REGIONALE BELASTING GROEP

# BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 163

26 januari 2026

Officiële uitgave van de gemeenschappelijke regeling Regionale Belasting Groep

## Besluit Privacybeleid Regionale Belasting Groep 2023

**Vaststelling**
Dit privacybeleid treedt in werking na vaststelling door het Dagelijks Bestuur van de Regionale Belasting Groep (de RBG). Het beleid wordt tenminste een keer per drie jaar geëvalueerd en indien nodig herzien. Aanpassingen van dit beleid worden bestuurlijk vastgesteld. De meest actuele versie van het beleid is binnen de organisatie beschikbaar door publicatie in de kennisbank van de RBG.

**Inleiding**
Bij de Regionale Belasting Groep wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden verzameld voor het uitvoeren van de wettelijke taken van het heffen en invorderen van lokale belastingen. De klant 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 hiervan bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole. Het bestuur en management spelen ook een cruciale rol bij het waarborgen van privacy. Daarbij is verantwoord en bewust gedrag van medewerkers essentieel.

In de bijlage is een begrippenlijst opgenomen.

**Doel**
Het privacybeleid heeft als doel dat het hele proces van gegevensverwerking binnen de RBG duidelijk en controleerbaar wordt.

De Regionale Belasting Groep geeft met het privacybeleid een duidelijke richting aan privacy en laat zien dat zij deze waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op 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 Algemene wet rijksbelastingen (AWR) en art 67 van de Invorderingswet 1990.

Voor de medewerkers geeft het privacybeleid helderheid over hoe invulling moet worden gegeven aan het privacybelang van de betrokkenen (klanten). Hierdoor worden fouten beperkt of voorkomen en loopt de RBG minder risico op reputatieschade en handhaving door de toezichthouder. Tevens draagt het privacybeleid bij aan de transparantie van de RBG. De verwerking van de gegevens wordt zo ingericht dat het altijd inzichtelijk kan worden gemaakt hoe de gegevens zijn verwerkt, welke keuzes er zijn gemaakt en waarom. Hiermee kan de RBG aantoonbaar verantwoording afleggen over de verwerking van de persoonsgegevens aan de betrokkenen, de media, de toezichthouder en de deelnemers.

Medewerkers (intern en extern) die werkzaam zijn voor de RBG, zijn verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. Daarbij wordt naar een evenwicht gezocht tussen privacy, doelmatigheid en klantgerichtheid zonder dat de privacy hierbij geschaad wordt.

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:

- De Algemene Verordening Gegevensbescherming (AVG)
- Uitvoeringswet Algemene Verordening Gegevensbescherming

**De zes beginselen voor verwerking van persoonsgegevens**
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 naast de wettelijke verplichtingen aan de volgende zes beginselen:

1. Rechtmatigheid, behoorlijkheid, transparantie

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat.

2. Grondslag en doelbinding

De Regionale Belasting Groep zorgt 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 verplichting (AVG art 6 lid c) en algemeen belang (AVG art 6 lid e). Het doel is veelal het heffen en innen van (lokale) belastingen.

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor deze persoonsgegevens in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De RBG voert, voordat de verwerking start, een toets uit om te bepalen of de verenigbaarheid van verwerking past binnen de andere doelen op grond van de wet- en regelgeving.

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

3. 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. Inbreuk op de persoonlijke levenssfeer van de betrokken klant wordt zoveel mogelijk beperkt. We zien af van de verwerking van persoonsgegevens indien hetzelfde doel ook langs een andere weg en met minder ingrijpende middelen kan worden gerealiseerd.

4. Juistheid

De RBG zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzameld zijn of vervolgens worden verwerkt. De RBG neemt maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

