellen.

Wanneer u bijvoorbeeld een aanvraag om een omgevingsvergunning indient, worden alle documenten die nodig zijn voor de beoordeling van die specifieke aanvraag ter inzage gelegd. Denk hierbij aan het aanvraagformulier, kaarten, tekeningen, rapporten en overige informatie. Op die manier kan eenieder zich een beeld vormen van waar de vergunning voor wordt gevraagd. Welke documenten ter inzage worden gelegd hangt af van het soort aanvraag. De overheidsorganisatie maakt deze afweging.

3. Deze gegevens vragen specifieke aandacht

Documenten die bestemd zijn om ter inzage te worden gelegd kunnen verschillende soorten gegevens bevatten. Bepaalde categorieën van gegevens vragen bijzondere aandacht:

- a) Persoonsgegevens;
- b) Vertrouwelijke bedrijfsgegevens;
- c) Veiligheidsgegevens.

In de volgende paragrafen worden deze categorieën nader toegelicht. In bijlage 1 is een overzicht opgenomen van veel voorkomende gegevens met adviezen over deze gegevens.

3.1 Persoonsgegevens

Persoonsgegevens zijn alle gegevens die iets zeggen over een mens van vlees en bloed. Denk aan namen, (e-mail)adressen, Burgerservicenummers (BSN-nummers), maar ook de medische gesteldheid van een persoon (zit hij/zij in een rolstoel) of een foto waarop een persoon herkenbaar in beeld is. Deze gegevens worden beschermd door privacywetgeving (de Algemene Verordening Gegevensbescherming: AVG). Wanneer u documenten aanlevert waarop dit soort gegevens staan bent u zelf verantwoordelijk voor het naleven van de privacywetgeving. Dit houdt in:

- Vermeld alleen persoonsgegevens die nodig zijn voor de beoordeling van de vergunningaanvraag. Volg hierbij de gegevens die gevraagd worden in de formulieren die de overheidsorganisatie ter beschikking stelt.
- Bevat een formulier open invulvelden, vul daar dan geen persoonsgegevens in ('de heer De Vries wenst een dubbele dakkapel' vervangen door 'opdrachtgever wenst een dubbele dakkapel'). Open invulvelden zijn moeilijk doorzoekbaar door bijvoorbeeld anonimiseringssoftware, waardoor het risico groot is dat daar vermelde persoonsgegevens over het hoofd worden gezien en ten onrechte gepubliceerd worden;
- Namen van uw eigen medewerkers zijn doorgaans niet nodig voor de beoordeling van de vergunningaanvraag. Zorg er dus voor dat deze namen verwijderd worden voordat het document wordt aangeleverd aan de overheidsorganisatie. Uitzondering hierop vormen de namen die nodig zijn voor de uitoefening van de auteursrechten, zie hierover onder b. en c.;
- Bevat de naam van uw organisatie een persoonsnaam (bijvoorbeeld 'Architectenbureau A. de Roos'), bedenk dan dat deze naam ook op internet gepubliceerd zal worden. Bent u zelf A. de Roos, bedenk dan of u er zwaarwegende bezwaren tegen heeft dat uw persoonsnaam in dit verband op internet wordt gepubliceerd en geef dit aan bij de aanvraag. De overheidsorganisatie maakt een eigen afweging of het gegeven wordt gepubliceerd, maar moet uw inbreng daarin meenemen.

a) Persoonsgegevens in briefhoofd, watermerk of stempel

Persoonsgegevens worden ook opgenomen in briefhoofden, watermerken en tekeninghoofden ('stempels'). Deze gegevens zijn vaak niet vindbaar voor anonimiseringssoftware en ook niet goed aanpasbaar door de overheidsorganisatie. Daarmee ontstaat een risico dat persoonsgegevens ten onrechte gepubliceerd worden, in strijd met de privacywetgeving. De overheidsorganisatie mag dit soort documenten terugsturen naar de aanvrager met het verzoek deze gegevens te verwijderen. Beter is natuurlijk om er al bij de aanlevering voor te zorgen dat er geen gevoelige gegevens zijn opgenomen op plaatsen die niet of slecht doorzoekbaar of aanpasbaar zijn.



Tuin Familie Jansen	
Definitief ontwerp	
Burgmans Ontwerp Schouwrooij 2 5281 RE Bostel	info@ontwerp.nl 0612345678
Ontwerper: C. Burgmans Datum: 05-09-2012	Schaal 1:100 Versie 1.2

In bovenstaand voorbeeld kunnen in het kader van anonimisering de volgende punten worden opgemerkt:

- Dat de tuin is bedoeld voor de familie Jansen is niet relevant, alleen het adres is relevant. Omwonenden moeten immers weten wat er in hun buurt gebeurt;
- De naam van de ontwerper is hier niet relevant. Voor omwonenden is alleen interessant wat er gaat gebeuren, niet door wie het ontwerp is gemaakt;
- De bedrijfsnaam 'Burgmans Ontwerp' bevat een persoonsnaam. Als u zwaarwegende bezwaren heeft tegen publicatie van die naam op internet moet u dit aangeven bij de aanvraag;
- De tekst staat in een zogenaamde stempel. De overheidsorganisatie kan hier digitaal (met gebruik van anonimiseringssoftware) geen wijzigingen in aanbrengen. Het handmatig aanpassen van de gegevens (die vaak op elke pagina van het document terug komen zou onevenredig veel inspanning vragen van de overheidsorganisatie. De overheidsorganisatie kan daarom het document terugsturen naar de aanvragen/opsteller van de documenten.

b) Auteursrechten

Op documenten die bij een vergunningaanvraag worden aangeleverd en die ter inzage moeten worden gelegd kunnen auteursrechten rusten. Denk bijvoorbeeld aan bouw- of constructietekeningen of specifieke berekeningen.

