Model Jaarverslag DPO/FG

|  |  |
| --- | --- |
| Versie: |  |
| Datum: |  |
| Toelichting: |  |
| Annex(en): |  |

**Algemene toelichting model jaarverslag**

Dit model is opgesteld door Bart van Buitenen voor Dasprive VZW (<https://dasprive.be>). Dit model is vrij te gebruiken volgens de licentievoorwaarden zoals genoemd op onze site[[1]](#footnote-1).

*TLDR; doe ermee wat je wilt, zelfs commercieel, zolang er maar ergens een bronvermelding is.*

Wij raden iedere DPO aan om een jaarverslag te maken en dit formeel te laten behandelen door het hoogste managementorgaan binnen de organisatie. Een jaarverslag kan namelijk meerdere doelen voor de DPO en de organisatie dienen:

* Transparantie over de invulling van de rol van DPO.
* Bewijs van het feit dat de DPO rapporteert aan het hoogste managementorgaan binnen de organisatie.
* Helpen om te voldoen aan de verantwoordingsplicht die rust op de verwerkingsverantwoordelijke (art 5.2 GDPR).
* Bij inspectie door een autoriteit onmiddellijk een gedetailleerd overzicht kunnen voorzien aan de inspecteurs.
* Voldoen aan een wettelijke verplichting (bv. Besluit van de Vlaamse Regering (BVR) over de FG, art 3, 3°[[2]](#footnote-2)).

Dit model is opgesteld op basis van de vereisten uit het BVR over de FG, eigen ervaring, en dingen die we terugzagen in andere verslagen en die ons een zinvolle toevoeging leken.

Dit model jaarverslag is dan ook opgesteld om zoveel mogelijk dingen op te sommen die nuttig kunnen zijn voor de DPO om mee te nemen in het jaarverslag. Dat betekent dat het zeer goed mogelijk is dat je er dingen uit schrapt die je niet zinvol vindt. Titels met een \* zijn verplicht volgens eerdergenoemd BVR en die laat je dus best staan als je een DPO bent in de context van de Vlaamse Overheid.

Vragen, opmerkingen of loftuitingen: [bart@dasprive.be](mailto:bart@dasprive.be).

Inhoudstafel

[1. Algemeen overzicht van JAAR \* 3](#_Toc163128270)

[2. Beleid en strategie 4](#_Toc163128271)

[2.1. Stuurgroep Gegevensbescherming / DPO-office / Privacy team / … 4](#_Toc163128272)

[2.2. Beleidsteksten 4](#_Toc163128273)

[2.3. Procedures 4](#_Toc163128274)

[2.4. DPO \* 4](#_Toc163128275)

[2.4.1. Tijd en middelen 4](#_Toc163128276)

[2.4.2. Competentie 4](#_Toc163128277)

[3. Verstrekte adviezen \* 5](#_Toc163128278)

[4. Bewustwordingsactiviteiten \* 5](#_Toc163128279)

[5. Register van verwerkingsactiviteiten (RVVA) 6](#_Toc163128280)

[6. Uitgevoerde controles 6](#_Toc163128281)

[6.1. Controle door de DPO \* 6](#_Toc163128282)

[6.2. Interne audits 6](#_Toc163128283)

[6.3. Externe audits 6](#_Toc163128284)

[7. Contact met een autoriteit / comité / commissie 8](#_Toc163128285)

[7.1. Contact #A 8](#_Toc163128286)

[8. Uitgevoerde DPIA’s 8](#_Toc163128287)

[8.1. DPIA 1 8](#_Toc163128288)

[9. Inbreuken ten aanzien van de beveiliging \* 8](#_Toc163128289)

[9.1. Inbreuk 1 9](#_Toc163128290)

[9.1.1. Context inbreuk 9](#_Toc163128291)

[9.1.2. Gevolgen betrokkenen inbreuk 9](#_Toc163128292)

[9.1.3. Maatregelen genomen n.a.v. inbreuk 9](#_Toc163128293)

[10. Rechten van de betrokkene 9](#_Toc163128294)

[11. Lopende activiteiten 10](#_Toc163128295)

# Algemeen overzicht van JAAR \*

Dit verslag is een overzicht van de wijze waarop de Data Protection Officer (DPO) in het afgelopen jaar de taken zoals benoemd in artikel 39 van de GDPR heeft ingevuld.

