REGIONALE BELASTING GROEP

# BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 226
13 maart 2020

Officiële uitgave van de gemeenschappelijke regeling Regionale Belasting Groep

## Besluit van het dagelijks bestuur van de gemeenschappelijke regeling Regionale Belasting Groep houdende regels omtrent privacy

Binnen de Regionale Belasting Groep wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld voor het goed uitvoeren van de wettelijke taken. De burger moet erop kunnen vertrouwen dat de Regionale Belasting Groep zorgvuldig en veilig met de persoonsgegevens omgaat. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De Regionale Belasting Groep is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.
Bestuur en management spelen een cruciale rol bij het waarborgen van privacy.
De Regionale Belasting Groep geeft middels dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen en gegevensverzamelingen (van zowel klanten als eigen medewerkers). Dit privacybeleid van de Regionale Belasting Groep is in lijn met het algemene beleid van de Regionale Belasting Groep en de relevante lokale, regionale, nationale en Europese wet- en regelgeving. Dit privacybeleid is niet van toepassing op gegevens over rechtspersonen. Op gegevens van rechtspersonen geldt de geheimhoudingsplicht volgens art. 67 van de AWR en art 67 van de Invorderingswet 1990.

### Wettelijke kaders voor de omgang met gegevens

De Regionale Belasting Groep is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor gelden onder andere de volgende wettelijke kaders:

- Wet Bescherming Persoonsgegevens (Wbp), vanaf 25 mei 2018 vervangen door de Europese Verordening: de Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet Algemene Verordening Gegevensbescherming;

### Uitgangspunten

De Regionale Belasting Groep gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De Regionale Belasting Groep houdt zich hierbij aan de volgende uitgangspunten:

*Rechtmatigheid, behoorlijkheid, transparantie*
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

*Grondslag en doelbinding*
De Regionale Belasting Groep zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt. De Regionale Belasting Groep verwerkt de persoonsgegevens (voornamelijk) op basis van een wettelijke grondslag. Het doel is het heffen en innen van (lokale) belastingen. Voor sommige persoonsgegevens is geen wettelijke grondslag aanwezig en zal de Regionale Belasting Groep de gegevens slechts opslaan en gebruiken na uitdrukkelijke toestemming van betrokkene.

*Dataminimalisatie*
De Regionale Belasting Groep verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De Regionale Belasting Groep streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

*Bewaartermijn*
Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens is nodig om de wettelijke taken goed uit te kunnen oefenen, of om wettelijke verplichtingen te kunnen naleven (bijvoorbeeld de archiefwet). Per verwerkingsdoel legt de Regionale Belasting Groep vast hoelang de gegevens worden bewaard.

*Integriteit en vertrouwelijkheid*
De Regionale Belasting Groep gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de

Regionale Belasting Groep voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid Regionale Belasting Groep.

*Delen met derden*
In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de Regionale Belasting Groep afspraken over de eisen waar beveiliging van gegevensuitwisseling en verwerking aan moet voldoen. Deze afspraken worden vastgelegd in een verwerkersovereenkomst en voldoen aan de wet. De Regionale Belasting Groep controleert deze afspraken minimaal één keer per jaar.

*Subsidiariteit*
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt. We zien af van de verwerking van persoonsgegevens indien hetzelfde doel ook langs andere weg en met minder ingrijpende middelen kan worden gerealiseerd.

*Proportionaliteit*
De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het te dienen doel. We verwerken niet meer gegevens dan noodzakelijk voor het doel waarvoor de gegevens nodig zijn.

*Rechten van betrokkenen*
De Regionale Belasting Groep honoreert alle rechten van betrokkenen.

*Verwerkingsregister*
De Regionale Belasting groep legt een verwerkingsregister aan waarin wordt vastgelegd voor welke processen welke gegevens worden gebruikt en aan wie deze verstrekt worden ter verdere verwerking.

*Bijlage*
Het Protocol meldingen aan Autoriteit Persoonsgegevens RBG is als bijlage opgenomen in het Privacybeleid RBG.
Dit privacybeleid treedt in werking na vaststelling door het dagelijks bestuur van de Regionale Belasting Groep. Het beleid wordt iedere drie jaar geëvalueerd en indien nodig herzien. Aanpassingen van dit beleid worden bestuurlijk vastgesteld. De meest actuele versie van het beleid wordt beschikbaar gesteld aan de organisatie middels publicatie op de gemeenschappelijke netwerkschijven (G-schijf).

*Vastgesteld in de vergadering van het dagelijks bestuur van de Regionale Belasting Groep op 26 april 2018.*

*Het dagelijks bestuur van de Regionale Belasting Groep,*

*directeur,*

*H.B. Sigmond*

*voorzitter,*

*drs. A.J.B. van der Klugt*

## Bijlage 1: Protocol meldingen aan Autoriteit Persoonsgegevens

**Bijzondere persoonsgegevens**

Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Bijlage
Inhoud

Inleiding

Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Het kan gaan om een kwijtgeraakte USB-stick of een gestolen laptop met persoonsgegevens maar ook om een inbraak in een datasysteem of per ongeluk verstrekte toegang tot gegevens aan personen of instanties die daartoe geen toegang zouden mogen hebben. Het verzenden van een e-mail aan een adressenbestand waarin alle e-mailadressen voor iedereen zichtbaar zijn is ook al een datalek. Als sprake is van een datalek, dan zijn we verplicht om dit te melden aan de Autoriteit Persoonsgegevens en soms ook aan de betrokkenen.

