Commissie toezicht bescherming persoonsgegevens

Auditrapport
Clean desk en Clear screen Beleid
Openbaar Lichaam Bonaire
Februari 2023

CBP/TH2021/07

Commissie toezicht bescherming persoonsgegevens CBP BES

Inhoud

Samenvatting 3

1 Inleiding 4

1.1 Aanleiding 4

1.2 Doel van het rapport 4

1.3 Opzet van het rapport 4

2 Onderzoek 5

2.1 Inleiding 5

2.2 Controle ter plaatse 6

3. Normering 8

3.1 Wettelijke kaders 8

3.1 Doel van de kaders 9

3.2 Beleid OLB 9

4. Analyse en conclusie 11

4.1 Inleiding 11

4.2 Toetsing normering 11

4.3 Analyse Clean desk 13

4.4 Analyse Clear screen 16

4.5 Conclusie 16

4.5.1 Algemeen 16

4.5.2 Conclusie Clean desk 17

4.5.3 Conclusie clear screen 19

5. Aanbevelingen 22

5.1 Sturing 22

5.2 Clean desk en Clear screen 22

5.3 Controle 24

5.4 Terugkoppeling aanbeveling 24

Bijlagen 25

Samenvatting

De wet bescherming persoonsgegevens BES (Wbp BES) is van toepassing op Bonaire, Sint Eustatius en Saba. In het jaar 2020 is de Commissie Bescherming Persoonsgegevens BES (de commissie) begonnen met programmatisch toezicht om op grond van de Wbp BES normconform gedrag bij de verwerking van persoonsgegevens te bevorderen. In het voorjaar van 2022 heeft de commissie een controle ter plaatse gehouden op alle locaties van het Openbaar Lichaam Bonaire (OLB). Het doel van deze controle was om te toetsen in hoeverre het OLB het clean desk en clear screen beleid 'Op weg naar bewustwording informatieveiligheid' (hierna het beleid) geïmplementeerd heeft. De implementatie van het Clean desk en clear screen beleid was een expliciet verzoek van de commissie aan het OLB.

Conform artikel 13 van het Wbp BES dient het OLB als verantwoordelijke de door haar verwerkte persoonsgegevens zowel organisatorisch als technisch adequaat te beveiligen. Dit betekent onder meer dat geen documenten of bestanden met persoonsgegevens voor onbevoegden toegankelijk mogen zijn. Een clean desk en clear screen beleid is een goed begin om persoonsgegevens te beveiligen.

De commissie heeft bij het OLB geconstateerd dat niet alle directies binnen het ambtelijke apparaat bekend zijn met het beleid. Bij de directies die wel bekend zijn met het beleid is de implementatie niet of nauwelijks zichtbaar. Hierbij speelt de sturing vanuit het Bestuurscollege én de directeuren een belangrijke rol.

Het beleid van het OLB is een goed begin maar zonder integrale implementatie hiervan blijft het bij de goede intenties. Het beleid geeft handvatten om op een zorgvuldige wijze om te gaan met de aanwezige persoonsgegevens. Opgeruimde bureaus en werkplekken verkleint de kans op fraude en datalek.

De controle ter plaatse bij het OLB heeft de commissie inzicht gegeven over de fasering van de implementatie van het beleid binnen het ambtelijk apparaat.

De commissie concludeert dat het beleid (nog) niet is geïmplementeerd door het OLB met als gevolg dat het OLB (nog) niet voldoet aan de adequate organisatorische- en technische bescherming van de persoonsgegevens aangetroffen bij de diverse werkplekken.

De commissie geeft aanbevelingen met een prioritering en te ondernemen stappen. De commissie ziet graag dat de implementatie en de controle zowel verticaal als horizontaal wordt aangestuurd. Regelmatige controle door het managementteam van de verschillende directies en de eilandsecretaris moet zorgen voor de juiste en structurele naleving van normen opgenomen in de Wbp BES en het beleid.

De commissie drukt het OLB op het hart om een privacy functionaris aan te trekken die o.a. het proces van implementatie kan begeleiden binnen het ambtelijk apparaat.

1 Inleiding

1.1 Aanleiding

De Commissie toezicht bescherming persoonsgegevens voor Bonaire, Sint Eustatius en Saba (hierna commissie) heeft in het jaar 2020 haar actieprogramma voor 2020 uitgerold, waarbij los van adhoc toezicht ook programmatisch toezicht zou worden uitgevoerd.
De commissie is belast met het toezicht op de naleving van de Wet bescherming persoonsgegevens BES, hierna Wbp BES. De Wbp BES geeft de kaders en normen aan bij de verwerking van persoonsgegevens op Bonaire, Sint Eustatius en Saba. Bij de verwerking van persoonsgegevens door de overheid dient de bescherming van persoonsgegevens van betrokkenen te stoelen op en te voldoen aan de Wbp BES en de beginselen van behoorlijk bestuur, waaronder de beginselen van proportionaliteit en subsidiariteit.

De commissie heeft, vóór de aankondiging van het programmatisch toezicht, diverse informatiesessies, workshop en presentaties gehouden bij de verschillende directies van het Openbaar Lichaam Bonaire (hierna OLB). Conform artikel 13 van het Wbp BES dient het OLB als verantwoordelijke de door haar verwerkte persoonsgegevens zowel organisatorisch als technisch adequaat te beveiligen. Tevens dienst het OLB een adequate informatie- en gegevenshuishouding op na te houden. Dit betekent onder meer dat het OLB documenten en/of bestanden met persoonsgegevens moet beveiligen tegen oneigenlijk gebruik. Het OLB heeft op verzoek van de commissie haar clean desk en clear screen beleid in 2021 opgeleverd. Het clean desk en clear screen beleid van het OLB is als leidraad gebruikt bij het opstellen van de vragen en bij de controle ter plaatse.

