GBLT gemeente- en waterschapsbelastingen

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 689

7 juli 2023

Officiële uitgave van de gemeenschappelijke regeling GBLT

Privacybeleid GBLT

1 Inleiding privacybeleid

Iedereen heeft recht op privacy. Gegevensverwerking vindt binnen GBLT plaats op een eerlijke, veilige en betrouwbare manier waarbij privacy is gewaarborgd. Persoonsgegevens worden door GBLT voornamelijk verwerkt voor het effectief uitvoeren van de aan de haar toebedeelde wettelijke taken. Een zorgvuldige omgang met de persoonsgegevens vormt een essentiële bouwsteen voor het vertrouwen van burgers in de overheid, maar ook van personeel in de organisatie.

GBLT geeft met dit beleid een duidelijke richting aan gegevensbescherming. Zij toont aan dat ze de privacy van haar burgers, medewerkers en (keten)partners waarborgt, beschermt en handhaaft.

Het privacybeleid van GBLT stuurt en controleert alle processen in de organisatie waarbij persoonsgegevens worden verwerkt. Het privacybeleid beschrijft de aanpak op het gebied van privacy en bescherming van persoonsgegevens waarmee gegevens op een zorgvuldige manier worden verwerkt.

Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van GBLT. Het beleid wordt jaarlijks geëvalueerd en indien nodig herzien.

De onderwerpen die in dit beleid onder andere aan de orde komen zijn onder andere het juridisch kader waarbinnen GBLT functioneert, uitgangspunten voor een veilige en rechtmatige verwerking van persoonsgegevens, de governance, het verwerkingsregister, DPIA's en de wijze waarop GBLT uitvoering geeft aan de rechten van betrokkenen.

1.1 Definities

De volgende definities worden in de AVG gebruikt (artikel 4):

1) persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene).
2) verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
3) anonimiseren: het verwerken van persoonsgegevens waarbij de bewerking onomkeerbaar is en de persoon niet valt te identificeren. Het zijn dan geen persoonsgegevens meer en is de AVG niet op van toepassing.
4) 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 persoonsgegevens vaststelt.
5) verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
6) inbreuk in verband met persoonsgegevens: 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 de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, ook wel bekend als 'datalek'.
7) Privacy Officer (PO): een privacy-adviseur die de GBLT adviseert op casusniveau bij gegevensbescherming binnen de organisatie.
8) Privacy by Design (Pbd): concept dat inhoudt dat privacy wordt meegenomen tijdens de ontwerpfase van een informatiesysteem of nieuw product.
9) Privacy by Default (Pbd): concept dat aangeeft dat instellingen van programma's, apps, websites, diensten of apparaten standaard zodanig zijn ingesteld dat maximale privacybescherming wordt nagestreefd.
10) Functionaris voor de gegevensbescherming (FG): de FG is de onafhankelijk toezichthouder op de omgang met persoonsgegevens binnen GBLT. De FG controleert en adviseert GBLT op het gebied van gegevensbescherming.
11) Grondslag: de juridische basis voor de gegevensverwerking.

12) Verwerkingsregister: in het verwerkingsregister staat informatie opgesomd van alle processen binnen GBLT waarbij persoonsgegevens worden verwerkt. Zoals de doeleinden, de soort persoonsgegevens en de bewaartermijnen.
13) Verwerkersovereenkomst: als een derde partij persoonsgegevens verwerkt voor GBLT dienen hiermee afspraken te worden gemaakt in de vorm van een verwerkersovereenkomst. Hierin staat onder andere opgenomen hoe de bescherming en verwerking van persoonsgegevens is geregeld.
14) DPIA (Data Protection Impact Assessment): ook wel bekend als PIA of gegevenseffectbeoordeling. Dit is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen.

2 Juridisch kader

2.1 Privacy als fundamenteel recht

Het recht op privacy is een fundamenteel recht. Dit recht is in verschillende Europese en internationale regels, maar ook in onze Grondwet verankerd. Het recht van privacy is breed en behelst niet alleen de bescherming van persoonsgegevens, maar ook de persoonlijke levenssfeer, de lichamelijke integriteit, de vrije en ongestoorde communicatie.

2.2 Wettelijk kader

De Algemene Verordening Gegevensbescherming (AVG) is de voornaamste regelgeving waar GBLT mee te maken heeft in het kader van privacywetgeving. De AVG is rechtstreeks van toepassing in alle lidstaten en heeft rechtstreekse werking. In de Uitvoeringswet op de AVG (UAVG) heeft Nederland haar aanvullende regels op de AVG opgenomen. Tevens gelden nog een aantal andere specifieke regels. Deze worden hieronder besproken.

GBLT voert voor een aantal gemeenten en waterschappen wettelijke taken uit. Dit zijn wettelijke taken die voortvloeien uit de Gemeentewet, Waterschapswet en de Wet WOZ. Het gaat om het heffen en invorderen van gemeentelijke- en waterschapbelastingen en het uitvoeren van de Wet Waardering Onroerende Zaken (Wet WOZ). Er is een gemeenschappelijke regeling in het leven geroepen waarin de GBLT als zijnde een openbaar lichaam, de uitvoering van deze taken overgedragen heeft gekregen.

GBLT is verplicht haar taken uit te voeren en daarbij persoonsgegevens te verwerken op basis van enkele wetten zoals de Algemene wet inzake rijksbelastingen, Invorderingswet 1990, Gemeentewet, Waterschapswet en de geldende belastingverordeningen van de deelnemende gemeenten en waterschappen. Voor het vaststellen van de WOZ-waarde verwerkt GBLT persoonsgegevens op basis van de Wet WOZ.

Het uitvoeren van de bovenvermelde wetten is een wettelijke plicht. Dat betekent dat voor het opleggen van de juiste belastingaanslag, het invorderen van de belasting en voor de juiste vaststelling en verstrekking van de waarde van onroerende zaken, GBLT persoonsgegevens moet gebruiken.
Hiernaast zijn ook nog andere verplichtingen van toepassing. Denk bijvoorbeeld aan de (fiscale)geheimhoudingsplicht uit de Algemene wet inzake Rijksbelastingen en Invorderingswet 1990, maar ook aan de beperkte openbaarmakingsregeling in de Wet WOZ. Tevens heeft de GBLT bij de uitoefening van haar taken zich te houden aan:

- De wet Basisregistratie Personen;
- De wet Algemene Bepalingen Burgerservicenummer;

Tenslotte heeft GBLT zich te houden aan de Baseline Informatiebeveiliging Overheid (BIO).

