Nieuwe Privacywetgeving

AVG - GDPR

Nieuwe wind, maar geen orkaan!

Wat

- **AVG**: Algemene Verordening Gegevensbescherming
- **GDPR**: General Data Protection Regulation (99 artikelen, 173 overwegingen, 88 blz)
- 7 basisbeginselen

Waarom

- Nood aan **harmonisatie** van de nationale privacywetgevingen binnen Europa
- Aanpassen van regels aan nieuwe **digitale realiteit**
- Burger **meer controle** geven over zijn gegevens

Wie

- Bedrijven & zelfstandigen
- organisaties & vzw's
- … iedereen die gegevens van burgers verwerkt

Wanneer

- 25 mei 2018

Definities

Persoonsgegevens

- Iedere informatie betreffende een identificeerbare natuurlijke persoon

Gezondheids- of medische gegevens

- Gegevens die door hun aard informatie verschaffen over de fysieke of mentale toestand van de betrokkene

Verwerking

- Elke bewerking met betrekking tot persoonsgegevens

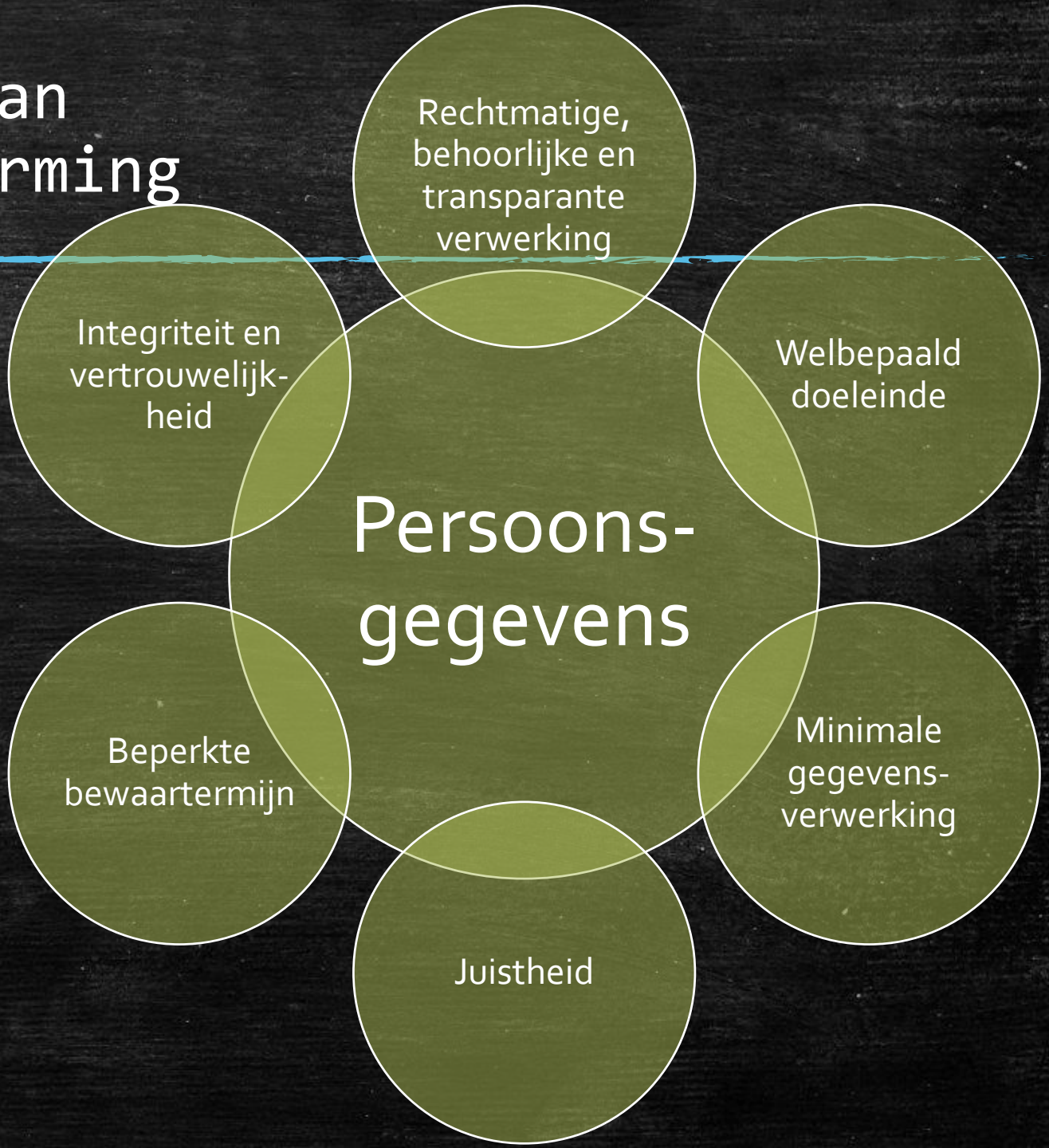
Betrokkene

- De natuurlijke persoon waarvan gegevens worden bewaard

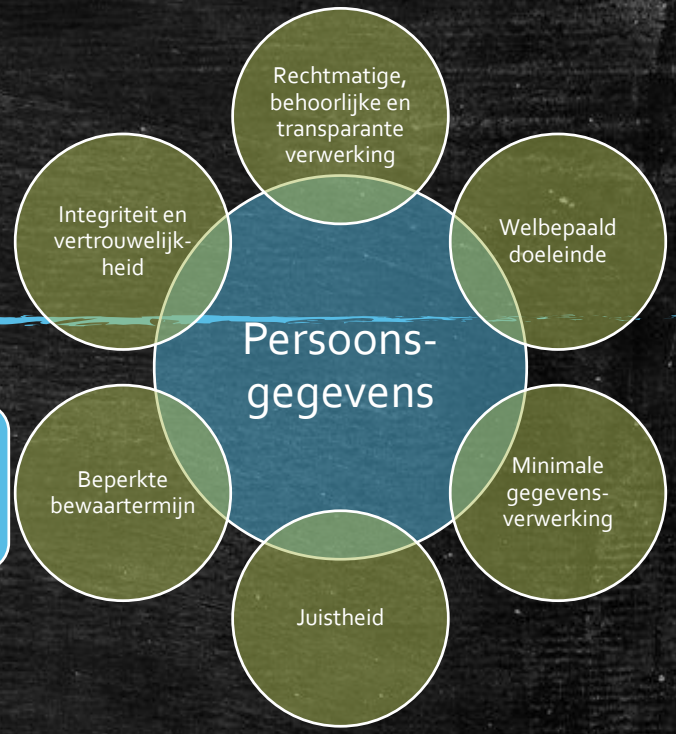
Verwerker

- De persoon of instantie die de gegevens van de betrokkene verwerkt

Basisbeginselen van de gegevensbescherming



Persoonsgegevens

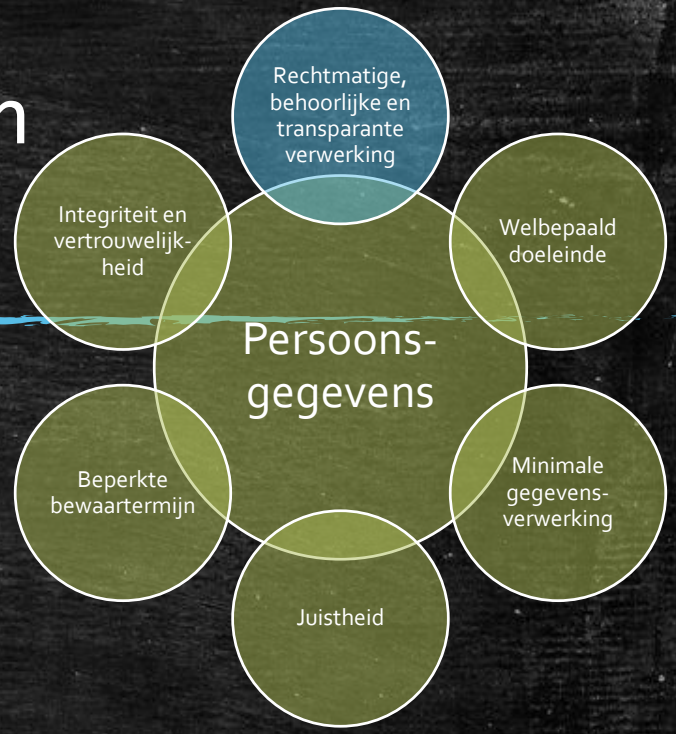


iedere informatie betreffende een persoon die rechtstreeks of onrechtstreeks geïdentificeerd kan worden. Bijvoorbeeld:

- een gebruikersnaam
- een naam
- een foto
- een nummer van de sociale zekerheid
- een intern registratienummer
- een nummerplaat
- een postadres
- een telefoonnummer,
- locatiegegevens
- …

De nieuwe privacywetgeving is niet van toepassing op de gegevens van overleden personen.