1.2 Doel van het rapport

Het doel van dit rapport is om inzichten te geven in de staat van de gegevenshuishouding van het OLB. Tevens zal het rapport als handhavingsinstrument gebruikt worden bij de opvolging van de aanbevelingen naar aanleiding van het rapport. De commissie heeft in 2022 reeds aangegeven dat de naleving van het eigen beleid door het OLB niet optimaal is. De verbeterpunten, opgenomen in dit rapport zullen als meting fungeren tijdens de handhavingsfase.

1.3 Opzet van het rapport

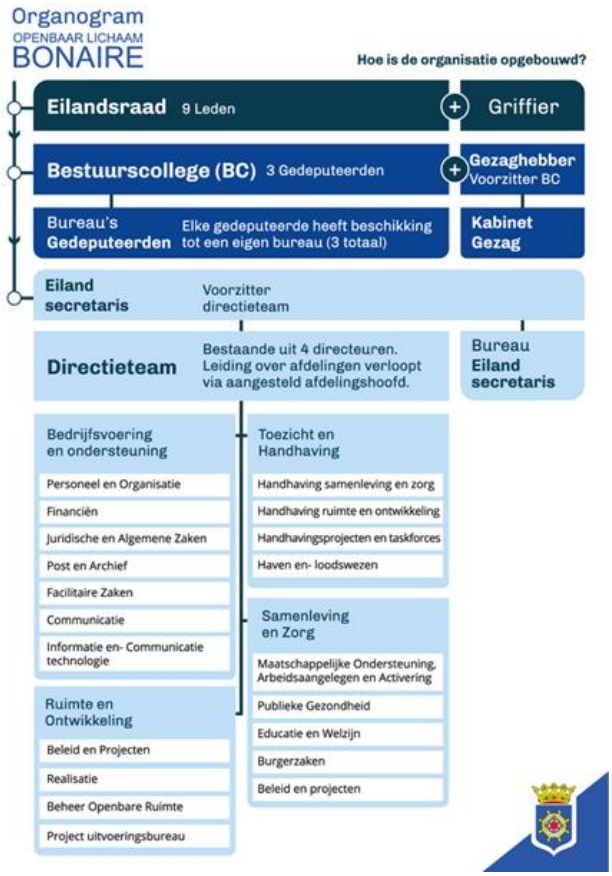
Hoofdstuk 2 geeft een uiteenzetting van de bevindingen tijdens de controle ter plaatse. Vervolgens wordt in hoofdstuk 3 een overzicht gegeven van de algemene normen en kaders waaraan getoetst wordt. In hoofdstuk 4 vindt de analyse plaats van de bevindingen gevolgd door de conclusie van de commissie waarbij de commissie een antwoord moet geven op de vraag: *Komt de situatie zoals aangetroffen in de periode tussen 14 februari 2022 en 8 maart 2022 overeen met het vastgesteld beleid (en de normering)?* In hoofdstuk 5 gaat de commissie in op de aanbevelingen en verbeterpunten per directie/departement.

2 Onderzoek

2.1 Inleiding

Op grond van artikel 50 lid 1 Wbp BES is de commissie bevoegd ambtshalve of op verzoek een onderzoek in te stellen naar de wijze waarop ten aanzien van gegevensverwerking toepassing wordt gegeven aan het bepaalde bij of krachtens de Wbp BES.

De commissie heeft controle uitgevoerd bij alle locaties waar de directies/departementen van het OLB zijn gehuisvest. De commissie heeft bij de uitvoering van de audit geen controle uitgevoerd bij de Eilandsraad en de Griffier.



De commissie heeft bij de voorbereiding op de controle ter plaatse een vragenlijst en een checklist[1] opgesteld. De checklist is gebaseerd op algemene kaders zoals neergelegd in de Wbp BES en op het beleid opgesteld door het OLB.

[1] Zie bijlage voor de vragenlijst en checklist.

2.2 Controle ter plaatse

De controle ter plaatse heeft in totaal 2 weken in beslag genomen. Het OLB omvat de volgende departementen: bureau gedeputeerden, Kabinet Gezaghebber en vier directies (Bedrijfsvoering en Ondersteuning, Toezicht en Handhaving, Ruimte en Ontwikkeling en Samenleving en Zorg). Deze 4 directies zijn op hun beurt onderverdeeld in verschillende afdelingen. Sommige afdelingen zijn allemaal in 1 gebouw gehuisvest en in andere gevallen zijn de afdelingen verspreid over verschillende gebouwen. Tijdens de controle op clean desk en clear screen heeft de commissie de volgende situatie aangetroffen.

Situatie op locatie[2]	Organisatorisch: Bewaren-vernietigen	Organisatorisch/technisch: Bescherming-beveiliging	Technische maatregelen: toegang
Kantoor	Er ontbreken afsluitbare kasten.	Documenten kunnen door derden worden ingezien.	Kantoren gaan niet op slot. Weinig kantoren kennen een systeem van toegangspas
Kantoor en omgeving	Documenten liggen zonder supervisie in kantoren (op de vloer en op bureaus) en op de gang .	Er wordt veel documenten geprint. Deze liggen soms in de printerbakken op andere locaties dan waar de opdracht wordt gegeven.	Medewerker kan in elk kantoor komen.
Bureaus	Er liggen veel documenten op bureaus zonder supervisie. Sommige documenten liggen al een tijd.	De documenten worden bij het verlaten van de bureau niet achter slot en grendel bewaard.	nvt
Documenten	Het opbergen van documenten gebeurt zowel centraal als decentraal.	De kamers waar documenten decentraal worden bewaard heeft geen beveiliging-systeem.	De documenten zijn voor een ieder op de gang toegankelijk.
Documenten	Veel documenten moeten worden vernietigd. Op diverse locatie is er behoefte aan een shredder	De documenten die vernietigd moeten worden staan in open ruimte waar er geen beveiliging is.	nvt

[2] De situatie zoals in de matrix omschreven is bij nagenoeg alle locaties aangetroffen.