2.3 Categorieen betrokkenen, persoonsgegevens, grondslagen, doeleinden

Voor het uitoefenen van de hierboven beschreven wettelijke taken worden door de GBLT persoonsgegevens verwerkt. Deze gegevens worden in onderstaande tabel weergegeven. Voor een volledig overzicht van verwerkingen van persoonsgegevens wordt verwezen naar het verwerkingsregister van GBLT. Dit is op te vragen bij de Privacy Officer.

CATEGORIE BETROKKENEN	PERSOONSGEGEVENS
Belastingplichtigen	Voor- en achternaam, adres en woonplaats, geboortedatum en geslacht, Burgerservicenummer (BSN), IBAN (bankrekeningnummer), kadastraal nummer, waterverbruik, soort eigendomsrechten, burgerlijke staat, contactgegevens erven (bij overlijden van belastingplichtige of -schuldige)

	In voorkomend geval wordt ook het e-mailadres en telefoonnummer van een belastingplichtige verwerkt. Gegevens uit de BRP worden verwerkt op basis van het Autorisatiebesluit. Deze gegevens zijn terug te lezen op: https://zoek.officielebekendmakingen.nl/stcrt-2022-22889.html
Medewerkers	Voor- en achternaam, adres en woonplaats, Burgerservicenummer (BSN), geslacht, geboortedatum,, IBAN (bankrekeningnummer), telefoonnummer en e-mailadres, functie Ingeval partner zijn/haar gegevens, indien er een partnerpensioen is, Een verklaring omtrent het gedrag De ambtseed of gelofte Kopie van CV, diploma's, getuigschriften Kenteken van auto (ingeval gebruik wordt gemaakt van parkeerplaats van GBLT) Verzuim en verlofgegevens Loggegevens en inloggegevens ID medewerker Huidige, geplande activiteit Huidige status, status verleden Skills (wat kan een medewerker) Afhandeltijd, gemiddelde afhandeltijd per gesprek Voicelogging

VERWERKINGSDOELEINDEN	WETTELIJKE GRONDSLAG
Het heffen van belastingen	Wettelijke verplichting, art. 6 lid 1 sub c AVG
Het invorderen van belastingschulden	Wettelijke verplichting, art. 6 lid 1 sub c AVG
Het uitvoeren van de Wet WOZ	Wettelijke verplichting, art. 6 lid 1 sub c AVG
Het verwerken van persoonsgegevens als werkgever	Wettelijke verplichting, art. 6 lid 1 sub c AVG Gerechtvaardigd belang: artikel 6 lid 1 sub f AVG

2.4 Toepassing AVG-beginselen

Tijdens de uitoefening van haar taken hanteert GBLT de beginselen inzake de verwerking van persoonsgegevens zoals aangegeven in de AVG. Dit zijn de volgende beginselen:[1]

1. **Rechtmatigheid, behoorlijkheid, transparantie**
   Persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. GBLT zorgt er voor dat haar verwerkingen uitsluitend plaatsvinden indien dit lijn is met dit beginsel.
2. **Grondslag en doelbinding**
   GBLT zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtmatige grondslag verwerkt. Voor elke verwerking van persoonsgegevens die plaatsvindt bestaat een wettelijke grondslag en een vooraf bepaald specifiek doel.
3. **Dataminimalisatie**
   GBLT verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. GBLT streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt. Medewerkers kiezen te allen tijde voor de minst ingrijpende manier op de privacy van betrokkenen om een bepaald doel te bereiken.
4. **Juistheid**
   GBLT zorgt ervoor dat de persoonsgegevens die het verwerkt juist zijn en zo nodig worden geactualiseerd. GBLT neemt alle redelijke maatregelen om de persoonsgegevens die onjuist zijn, gelet op het doel waarvoor zij worden verwerkt, onverwijld te wissen of te (laten) rectificeren.
5. **Bewaartermijn**
   Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de taken goed uit te kunnen voeren of om wettelijke verplichtingen te kunnen naleven. Medewerkers volgen de Archiefwet en de vastgestelde bewaartermijnen voor persoonsgegevens binnen hun afdeling, als er geen vastgestelde termijn is wordt deze opgesteld in lijn met het doel van de verwerking.

1) Art. 5 AVG.

6. **Integriteit en vertrouwelijkheid**
GBLT 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 worden verzameld. Daarbij zorgt GBLT voor passende beveiliging van persoonsgegevens.
Persoonsgegevens worden alleen gedeeld met collega's die vanuit hun functie direct betrokken zijn. Bij een uitwisseling van persoonsgegevens vindt er een belangenafweging plaats omtrent het juiste gebruik van persoonsgegevens.

3 Ambitie

GBLT is een transparante, vooruitstrevende en innovatieve organisatie. Binnen de organisatie wordt veel gewerkt met vertrouwelijke informatie zoals persoonsgegevens van burgers en medewerkers en gevoelige financiële gegevens van burgers en bedrijven. Dat stelt hoge eisen aan medewerkers als het gaat om betrouwbaarheid en integriteit en daarmee dus de zorgvuldige omgang met bedrijfs- en persoonsgegevens. Hiervoor neemt GBLT conform AVG passende technische- en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Bescherming van persoonsgegevens en bedrijfsinformatie is essentieel voor de goede dienstverlening.