rechtmatigheid, behoorlijkheid en transparantie



Gerechtvaardigde verwerkingsgrond

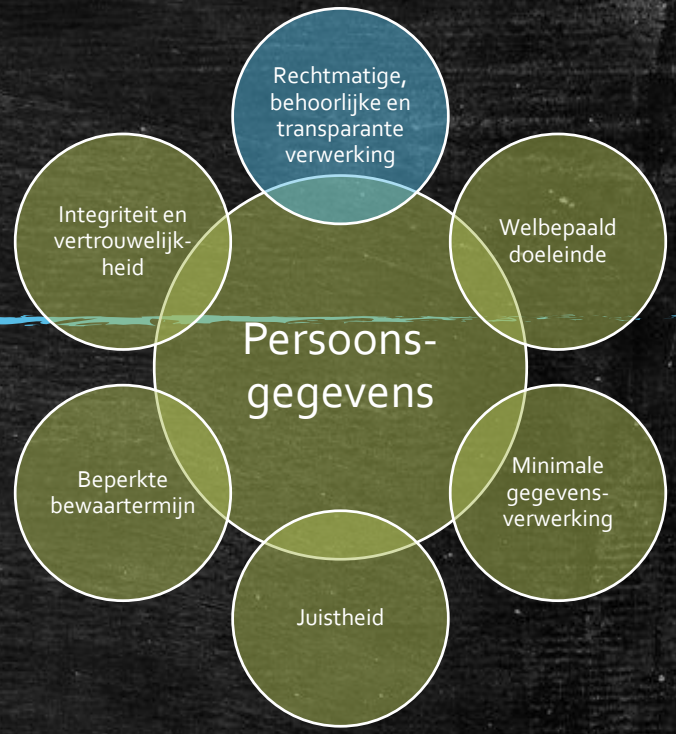
Eerlijke, loyale verwerking

Informatie aan de betrokkene

- Duidelijke taal
- Regels, risico's en rechten

Rechtmatigheid van de verwerking

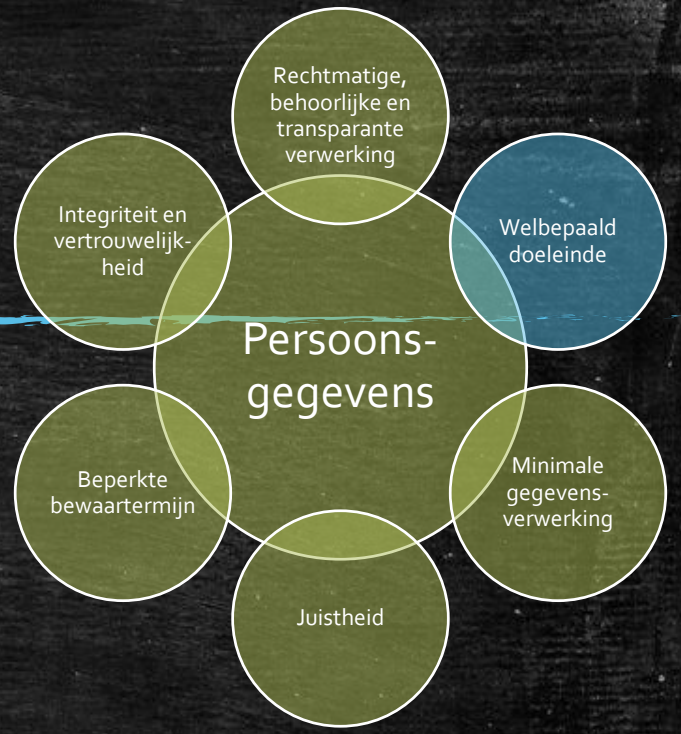
- Toestemming van de betrokkene
- Overeenkomst
- Wettelijke plicht
- Vitaal belang van de betrokkene of een ander persoon
- Algemeen belang
- Gerechtvaardigd belang