Computer	nvt	Clt-Alt-DlT wordt door de meeste medewerkers gebruikt. Wachtwoord wordt niet gedeeld onderling.	Automatische vergrendeling kan worden ingezet. Niet alle gebruikers maken daar gebruik van. Er zijn geen privacy screens aangetroffen bij de gecontroleerde schermen.
Computer	Er wordt nog steeds gebruik gemaakt van geeltjes op scherm en toetsenbord met daarop persoonsgegevens	Door de makkelijke toegankelijkheid zijn deze persoonsgegevens zichtbaar voor derden	Weinig gebruikers maken gebruik van digitale notepads
Printer	Er zijn zowel gezamenlijke printers als individuele printers. De gezamenlijke printers staan vaak in een open ruimte, toegankelijk voor personeel. Er zijn bij een aantal printers ook printopdrachten aangetroffen in de printbakken	Kopietjes en printopdrachten worden niet meteen opgehaald. Er wordt geen gebruik gemaakt van secure printen met als gevolg dat sommige printopdrachten lang blijven liggen in andere gebouwen voordat ze worden opgehaald. Dit betreft ook printopdrachten met bijzondere gegevens.	Er wordt geen gebruik gemaakt van secure printen. De individuele printers staan in kantoor van de gebruiker.

3. Normering

3.1 Wettelijke kaders

De kaders zijn opgenomen in art. 13 Wbp BES:

> ''de verantwoordelijke legt passende technisch- en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen''.

Het gaat bij de normering om de volgende criteria:

- Persoonsgegevens: gegevens die direct/indirect herleidbaar zijn naar natuurlijke personen,
- Verwerking: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens (in casu het verzamelen, vastleggen, bewaren, bijwerken, wijzigen, raadplegen, gebruiken, door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling van gegevens),
- In een bestand: een bestand (digitaal of fysiek) is elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen,
- Door een verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
- Door een bewerker: deze is degene die ten behoeve van de verantwoordelijke (RCN-diensten) persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen,
- Betrokkene: degene op wie een persoonsgegeven betrekking heeft.

De werking van persoonsgegevens

Persoonsgegevens dienen in overeenstemming met de wet, op behoorlijke en zorgvuldige wijze en voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verwerkt[3].

De bescherming en beveiliging

De verantwoordelijke (en de bewerker) zijn verplicht passende technische en organisatorische maatregelen te treffen om de verwerkte persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking[4]. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

[3] Artikel 6 en 7 Wbp BES.
[4] Artikel 13 Wbp BES.

Bewaren van persoonsgegevens

Persoonsgegevens, in een vorm die het mogelijk maakt de betrokken te identificeren, mogen niet langer worden bewaard dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.
Uitzondering voor het langer bewaren dan noodzakelijk kan voor zover ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard én de verantwoordelijke de nodige voorzieningen heeft getroffen om te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.

3.1 Doel van de kaders

De algemene kaders voor bescherming moeten een preventieve werking hebben bij de verwerking van persoonsgegevens.
Organisatorische maatregelen zijn handleidingen in de vorm van o.a. beleid en richtlijnen. Deze maatregelen ondersteunen het proces van gegevensverwerking binnen een organisatie. Bij een adequate uitvoering van de richtlijnen wordt de kans op oneigenlijk gebruik van persoonsgegevens verkleind.

3.2 Beleid OLB

December 2020 heeft het OLB, naar aanleiding het verzoek van de commissie per brief van juli 2020[5], haar beleid "Op weg naar bewustwording informatieveiligheid-clean desk en clear screen beleid"[6] opgesteld (hierna het beleid).
Het OLB heeft een stappenplan opgesteld voor het jaar 2021 met als eindresultaat: volledige implementatie van het beleid per 31 december 2021.
Het doel van een clean desk en clear screen beleid is om bewuster om te gaan met documenten. Dit houdt onder andere in dat er een uniforme wijze is vastgesteld voor het opbergen en vernietigen van documenten. Een clean desk en clear screen beleid draagt bij aan een adequate beveiliging en bescherming van persoonsgegevens binnen een organisatie. Opgeruimde bureaus en werkplekken verminderen de kans op fraude en/of datalekken.

In het beleid komen de volgende onderdelen aan bod:

- Wat is informatie: voorbeelden hiervan zijn naam, telefoonnummer, geboortedatum.
- De wijze van verkrijgen van informatie
- Informatiebeveiliging: waarom is het belangrijk? Hoe kunnen we informatie beter beveiligen? (voorbeeld filekasten met sloten, shredders, toegangspassen)
- Wie is verantwoordelijk bij de verwerking?
- Wat is een clean desk? (voorbeelden van hoe het niet hoort te zijn)
- Wat is clear screen? Hoe zorg je voor het vergrendelen van je scherm? Do's and dont's zijn opgenomen.

[5] In het kader van het toezicht op de naleving van de Wbp BES heeft de commissie aan het Openbaar Lichaam Bonaire verzocht om uiterlijk 31 december 2020 een integraal clean desk- en clear screen beleid op te stellen en te implementeren.
[6] Ze bijlage voor het beleid van het OLB.

- Wat wordt van de ambtenaar verwacht ten aanzien van Clean desk en clear screen? (hier wordt aangegeven welke gedragingen van de ambtenaar wordt verwacht ten aanzien van clean desk en clear screen)
- Wat zijn beveiligingsmaatregelen voor laptops/ipads en mobiele telefoons van de zaak?
- Datum inwerkingtreding van het clean desk en clear screen beleid: 31 december 2021

Onderstaande matrix geeft een overzicht van het beleid voor de diverse componenten behorende bij een werkplek:

Situatie	Beleid	Maatregelen	Hulpmiddel
Toegang Kantoor	Deur dicht/op slot bij vertrek	Afsluitbare deuren	Sloten, toegangspas
Kantoor en omgeving	Alleen hulpmiddelen die nodig zijn tijdens het werk	Gebruik van digitale dossiers in plaats van hard copy dossiers	Laptop
Bureaus	Opgeruimd achterlaten	Informatie opbergen	Afsluitbare kasten
Documenten	Niet zichtbaar voor derden	Persoonsgegevens opbergen	Afsluitbare kasten, manila hoesjes
Documenten	Noodzakelijk documenten bewaren conform Archiefwet BES	Niet noodzakelijke documenten vernietigen in overeenstemming met Archiefwet BES	Shredder
Computer	Vergrendelen bij geen gebruik	Clt-Alt-Dlt gebruiken (log uit), wachtwoord niet delen onderling	Automatische vergrendeling, privacy screens, veilige plek voor opbergen wachtwoord
Computer	Geen notes op scherm	Notitie digitaal plakken	Digitale notes
Printer	Geen print opdracht laten liggen	Kopietjes en printopdrachten meteen ophalen	Secure printen, printen met een inlogcode