3.1 Context verwerking persoonsgegevens.

Voor het voldoen aan de AVG dient GBLT rekening te houden met de aard, de omvang, de context en het doel van de verwerking (artikel 24 AVG). GBLT treedt op als verwerkingsverantwoordelijke en voor verwerkingen van persoonsgegevens betekent dit het volgende:

- het verwerken van persoonsgegevens van natuurlijke personen en ondernemingen (bijvoorbeeld eenmanszaken, vennoten onder firma of maatschappen) in het kader van het heffen en invorderen van gemeentelijke- en waterschap belastingen en het uitvoeren van de Wet WOZ.
- Het verwerken van persoonsgegevens van medewerkers die in dienst of in opdracht van GBLT werkzaam zijn.
- het verwerken van persoonsgegevens heeft een omvang van grote schaal (verzorgingsgebied van 7 gemeenten en 5 waterschappen).
- De context van de organisatie is een overheidsorgaan.

3.2 Ambitieniveau

Op basis van de aard, omvang en risico van verwerking van persoonsgegevens en de ambitie aantoonbaar te voldoen aan de AVG heeft GBLT haar ambitie geformuleerd. In het kader van verwerken van persoonsgegevens en benodigd volwassenheidsniveau ambieert zij het ''voorspelbaar"niveau. Het ''voorspelbaar" niveau omvat de volgende kenmerken;

- De procedures en de processen worden door middel van controles periodiek beoordeeld om na te gaan of deze effectief zijn.
- Het Privacybeleid wordt periodiek herzien om na te gaan of het nog aansluit bij GBLT en de geldende wet- en regelgeving.
- Het informatiebeveiligingsbeleid- en plan wordt minimaal jaarlijks herzien waarbij wordt gekeken of de genomen maatregelen met de stand van techniek, de veranderingen in de organisatie, maatschappij en wet- en regelgeving voldoen.
- Het recht van audit wordt benut om na te gaan of de (sub-)verwerkers zich houden aan de afspraken die in de verwerkersovereenkomsten zijn vastgelegd.
- Het verwerkingsregister wordt minimaal jaarlijks geactualiseerd om een actueel beeld te geven van te verwerken persoonsgegevens. Verwerkingen die niet meer aan de orde zijn worden uit het register verwijderd en nieuwe verwerkingen worden toegevoegd.
- De wettelijke bewaartermijnen worden toegepast en bewaakt.
- Datalekken worden bijgehouden, gerapporteerd en gemonitord.
- Cursussen en trainingen voor medewerkers worden minimaal jaarlijks herhaald.

Nadere uitwerking van volwassenheidsniveau ''voorspelbaar" in wat het betekent ten aanzien van de "monitoring, de onderbouwing, de mensen en de inrichting en structuur".

Scope bepalen	Geïntegreerd	Privacy is onderdeel van verwerken van persoonsgegevens (in ieder relevant proces).
Monitoring	Planning en control	PDCA gestructureerd aanwezig, bijvoorbeeld in jaarplannen.

	Directieteam (Strategisch)	Nieuwe ontwikkelingen op het gebied van de privacywet- en regelgeving worden gesignaleerd en verwerkt in de strategische planning van de organisatie.
	Management (Tactisch)	Het beleid voor privacy en informatiebeveiliging is geoperationaliseerd naar methodes voor afgewogen keuzes (risico management en kosten/basten voor personen (betrokkenen) en daarna gerealiseerd in maatregelen.
	Afdelingen (Operationeel)	Het beleid voor privacy en de classificatie van persoonsgegevens wordt periodiek geëvalueerd op de uitvoering in de praktijk. De gerealiseerde maatregelen worden geëvalueerd en bijgesteld.
Aantoonbaarheid	Proceseigenaar is zelf aan zet	Actieve intervisie op best practices, aantoonbare sturing op het AVG, zelf evaluatie, zoekt de FG zelf op voor advies.
	FG houdt toezicht op het beleid	Interne en externe audits, DPIA beoordelen, contact met de Autoriteit Persoonsgegevens.
	Vastgestelde processen en documentatie	Processen zijn vastgesteld en worden geëvalueerd. Risicoanalyse en regelmatige review. Kwaliteit van resultaten is gedefinieerd (KPI's). Proceseigenaren voeren zelf de administratie (Register van verwerkingen) en beheren hun verwerkingsovereenkomsten.
	Kwaliteitsverbetering	Proactieve monitoring op het detecteren van incidenten vindt plaats in het verwerkende proces. Centrale analyse van incidenten en problemen leiden tot verbetering van communicatie.
Mensen	Onbewust en aantoonbaar voldoen aan privacy	Leidinggevenden geven voorbeeldgedrag en verbinden consequenties aan ongewenst gedrag.
		Medewerkers en leiding committeren zich (expliciet) aan het leveren van een bijdrage aan goede informatiebeveiliging en het borgen van privacy.
	Continuïteit in leren	Mensen delen onderling actief kennis, 'best practises' en ervaringen over de omgang met privacy en informatiebeveiliging. Meerjarig opleidingsplan.
Inrichting en structuur	AVG beginsel zijn aanwezig (werking)	De AVG beginselen worden altijd gebruikt, administraties zijn inhoudelijk meestal op orde.

