
# DE IMPACT VAN GDPR / AVG OP HET SURINAAMS BEDRIJFSLEVEN

IBDO

# WELKE VRAGEN HEBBEN U EN IK?

- Zijn wij voorbereid?
- Wat is GDPR / AVG precies?
- Moeten, willen we GDPR / AVG compliant zijn?
- (Hoe) kunnen we GDPR / AVG compliant zijn?

- Wat moeten we doen om GDPR / AVG compliant te zijn?
- Hoe pakken we GDPR / AVG programma gestuctureerd aan?

# ZIJN WIJ VOORBEREID?

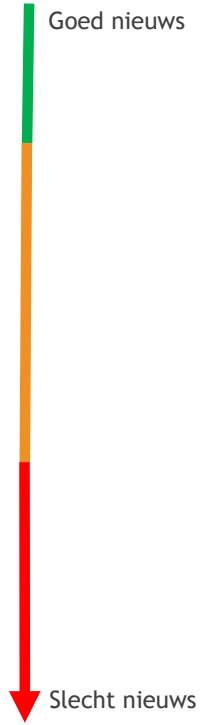
## Resultaten van de mini enquête

| MANAGEMENT DASHBOARD | SCHAAL |
|---|---|
| | 0% 100% |
| 1. Organisatorische maatregelen | |
| 2. Privacy bewustzijn | |
| 3. Gegevensregister | |
| 4. Verwerking | |
| 5. Gegevensbeschermingseffectbeoordeling | |
| 6. Rechten van betrokkenen | |
| 7. Datalek notificatie | |

# WAT IS GDPR / AVG PRECIES?

## Goed en slecht nieuws m.b.t. deze wet?

- Per 25 mei 2018 van kracht, maar ook veel bedrijven in EU zijn nog lang niet gereed (in Nederland is slechts 21% compliance tot nu toe)
- Autoriteit Persoonsgegevens heeft geen juridische bevoegdheden in SU
- Er bestaat 1 (een) verordening, maar per land een uitvoeringwet, bedoeld om invulling te geven aan de verordening en deze kunnen van elkaar verschillen
- (Gevoelige) persoonsgegevens van betrokkenen die zijn/haar woonplaats heeft binnen de EU, onafhankelijk van zijn/haar nationaliteit
- (Gevoelige) persoonsgegevens van betrokkenen in relatie tot een onderneming die gevestigd is in de EU, onafhankelijk van betrokkenen en verwerkingslocatie



# WAT IS GDPR / AVG PRECIES?

## Is de verordening op mij van toepassing?


**Niet persoonlijke gegevens**
Gegevens welke niet gerelateerd zijn aan herkenbare (identificeerbaar) personen

**Persoonlijke gegevens**
Informatie die betrekking heeft op geïdentificeerde of identificeerbare personen. Een persoon die direct of indirect kan worden geïdentificeerd met deze categorie van gegevens

**Gevoelige, persoonlijke gegevens**
Speciale categorie van persoonsgegevens, die lichamelijke of geestelijke status van een persoon onthullen. Bijvoorbeeld seksuele geaardheid, etniciteit, geloofsovertuiging

# WAT IS GDPR / AVG PRECIES?

## Wat zijn de 8 beginselen van verwerking van persoonsgegevens?

- **Rechtmatig en behoorlijk**
  De gegevens moeten rechtmatig, eerlijk en transparant worden verwerkt ten aanzien van de betrokkene.

- **Transparant (en eerlijk)**
  Begrijpelijk en gemakkelijke toegankelijke vorm, in duidelijke en eenvoudige taal.

- **Doelbinding**
  De gegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld.