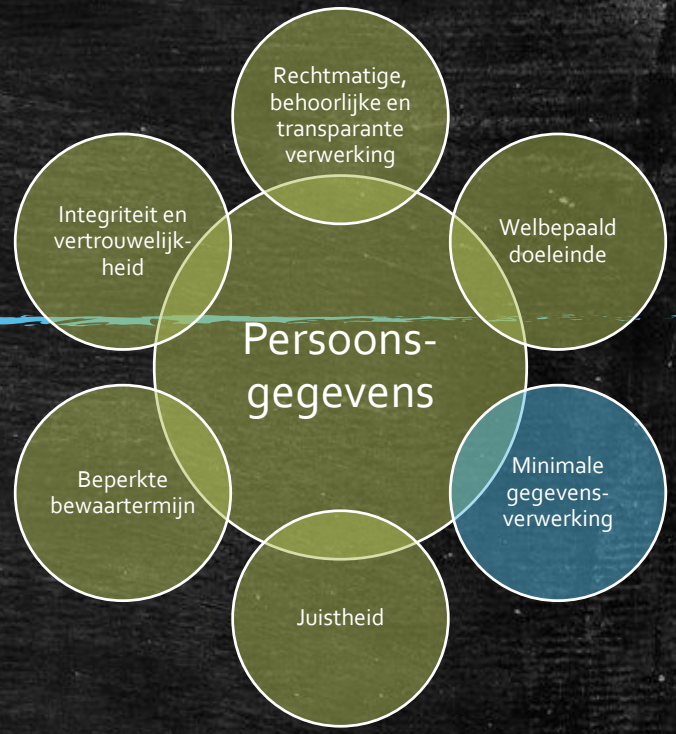
Doelbinding

Welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden

Geen verdere verwerking op een manier die onverenigbaar is met die doeleinden



Minimale gegevensverwerking

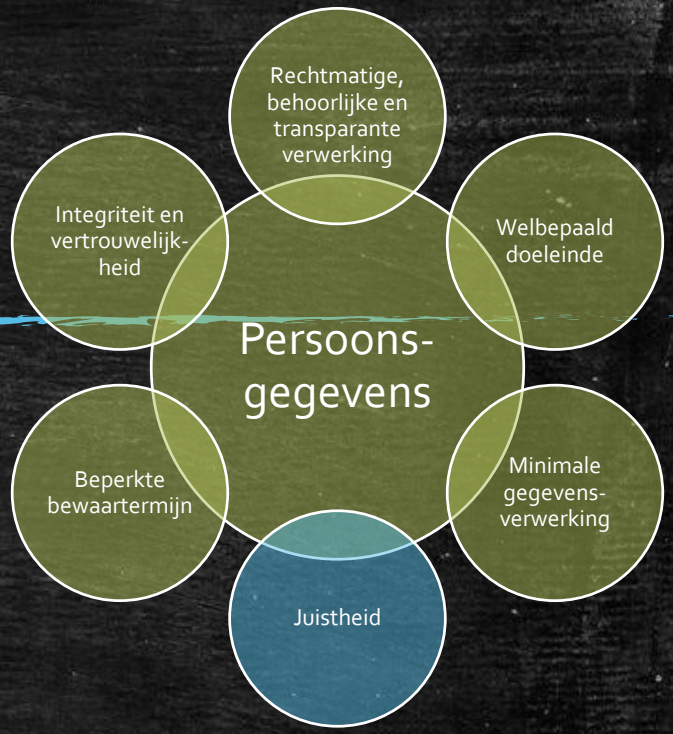


Toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor het doeleinde waarvoor de gegevens worden verwerkt

Verwerk dus enkel het strikte minimum

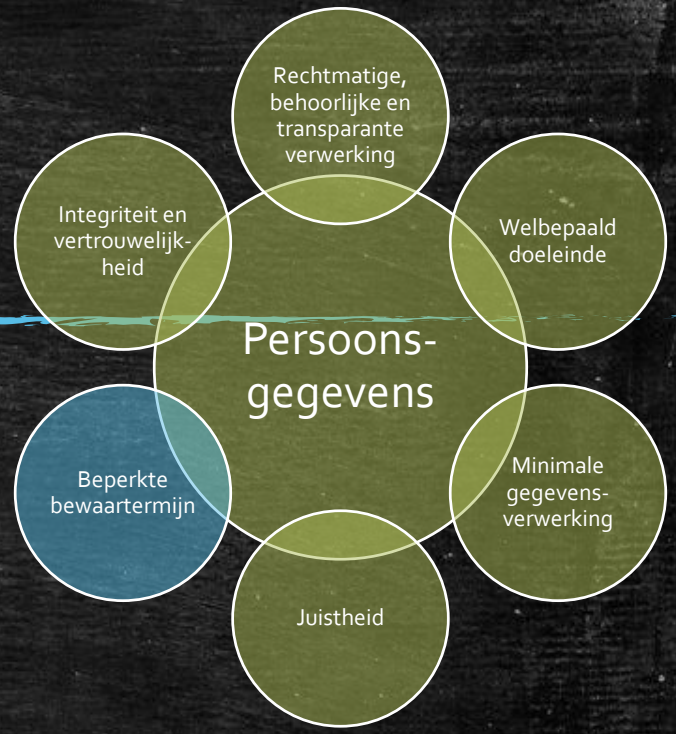
Het juistheidsbeginsel

De gegevens moeten accuraat zijn

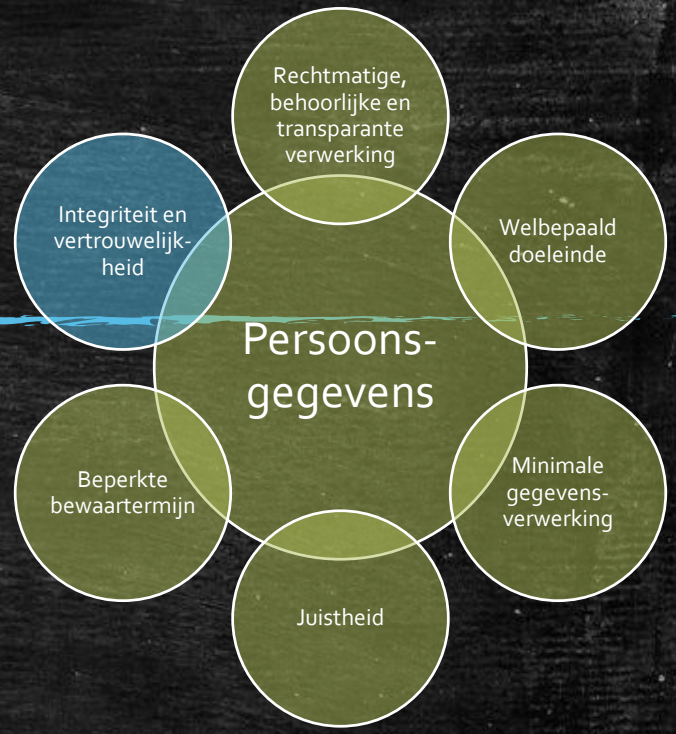


Het beginsel van de beperkte bewaartermijn

De gegevens mogen niet langer worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt