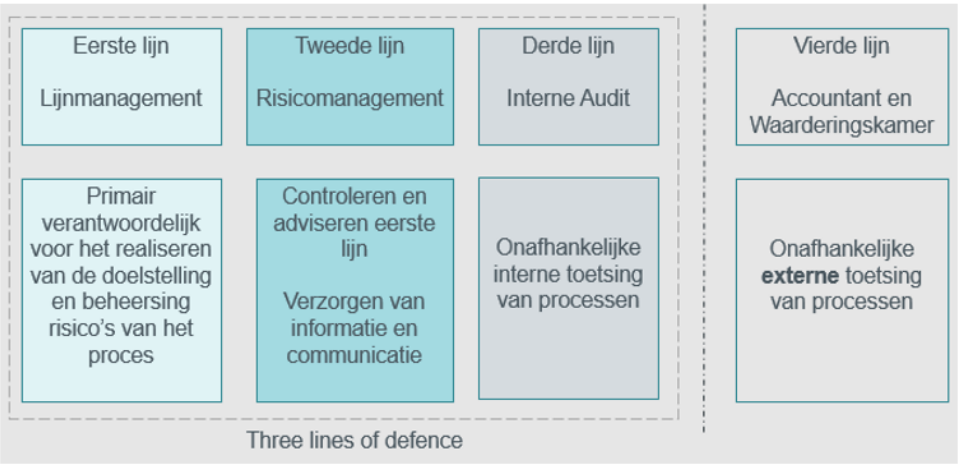
4 Governance

De wijze van verankering van het privacybeleid binnen GBLT vormt als het ware het fundament van de borging van dit belangrijke thema. Op grond van de AVG is het hoogst leidinggevende niveau in de organisatie eindverantwoordelijk voor de rechtmatige en verantwoorde verwerking van persoonsgegevens. Dat is in het geval van GBLT het Dagelijks Bestuur. Daarnaast draagt elke medewerker in de organisatie, die te maken heeft met verwerkingen van persoonsgegevens, zorg voor de verantwoorde en zorgvuldige omgang met deze gegevens. Ook de proceseigenaren hebben een taak hierin. In dit onderdeel van het privacybeleid wordt de wijze waarop de taken, verantwoordelijkheden en de borging van het beleid binnen GBLT zijn georganiseerd en belegd uitgewerkt.

4.1 Governance met behulp van three lines of defence

Governance model

Voor het bepalen van de taken, verantwoordelijkheden en bevoegdheden met betrekking tot risicomanagement wordt binnen GBLT het "three lines of defence" model (3LoD model) gevolgd.



Dagelijks bestuur GBLT
Het dagelijks bestuur draagt de eindverantwoordelijkheid voor informatiebeveiliging en bescherming van persoonsgegevens. Het dagelijks bestuur stelt het Privacybeleid vast en zet hiermee de gekozen richting ter bescherming van persoonsgegevens uit. Het dagelijks bestuur is eindverantwoordelijk voor het toezicht houden en het handhaven van de "three lines of defence".

De verantwoordelijkheden van het dagelijks bestuur bestaan uit:
- Het toewijzen van de verantwoordelijkheden ten aanzien van het inrichten, uitvoeren en documenteren van het privacybeleid.
- Het vaststellen van het privacybeleid.
- De criteria vast te stellen voor de aanvaarding van risico's en privacy ambitie niveau.
- Het kunnen leveren van bewijs van hun betrokkenheid met betrekking tot het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van beschermen van persoonsgegevens.
- Het dagelijks bestuur wordt over de bescherming van persoonsgegevens periodiek geïnformeerd.

Directeur
De directeur geeft dagelijks leiding aan de organisatie van GBLT. Hij is ook secretaris van het algemeen bestuur en het dagelijks bestuur. Afdelingsmanagers/Proceseigenaren rapporteren aan de directeur over hun verantwoordelijkheden in de 1e lijn.

Chief Information Security Officer (CISO)
De CISO is gedelegeerd verantwoordelijk namens dagelijks bestuur voor het implementeren van informatiebeveiligingsbeleid én het toezicht daarop. Hij geeft namens het dagelijks bestuur op dagelijkse basis invulling aan de sturende rol door besluitvorming voor te bereiden en toe te zien op de uitvoering. Tot zijn taken behoren:
- Het implementeren van informatiebeveiligingsbeleid én het toezicht daarop. Het opstellen en uitvoeren van informatiebeveiligingsplan.
- Aandacht besteden binnen de organisatie aan bewustwording met betrekking tot informatiebeveiliging.
- Het borgen van informatiebeveiliging met behulp van het Information Security Management System (ISMS).
- Op verschillende niveaus deelnemen aan overleggen voor signalerend en corrigerend vermogen.
- Periodiek rapporteren aan het dagelijks bestuur en het MT.

1e lijn: Afdelingen, afdelingsmanagers/proceseigenaren
Uitgangspunt van het 3LoD model is dat het lijnmanagement verantwoordelijk is voor hun eigen processen. Om de doelstellingen te realiseren en risico's te minimaliseren zijn beheersmaatregelen opgesteld en vinden allerlei controles plaats. Niet het controleren om het controleren, maar controleren om vast te stellen dat de goede dingen worden gedaan en de doelstellingen niet in gevaar komen.
Verantwoordelijkheden van de eerste lijn zijn dan ook:
- Het toepassen en opvolgen van het privacybeleid GBLT.
- Het onderhouden en opvolgen van het register van verwerkingsactiviteiten.
- Het signaleren en melden van beveiligingsincidenten.

- Indien van toepassing opstellen en onderhouden van DPIA, instellen en monitoren van beheermaatregelen.
- Het controleren en monitoren op de effectiviteit op processen waarbij persoonsgegevens worden verwerkt.
- Bij ontwikkelen van systemen en processen toepassen van privacy by design en default.
- Het toepassen van het informatiebeveiligingsbeleid en opvolgen met behulp van technische- en organisatorische maatregelen.

Afdelingsmanager/Proceseigenaar
De proceseigenaar is gedelegeerd integraal verantwoordelijk voor processen waar persoonsgegevens worden verwerkt. Inclusief de daarbij benodigde beheermaatregelen zoals register van verwerkingen, DPIA en verwerkingsovereenkomst met opdrachtgevers en leveranciers.

Medewerker van GBLT

Een 1e lijn/operationeel medewerker draagt bij aan verwerkingen van persoonsgegevens conform AVG. Voor de medewerker van GBLT schept het privacybeleid zekerheid over de manier waarop hij/zij invulling moet geven aan het privacybelang van de betrokkenen. Hierdoor worden persoonsgegevens één keer goed verwerkt en loopt GBLT minder risico op reputatieschade.

2e lijn: Ondersteuning Controle en Adviseren

Daarnaast is er een functie die de 1e lijn ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt, dit is vanuit Privacy met name de PO. Ook het verzorgen van integrale managementinformatie omtrent risico's en daarover rapporteren is een taak van de 2e lijn.