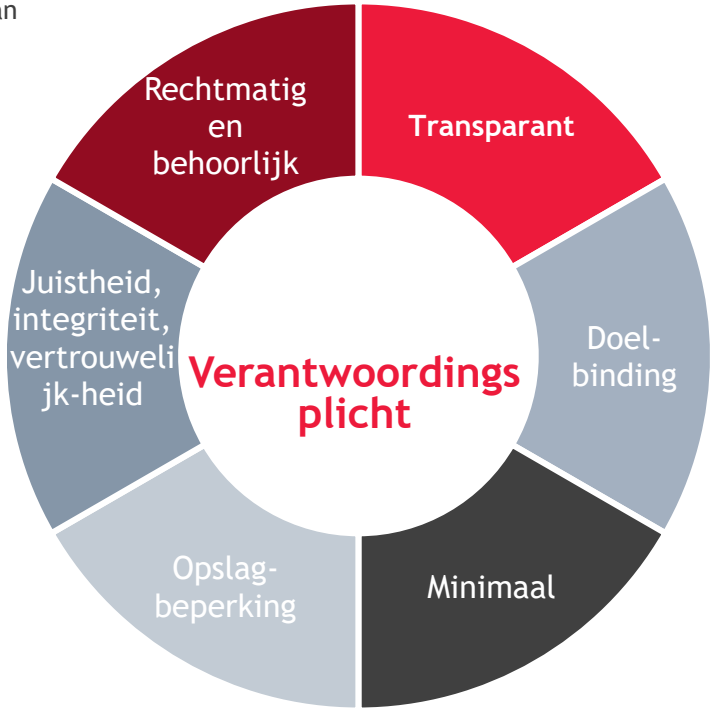
- **Minimaal**
  Verwerking is beperkt tot wat noodzakelijk is voor het doeleinde waarvoor verwerkt.

- **Juistheid**
  Gegevens worden zo nodig geactualiseerd.

- **integriteit en vertrouwelijkheid**
  Passende technische en organisatorische maatregelen voor bescherming tegen onrechtmatige verwerking en verlies, vernietiging of beschadiging van gegevens.

- **Opslagbeperking**
  gegevens worden niet langer bewaard dan noodzakelijk voor verwerking.

- **Verantwoordingsplicht**
  De verwerkingsverantwoordelijke is verantwoordelijk voor naleving en kan deze aantonen.



# WAT IS GDPR / AVG PRECIES?

## Wie zijn wij precies?

- Zijn wij een verwerkingsverantwoordelijke, die doel en middel van de verwerking bepaalt
- Zijn wij een verwerkingsverantwoordelijke, die samen met andere verwerkingsverantwoordelijke, doel en middel van de verwerking bepaalt
- Zijn wij een verwerker, die namens een verwerkingsverantwoordelijke, de persoonsgegevens verwerkt
- Zijn wij een (sub)verwerker, die namens een andere verwerker, persoonsgegevens verwerkt

# WAT IS GDPR / AVG PRECIES?

## Welke 12 rechten hebben betrokkenen?

- Recht op informatie over de verwerking
- Recht op inzage in zijn/haar gegevens
- Recht op correctie van gegevens, die niet kloppen
- Recht op verwijdering, vergeten te worden
- Recht op beperking van de gegevensverwerking
- Recht op verzet tegen gegevensverwerking
- Recht op overdracht van zijn/haar gegevens
- Recht op niet onderworpen te zijn aan geautomatiseerde verwerking
- Recht op een klacht bij de toezichthouder
- Recht op doeltreffende voorziening in rechte
- Recht op vertegenwoordiging
- Recht op schadevergoeding

# MOETEN, WILLEN WE GDPR / AVG COMPLIANT ZIJN?

## Is het een kwestie van MOETEN of WILLEN?

- GDRP / AVG compliant als verplichte naleving van toepasselijke wet- en regelgeving
- GDPR / AVG compliant als “License to Operate”
- GDPR / AVG compliance als strategische keuze om onderscheidend te zijn

# MOETEN, WILLEN WE GDPR / AVG COMPLIANT ZIJN?

## Wanneer is de verordening van toepassing voor SU bedrijven (MOETEN)?

- SU Organisaties die goederen en diensten aanbieden of voornemens zijn geweest deze aan te bieden, aan betrokkenen die zich in de EU bevinden en daartoe persoonsgegevens verwerken

- SU organisatie, die gedrag van personen monitoren, voor zover gedrag binnen EU plaatsvindt (b.v. volgen van personen via Web t.b.v. klantprofilering)

- SU organisatie die diensten aanbiedt aan organisaties die in de EU zijn gevestigd, en die persoonsgegevens verwerkt, onafhankelijk wie de betrokkenen zijn en waar de verwerking plaatsvindt

# (HOE) KUNNEN WE GDPR / AVG COMPLIANT ZIJN?

## Wat zijn de 10 stappen op weg naar GDRP/AVG compliance?

1. **Bewustwording**
   Zorg ervoor dat de relevante mensen in uw organisatie op de hoogte zijn van de nieuwe privacyregels.