Wat is een datalek

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 33 lid 1 van de Algemene Verordening Gegevensbescherming). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden. Is dit het geval of is dit niet met zekerheid uit te sluiten dan dient dit als een datalek gemeld te worden bij de Autoriteit Persoonsgegevens.
Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. Er hoeft dan geen melding gedaan te worden aan de Autoriteit Persoonsgegevens.
Indien er sprake is van een beveiligingsincident dient, ongeacht of er sprake is van een datalek, de manager Informatiebeveiliging te worden ingelicht.

Wat te doen bij het vermoeden van een datalek

Om te zorgen voor een eenduidig beleid en om te voorkomen dat onnodig een melding van een datalek wordt gemaakt, dienen mogelijke datalekken bij de manager Informatiebeveiliging (MI) of bij de Functionaris Gegevensbescherming (FG) gemeld te worden. Zij bepalen of er daadwerkelijk sprake is van een datalek.

De manager Informatiebeveiliging is : J.F.Kooistra
De Functionaris Gegevensbescherming is : .....*

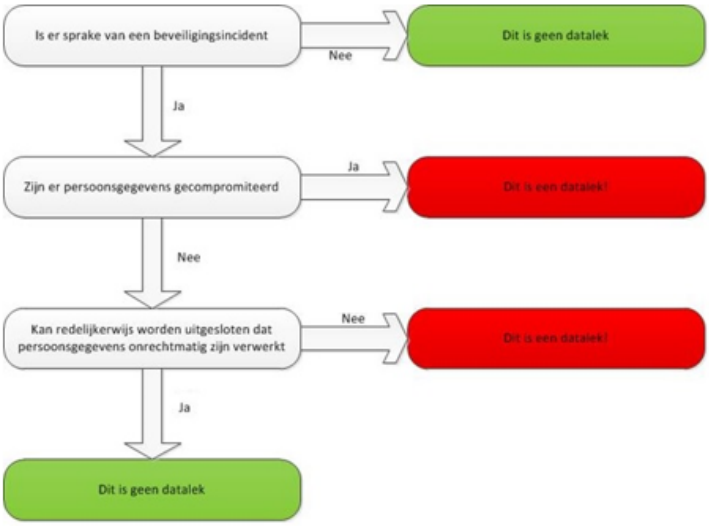
*deze functionaris wordt nog aangewezen door de directeur en zal voor 25 mei 2018 worden aangemeld bij de Autoriteit Persoonsgegevens.

**Stappenplan**

1. Onmiddellijk nadat een medewerker ontdekt of ter ore komt dat er sprake kan zijn van verlies of onrechtmatige verwerking van persoonsgegevens binnen de RBG, meldt hij dat aan de manager Informatiebeveiliging (MI) of aan de Functionaris Gegevensbescherming (FG).
2. De MI en/of de FG beslissen of er sprake is van een (mogelijk) datalek en of dit (mogelijke) datalek moet worden gemeld bij de Autoriteit Persoonsgegevens en/of bij de betrokkenen.
3. De MI en/of FG zorgen dat een melding aan de Autoriteit Persoonsgegevens en/of de betrokkenen wordt gedaan. Het is de medewerker niet toegestaan om het (mogelijke) datalek zelf aan de Autoriteit Persoonsgegevens en/of de betrokkenen te melden.
4. Als de medewerker het niet eens is met de beslissing van de MI en/of FG om het (mogelijke) datalek wel - of niet te melden aan de Autoriteit Persoonsgegevens en/of de betrokkenen, dan kan hij zich richten tot de directeur.

**Meldingen Autoriteit Persoonsgegevens**

Niet elk datalek hoeft gemeld te worden aan de Autoriteit Persoonsgegevens. Volgens de wet dient slechts melding aan de Autoriteit Persoonsgegevens gedaan te worden, als het datalek leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