4. Analyse en conclusie

4.1 Inleiding

De commissie heeft in het kader van haar programmatisch toezicht een controle ter plaatse uitgevoerd bij alle kantoren van het OLB. Bij de controle heeft de commissie aandacht gegeven aan de volgende onderdelen:

1. Clean desk
    - Gegevensbescherming documentatie (waaronder printopdrachten)
    - Gegevensbeveiliging (waaronder bewaren en vernietigen)
    - Staat van werkplek en omgeving
    - Toegang (organisatorische en technische bescherming)
2. Clear screen:
    - Gegevensbeveiliging
    - Inkijk op andermans scherm tijdens kantooruren

4.2 Toetsing normering

De bevindingen tijdens de controle ter plaatse worden getoetst aan de kaders opgenomen in artikel 13 van het Wbp BES én het beleid van het OLB.

Bij de verwerking gaat het om:

Verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

Toepassen van technische en organisatorische maatregelen: deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen;

Persoonsgegevens: gegevens die direct/ indirect herleidbaar zijn naar een natuurlijke persoon;

Verwerking: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling.

Het Bestuurscollege is conform art. 1 van de Wbp BES de verantwoordelijke voor de beveiliging en bescherming van persoonsgegevens die binnen het OLB verwerkt worden.

Het OLB heeft voor de uitvoering van haar taak een clean desk en clear screen beleid opgesteld. De implementatie van het beleid binnen alle directies van het ambtelijk apparaat is een onderdeel hiervan.

De volgende matrix geeft een kwalificatie van bevindingen bij de toetsing aan de normen en het beleid. De volgende kwalificaties zijn mogelijk:

- Voldoet aan de normen: JA
- Voldoet niet aan de normen: NEE
- Voldoet deels aan de normen: DEELS

Situatie	Beleid OLB	Artikel 13 Wbp BES	Bevindingen commissie	Kwalificatie: bevindingen voldoen aan normen (het beleid en regelgeving)
Toegang Kantoor	Deur dicht/op slot bij vertrek	Afsluitbare deuren	Geen afsluitbaar ruimtes	NEE
Kantoor en omgeving	Alleen hulpmiddelen die nodig zijn tijdens het werk. Kantoor netjes achterlaten	Gebruik van digitale dossiers in plaats van hard copy dossiers. Geen documenten onbeheerd achterlaten	Documenten worden onbeheerd achtergelaten op bureaus en omgeving	NEE
Bureaus	Opgeruimd achterlaten	Informatie opbergen	Afsluitbare kasten	NEE
Documenten	Niet zichtbaar voor derden	Persoonsgegevens opbergen	Afsluitbare kasten, manila hoesjes	NEE
Documenten	Noodzakelijk documenten bewaren conform Archiefwet BES	Niet noodzakelijke documenten vernietigen in overeenstemming met Archiefwet BES	Shredder niet in alle kantoren aanwezig	DEELS
Computer	Vergrendelen bij geen gebruik	Clt-Alt-Dlt gebruiken (log uit), wachtwoord niet delen onderling	Meeste schermen worden handmatige vergrendeld	JA
Computer	Geen notes op scherm	Notitie digitaal plakken	hardcopy notes zijn zichtbaar	NEE
Printer	Geen print opdracht laten liggen	Kopietjes en printopdrachten meteen ophalen	Geen secure printing. Printopdrachten in printbak	NEE

4.3 Analyse Clean desk

a. Gegevensbescherming (waaronder printopdrachten)

Printers staan in een aparte ruimte, een 'printhok' of op de gang. De printopdrachten liggen in de bakken en worden zonder secureprint gestuurd. Door geen gebruik te maken van secure printen of een andere vorm van beveiliging, wordt de kans dat verwerkte persoonsgegevens in handen van onbevoegden terecht komen vergroot.

b. Gegevensbeveiliging (waaronder bewaren en vernietigen)

Om het clean desk en clear screen beleid te implementeren zijn de juiste opbergsystemen en materialen vereist. Binnen de afdelingen en kantoorruimten moeten voldoende afsluitbare kasten en ladekasten aanwezig zijn waarin de persoonsgegevens opgeborgen/bewaard kunnen worden. Daarnaast is het belangrijk dat op alle afdelingen een papierversnipperaar aanwezig is om ingeval persoonsgegevens vernietigd moeten worden, dit op de adequate manier gebeurd. Er is geconstateerd dat bij nagenoeg alle kantoren de kasten **niet** op slot kunnen. Voor OLB breed geldt dat de essentiële opbergsystemen en materialen die nodig zijn om het clean desk en clear screen beleid adequaat te implementeren, niet beschikbaar zijn. Het uitblijven of niet hebben van een vernietigingsbeleid speelt hierbij ook een rol.

c. Staat van de werkplek en omgeving

Bij de toetsing is gekeken naar de gegevens en informatiehuishouding bij elk locatie. Hierbij is tevens getoetst hoe de locatie (vb kantoor, bureau) op het eerste oog eruit ziet rekening houdend met bescherming van de persoonsgegevens.

d. Toegang tot persoonsgegevens (organisatorische en technische bescherming)

Organisaties moeten moderne techniek gebruiken om persoonsgegevens te beveiligen. Denk hierbij aan een beschermd online omgeving en het introduceren van een veilig wachtwoordsysteem met behulp van onder andere tweefactor-authenticatie. Artikel 13 van het Wbp BES bepaald dat de aangewende technische maatregelen een passend beveiligingsniveau moet garanderen