De 2e lijn omvat de volgende activiteiten;
- Identificeren van risico's bij het verwerken van persoonsgegevens.
- Periodiek het privacybeleid actualiseren op basis van de herijking van de vastgestelde risicobereidheid.
- Het faciliteren van het proces van risicomanagement in de vorm van sessies, formats, tooling.
- Doelgerichte communicatie over risico's organiseren/faciliteren, zowel binnen als buiten de reguliere risico overlegstructuur.
- Het proactief verbetervoorstellen aandragen bij de 1e lijn.
- Een actieve bijdrage leveren aan het formuleren van voorstellen voor behandeling van risico's en het formuleren van beheermaatregelen welke ter goedkeuring worden voorgelegd aan het managementteam.
- Advisering en monitoring van verbeteracties (bevindingen o.b.v. beoordeling beheersmaatregelen).
- Monitoring van de eerste lijn op naleving van wet- en regelgeving ter bescherming van persoonsgegevens.
- Ondersteuning in de opzet en werking ter bescherming van persoonsgegevens.

Privacy Officer (PO);

De PO ondersteunt, controleert en adviseert de 1e lijn.

De taken die tot de Privacy Officer behoren zijn:
- Beheren register van verwerkingsactiviteiten.
- Opstellen van model verwerkingsovereenkomst/-afspraken.
- Coachen op toepassen en sluiten van verwerkersovereenkomsten/afspraken met derde partijen wanneer deze in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.
- Opstellen en onderhouden van het privacybeleid en voorleggen ter vaststelling.
- Opstellen privacyverklaring voor betrokkenen.
- Het analyseren van (potentiële) datelekken en zo nodig melden bij Autoriteit Persoonsgegevens en betrokkene(n).
- Coachen op werkinstructies conform aanverwante wet- en regelgeving en GBLT beleid.
- Sturen op integreren privacy in de werkprocessen en de procesbeschrijvingen.
- Opstellen procedures uitoefening rechten van de betrokkenen.
- Ondersteuning 1e lijn bij procesinrichting en werkinstructies.
- Contactpunt binnen de organisatie voor privacyvraagstukken.
- Behandelen verzoeken van betrokkenen ten aanzien van de uitoefening van hun rechten.
- Uitvoeren of sturen op de uitvoering van de DPIA's.
- Periodiek overleg met de FG en de CISO.

Security Officer (SO)

- Het onderhouden van de beleids- en kaderdocumenten op het gebied informatiebeveiliging van GBLT.
- Het uitvoeren van de informatiebeveiligingsafspraken van de CISO.
- Het maken van risico-analyses op het gebied van informatiebeveiliging
- Het opstellen van security-ontdekkende systemen.
- Het opstellen van minimum veiligheidseisen en het digitaal rechercheren.

Adviesgroep Beveiliging, Continuïteit en Privacy (ABC&P)
Het ABC&P is een interne adviesgroep op het vlak van Informatiebeveiliging, Archiefbeheer en Privacy. Vanuit elk van de disciplines zijn één of meerdere medewerkers die hieraan deelnemen. De adviesgroep heeft een periodiek overleg waarbij voor hen relevante onderworpen worden besproken en beleidstukken kunnen worden vastgesteld. Bijvoorbeeld jaarplannen of relevant beleid. De adviesgroep heeft een sturende, adviserende functie zowel richting management als richting medewerkers.

Recordmanager
Naast de privacy gerelateerde functies zoals Privacy Officer en Security Officer is er de functie van Recordmanager. De recordmanager houdt zich voornamelijk bezig met werkzaamheden op het gebied van de duurzame toegankelijkheid van digitale archiefinformatie en het bewaken van de wettelijke bewaartermijnen.

3e lijn: Interne Audit en Toezicht

De 3e lijn betreft zowel interne audit als de toezichthoudende rol. Vanuit de gesignaleerde risico's door de Privacy Officer worden de meest risicovolle processen geaudit. Daarnaast heeft GBLT een FG aangesteld voor een onafhankelijke audit op het voldoen aan de AVG. Jaarlijks beoordeelt de FG de mate waarin in opzet en werking voldaan wordt aan de relevante normenkaders van de AVG in relatie tot de verwerkingen van persoonsgegevens door GBLT.

Functionaris voor Gegevensbescherming[2] (FG)
De FG is verantwoordelijk voor onafhankelijk toezicht op naleving van relevante wet- en regelgeving, waaronder de AVG, inzake de bescherming van persoonsgegevens en informatiebeveiliging.

1. De taken van de Functionaris voor Gegevensbescherming.
   a. De verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van de AVG en andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen.
   b. Toezien op naleving van de AVG en van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits.
   c. Desgevraagd advies verstrekken met betrekking tot DPIA's en toezien op de uitvoering daarvan in overeenstemming met artikel 35 AVG.
   d. Met de toezichthoudende Autoriteit Persoonsgegevens samenwerken.
   e. Optreden als contactpunt voor de toezichthoudende autoriteit inzake aangelegenheden die verband houden met verwerking , met inbegrip van in artikel 36 AVG bedoelde voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid.

2. De Functionaris voor Gegevensbescherming houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

5 Plichten om aantoonbaar te voldoen

Overeenkomstig de AVG zal de verwerking van persoonsgegevens verantwoord moeten geschieden. GBLT moet aantoonbaar verantwoord met persoonsgegevens omgaan. Dit wordt ook wel de verantwoordingsplicht genoemd. Hieronder wordt dit toegelicht.

5.1 Register van verwerkingsactiviteiten (artikel 30 AVG)
Het register van verwerkingsactiviteiten is een opsomming van de verwerkingen van persoonsgegevens binnen GBLT. De organisatie dient dit register jaarlijks actueel bij te houden.

Het register van verwerkingen heeft meerdere doelen, zoals:

2) **Artikel 37, 38 en 39 AVG**

- Wat gebeurt er met persoonsgegevens binnen de organisatie?
- Zijn alle verwerkingen van persoonsgegevens legitiem (doelbinding)?
- Een inzicht te verschaffen van verwerkingen aan verwerkingsverantwoordelijke, betrokkene en/of toezichthouder.
- Inzicht te hebben van wie men persoonsgegevens ontvangt en aan wie deze worden verstrekt.
- Inzicht te verschaffen in welke databases / systemen / processen hoog risico verwerkingen plaatsvinden.
- Welke (bijzondere) persoonsgegevens van betrokkene zijn in scope in geval van een beveiligingsincident en/of datalek?