Geef als indiener altijd aan dat op een werk auteursrecht rust. Dit ter onderscheiding van door de overheid zelf opgestelde documenten waarop in de regel geen auteursrecht rust. De overheidsorganisatie kan bij de terinzagelegging een waarschuwing plaatsen dat op sommige documenten auteursrechten rusten en dat – wanneer iemand om welke reden dan ook gebruik wil maken van het document – toestemming aan de auteur gevraagd moet worden.

Auteursrecht: De documenten die ter inzage liggen zijn (deels) niet opgesteld door de overheid. Op deze documenten kan auteursrecht rusten.

Tekst die door de overheidsorganisatie geplaatst zal worden bij documenten waarop auteursrecht kan berusten

c) Vermelden van copyright

Om duidelijk te maken bij wie het auteursrecht berust wordt vaak gebruik gemaakt van een copyrightvermelding als ©jandevries. Ondanks dat deze copyrightvermelding een persoonsnaam bevat, is het niet de bedoeling dat de persoonsnaam wordt verwijderd uit de te publiceren documenten. Dan zou het immers onmogelijk zijn om de rechthebbende te benaderen.

De persoon die als houder van het auteursrecht (exploitatie rechten) staat vermeld is niet altijd de persoon die de tekening heeft gemaakt. Dit kan ook de werkgever zijn bij wie de verantwoordelijke architect in dienst is. De oorspronkelijke maker (de werknemer) behoudt echter de zogenaamde persoonlijkheidsrechten (recht op naamsvermelding en verzet tegen aantasting van het werk) uit artikel 25 van de Auteurswet. Om met beide rechten rekening te kunnen houden zullen dus in die situatie de naam van de werkgever én van de maker vermeld moeten worden.

3.2 Bedrijfsgegevens

Voor bepaalde vergunningaanvragen is het nodig om in de bij de aanvraag horende documenten (vertrouwelijke) informatie over een bedrijf aan te leveren (van het eigen bedrijf of eventueel van een bedrijf waarvan de aanvrager diensten of producten afneemt). Ook deze informatie moet de overheidsorganisatie in beginsel op internet openbaar maken, tenzij het gaat om 'bedrijfsvertrouwelijke informatie die in vertrouwen aan de overheidsorganisatie is meegedeeld'. Is dat het geval? Is er bijvoorbeeld sprake van informatie over:

- de technische bedrijfsvoering (zoals de beveiliging van een product, specifieke kenmerken, alleen door het bedrijf gebruikte terminologie of een unieke aanpak);
- het productieproces;
- de afzet van de producten of de kring van afnemers en leveranciers, of
- de financiële bedrijfsvoering,

én kan publicatie van die gegevens ervoor zorgen dat het betreffende bedrijf wordt benadeeld in zijn concurrentiepositie? Geef dan direct bij de aanvraag aan (of verzoek de daadwerkelijke aanvrager om dit voor u te doen) dat u bezwaar heeft tegen publicatie van deze gegevens.

Als de gegevens (mede) een ander bedrijf betreffen heeft u toestemming van dat bedrijf nodig voordat u de gegevens aanlevert bij de overheidsorganisatie.

Dat bedrijfsvertrouwelijke informatie uit zeer diverse componenten kan bestaan blijkt wel uit verschillende rechterlijke uitspraken. Zo werd als bedrijfsvertrouwelijke informatie aangemerkt:

- De wijze waarop een casino haar preventie en verslavingszorg had ingericht;
- Kostenramingen binnen een aanbesteding over de sanering van een gebouw;
- Namen van de bollenrassen binnen de bloembollenbranche.

Het is aan de aanleverende partij om aan te geven welke gegevens om welke reden als bedrijfsgevoelig aangemerkt moeten worden.

3.3 Veiligheidsgegevens

Het komt in beperkte mate voor dat informatie in de vergunningaanvraag kan leiden tot een mogelijk gevaarlijke situatie wanneer die informatie in verkeerde handen komt. Denk aan de aanvraag omgevingsvergunning voor een bankgebouw: bouwtekeningen bij die aanvraag zouden bijvoorbeeld de plaats van de kluis kenbaar maken. Dit kan het voor criminelen makkelijker maken om een overval te plegen. Informatie over de indeling van een festivalterrein kan voor een terrorist relevant zijn wanneer hij een aanslag voorbereidt. Bedrijfsinformatie over het uitvoeren van dierproeven kan na openbaarmaking leiden tot bedreigingen en intimidatie door dierenrechtenextremisten.