Situatie ten aanzien van Clean desk op locatie	**Kwalificatie: gecontroleerde locaties voldoen aan Gegevensbescherming (waaronder beschermd print opdrachten)**	**Kwalificatie: De gecontroleerde locaties voldoen aan de gegevensbeveiliging (waaronder bewaren en vernietiging)**	**Kwalificatie: De diverse kantoren laten hun kantoor en omgeving netjes achter zonder documenten op bureaus of elders (staat van werkplek)**	**Kwalificatie: De gecontroleerde locaties zorgen voor beperkte toegang tot persoonsgegevens (organisatorische en technische bescherming)**
Bureau Gedeputeerden	NEE	Bewaren: DEELS (niet alle kantoren beschikken over afsluitbare kasten) Vernietigen: NEE (Geen eigen shredder)	NEE	DEELS (toegang tot bestuurskantoor is middels toegangspas. Toegang overige kantoren: niet alle kantoren gaan op slot)
Kabinet Gezaghebber	NEE	Bewaren: DEELS (niet alle kantoren beschikken over afsluitbare kasten) Vernietigen: NEE (Geen eigen shredder)	NEE	DEELS (toegang tot bestuurskantoor is middels toegangspas. Toegang overige kantoren: niet alle kantoren gaan op slot)
Directie Bedrijfsvoering & Ondersteuning	NEE	Bewaren: DEELS (niet alle kantoren beschikken over afsluitbare kasten) Vernietigen: DEELS	NEE	DEELS
Directie Samenleving en Zorg	NEE	Bewaren: NEE Vernietigen: NEE (Geen eigen shredder)	NEE	NEE
Directie Ruimte en Ontwikkeling	NEE	Bewaren: NEE	NEE	NEE

		Vernietigen NEE (Geen eigen shredder)		
Directie Toezicht en Handhaving	NEE	Bewaren DEELS (niet alle kantoren beschikken over afsluitbare kasten)	NEE	NEE
		Vernietigen NEE (Geen eigen shredder)		

4.4 Analyse Clear screen

Bij de toetsing per werkplek van het gebruik van Clear screen bij het verlaten van de werkplek zijn de volgende componenten gekwalificeerd:

- Gegevensbescherming (vergrendeling scherm, 2 factor authenticatie)
- Gegevensbeveiliging van de werkcomputer (geplakte notities op scherm)
- Inkijk op andermans scherm tijdens het werk

Situatie ten aanzien van Clear Screen op locatie	Kwalificatie: gecontroleerde locaties voldoen aan gegevensbescherming ten aanzien van hun computerscherm	Kwalificatie: De gecontroleerde locaties voldoen aan de gegevensbeveiliging van hun werkcomputer (waaronder geen geplakte notities op scherm en omgeving	Kwalificatie: De gecontroleerde bureaus voldoen aan de gegevensbeveiliging van hun werkcomputer (waaronder geen inkijk op andere schermen tijdens het werk)
Bureau Gedeputeerden	JA (Ctr-Alt-Dlt)	JA	DEELS
Kabinet Gezaghebber	JA (Ctr-Alt-Dlt)	JA	JA
Directie Bedrijfsvoering & Ondersteuning	JA (Ctr-Alt-Dlt)	JA	NEE
Directie Samenleving en Zorg	DEELS	NEE	NEE
Directie Ruimte en Ontwikkeling	DEELS	NEE	NEE
Directie Toezicht en Handhaving	JA (Ctr-Alt-Dlt)	NEE	DEELS

4.5 Conclusie

4.5.1 Algemeen

De Wbp BES bepaalt dat persoonsgegevens zorgvuldig verwerkt en beveiligd moet worden en is van toepassing op zowel digitale als hardcopy verwerkte persoonsgegevens.
Documenten met persoonsgegevens onbeheerd achterlaten kan leiden tot overtreding van de normen in de Wbp BES. Elk ambtenaar krijgt weleens documenten met vertrouwelijke informatie in handen. Of het (bijzondere) persoonsgegevens zijn of niet, moet de ambtenaar zorgvuldig omgaan met deze vertrouwelijke informatie.

Het OLB is in bezit van een Clean Desk en Clear Screen beleid, 'Op weg naar bewustwording informatieveiligheid'. Dit is een goed begin, echter zijn niet alle directies (en ambtenaren) van het ambtelijk apparaat bekend met dit beleid. Om de naleving van het beleid binnen het gehele ambtelijke apparaat te bereiken is sturing vanuit het Bestuurscollege en in het bijzonder de eilandsecretaris én directeuren noodzakelijk. Zolang sturing niet optimaal is en/of uitblijft kan het naleven van het beleid niet effectief geschieden.
Het opstellen van het beleid is een belangrijke stap om zorgvuldige omgang met persoonsgegevens te bevorderen.
De controle ter plaatse bij de diverse panden waar departementen/directies van het OLB zijn gehuisvest heeft de commissie meer helderheid gegeven op de wijze en met name de fase waarin de implementatie van het beleid zich bevindt. Het OLB voldoet **niet** aan de bepalingen van artikel 13 van de Wbp BES.
De commissie trekt aan de hand van de bevindingen en de analyse de volgende algemene conclusie:

1. sturing op het beleid vanuit het Bestuurscollege is (nog) niet optimaal;
2. sturing op het beleid vanuit de eilandsecretaris en de directeuren is (nog) niet optimaal;
3. De (magere) richtlijnen die gestipuleerd zijn in het beleid zijn over het algemeen (nog) niet bekend bij de ambtenaren;
4. Er is weinig tot geen controle in de verticale én horizontale implementatie van het beleid;

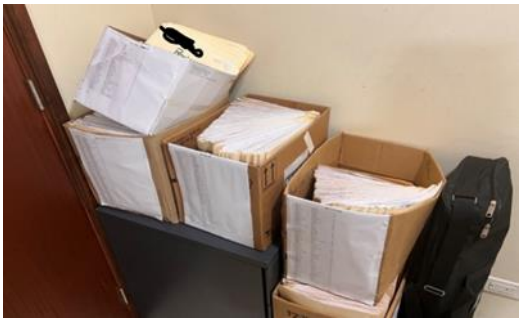
4.5.2 Conclusie Clean desk

Gegevensbeveiliging (waaronder bewaren en vernietigen)