In het register van verwerkingen worden minimaal de volgende onderdelen van verwerkingen vastgelegd:
- Naam gegevensverwerking (bijv. proces)
- Verwerkingsverantwoordelijke
- Doel van de verwerking, artikel 5.1.b
- Wettelijke grondslag, artikel 6
- Categorie van betrokkene (burger, zakelijke relatie of medewerker)
- Categorie van persoonsgegevens (bijv. naam, adres, emailadres)
- Bron van de persoonsgegevens
- Ontvangers van persoonsgegevens
- Bewaartermijn
- Verwerker
- Systemen/applicaties waarin persoonsgegevens worden verwerkt
- Locatie van verwerkingen (Nederland, EU of buiten EER)

Jaarlijkse review Register van verwerkingsactiviteiten
GBLT treedt op als verwerkingsverantwoordelijke bij hun wettelijke taken. Ook is GBLT verwerkingsverantwoordelijke als werkgever. Voor deze verwerkingen van persoonsgegevens binnen de organisatie wordt een register van verwerkingsactiviteiten onderhouden. Per team is de proceseigenaar rolverantwoordelijk, gegevensbeheerder, om het register actueel te houden en minimaal eenmaal per jaar te reviewen. Voor begeleiding in deze taak kan de rolverantwoordelijke (proceseigenaar of gegevensbeheerder) een beroep doen op de PO en FG.

5.2 Verwerkersovereenkomsten
In het geval dat GBLT verwerkers (leveranciers) inschakelt voor het verwerken van persoonsgegevens dient zij hiermee een verwerkersovereenkomst af te sluiten.

In de verwerkersovereenkomst worden tenminste de volgende zaken vermeld:
- Het onderwerp en de duur van de verwerking.
- De aard en het doel van de verwerking.
- Het soort persoonsgegevens en de categorieën van betrokkenen.
- De rechten en verplichtingen van de verwerkingsverantwoordelijke.

5.3 Privacyverklaring (art. 13)
Betrokkenen hebben het recht door de verwerkingsverantwoordelijke te worden geïnformeerd over de verwerkingen van persoonsgegevens. Deze doet dit met behulp van een privacyverklaring.

De organisatie onderscheidt de volgende categorieën betrokkenen;

a) Natuurlijke personen (niet zijnde werknemers van of voor GBLT)
Natuurlijke personen waarvan GBLT persoonsgegevens verwerkt conform de AVG. Op de website van GBLT kunnen burgers informatie vinden over de verwerking van persoonsgegevens in de externe privacy verklaring. Bij vragen kan de burger terecht bij het Klant Contactcentrum of deze direct stellen aan de Functionaris voor Gegevensbescherming van GBLT. De privacyverklaring wordt minimaal éénmaal per jaar gereviewed.

b) Medewerkers van GBLT
De organisatie treedt op als verwerkingsverantwoordelijke bij alle medewerkers waarvan persoonsgegevens worden verwerkt, ongeacht de vorm van dienstverband. Dit geldt ook voor personen die krachtens opdracht, of een andere overeenkomst, voor GBLT werken. Op het intranet is de privacyverklaring voor medewerkers te raadplegen. Bij vragen kan de medewerker terecht bij zijn leidinggevende, HR of de Functionaris Gegevensbescherming. De privacyverklaring wordt minimaal éénmaal per jaar gereviewed.

In de privacyverklaring wordt minimaal de volgende informatie verstrekt aan betrokkene:

- De contactgegevens van de organisatie.
- De contactgegevens van de Functionaris Gegevensbescherming.
- De doelen waarvoor persoonsgegevens worden verwerkt.
- De grondslag(en) waarop verwerkingen zijn gebaseerd:
  - In geval van toestemming, dat betrokkene toestemming altijd weer kan intrekken.
  - In geval van gerechtvaardigd belang, motivatie van het belang.

- De eventuele ontvangers of categorieën ontvangers van persoonsgegevens.
- In geval van verstrekking aan derde landen, buiten EER, de passende waarborgen.
- De gehanteerde bewaartermijn of uitleg keuze bewaartermijnen.
- De rechten van betrokkene.
- Dat betrokkene het recht heeft een klacht in te dienen over de verwerking(en) bij de Autoriteit Persoonsgegevens.

Verder moet alle andere informatie worden verstrekt die noodzakelijk is om tegenover betrokkene een behoorlijke en transparante verwerking te waarborgen.

5.4 DPIA[3] Beheer (artikel 35 AVG)

In geval van verwerking van persoonsgegevens waarbij sprake is van hoge risico's is een DPIA volgens de AVG verplicht. Het doel van de DPIA is vooraf de risico's te inventariseren voor de persoonsgegevensverwerking en daar vooraf beheermaatregelen voor te treffen. De proceseigenaar is verantwoordelijk voor het opstellen van een DPIA op een proces.
In de AVG spreekt men van de volgende hoog risico verwerkingen:

- Worden in het proces de rechten en vrijheden van betrokkene beoordeeld in geval van profilering van individuele gedrag (voor evaluatie of scoring)?
- Worden in het proces de betrokkene systematisch gemonitord?
- Vindt er in het proces geautomatiseerde besluitvorming plaats?
- Worden in het proces op grote schaal persoonsgegevens verwerkt?
- Worden in het proces gegevens van verschillende applicaties gecombineerd verwerkt?

Heeft uw verwerking betrekking op gegevens over kwetsbare betrokkenen?
Worden er in het proces innovatieve verwerkingen toegepast op persoonsgegevens?
Is er sprake van gegevensverwerking(en) die tot gevolg hebben dat betrokkenen een recht niet kunnen uitoefenen of een dienst niet kunnen gebruiken of een contract niet kunnen afsluiten?

Voor de uitvoering van een DPIA heeft GBLT een vast format en een beslisboom DPIA om te bepalen of een DPIA noodzakelijk is.

Advies FG
Als de DPIA is uitgevoerd wint de eigenaar van de DPIA een advies in van de FG. De FG zal de aanwezigheid van hoog risico verwerkingen en bijbehorende beheermaatregelen beoordelen ter bescherming van de rechten en vrijheden van betrokkene.