2. **Rechten van betrokkenen**
   Zorg ervoor dat betrokkenen hun verbeterde privacy rechten goed kunnen uitoefenen.

3. **Overzicht verwerkingen**
   Onder de AVG heeft u een documentatieplicht. Documenteer welke persoonsgegevens u verwerkt, met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt.

4. **Privacy Impact Assessment**
   U moet een PIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacy risico met zich meebrengt.

5. **Privacy-by-Design & Privacy-by-Default**
   Ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

6. **Functionaris Gegevensbescherming**
   Bepaal of uw organisatie verplicht is om een FG aan te stellen.

7. **Meldplicht Datalekken**
   De AVG stelt strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. Zorg ervoor dat u moet alle datalekken documenteert.

8. **Bewerkersovereenkomsten**
   Beoordeel of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds voldoen aan de vereisten in de AVG.

9. **Leidende Toezichthouder**
   Indien uw gegevensverwerkingen in meerdere EU-lidstaten impact hebben dan hoeft u onder de AVG nog maar met één privacy toezichthouder te werken.

10. **Toestemming**
    De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert.

# (HOE) KUNNEN WE GDPR / AVG COMPLIANT ZIJN?

## Waar moeten we nog meer rekening mee houden?

- Relatie met SU wetgeving (wet op elektronisch rechtsverkeer en wet op Toezicht kredietwezen)

- Relatie met internationale kwaliteitsstandaarden, die vaak hun oorsprong hebben in EU

- USA, ACP en andere landen zijn ook bezig aan het voorbereiden. Er bestaat een grote kans dat zij deze regelgeving misschien in enigszins gewijzigde vorm overnemen. Wij zijn dan niet ver verwijderd van een wereldwijde standaard. Dus vroege voorbereiding is een luxe

# WAT MOETEN WE DOEN OM GDPR / AVG COMPLIANT TE ZIJN?

## Privacy & Security

- Privacy compliance beschrijft de regels en standaarden die geïmplementeerd moeten worden om de privacy van persoonsgegevens te beschermen.
- Security compliance beschrijft de regels en standaarden die geïmplementeerd moeten worden om alle relevante bedrijfsgegevens te beschermen.
- Privacy en security zijn dus sterk aan elkaar gerelateerd en overlappen elkaar deels op het gebied van beveiligingsmaatregelen.
- Vertrouwelijkheid is het belangrijkste kwaliteitsaspect voor privacy; vertrouwelijkheid, beschikbaarheid en integriteit zijn de belangrijkste kwaliteitsaspecten met betrekking tot security.
- Tegelijkertijd is privacy compliance wettelijk verplicht en vereist dit afzonderlijke identificatie en classificatie van persoonsgegevens en afzonderlijke maatregelen met betrekking tot opslag, verwerking en vernietiging van persoonsgegevens.