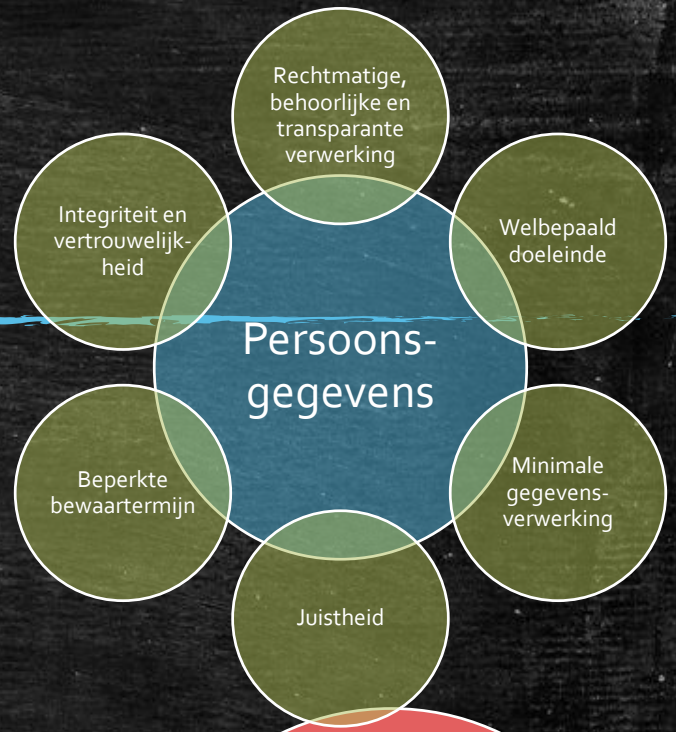
Het integriteits- en vertrouwelijkheidsbeginsel



Verwerking volgens afdoend veiligheidsniveau door gebruik te maken van passende, technische en organisatorische maatregelen

Bescherming tegen iedere niet toegelaten of onwettige verwerking, tegen verlies, vernietiging of kwaliteitsverlies van de gegevens

Bijzondere categorieën van persoonsgegevens



Verwerking van

- ras
- etnische afkomst
- politieke opvattingen
- religieuze of levensbeschouwelijke overtuigingen
- lidmaatschap vakbond

+

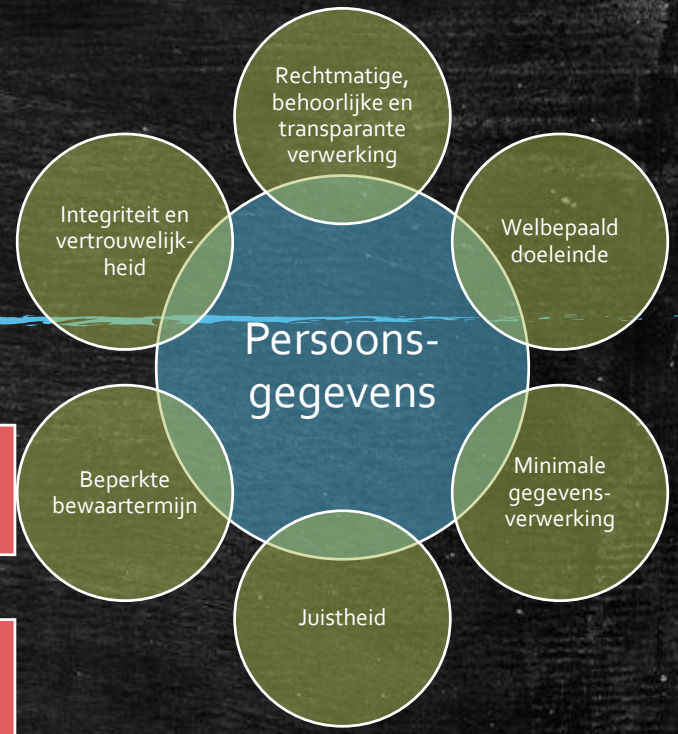
Verwerking van

- genetische gegevens
- biometrische gegevens met oog op unieke identificatie
- gegevens gezondheid
- gegevens over seksuele geaardheid of gedrag

=

Verboden
behalve als …

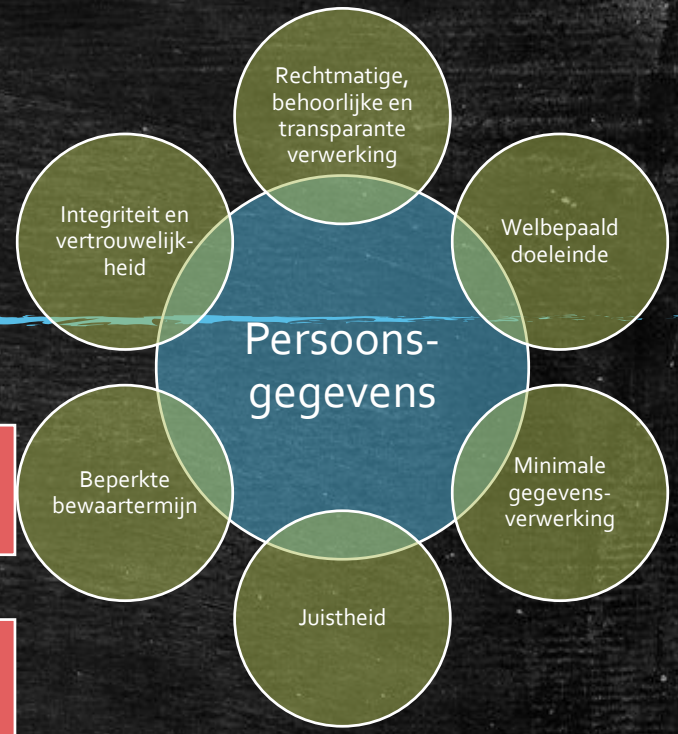
Uitzonderingen op principieel verwerkingsverbod (1)