De overheidsorganisatie kan dergelijke informatie uitzonderen van de openbaarmakingsplicht. Maar als aanvrager of opsteller van de bijbehorende documenten kunt u hierin ondersteunen door direct bij de aanvraag aan te geven dat sprake is van zogenaamde veiligheidsgegevens en de veiligheidsgegevens te benoemen en door een tweede versie van de tekeningen en documenten aan te leveren waar de gevoelige informatie niet is opgenomen. Deze laatste documenten zijn daarmee geschikt voor terinzagelegging.

Bijlage 1 Overzicht van veel voorkomende gegevens

W (Weglaten): deze gegevens zijn doorgaans niet nodig voor de vergunningsaanvraag en kunnen nadeel opleveren voor betrokkene als deze gegevens door de overheidsorganisatie ter inzage worden gelegd. Wanneer de gegevens (eenmalig) nodig zijn voor de vergunningaanvraag worden deze vermeld, maar vervolgens wordt volstaan met ‘opdrachtgever’;

O (Opnemen): deze gegevens kunnen zonder voorbehoud worden opgenomen in de documenten, tenzij er sprake is van een heel bijzondere omstandigheid, waardoor publicatie van deze

gegevens een onevenredige inbreuk zou betekenen voor de privacy van de persoon op wie of het bedrijf waarop de gegevens betrekking hebben;

V (Vertrouwelijkheid vragen): deze gegevens worden wel opgenomen in de documenten, omdat deze nodig zijn voor de beoordeling van de aanvraag. Maar direct bij de aanvraag geeft de aanvrager aan dat en waarom de gegevens niet geschikt zijn voor publicatie.

Soort gegevens	W	O	V	Toelichting
Persoonsgegevens				
Naam opdrachtgever	✓			Deze gegevens alleen op de documenten laten als deze nodig zijn voor de aanvraag. En dan slechts eenmaal gebruiken (daarna kan volstaan worden met bijvoorbeeld ‘opdrachtgever’).
Adresgegevens opdrachtgever	✓			
Telefoon/e-mail opdrachtgever	✓			
Namen medewerkers	✓			Zijn doorgaans niet nodig voor de (onderbouwing van) de aanvraag, dus worden niet aangeleverd.
Adresgegevens/telefoonnummer/e-mail medewerkers (bedrijfsmatig gebruik)		✓		Kunnen worden verstrekt. Het heeft de voorkeur om algemene adresgegevens op te nemen (info@bedrijfsnaam.nl) i.p.v. door kiesgegevens.
Burgerservicenummer (BSN) (bijvoorbeeld bij gebruik van DigiD)	✓			Er mag nooit een BSN van een andere persoon worden gebruikt. Inloggen via DigiD namens een andere persoon kan via DigiD Machtigen.
Foto's waarop mensen herkenbaar in beeld staan.	✓			Maak deze personen onherkenbaar.
Kopie van identiteitsbewijs	✓			Bij verkeerd gebruik is hier een groot risico op misbruik van gegevens (identiteitsfraude). Let dus extra goed op dat dit soort documenten niet wordt verstrekt aan de overheidsorganisatie tenzij hier expliciet om wordt gevraagd. En zorg dan voor een veilige aanlevering.
Bedrijfsgegevens				
Naam bedrijf		✓		Kan in beginsel gewoon worden aangeleverd. Als een persoonsnaam onderdeel uitmaakt van de bedrijfsnaam en de houder van die persoonsnaam heeft er bezwaar tegen dat die naam openbaar wordt gemaakt moet hij/zij dit aangeven bij de overheidsorganisatie.
KVK-nummer		✓		Is een openbaar gegeven dus kan worden aangeleverd.
Btw-nummer	✓			Is alleen nodig voor facturen en offertes, dus niet in overige documenten.
Concurrentiegevoelige gegevens (productie, beveiliging, klantenkring, tarieven etc.)			✓	Deze gegevens kunnen – als zij nodig zijn voor de aanvraag – wel aan de overheidsorganisatie worden aangeleverd. Wanneer u openbaarmaking wilt voorkomen geeft u aan bij de overheidsorganisatie dat het vertrouwelijke gegevens betreft (zie par. 3.2)
Veiligheidsgegevens				
Tekeningen/plattegronden etc. van risico-gebouwen (banken, blijf-van-mijn-lijfhuizen)			✓	Als u denkt dat het openbaar maken van deze informatie gevaar op kan leveren voor de maatschappij dan geeft u dat aan bij de overheidsorganisatie
Informatie over evenementen			✓	

KOOP is een onderdeel van UBR. UBR is een rijksbrede dienstverlener bij organisatie- en ontwikkelvraagstukken, complexe digitale trajecten en innovaties in de bedrijfsvoering. UBR voert taken uit op het gebied van interim management, HRM, ICT, inkoop en financiën. Wij zijn deskundig, innovatief en leveren resultaat.

UBR. Voor een ambitieuze overheid.

www.ubrijk.nl