# WAT MOETEN WE DOEN OM GDPR / AVG COMPLIANT TE ZIJN?

## Kwaliteitscriteria

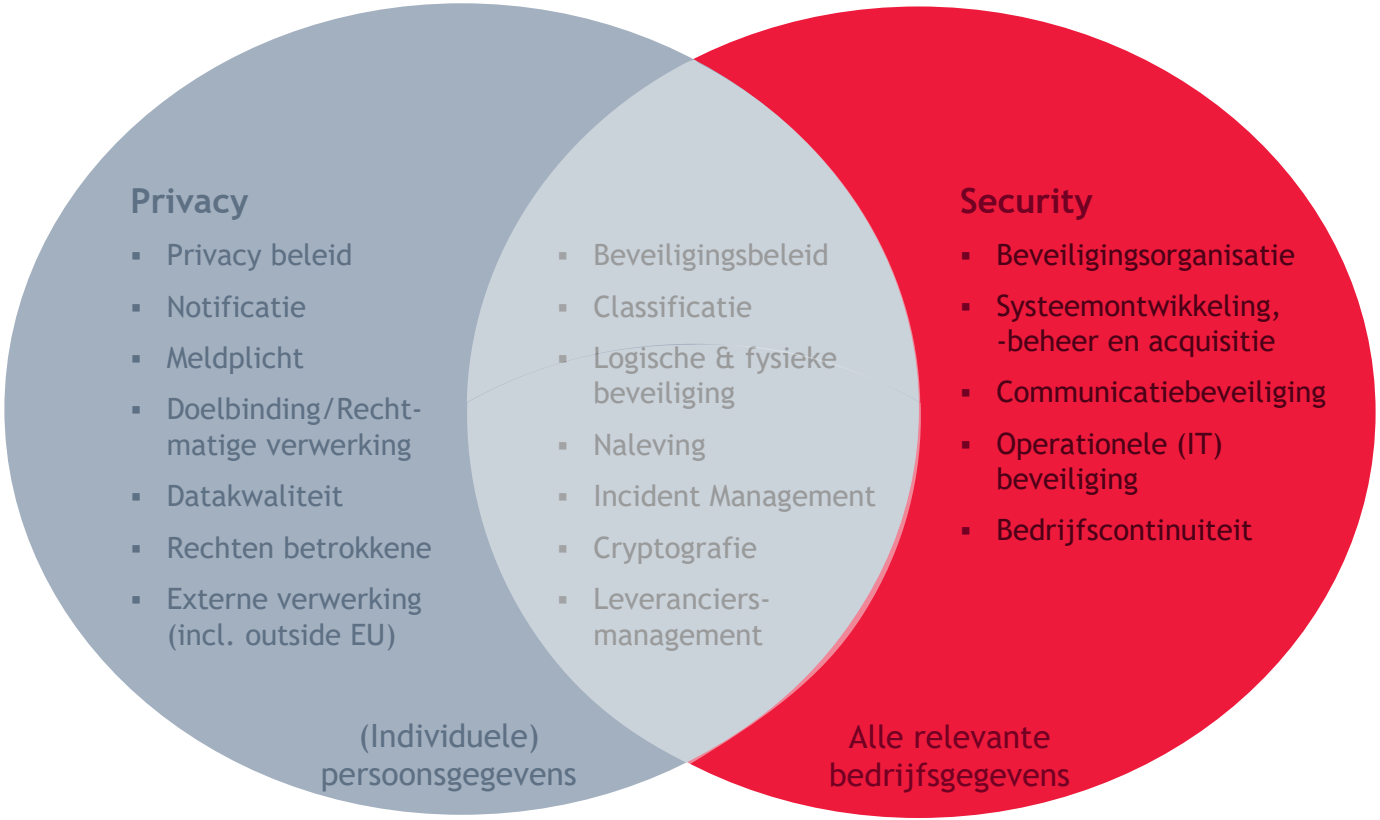
- **Vertrouwelijkheid:**
  De mate waarin uitsluitend geautoriseerde personen via geautoriseerde procedures en beperkte bevoegdheden kennisnemen van gegevens. (Vertrouwelijkheid kan worden gezien als een subset van exclusiviteit).
- **Exclusiviteit:**
  De mate waarin uitsluitend geautoriseerde personen of apparatuur via geautoriseerde procedures en beperkte bevoegdheden gebruikmaken van een object (IT-dienst of IT-middel) of toegang hebben tot een object (creëren, wijzigen, verwijderen of lezen van gegevens).
- **Beschikbaarheid:**
  De mate waarin een object (informatie, IT-dienst of IT-middel) continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben.
- **Integriteit:**
  De mate waarin het object (gegevens, IT-dienst of IT-middel) in overeenstemming is met de beoogde werkelijkheid.