Om het clean desk en clear screen beleid te implementeren zijn de juiste opbergsystemen en materialen vereist. Binnen de afdelingen en kantoorruimten moeten voldoende kasten en ladekasten aanwezig zijn die op slot kunnen waarin de persoonsgegevens opgeborgen kunnen worden. Daarnaast is het belangrijk dat op alle afdelingen een papierversnipperaar aanwezig is om ingeval persoonsgegevens vernietigd moeten worden, dit op de adequate manier gebeurt. Tijdens toezicht werd opgemerkt dat alle directies een ruimte hebben waar gegevens, waaronder ook persoonsgegevens, voor een langere periode bewaard worden. Het gaat hierbij om kantoorruimte waarin dozen met persoonsgegevens op de vloer bewaard worden zonder enige vorm van beveiliging. De archiefruimten bij de directies voldoen niet aan de organisatorische maatregelen die conform het Wbp BES nageleefd moeten worden indien persoonsgegevens verwerkt en bewaard worden.

Samenvattend:

5. Verwerkte persoonsgegevens worden niet altijd op de juiste manier vernietigd;
6. Archiefruimten en bewaarplaatsen bieden onvoldoende bescherming aan verwerkt, bewaard en gearchiveerde persoonsgegevens;



Gegevensbescherming (waaronder printopdrachten en printomgeving)

Printers staan binnen de meeste directies in een aparte ruimte, een 'printhok' of op de gang. Met de meeste printers binnen het gehele ambtelijk apparaat van het OLB kan geprint worden via een secure print systeem. Dit systeem wordt echter niet gebruikt. Door geen gebruik te maken van secure printen of een andere vorm van beveiliging, wordt de kans dat verwerkte persoonsgegevens in handen van onbevoegden terecht komt vergroot. Printhok wordt bij één van de directies ook gebruikt als archiefruimte.

Samenvattend:

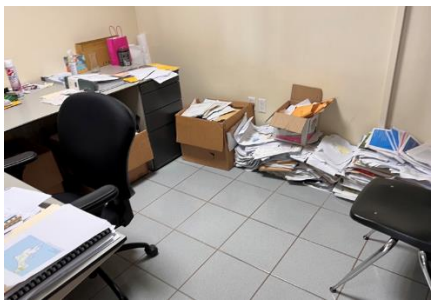
7. Er zijn geen richtlijnen opgesteld om secure printen af te dwingen, terwijl het technisch wel georganiseerd kan worden.

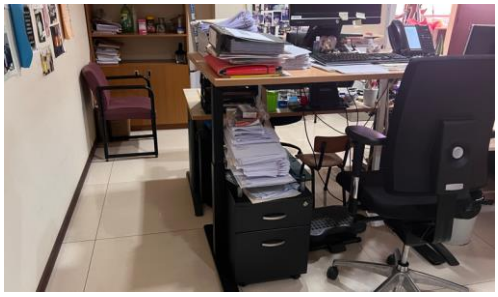
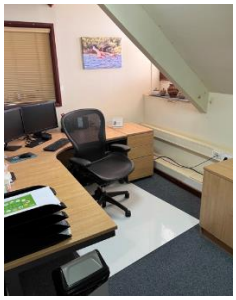
Staat van de werkplek en omgeving

De commissie concludeert dat bijna alle werkplekken niet voldoen aan de normen zoals opgenomen in het beleid met als gevolg dat de kans op een datalek exponentieel toeneemt. De laatste foto is van een werkplek waarbij wel wordt voldaan aan een clean desk.

Samenvattend:

8. er zijn onvoldoende organisatorische maatregelen geïntroduceerd binnen de verschillende directies van het OLB om verwerkte persoonsgegevens op een adequate wijze te beveiligen;



Toegang tot persoonsgegevens (organisatorische en technische bescherming)

Organisaties moeten moderne techniek gebruiken om persoonsgegevens te beveiligen. Denk hierbij aan een beschermd online omgeving en het introduceren van een veilig wachtwoordsysteem met behulp van onder andere tweefactor-authenticatie. Artikel 13 van het Wbp BES bepaalt dat de aangewende technische maatregelen een passend beveiligingsniveau moet garanderen. Digitaal verwerkte persoonsgegevens moeten goed beveiligd worden.
Echter niet alle ambtenaren van het OLB zijn zich hiervan bewust. Er wordt niet verantwoord omgegaan met wachtwoorden en automatisch gegenereerde wachtwoorden worden niet gewijzigd.

Met uitzondering van de afdeling Personeel en Organisatie en het Bestuurskantoor (boven) zijn de gebouwen waarin de directies/ afdelingen van het OLB gevestigd zijn niet voldoende beveiligd. Er bestaat geen systeem waarmee gecontroleerd kan worden wie het gebouw wanneer betreedt en/of verlaat. Dit geldt ook voor kantoorruimtes en afdelingen binnen de gebouwen.
De huidige panden van de verschillende directies van het OLB beschikken niet over de adequate technische systemen om het juiste beveiligingsniveau te garanderen. Zowel van buiten af als van binnen is het beveiligingsniveau zeer laag.
Over het algemeen wordt gebruik gemaakt van sleutels die toegankelijk zijn voor onbevoegden. Het opbergsysteem dat OLB gebruikt om deze sleutels te bewaren/beveiligen voldoet niet aan de vereiste standaarden. Bij sommige afdelingen hebben o.a. interieurverzorgster ongecontroleerd toegang tot gebouwen en kantoren (foto 2: dozen in het trappenhuis bij directie Samenleving en Zorg)
Samenvattend:

9. Er zijn geen passende technische maatregelen beschikbaar om persoonsgegevens te beschermen tegen verlies of enige vorm van onrechtmatige verwerking;
10. De meeste overheidsgebouwen zijn makkelijk toegankelijk (geen toegangscontrole)