*Benoem kort hoe het afgelopen jaar is verlopen. Hou er rekening mee dat veel mensen enkel dit stuk zullen lezen dus wat wil je zeker kwijt als DPO?*

*Zijn er veel incidenten? Ontbreekt de bewustwording? Krijg je veel te weinig tijd? Lopen er allerlei klachten? En natuurlijk: wat gaat er goed?*

*Kortom: overloop de belangrijkste zaken uit de rest van het jaarverslag en geef de hoogte- en dieptepunten.*

*In de context van het BVR voorzie je hier een algemeen overzicht van de veiligheidstoestand, de ontwikkeling in het afgelopen jaar en de nog te realiseren doelstellingen.*

# Beleid en strategie

## Stuurgroep Gegevensbescherming / DPO-office / Privacy team / …

Benoem hier het overlegorgaan binnen de organisatie dat zich bezig houdt met gegevensbescherming / privacy / security. Benoem ook op welke manier de uitkomsten van dit orgaan hun weg vinden naar het hoogste managementorgaan binnen de organisatie.

|  |  |
| --- | --- |
| **Data Samenkomsten** | **Link naar meeting minutes** |
| xx/xx/xx |  |
|  |  |
|  |  |

## Beleidsteksten

*Welke beleidsteksten werden tijdens het afgelopen jaar opgemaakt of herzien?*

## Procedures

*Welke procedures werden tijdens het afgelopen jaar opgemaakt of herzien?*

## DPO \*

### Tijd en middelen

*Beschikt de DPO over voldoende tijd en middelen om de rol in te vullen? Zijn er zaken veranderd in het afgelopen jaar die hier verandering in hebben gebracht? Heeft de DPO een taakomschrijving en is deze actueel?*

### Competentie

*Is de DPO competent (jaren ervaring, min. 3 of ondersteund door collega’s)?*

*Welke opleidingen heeft de DPO gevolgd om kennis actueel te houden, welke conferenties[[3]](#footnote-3) werden bezocht?*

# Verstrekte adviezen \*

*Wij raden aan om hier enkel de formele adviezen in op te nemen, niet de informele adviezen.*

* *Informele adviezen zijn het soort adviezen die een DPO continu geeft: als antwoord op een mailtje, tijdens een bespreking of eventueel zelfs telefonisch. Wij raden altijd aan om zoveel mogelijk van deze informele adviezen op een bepaalde manier vast te leggen (meeting minutes, mails, helpdesktickets, etc.).*
* *Formele adviezen zijn adviezen die buiten de dagdagelijkse communicatie met de DPO om zijn uitgebracht, op verzoek of op eigen initiatief van de DPO, en een formeler karakter hebben omdat ze geformuleerd zijn aan het hoogste management van de organisatie. Formele adviezen krijgen ook een formeel antwoord van de directie.*

|  |  |  |
| --- | --- | --- |
| **Datum Advies** | **Korte omschrijving** | **Beslissing directie** |
| Advies xx/xx/xx | Omschrijf kort de context van het advies, en wat de DPO daarover te zeggen had. | Wat deed de directie met die advies? Indien niet gevolgd, is die beslissing gemotiveerd en hoe? |
|  |  |  |
|  |  |  |

# Bewustwordingsactiviteiten \*

*Welke awareness activiteiten zijn er uitgevoerd het afgelopen jaar?*

*Bv: spreken op personeelsevenementen, sessie binnen bepaalde afdeling(e)n), ophangen posters, versturen informatiemails, phishing tests, etc.*

|  |  |  |
| --- | --- | --- |
| **Datum activ.** | **Korte omschrijving** | **Doeleinde** |
| xx/xx/xx | Wat voor activiteit was het? | Bv. Verhogen van phishing awareness, meer kennis van “privacy by design”, … |
|  |  |  |

# Register van verwerkingsactiviteiten (RVVA)

*Op welke manier is het RVVA dit jaar beoordeeld en/of herzien? Welke belangrijke activiteiten zijn er bijgekomen? Enige activiteiten met specifieke opmerkingen?*

# Uitgevoerde controles

## Controle door de DPO \*

|  |  |  |
| --- | --- | --- |
| **Datum Controle** | **Korte omschrijving** | **Resultaat** |
| xx/xx/xx | Wat is er gecontroleerd? (opvolging DPIA A, nazicht logbestanden van applicatie X, kennistoets medewerkers, | Overzicht van de resultaten van de controles. Waar mogelijk: benoem concrete aantallen, bv. 10 raadplegingen dossier geselecteerd, 1 onrechtmatigheid vastgesteld. |
|  |  |  |
|  |  |  |

## Interne audits

|  |  |  |
| --- | --- | --- |
| **Datum Audit** | **Korte omschrijving** | **Resultaat** |
| xx/xx/xx | Wat is er geaudit? | Kort overzicht van de belangrijkste bevindingen. |
|  |  |  |
|  |  |  |

## Externe audits

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum Audit** | **Uitgevoerd door?** | **Korte omschrijving** | **Resultaat** |
| xx/xx/xx | Wie voerde de externe audit uit? | Wat was de scope van de audit? | Korte weergave van de belangrijkste bevindingen. |
|  |  |  |  |
|  |  |  |  |