Monitoring van de beheermaatregelen
De proceseigenaar is verantwoordelijke voor de DPIA en monitort minimaal per jaar de opvolging en effectiviteit van de genomen beheermaatregelen in de DPIA.

Periodieke review DPIA
Als een DPIA is opgesteld, vindt er minimaal binnen 3 jaar vanaf datum vaststelling een review plaats. Doel is vast te stellen of er wijzigingen hebben plaatsgevonden in de verwerking van persoonsgegevens en de genomen beheermaatregelen effectief zijn.

5.5 Bewaarbeleid (artikel 5.1.e)

De AVG schrijft voor dat persoonsgegevens niet langer worden bewaard dan noodzakelijk. Elke gekozen bewaartermijn is mogelijk mits de termijn van noodzakelijkheid voldoende wordt gemotiveerd.

De Archiefwet en de daar mee in verband staande wet- en regelgeving geldt als normkader voor de door Minister van Onderwijs, Cultuur en Wetenschap goedgekeurde selectielijst met de daar in beschreven bewaartermijnen. De bewaartermijn wordt vastgelegd in de het verwerkingsregister. Vervolgens zal de (proces)eigenaar verantwoordelijkheid nemen dat na afloop van de bewaartermijn persoonsgegevens worden verwijderd.

3) **Data Protection Impact Assessment**

GBLT streeft er naar dat bewaartermijnen automatisch worden gemonitord. Doch in veel gevallen zal dat niet altijd mogelijk zijn en dient de (proces)eigenaar over het beheer van persoonsgegevens beheermaatregelen in te stellen zodat periodiek de overschrijding van bewaardata wordt gecheckt en persoonsgegevens handmatig worden verwijderd door een verantwoordelijk medewerker. De (proces)eigenaar van persoonsgegevens geeft indien van toepassing autorisatie voor het verwijderen van (persoons)gegevens in het archief.

Geautomatiseerd bijhouden van bewaartermijnen
In de software van applicaties is ingebouwd dat bewaartermijnen automatisch bijgehouden worden. De software biedt de mogelijkheid een vernietigingslijst aan te maken en informatie te vernietigen wanneer het termijn verstreken is.

Handmatige verwijdering
Elke medewerker is verantwoordelijk om periodiek conform afgesproken bewaartermijnen persoonsgegevens handmatig te verwijderen. Er dient dan gecontroleerd te worden of in de digitale afvalbak of verwijderde items (Outlook) de persoonsgegevens ook zijn verwijderd. De proceseigenaren zijn eindverantwoordelijk en zien er op toe dat persoonsgegevens daadwerkelijk worden verwijderd. Hierbij dient ook rekening te worden gehouden met logging en backups. Afdeling I&A neemt de verantwoordelijkheid persoonsgegevens met betrekking tot logging en back-ups periodiek conform afgesproken termijn te verwijderen. Nadat persoonsgegevens op de bron locatie zijn verwijderd, zullen de persoonsgegevens nog tijdelijk op back-up media blijven bestaan conform de afgesproken bewaartermijnen. Daarna worden ook de persoonsgegevens op back-up media ook vernietigd.

Monitoring
Periodiek worden bewaartermijnen en beleid gemonitord om met behulp van een analyse te onderzoeken of er andere oorzaken ten grondslag liggen aan het niet opvolgen van vastgelegde bewaartermijnen. Met behulp van deze analyse vindt er dan bijsturing plaats op de gevonden oorzaken om toekomstige overschrijdingen van bewaartermijnen of verstoringen in processen te voorkomen.
Voor de exacte bewaartermijnen van persoonsgegevens:
Raadpleeg het register van verwerkingsactiviteiten.

5.6 Datalekken Beheer (artikel 33)
Er is een interne procedure ingericht voor het melden van datalekken en beveiligingsincidenten. Een ieder die werkzaam is voor GBLT kan via deze procedure op een laagdrempelige manier elk (vermoeden van een) datalek of beveiligingsincident melden. De beoordeling of er daadwerkelijk sprake is van een datalek of beveiligingsincident ligt bij de Privacy Officer en/of de Security Officer.

De Privacy Officer houdt een register van datalekken bij.

De proceseigenaar is verantwoordelijk het herstellen van de gevolgen van een datalek of beveiligingsincident en het beoordelen of er maatregelen noodzakelijk zijn om toekomstige datalekken te voorkomen. De proceseigenaar legt dit vast in het register van datalekken.

De Privacy Officer rapporteert jaarlijks over de gemelde datalekken en beveiligingsincidenten.

5.7 Rechten van betrokkene (artikel 12 – 23 AVG)
Om een rechtmatige verwerking van persoonsgegevens te waarborgen geeft de AVG diverse rechten aan de betrokkene. De betrokkene kan deze rechten uitoefenen tegen de organisatie als deze optreedt als verwerkingsverantwoordelijke.

Overzicht rechten van betrokkene

- Recht op inzage en rectificatie:
  Betrokkene heeft het recht om na te vragen of en welke persoonsgegevens wij van de betrokkene verwerken. Indien de betrokkene van mening is dat gegevens onjuist of onvolledig zijn, kan hij een verzoek indienen om deze gegevens te wijzigen of aan te vullen.
- Recht op vergetelheid:
  Betrokkene kan bij de verwerkingsverantwoordelijke een verzoek indienen om zijn gegevens te wissen. Bijvoorbeeld als hij bezwaar heeft tegen de verwerking van zijn gegevens. Het belang van de betrokkene moet dan boven het belang van de verwerkingsverantwoordelijke gaan om de persoonsgegevens te verwerken.
- Recht op beperking:
  De betrokkene heeft het recht van de verwerkingsverantwoordelijke de beperking van de verwerking te verkrijgen indien een van de volgende elementen van toepassing is:

De juistheid van de persoonsgegevens wordt betwist door de betrokkene, gedurende een periode die de organisatie in staat stelt de juistheid van de persoonsgegevens te controleren;
De verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens.