BDO

# HOE PAKKEN WE GDPR / AVG PROGRAMA GESTRUCTUREERD AAN?

## Welke IT maatregelen moeten (kunnen) wij alvast nemen?



# HOE PAKKEN WE GDPR / AVG PROGRAMA GESTRUCTUREERD AAN?

## Welke organisatorische maatregelen moeten (kunnen) wij alvast nemen?

- Wijs een functionaris gegevensbescherming of DPO aan
- Inventarisatie en classificatie van persoonsgegevensverwerking
- Verwerkingsovereenkomsten voor sub-verwerkers opstellen indien van toepassing
- Awareness campagne voor de interne organisatie
- Installeren van een multidisciplinair projectteam, bemenst o.a. met een jurist, een IT deskundige, proceseigenaren, hoofd IAD en CMD
- C-level sponsorship door COO of CRO
- Periodiek uitvoeren van een GDPR Readiness Assessment, als een soort business case
- Ontwikkel, al dan niet in samenwerking met uw accountant/adviseur, een GDPR/AVG tool box, toegesneden op uw specifieke situatie

# HOE PAKKEN WE GDPR / AVG PROGRAMMA GESTRUCTUREERD AAN?

## Voorbeeld BDO GDPR Toolbox (intern gebruik).

- **Algemeen**
  - Privacybeleid document
  - Effect privacy beleidsregels op functioneren organisatie(eenheden)
  - Checklist van beleid en procedures om GDPR readiness te implementeren
  - Implicatie voor de organisatie als “verwerkingsverantwoordelijke” en als “verwerker”
  - Stroomdiagram om grondslag van de verwerking te bepalen


- **Transparantie**
  - Privacy verklaring t.b.v. verschillende categorieën betrokkenen (personeel, klanten, sollicitanten, leveranciers)
  - Privacy verklaring t.b.v. leveranciers, derden die goederen, diensten leveren aan de organisatie
  - Privacy verklaring t.b.v. websites en cookies
  - Privacy verklaring t.b.v. klantprofilering en ander marketinguitingen
  - Templates voor GDPR compliant clausules voor contracten, die men aan kan gaan
- **Data kwaliteit**
  - Beleidsdocument m.b.t. archivering en verwijdering van persoonsgegevens
  - Vragenlijst t.b.v. gegevensverwerkingseffectbeoordeling (DPIA)
  - Vragenlijst t.b.v. privacy effectbeoordeling (PIA)
  - Template t.b.v. rapportage DPIA resultaten
  - Tool voor inventarisatie/vastlegging van gegevensverwerking processen als ‘verantwoordelijke” en als “verwerker”
  - Tool voor inventarisatie/vastlegging verwerkte gegevens

# HOE PAKKEN WE GDPR / AVG PROGRAMMA GESTRUCTUREERD AAN?

## Voorbeeld BDO GDPR Toolbox (intern gebruik).

- **Individuele rechten**
  - Procedures voor beantwoorden vraag van betrokkenen om toegang tot persoonsgegevens
  - Beleid en richtlijnen m.b.t. direct marketing
- **Beveiliging**
  - Inventarisatie/vastlegging impact GDPR op IT beveiliging regiem en infrastructuur
  - Due diligence procedure voor identificeren en selecteren van een externe dienstverlener
  - Beleid en procedures voor omgaan met datalekken
- **Derden**
  - Standaard gegevensverwerkingscontract voor verwerking binnen SU
  - Standaard gegevensverwerkingscontract voor verwerking buiten SU