5. Bewaartermijn

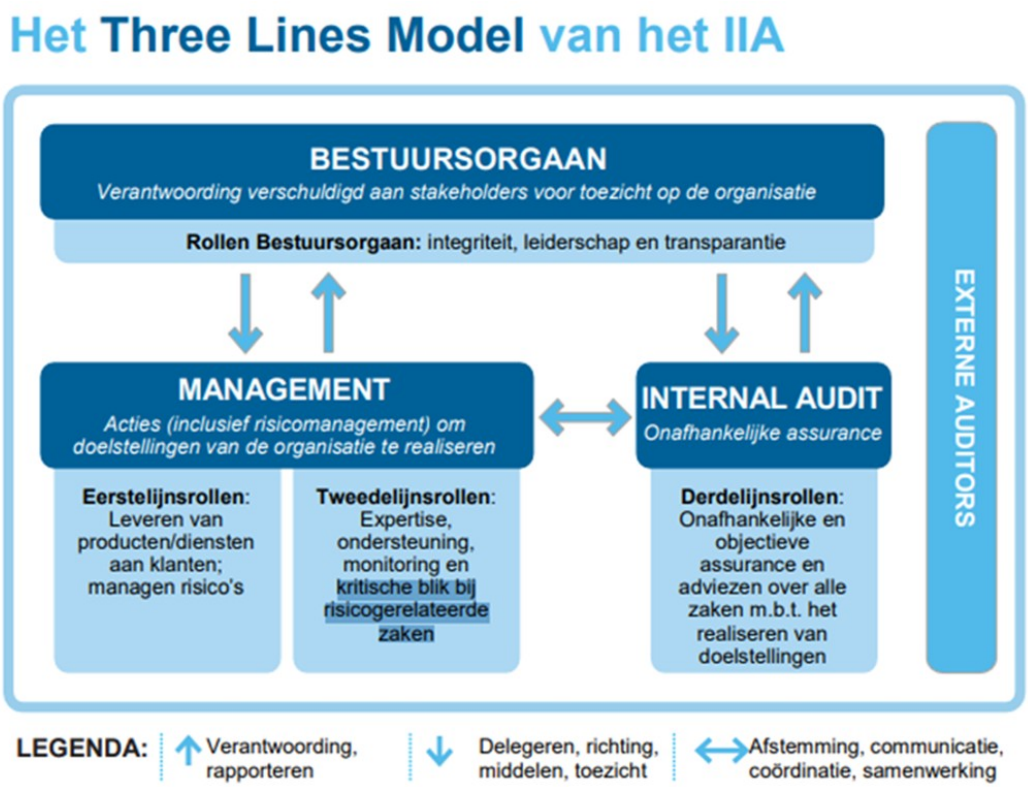
Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de wettelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven (bijvoorbeeld de archiefwet). Per verwerkingsdoel legt Regionale Belasting Groep vast hoelang de gegevens worden bewaard. De bewaartermijnen van de persoonsgegevens liggen vast in het verwerkingsregister.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijst kan worden vastgesteld, stelt de RBG de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De RBG bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

6. 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. Elke vaste medewerker heeft de belofte of de eed afgelegd, is op de hoogte van het integriteit protocol, het informatiebeveiligingsbeleid en het privacybeleid. Per functie is bepaald welke gegevens een medewerker mag inzien (need to know). Het beheer van bevoegdheden wordt periodiek gecontroleerd.

**Governance**
Dit hoofdstuk beschrijft de taken en de verantwoordelijkheden voor het verwerken van persoonsgegevens binnen de RBG. De verdeling van de verantwoordelijkheden van het management en de functies binnen de RBG is gebaseerd op het "Three Lines Model" van het IIA, het Instituut van Internal Auditors.




Binnen dit model zijn de volgende rollen en taken voorzien:

| | | |
|---|---|---|
| a. | Het bestuursorgaan | directeur; Dagelijks Bestuur van de RBG |
| b. | De 1e lijns-rollen | managers; teamleiders; specialisten |
| c. | De 2e lijns-rollen | o.a. medewerkers kwaliteitszorg, Privacy Officer, CISO |
| d. | De 3e lijn | medewerker Interne controle/audit ; Functionaris Gegevensbescherming |
| e. | Externe auditors | accountant |

Rollen en taken
a) Het bestuursorgaan

Het Dagelijks Bestuur van de RBG stelt het privacybeleid vast en bepaalt hiermee de kaders van de bescherming van de persoonsgegevens. De directeur is eindverantwoordelijk voor de uitvoering van de bescherming van de persoonsgegevens.

De verantwoordelijkheden bestaan o.a. uit:
- Het vaststellen van het privacybeleid
- Het toewijzen van de verantwoordelijkheden voor het inrichten, uitvoeren en documenteren van het privacybeleid
- Het vaststellen van de criteria voor het aanvaarden van risico's en privacy ambitieniveau
- Het (periodiek) informeren over de kwaliteit van bescherming van de persoonsgegevens.

b) De 1e lijn

De 1e lijn is primair verantwoordelijk voor de dienstverlening en de bedrijfsvoering. Daarbij hoort ook het voldoen aan de wet- en regelgeving en het zorgen voor de bescherming van de persoonsgegevens.

De 1e lijn hanteert hierbij de instrumenten vanuit de AVG zoals het register van verwerkingen, Data protection impact assessments (DPIA) en verwerkingsovereenkomsten.

De verantwoordelijkheden van de 1e lijn zijn:
- Het toepassen en het opvolgen van dit privacybeleid
- Het signaleren en het melden van beveiligingsincidenten
- Indien van toepassing het opstellen en het onderhouden van een DPIA
- Het toepassen van Privacy by Design bij systemen en processen.