- Uitdrukkelijke toestemming van de betrokkene
- de verwerking noodzakelijk is op gebied van het arbeidsrecht en socialezekerheidsrecht
- De verwerking noodzakelijk is om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen
- door een vereniging zonder winstoogmerk die op vakbondsgebied werkzaam is, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen
- de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt

Uitzonderingen op principieel verwerkingsverbod (2)

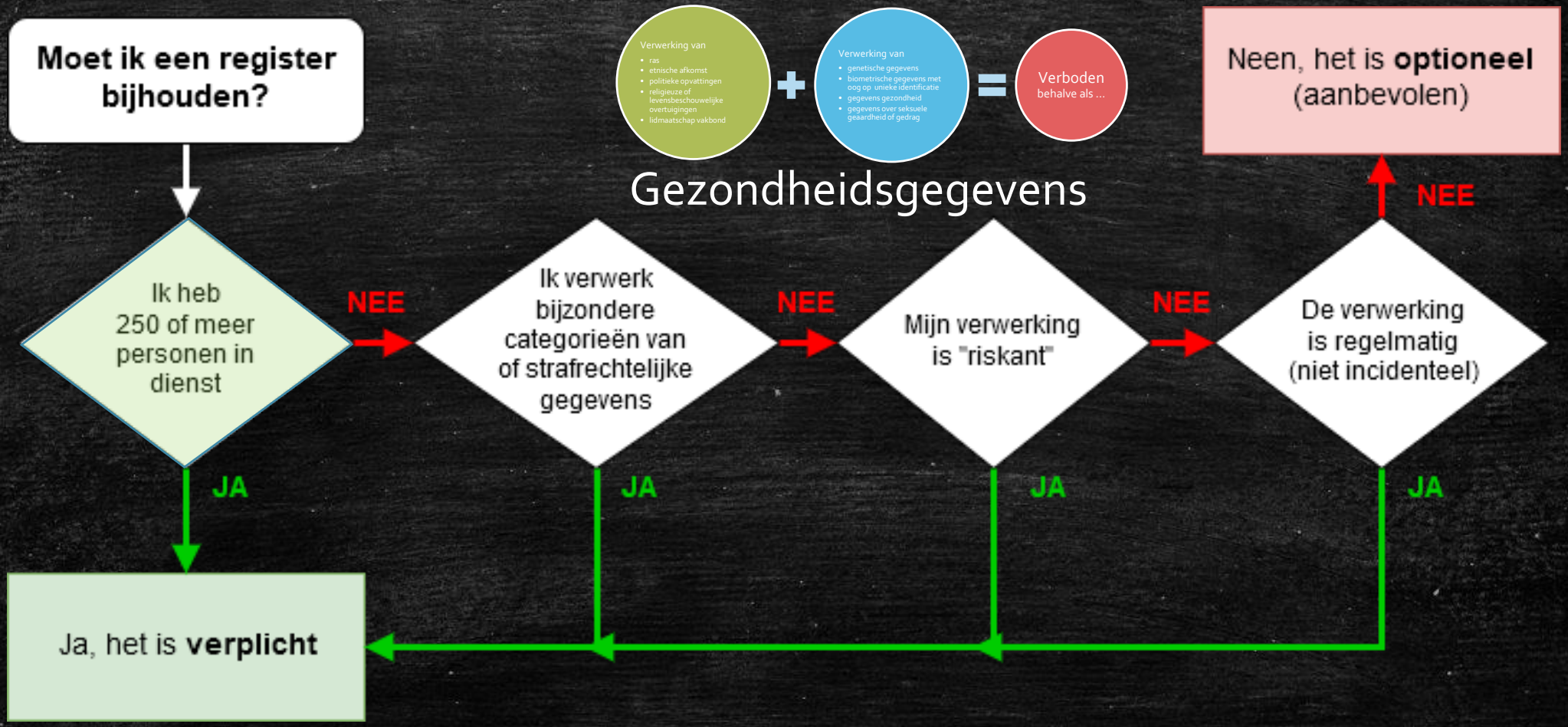
- de verwerking is noodzakelijk voor de vaststelling, de uitoefening of de verdediging van een recht in rechten
- de verwerking is noodzakelijk wegens gewichtige redenen van algemeen belang
- de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, de beoordeling van de arbeidsgeschiktheid van de werknemer of medische diagnoses
- de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van volksgezondheid
- de verwerking is noodzakelijk voor archivering in het algemeen belang, voor wetenschappelijk of historisch onderzoek of statistische doeleinden



Hoe aanpakken?