# Contact met een autoriteit / comité / commissie

*Er kan op verschillende manieren contact zijn geweest met een relevante autoriteit of ander orgaan zoals de Gegevensbeschermingsautoriteit, de AP, de Vlaamse Toezichtcommissie (VTC), het Vlaams Comité voor de Mededeling van Gegevens, het Informatieveiligheidscomité (IVC), een andere DPO, over:*

* *informatievragen,*
* *protocollen voor gegevensuitwisselingen,*
* *beraadslagingen,*
* *klachten,*
* *inspecties,*
* *voorafgaande raadplegingen,*
* *etc.*

*In functie van de frequentie en het belang kunnen deze contacten hieronder worden benoemd. Is er een bepaald soort contact dat veelvuldig voorkomt, overweeg dan om hier een apart hoofdstuk van te maken (bijvoorbeeld protocollen in de Vlaamse context).*

## Contact #A

*Beschrijf hier kort de context van het contact met de autoriteit. Waar ging het over? Wat is de huidige stand van zaken (in welk stadium bevinden we ons: lopend, afgesloten, …)? Wat zijn de gevolgen voor de organisatie?*

# Uitgevoerde DPIA’s

*In dit hoofdstuk overlopen we de DPIA’s die in het afgelopen jaar zijn uitgevoerd. Het is niet de bedoeling de volledige DPIA of alle risico’s hier te hernemen. Wel vatten we de DPIA samen. Neem zeker de volgende onderdelen mee in de samenvatting: waar ging de DPIA over, welk advies heeft DPO gegeven, en wat is er met dit advies gebeurd, verwijzing naar waar de DPIA zelf gevonden kan worden.*

## DPIA 1

# Inbreuken ten aanzien van de beveiliging \*

*Neem hier een verwijzing op naar het inbreukenregister of andere vastlegging waar alle inbreuken in terug te vinden zijn. Wij raden aan om, naast de algemene verwijzing naar het inbreukenregister, in het jaarverslag enkel die inbreuken te benoemen die hebben geleid tot een melding bij een autoriteit en dus van een bepaald risiconiveau zijn.*

*Indien dat er ook teveel zijn[[4]](#footnote-4) kan worden volstaan met een overzicht van de inbreuken die geleid hebben tot mogelijk hoge risico’s voor betrokkenen.*

## Inbreuk 1

### Context inbreuk

*Korte omschrijving van de inbreuk. Vermeld zeker de concrete data waarop de inbreuk is vastgesteld, wanneer de inbreuk is gemeld bij de autoriteit en verwijs naar de opgeslagen melding aan de autoriteit.[[5]](#footnote-5)*

### Gevolgen betrokkenen inbreuk

*Welke gevolgen had deze inbreuk (mogelijk) voor betrokkenen? Vermeld specifiek of de inbreuk ook gemeld is aan de betrokkenen en zo nee, waarom niet.*

### Maatregelen genomen n.a.v. inbreuk

*Geef een opsomming van de belangrijkste maatregelen (zie ook de inbreukenmelding zoals ingediend bij de autoriteit).*

# Rechten van de betrokkene

*Benoem hier op welke manier de organisatie te maken heeft gehad met ontvangen verzoeken van een betrokkene (tot inzage, wissing, verzet, data portabilititeit, etc). Afhankelijk van de organisatie en het aantal (de ene organisatie krijgt er geen, de andere honderden per jaar) is het de bedoeling om hier een overzicht te verschaffen van inzageverzoeken die zijn afgehandeld, of nog in behandeling zijn.*

*Verlopen deze vlot? Zijn het er veel? Zijn er specifieke problemen bij het invullen van inzageverzoeken in zijn algemeenheid, of bij welbepaalde verzoeken die mogelijk kunnen leiden tot een klacht?*

# Lopende activiteiten

*Andere belangrijke activiteiten die nuttig zijn om te vermelden?*

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Omschrijving | Wie? | Tegen wanneer? |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. <http://creativecommons.org/licenses/by/4.0/> [↑](#footnote-ref-1)
2. <https://etaamb.openjustice.be/nl/besluit-van-de-vlaamse-regering-van-23-november-2018_n2018015351.html> [↑](#footnote-ref-2)
3. Naast PrivCon, dé jaarlijkse Nederlandstalige privacyconferentie van Dasprive, die iedere DPO die dit leest uiteraard met stip in de agenda heeft staan. [↑](#footnote-ref-3)
4. Hopelijk niet, maar shit happens. Toch, UWV? <https://www.security.nl/posting/835468/UWV+en+SVB+hadden+duizend+datalekken+in+eerste+acht+maanden+2023> [↑](#footnote-ref-4)
5. Bewaar altijd een kopie van het ingediende meldingsformulier bij de autoriteit. Verwijs hier naar de locatie van de kopie. [↑](#footnote-ref-5)