De verantwoordelijkheid is primair belegd bij de proceseigenaar van het betreffende proces waarin de verwerking van persoonsgegevens plaatsvindt. De manager ziet vanuit zijn rol er op toe dat proceseigenaar de verantwoordelijkheden vervult en ondersteunt waar nodig.

c) De 2e lijn

De 2e lijn ondersteunt, controleert en adviseert de 1e lijn bij het voldoen aan de wet- en regelgeving en het nemen van passende beveiligingsmaatregelen, zoals:
- Het identificeren van risico's bij het verwerken van persoonsgegevens
- Het instellen van beheersmaatregelen
- Het controleren van de processen waarbij de persoonsgegevens worden verwerkt
- Het toepassen van het informatiebeveiligingsbeleid en het opvolgen met behulp van technische- en organisatorische maatregelen
- Het periodiek actualiseren van het privacybeleid bij de herijking van de vastgestelde risicobereidheid
- Het adviseren en monitoren van verbeteracties (bevindingen o.b.v. beoordeling beheersmaatregelen)
- Het ondersteunen in de opzet en werking, ter bescherming, van persoonsgegevens
- Het onderhouden van het register van de verwerkingen
- Het opvolgen van de bewaartermijnen.

d) De 3e lijn

De 3e lijn bevat de volgende rollen en taken:

- Interne controle

De 3e beheersingslijn wordt gevormd door de onafhankelijke discipline interne controle. De medewerker interne controle helpt de RBG haar doelstellingen te realiseren. Dit gebeurt door met een systematische en gedisciplineerde aanpak de effectiviteit van de processen van risicomanagement, beheersing en governance te evalueren en te verbeteren.

- Functionaris voor de Gegevensbescherming

De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk om onafhankelijk toezicht te houden op naleving van de relevante wet- en regelgeving, waaronder de AVG, over de bescherming van persoonsgegevens en informatiebeveiliging. De FG houdt rekening met risico's, aard, omvang, context en de doeleinden waarvoor gegevens door de RBG worden verwerkt.

e) Externe auditors

De RBG wil voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). Hiervoor laat zij periodiek door een onafhankelijke derde partij een audit op haar Information Security Management System (ISMS) uitvoeren. De BIO en ISMS dragen bij aan de bescherming persoonsgegevens. Jaarlijks beoordeelt de onafhankelijke derde partij de mate waarin voldaan wordt aan de relevante normenkaders. De volgende externe audits vinden onder andere plaats binnen de RBG:

- DigiD audit (voor het verkrijgen van de assurance verklaring van Logius t.b.v. MijnRBG)
- IT-audit (controle op toegang, autorisatiebeheer en wijzigingenbeheer van applicaties van financiële processen).

## Planning & control cyclus

Voor realisatie van de doelen van het Privacybeleid is een Information Security Management System (ISMS) ingericht. Dit is een managementsysteem gericht op het documenteren, implementeren en

evaluatie van maatregelen m.b.v. PDCA-cyclus voor de bescherming van de rechten en vrijheden van betrokkenen bij de verwerking van persoonsgegevens conform het Privacybeleid van de RBG.

De opzet van ISMS bestaat uit de volgende elementen;
- Dat verwerkingen van persoonsgegevens worden opgezet in lijn met de eisen van de AVG en belangen van betrokkene
- Dat overeenkomstig de opzet de verwerkingen en benodigde beheersmaatregelen worden geïmplementeerd
- Dat verwerkingen van persoonsgegevens stelselmatig op hun effectiviteit worden beoordeeld
- Dat verwerkingen op continue basis worden verbeterd

De verantwoordelijkheden worden belegd conform de governance zoals beschreven in dit Privacybeleid (taken 1e, 2e en 3e lijn). De RBG kan daarmee aantoonbaar voldoen aan de AVG en vinden er periodieke rapportages plaats om de opzet, bestaan en werking van het Privacybeleid te monitoren en daarop bij te sturen.

De interne 2e lijn, de Privacy Officer (PO), toetst 3-maandelijks het bestaan en werking van het Privacybeleid. De PO rapporteert aan het MT.

## Overige aandachtspunten

**Privacy by Default en Privacy by Design**
De RBG houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens. Dit uitgangspunt wordt privacy by design genoemd. De RBG draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de RBG Privacy by Default als uitgangspunt: de standaardinstellingen zijn zo privacy-vriendelijk mogelijk.

**Inbreuk in verband met persoonsgegevens**
Bij toegang tot, verlies of wijziging van persoonsgegevens bij de RBG, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. De RBG registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan.