13 Stappenplan

2 Moet ik een verwerkingsregister bijhouden?



Rechten van de betrokkene

De betrokkene heeft recht op

- informatie
- toegang tot persoonsgegevens
- verbetering
- vergeten te worden
- beperking van de verwerking
- bezwaar
- verzet tegen geautomatiseerde besluitvorming, inclusief profilering
- overdraagbaarheid van gegevens

Betrokkene heeft recht op toegang

Privacy verklaring

Welke data

- Of er data worden verwerkt
- Zo ja, toegang en informatie verschaffen over de verwerking: welke data, welk doel, bewaartermijn, …
- Informeren over partners met wie je de data deelt

Recht op de data

- Verwerkingsverantwoordelijke verschaft kosteloze kopie van de data aan de betrokkene
- Extra kopieën kunnen aangerekend worden
- Zonder afbreuk te doen aan de rechten van anderen: beroepsgeheim, intellectueel eigendomsrechten, copyright

Betrokkene heeft recht op verbetering

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke verbetering van de hem betreffende onjuiste gegevens te verkrijgen

Rekening houdende met de doeleinden van de verwerking, heeft de betrokkene het recht vervollediging van onvolledige gegevens te verkrijgen, o.m. door aanvullende info te verstrekken

Betrokkene heeft recht op gegevenswissing

Onmiddellijke wissing

- Gegevens zijn niet langer noodzakelijk voor de doeleinden
- Betrokkene trekt de toestemming in waarop verwerking is gesteund
- Betrokkene maakt bezwaar tegen de verwerking
- Gegevens zijn onrechtmatig verwerkt
- Gegevens moeten worden gewist om te voldoen aan wettelijke verplichting
- Gegevens zijn verzameld in verband met een aanbod van diensten, als bedoeld in artikel 8 (1)

t.a.v. derde partijen

- Als de verwerkingsverantwoordelijke de gegevens openbaar heeft gemaakt, neemt hij, rekening houdend met de beschikbare technologie en kosten, redelijke maatregelen om derde partijen met wie de gegevens werden gedeeld ervan op de hoogte te brengen dat betrokkene elke link, of kopie of reproductie van die gegevens wenst te wissen.

Uitzonderingen voor betrokkene op recht om vergeten te worden

- Voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
- Voor het nakomen van een wettelijke verwerkingsplicht of voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag
- Om redenen van algemeen belang op gebied van volksgezondheid
- Met het oog op archivering, wetenschappelijk of historisch onderzoek of statistische doeleinden
- Voor de instelling, uitoefening of onderbouwing van een rechtsvordering

5 Verzoek tot toegang

- Iedere betrokkene heeft het recht om zijn gegevens in te zien!
- Hoe ga je dit realiseren?

10 Bescherming/beveiliging van gegevens

- Privacywet – Artikel 16. §4
  - Om de veiligheid van de persoonsgegevens te waarborgen, (moeten de verantwoordelijke van de verwerking, en in voorkomend geval zijn vertegenwoordiger in België, alsmede de verwerker, de gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de bescherming van de persoonsgegevens) tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

Pauze

13 stappenplan

Gedetailleerde informatie bij elke stap in het plan

1 Bewustmaking

- Zorg dat de sleutelfiguren en beleidsmakers in jouw bedrijf of organisatie op de hoogte zijn van de regelgeving.
  - Zij moeten de gevolgen hiervan inschatten en aanwijzen welke domeinen vandaag mogelijks problematisch kunnen zijn in het licht van de nieuwe privacywetgeving. Indien jouw bedrijf of organisatie over een risicoregister beschikt, kan dit een werkbaar vertrekpunt zijn.
  - Het implementeren van de nieuwe privacywetgeving kan een behoorlijke invloed hebben op de beschikbare middelen, zeker voor wat betreft grote en meer complexe bedrijven of organisatiestructuren. Ga na of er voor jouw sector modellen bestaan of gedragscodes ontwikkeld werden door de sectorverenigingen.

2 Register van verwerkingsactiviteiten

- Breng zorgvuldig in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld.
  - Je doet er goed aan al je verwerkingen te registreren. Mogelijks dien je hiervoor een informatie-audit te organiseren. Dit kan dan van het volledige bedrijf of enkel van welbepaalde afdelingen.
  - De AVG geeft de betrokkenen een aantal rechten, specifiek op maat van de netwerkwereld. Wanneer jouw bedrijf bijv. onnauwkeurige persoonsgegevens bijhoudt, en heeft gedeeld met andere organisaties, zal je deze laatste moeten inlichten over de onnauwkeurigheid zodat deze een correctie kan aanbrengen in haar eigen gegevens. Deze documentatieplicht helpt je bovendien de verantwoordelijkheidsvereiste uit de AVG na te leven. Volgens dit principe dient een bedrijf of organisatie te bewijzen dat ze in overeenstemming met de gegevensbeschermingsprincipes handelt.

- Om hierbij te helpen, stelt de Autoriteit op haar website een modelregister van verwerkingsactiviteiten ter beschikking met een bijbehorende handleiding.