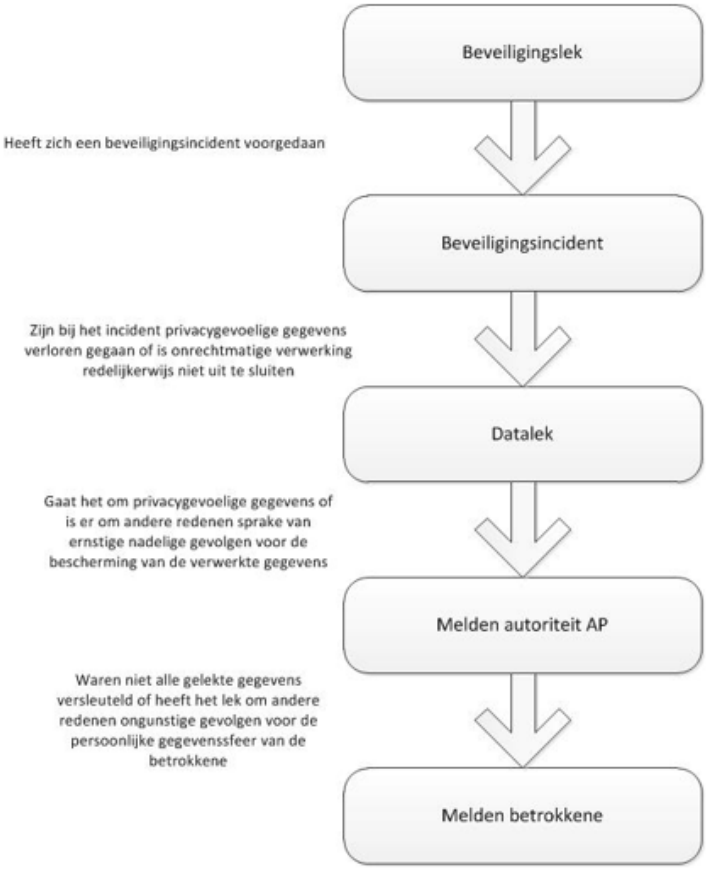



Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk. Bij persoonsgegevens van gevoelige aard kan gedacht worden aan:
**Bijzondere persoonsgegevens zoals bedoeld in artikel 4 lid 1 AVG**
Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

**Gegevens over de financiële of economische situatie van de betrokkene**
Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.

**Gebruikersnamen, wachtwoorden en andere inloggegevens**
De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet rekening worden gehouden dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

**Gegevens die kunnen worden misbruikt voor (identiteits-)fraude**
Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).



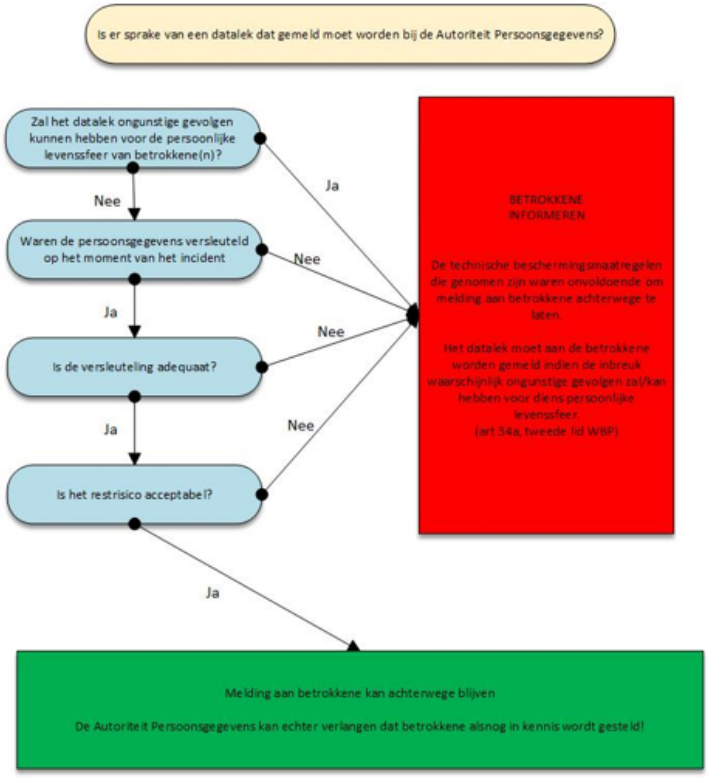

Een melding moet gedaan worden zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel dit webformulier beschikbaar gesteld.

**Melding aan de Autoriteit Persoonsgegevens**

1. De aard van de inbreuk
2. De instanties waar meer informatie over de inbreuk kan worden verkregen
3. De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken
4. Een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens
5. De RBG documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.
6. Er is vanaf 1-1-2016 een speciale webpagina beschikbaar voor het doen van de melding. https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

**Melding aan de betrokkene**

Als geconcludeerd wordt dat een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens, dan betekent dat niet automatisch dat dit datalek ook gemeld dient te worden aan de betrokkene. Hiervoor dient een aparte afweging gemaakt te worden.
In het algemeen kan gesteld worden dat wanneer sprake is van persoonsgegevens van gevoelige aard de betrokkene geïnformeerd moet worden over het datalek.




Aan betrokken worden minimaal de volgende gegevens verstrekt (volgens artikel 34 lid 2 AVG):

1. In duidelijk Nederlands de omschrijving van de aard van de inbreuk
2. De instanties waar meer informatie over de inbreuk kan worden verkregen
3. De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken

Bij het beschrijven van de aard van de inbreuk kan doorgaans volstaan worden met een algemene omschrijving. Voorts wordt hierbij de contactgegevens opgenomen zodat de betrokkene waar hij/zij terecht kan indien hij/zij vragen heeft over het datalek. Verder kan aangegeven worden wat de betrokkene zelf kan doen om de negatieve gevolgen van het datalek te beperken.