**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 een keer per jaar.

**Doorgifte buiten de EER**
Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie door de RBG, geschiedt alleen in overeenstemming met de relevante bepalingen van wet- en regelgeving en dit privacybeleid.

**Transparantie**
De RBG informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt de RBG van deze informatieplicht af.

**Rechten van betrokkenen**
Iedereen heeft het recht om te vernemen welke persoonsgegevens de RBG over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. De Regionale Belasting Groep honoreert alle rechten van betrokkenen.

**Verwerkingsregister**
De RBG heeft een verwerkingsregister waarin wordt vastgelegd voor welke processen welke gegevens worden gebruikt en aan wie deze verstrekt worden ter verdere verwerking.

**Data Protection Impact Assessment (DPIA)**

Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de RBG een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De RBG voert in dat geval een gegevenseffect-beoordeling (ook wel Data Protection Impact Assessment of DPIA genoemd) uit. Als uit de DPIA blijkt dat er hoge risico's zijn verbonden aan de verwerking, moet de RBG voldoende maatregelen nemen om de risico's te verminderen.

**PDCA Cyclus**
De RBG streeft ernaar om rondom de verwerking van persoonsgegevens in control te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de RBG weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

**Bewustwording**
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn binnen de RBG voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

*Vastgesteld in de vergadering van het dagelijks bestuur van de Regionale Belasting Groep d.d. 24 augustus 2023.*

*Het dagelijks bestuur van de Regionale Belasting Groep,*

*Directeur,*
*Wg*
*H.B. Sigmond*

*Voorzitter,*
*wg*
*drs. A.J.B. van der Klugt*

## Bijlage Begrippenlijst

**AP**: De Autoriteit Persoonsgegevens is de toezichthoudende autoriteit in Nederland op de Algemene Verordening Gegevensbescherming.

**Anonimiseren**: het verwerken van persoonsgegevens waarbij de bewerking onomkeerbaar is en de persoon niet valt te identificeren. Vanaf dat moment zijn het geen persoonsgegevens meer en is de AVG niet meer van toepassing.

**Beperken van de verwerking**: het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken.

**Bestand**: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.

**BIO**: De Baseline informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Had voorheen iedere overheidslaag zijn eigen baseline, nu is er met gezamenlijke inspanning één BIO voor de gehele overheid.

**CISO**: Chief Information Security Officer verantwoordelijk voor informatiebeveiliging binnen de RBG.

**Derde**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

**DPIA**: DPIA staat voor Data Protection Impact Assessment en wordt in Nederland ook wel de gegevensbeschermingseffect-beoordeling genoemd. Is bij het verwerken van persoonsgegevens sprake van hoge risico's, dan is een DPIA volgens de AVG verplicht. Het doel van de DPIA is vooraf aan de verwerking van persoonsgegevens de risico's te inventariseren en daar vooraf beheersmaatregelen voor te treffen.

**Gegevens over gezondheid**: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon.

**Governance**: het uitvoeren van beleid, controle, macht, regels en principes van de RBG.

**Inbreuk in verband met persoonsgegevens/datalek**: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of door de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

**ISMS**: ISMS staat voor Information Security Management System en is een managementsysteem voor beheersing van privacy maatregelen. Het ISMS bestaat voor een deel uit IT onderdelen, maar daarnaast komt ook het gedrag van medewerkers, standaard procedures (bijv. register van verwerkingen) en bedrijfsrichtlijnen aan de orde. Met ISMS wil de RBG haar privacy verantwoordelijkheden, complementair met informatiebeveiliging, beheersen en monitoren.

**Ontvanger**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden gegeven.

**Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

**Privacy by design**: dit houdt in dat al bij de ontwikkeling van producten en diensten aandacht moet worden besteed aan privacy. In het bijzonder bij ICT-producten en -diensten gaat het erom dat al in het ontwikkelproces gebruik gemaakt wordt van privacy-verhogende maatregelen

**Profilering**: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van de persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met de bedoeling zijn/haar beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

**Pseudonimisering**: het verwerken van persoonsgegevens op een zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld. Er worden geen aanvullende gegevens gebruikt, mits deze apart worden bewaard en er technische- en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

**Toestemming van de betrokkene**: De burger (betrokkene) heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden.

**Verwerker**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke de persoonsgegevens verwerkt.

**Verwerking**: een bewerking of een geheel van de bewerkingen van de persoonsgegevens, al dan niet geautomatiseerd. Denk hierbij aan het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of het op een andere manier beschikbaar stellen, aligneren of combineren, afschermen, wissen of vernietigen van de gegevens.

**Verwerkingsverantwoordelijke**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van de persoonsgegevens vaststelt.