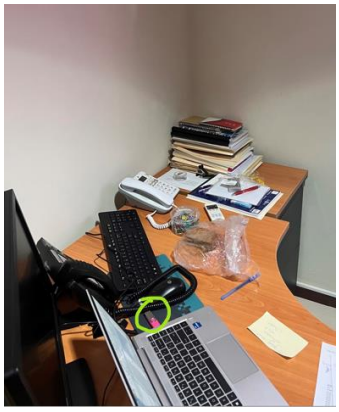
4.5.3 Conclusie clear screen

Gegevensbescherming (vergrendeling scherm en beveiliging gegevensdragers)

Binnen het ambtelijk apparaat OLB bestaat geen structuur/ proces waarmee het naleven van het clear screen beleid en de beveiliging van computers en computerprogramma's getoetst wordt.
Over het algemeen weten de medewerkers dat ze hun scherm moeten vergrendelen als ze weg zijn van hun werkplek maar niet iedereen houdt zich hieraan.
Het OLB heeft geen specifieke richtlijnen voor de omgang met gegevensdragers (zoals een computer, laptop, usbstick), waardoor adequate controle achterwege blijft. Op de vraag of medewerkers op structurele wijze geïnformeerd worden over het veilig omgaan met de gegevensdragers, wordt aangegeven dat de medewerkers adhoc informatie krijgen in geval er sprake is van een incident.

Samenvattend:

11. Er is geen uniforme en passende beveiliging aanwezig voor gegevensdragers zoals computers en computerprogramma's waarmee persoonsgegevens digitaal verwerkt worden;

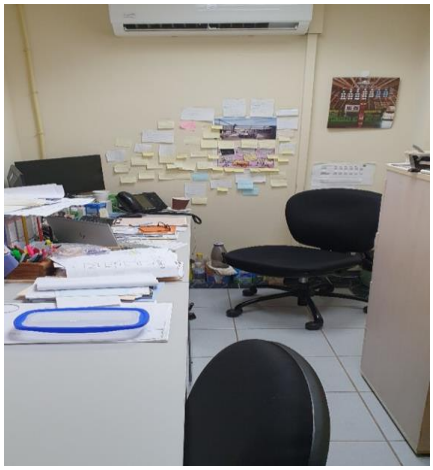


Gegevensbeveiliging van de werkcomputer (geplakte notities op scherm)

De meeste bureaus maken nog steeds gebruik van hardcopy notitieblaadjes. Deze worden aan de werkcomputer en de muren opgeplakt. Bij het verlaten van de werkplek worden de notities niet weggehaald met als gevolg dat persoonsgegevens (vaak zijn het namen met telefoonnummers) toegankelijk zijn voor onbevoegden.

Samenvattend:

12. Hardcopy notities worden onbeheerd achtergelaten in een werkomgeving zonder dat deze beveiligd is.



Inkijk op andermans scherm tijdens het werk

Bij de diverse locaties is er sprake van het delen van een kantoor met andere collega's. In geval de werkzaamheden van de collega's met elkaar overeenkomen is structurele inkijk op elkaars scherm geen probleem. Op het moment dat de collega's niet hetzelfde werk uitvoeren is het aan te raden om inkijk in elkaar schermen te beperken. De commissie concludeert dat privacy niet geborgd kan worden op het moment dat meerdere personen die **niet** hetzelfde werk verrichten een kamer delen. Er is sprake van structureel risico van inkijk in elkaars scherm (en dus werk). De commissie is zich terdege bewust dat het niet haalbaar is om elk ambtenaar een apart kantoor te geven.

Toch ziet de commissie een **quickwin** voor het OLB ten aanzien van dit onderwerp. In het volgende hoofdstuk zullen we de aanbevelingen bespreken waarbij een minimale inzet voldoende is om een maximale output te krijgen ten aanzien van compliancy.

5. Aanbevelingen

5.1 Sturing

Het Clean Desk en Clear Screen beleid 'Op weg naar bewustwording informatieveiligheid' is een goede eerste stap in het bewustwordingsproces waarbij het OLB haar verantwoordelijkheid ten aanzien van de bescherming en beveiliging van de onder haar ressorterende persoonsgegevens vorm geeft. Het Bestuurscollege is verplicht zorg te dragen dat het beleid binnen het gehele ambtelijke apparaat bekend is. Binnen de directies moeten alle lagen van de dienstverlening bekend zijn met het beleid. Een prioriteitenlijst is van eminent belang voor de (verdere) implementatie van de aanbevelingen. Een goede prioritering met een stappenplan met te behalen mijlpalen wordt met klem aanbevolen. Vervolgens moet er nauwlettend op werden toegezien dat de stappen ook worden genomen en dat iedereen zich houdt aan het beleid en de richtlijnen.
Nadat de prioriteiten én een stappenplan zijn vastgesteld moet het Bestuurscollege en de eilandsecretaris nauwlettend erop toezien dat de stappen ook worden genomen en dat iedereen zich houdt aan het beleid en de richtlijnen. Frequente controles vanuit het managementteam van de directies moet de naleving van het beleid bevorderen.
De commissie onderstreept hoe belangrijk het is om een gezonde gegevenshuishouding te hebben in het ambtelijk apparaat. Gelet op de urgentie om naleving van de wet- en regelgeving te bevorderen concludeert de commissie dat een privacyfunctionaris onontbeerlijk is bij het OLB. De commissie geeft het Bestuurscollege in overweging om een privacyfunctionaris aan te trekken belast met vraagstukken rondom privacy in het algemeen en de implementatie en controle van het beleid in het bijzonder.