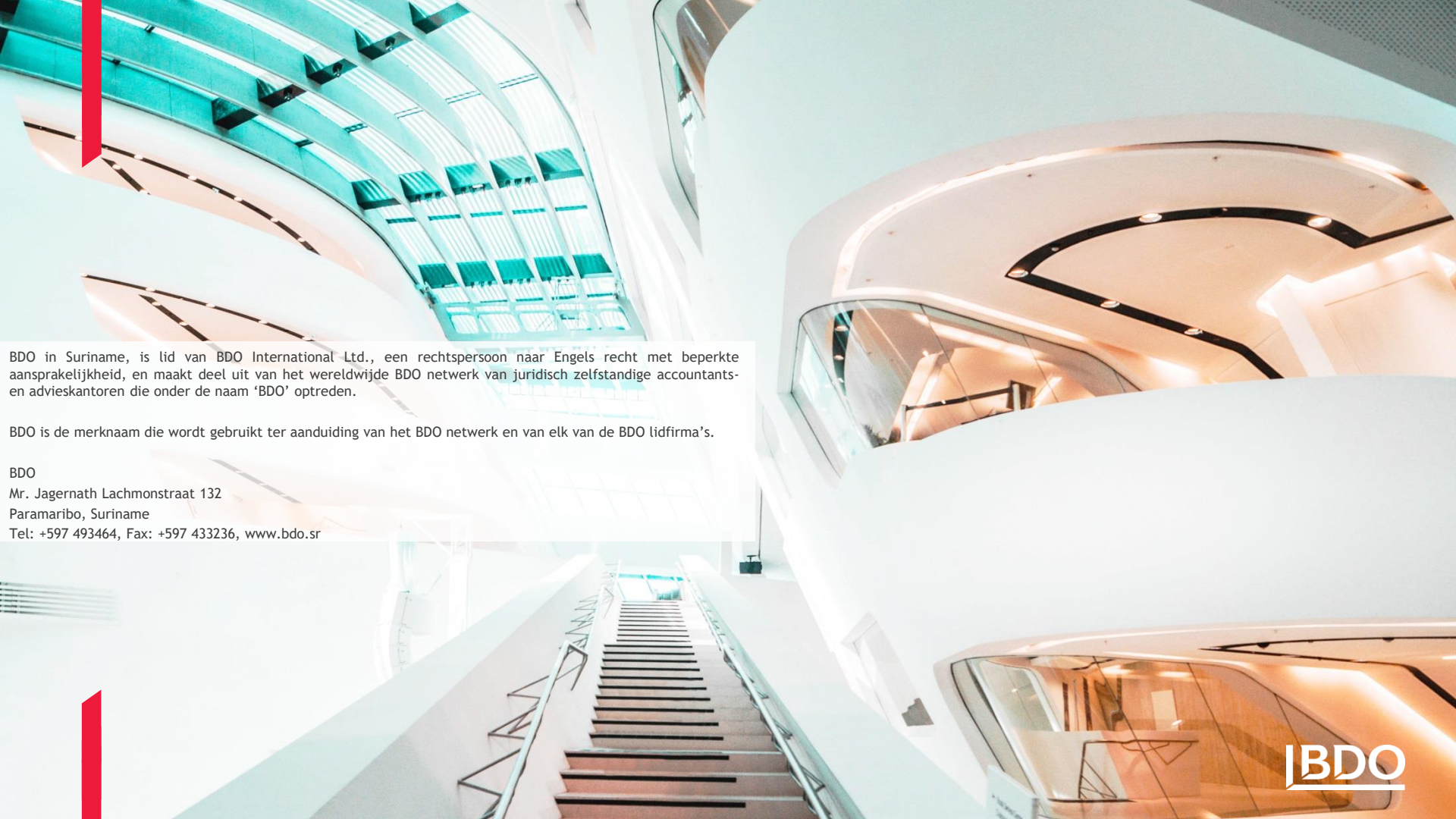

Interne Bulletin Board om informatie en kennis te delen binnen de organisatie m.b.t. GDPR/AVG

# Algemene Verordening Gegevensbescherming in vogelvlucht

**Een aantal speerpunten**

| | | |
|---|---|---|
| Boetes (€20.000.000 of 4% wereldwijde omzet) | Meldplicht Datalekken | Functionaris Gegevensbescherming |
| Strengere informatieverplichting | Verwerking gegevens kinderen (< 16 jaar) | Recht om vergeten te worden |
| Meer aandacht voor plichten verwerker | Verbetering rechten van betrokkenen | Verplichting tot Privacy-by-Design en Privacy-by-Default |

BDO





BDO
Mr. Jagernath Lachmonstraat 132
Paramaribo, Suriname
Tel: +597 493464, Fax: +597 433236, www.bdo.sr