- Recht op dataportabiliteit:
  Betrokkene heeft het recht om gegevens die hij in het kader van een overeenkomst met GBLT of met zijn toestemming heeft verstrekt in een gestructureerde en leesbare vorm te verkrijgen. Betrokkene kan verzoeken om deze gegevens rechtstreeks over te dragen aan een derde partij. Dit laatste is alleen mogelijk indien dit ook technisch mogelijk is.
  Recht van bezwaar (recht op verzet):
  Betrokkene heeft het recht om bewaar te maken tegen de verwerking van zijn persoonsgegevens die op basis van het gerechtvaardigd belang worden verwerkt (artikel 6 lid 1 sub f AVG). Hij kan bezwaar maken vanwege specifieke omstandigheden. Op basis van deze omstandigheden zal de verwerking opnieuw door GBLT beoordeeld moeten worden.
- Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming:
  De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.

In de privacyverklaring op de website van de GBLT is opgenomen hoe betrokkene beroep kan doen op zijn of haar rechten. Indien de organisatie de verantwoordelijke is voor de verwerking van de persoonsgegevens, kan betrokkene een e-mail sturen naar de Functionaris voor de Gegevensbescherming privacy@gblt.nl. De FG en/of Privacy Officer zal binnen een maand na ontvangst van het verzoek de betrokkene informeren over de uitvoering van het verzoek. Ook wanneer er geen gehoor wordt gegeven aan het verzoek van de betrokkene moet dit binnen een maand kenbaar gemaakt worden. Een weigering moet worden gemotiveerd. Tenslotte moet de betrokkene informatie krijgen over het klachtrecht bij de toezichthouder.

Privacy klachten
Elke uiting van onvrede betreffende de verwerking van persoonsgegevens is een klacht. Een klacht kan door een betrokkende of een derde worden geuit, in het geval een derde de klacht indient is het relevant te controleren of deze derde gemachtigd is op te treden namens de betrokkene. De privacyklacht wordt geregistreerd conform de ‘instructie klachtenregistratie’. De afhandeling van een privacyklacht geschiedt altijd met behulp van de PO en/of FG

5.8 Beveiligingsmaatregelen (artikel 32 AVG)

De AVG schrijft voor om rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking beveiligingsmaatregelen te treffen. De verwerkingsverantwoordelijke treft technische en organisatorische maatregelen die passen bij de kans en ernst van uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen die aan de verwerking zijn verbonden. In geval men optreedt als verwerker treft men gelijke beveiligingsmaatregelen als verwerkingsverantwoordelijke.

GBLT heeft de onderstaande technische en organisatorische maatregelen getroffen op basis van de Baseline Informatiebeveiliging Overheid (BIO). Dit betreft het normenkader voor overheidsorganisaties op het gebied van informatiebeveiliging

- Technische maatregelen
  Een procedure op basis van (PDCA) Plan, Do, Check, Act voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.
- Organisatorische maatregelen
  - Information Security Management System GBLT (ISMS)
  - Informatiebeveiligingsbeleid GBLT (strategisch en tactisch)
  - Informatie & Advisering (incl. IT leveranciers)

- BIV classificaties op systemen, processen en diensten.
  Het vermogen om op permanente basis de vertrouwelijkheid, integriteit en beschikbaarheid van de verwerkingssystemen en diensten te garanderen.
- Business continuïteit management (BCM).
  Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen. Dit is beschreven in het Informatiebeveiligingsbeleid van GBLT.
- Strategisch informatiebeveiligingsbeleid
  Een beleid over kaders hoe GBLT de informatiebeveiliging vorm zal geven.

- Tactisch informatiebeveiligingsbeleid
  Invulling geven aan het strategisch informatiebeveiligingsbeleid.

Autorisatie van medewerkers
In het kader van bescherming van persoonsgegevens hebben medewerkers autorisaties om persoonsgegevens te raadplegen en/of te muteren. Vanuit een rollenmatrix worden autorisaties toegekend in processen voor de raadpleeg- en/of mutatiefunctie. Hierbij wordt vooraf beoordeeld of een functie beschikt over de juiste rollen en niet meer persoonsgegevens kan verwerken dan noodzakelijk. Er kan sprake zijn van een inbreuk/datalek als een medewerker ongeoorloofd persoonsgegevens kan raadplegen.

De proceseigenaar is eindverantwoordelijk om de rollen toe te kennen in processen en de noodzakelijkheid vooraf te beoordelen. De leidinggevende van een medewerker is verantwoordelijk om de medewerker bij indiensttreding op basis van zijn functie en taken de beschikking te geven over de juiste rollen.

5.9 Awareness op bescherming van persoonsgegevens (artikel 32.1.b)
Voor een effectieve werking van het privacybeleid is voldoende awareness van management en medewerkers van belang bij het verwerken en beschermen van persoonsgegevens. Dit is bepalend in de effectieve werking van technische- en organisatorische maatregelen. De effectiviteit van awareness wordt bepaald door de kennis van medewerkers op het gebied van beschermen van persoonsgegevens en hun handelen bij verwerkingen van persoonsgegevens.

Tijdens het arbeidsvoorwaardengesprek wordt het belang van integriteit en geheimhouding benadrukt en wordt aan medewerker gemeld dat hij/zij de eed/gelofte moet afleggen. De eed/gelofte wordt na indiensttreding afgelegd, waarbij de gedragscode wordt uitgereikt en besproken.

Geheimhoudingsverklaring
Als er sprake is van een externe medewerkers tekent hij/zij voor indiensttreding of het aangaan van de werkrelatie met GBLT een geheimhoudingsverklaring.

Awareness Privacy
Door middel van verplichte e-learning worden medewerkers geïnformeerd over de regelgeving en het privacybeleid binnen de organisatie.

Awareness Informatiebeveiliging
Door middel van verplichte e-learning worden medewerkers geïnformeerd over de regelgeving en het informatiebeveiligingsbeleid binnen de organisatie.

Vanuit de 2e lijn worden in samenwerking met de 1e lijn en HR periodiek in verschillende werkvormen awareness activiteiten georganiseerd ter bescherming van persoonsgegevens en kennis van het privacybeleid.