5.2 Clean desk en Clear screen

Clean desk

Clean desk is niet alleen het zo min mogelijk spullen op je bureau hebben maar vooral ervoor zorgen dat wanneer een werkplek niet in gebruik is, deze ontdaan wordt van alle mogelijke documenten die (bijzondere) persoonsgegevens kunnen bevatten. De commissie heeft geconstateerd dat de grootste uitdaging bij de clean desk ligt. De commissie doet, gelet op haar analyse (zie paragraaf 4.3), de volgende aanbevelingen bij de clean desk in volgorde van urgentie/risico (1 is hoog en 4 is laag):

1. Staat van de werkplek en omgeving:
2. Adequate gegevens bescherming waaronder secure printen:
3. Adequate gegevens beveiliging waaronder bewaren en vernietigen
4. Toegang persoonsgegevens waaronder toegang tot gebouwen

Met referte naar bovenstaande aanbevelingen kan het OLB de volgende stappen ondernemen:

Aanbeveling	Te ondernemen stappen	Hulpmiddelen
1.Staat van de werkplek en omgeving	(Bijzondere) persoonsgegevens dienen bij verlaten van de werkplek opgeborgen te worden in (lade) kasten die op slot kunnen.	Bewustwordingstraject en controle. Alle dossiers moeten achter slot en grendel.

2.Adequate gegevensbescherming waaronder secure printen	Introduceer binnen het gehele ambtelijke apparaat een secure printsysteem waarbij uitgeprinte documenten niet onbeheerd achterblijven en zo niet in handen van onbevoegden terecht komt.	Dit kan bijvoorbeeld door te werken met een pasjessysteem of pincode
3.Adequate gegevens-beveiliging waaronder bewaren en vernietigen	Bepaal door middel van een inventarisatie welke opbergsystemen en materialen nodig zijn bij de diverse directies en afdelingen. Stel richtlijnen op voor inhouse archivering	Aanschaf afsluitbare kasten Aanschaf van meer shredders
4.Toegang tot persoonsgegevens waaronder toegang tot gebouwen	Introduceer toegangscontroles waarmee een verantwoord evenwicht gemaakt kan worden tussen selectieve gastvrijheid en maximale beveiliging.	Dit kan makkelijk door een systeem van toegangspasje of toegang via een pincode.

Clear screen

De commissie doet, gelet op haar analyse (zie paragraaf 4.4), de volgende aanbevelingen bij de clear screen in volgorde van urgentie/risico (1 is hoog en 3 laag is):

1. Gegevensbeveiliging waaronder beperken van inkijk op andermans scherm
2. Gegevensbeveiliging waaronder geen hardcopy notities op scherm (of bureau)
3. Gegevensbescherming waaronder vergrendeling scherm en beveiliging gegevensdragers (2 factor authenticatie.

Met referte naar bovenstaande aanbevelingen kan het OLB de volgende stappen ondernemen:

Aanbeveling	**Te ondernemen stappen**	**Hulpmiddelen**
1.Gegevensbeveiliging waaronder beperken van inkijk op andere schermen)	Zorg dat slechts medewerkers met hetzelfde takenpakket een kamer delen. Als dit niet lukt zorg dat het scherm geen inkijk mogelijk maakt.	De schermen kunnen makkelijk gedraaid worden zodat structurele inkijk niet mogelijk is. Dit is een **quickwin** voor het OLB.
2.Gegevenbeveiliging waaronder geen hardcopy notities op scherm (of bureau)	Alle hardcopy notities vervangen voor digitale notities	Digitale notities beschikbaar maken op alle computers.
3.Gegevensbescherming waaronder vergrendeling scherm en 2factor authenticatie	Geautomatiseerde vergrendeling als default zetten op alle computers. Inloggen verplichten met minimaal 1 zelf bedacht password dat voldoende veilig is.	Default setting aanpassen voor alle gebruikers. Nieuwe gebruiker verplichten om een nieuw password in te voeren. Duidelijke richtlijnen opstellen voor de veilige omgang met gegevensdragers

5.3 Controle

Het opstellen van duidelijke en concrete richtlijnen is de eerste stap om structuur te brengen en controles uit te voeren.
Zonder richtlijnen kan niet gecontroleerd worden of de medewerkers doen wat van hen verwacht wordt. Stel richtlijnen op voor het beveiligen van computers, computerprogramma's en gegevensdragers in het algemeen. Controleer de naleving van deze richtlijnen regelmatig. Nadat het Bestuurscollege zorg heeft gedragen om het beleid binnen het gehele ambtelijk apparaat te implementeren is het aan de directeuren van de verschillende directies om ervoor te zorgen dat de medewerkers de richtlijnen ook naleven.
De aanbevelingen gelden voor de volgende departementen:

- Bureau Gedeputeerden (3)
- Kabinet Gezaghebber
- Eilandsecretaris
- Directie Bedrijfsvoering en Ondersteuning
- Directie Samenleving en zorg
- Directie Ruimte en Ontwikkeling
- Directie Toezicht en Handhaving

5.4 Terugkoppeling aanbeveling

Clean desk en clear screen

De commissie brengt bovenstaande aanbevelingen (en te ondernemen stappen) onder de aandacht van het Bestuurscollege (als eindverantwoordelijke) en de eilandsecretaris (q.q. als hoofd van het ambtelijk apparaat en algemeen directeur bij het OLB) met het verzoek om **binnen 6 maanden** actie te ondernemen teneinde concrete en tastbare verbetering aan te brengen in de geconstateerde situatie[7].

De commissie is zich ervan bewust dat niet alle aanbevelingen van de clean desk tegelijk opgepakt kunnen worden.
Voor de **clean desk** ziet de commissie graag dat de aanbevelingen als volgt gefaseerd worden:

- Aanbevelingen 1 en 2 dienen per **1 oktober 2023** opgepakt en doorgevoerd te zijn.
- Aanbevelingen 3 en 4 dienen per **1 maart 2024** opgepakt en doorgevoerd te zijn.

Voor de **clear screen** ziet de commissie graag dat de aanbevelingen 1 tot en met 3 per **1 oktober 2023** opgepakt en doorgevoerd zijn.

[7] In paragraaf 4.3 is een overzicht gemaakt met de analyse van de bevindingen per departement. Directie Samenleving en Zorg en Directie Ruimte en Ontwikkeling zijn de 2 directies die geheel niet voldoen aan de normen.

Bijlagen

- Op weg naar bewustwording informatieveiligheid - Clean desk - en clear screenbeleid
- Vragenlijst