3 Communicatie

- Evalueer je bestaande privacyverklaring en bekijk deze in het licht van de nieuwe privacywetgeving.
  - Wanneer jouw bedrijf of organisatie persoonsgegevens verwerkt, dien je aan de betrokkene bepaalde informatie te verschaffen, zoals de identiteit van de verwerker en de wijze waarop die de gegevens zal aanwenden. Doorgaans wordt deze informatie verstrekt in de vorm van een privacyverklaring.
  - De nieuwe privacywetgeving stelt inhoudelijke eisen aan deze privacyverklaring. Zo zal je de wettelijke grondslag voor de gegevensverwerking moeten meedelen, de termijnen gedurende dewelke je de informatie zal bijhouden, of je de gegevens uitwisselt buiten de Europese Unie en de mogelijkheid voor de betrokkene om een klacht in te dienen bij de toezichthoudende autoriteit indien deze meent dat zijn persoonsgegevens foutief worden verwerkt. De nieuwe privacywetgeving vereist dat deze informatie wordt verschaft in beknopte, begrijpbare en duidelijke taal.

4 Rechten van de betrokkene

- Je dient na te gaan of de procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.
  - De nieuwe privacywetgeving voorziet o.a. in de volgende rechten voor de betrokkene:
    - Informatie en toegang tot persoonsgegevens;
    - Correctie en uitwissing van de gegevens;
    - Bezwaar tegen direct marketingpraktijken;
    - Bezwaar tegen geautomatiseerde besluitvorming en profilering;
    - Overdraagbaarheid van de gegevens.
  - Zorg voor draaiboeken die uitstippelen wat te doen wanneer iemand zijn of haar recht wil uitoefenen. Wie neemt de beslissing? Zijn je systemen hiertoe uitgerust?
  - Het recht op overdraagbaarheid van de gegevens verdient bijzondere aandacht. Dit is een versterkte vorm van toegang waarbij de betrokkene het recht heeft de persoonsgegevens die op hem van toepassing zijn in een gestructureerde, gangbare en elektronische vorm te verkrijgen. De meeste bedrijven en organisaties deden dit al, maar let er op dat papieren print-outs of een ongebruikelijke elektronische vorm niet volstaan voor de nieuwe privacywetgeving.
  - Doe je aan geautomatiseerde individuele besluitvorming? Wees je dan bewust van de bijzondere spelregels die hiervoor gelden onder de nieuwe privacywetgeving.

5 Verzoek tot toegang

- Bedenk hoe je verzoeken tot toegang zal behandelen onder de termijnen in de nieuwe privacywetgeving en voorzie eventueel een update van je bestaande toegangsprocedures.
  - De nieuwe privacywetgeving legt vast hoe met toegangsverzoeken om te gaan. In de meeste gevallen moet gratis en binnen de 30 dagen gevolg worden gegeven aan het verzoek tot toegang. Manifest ongegronde of overmatige verzoeken kunnen worden aangerekend of worden geweigerd. Indien jouw bedrijf of organisatie in staat wil zijn om toegangsverzoeken te weigeren, moet je daarvoor een beleid en aangepaste procedures hebben.
  - Je dient de betrokkene die om toegang verzoekt bepaalde bijkomstige informatie te verschaffen, zoals de termijnen gedurende dewelke je informatie bijhoudt en het recht om onnauwkeurige gegevens te laten verbeteren. Indien jouw bedrijf of organisatie een groot aantal toegangsverzoeken behandelt, is een goed draaiboek cruciaal. Het moet logistiek mogelijk zijn om alle verzoeken binnen de voorziene tijdspanne te verwerken en de betrokkene van de noodzakelijke informatie te voorzien. Hierover moet zorgvuldig worden nagedacht.
  - Op termijn kan het kostenbesparend zijn een systeem te ontwikkelen dat de betrokkene in staat stelt de gegevens zelf online te raadplegen. Bedrijven en organisaties worden aangespoord een kosten/baten analyse uit te voeren van een dergelijk online toegangssysteem.

6 Wettelijke grondslag voor het verwerken van persoonsgegevens

- Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.
  - Je moet kiezen uit de grondslagen opgesomd in de nieuwe privacywetgeving, maar let op het verschil tussen 'gewone' en 'bijzondere' gegevens.
  - Onder de nieuwe privacywetgeving kunnen de rechten van de betrokkene variëren naargelang de wettelijke basis van de gegevensverwerking. Het meest voor de hand liggende voorbeeld is dat de betrokkene een sterker recht heeft om de verwijdering van zijn gegevens te vragen indien zijn toestemming aan de grondslag lag voor de verwerking.
  - Het is belangrijk om de gekozen wettelijke grondslag voor de gegevensverwerking te verduidelijken in de privacyverklaring en telkens wanneer je een toegangsverzoek beantwoordt. Kijk dus na welke gegevensverwerkingen je uitvoert; bepaal de wettelijke basis en documenteer dit zorgvuldig in het licht van de verantwoordelijkheidsvereiste.

7 Toestemming

- Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert. De nieuwe privacywetgeving vermeldt “toestemming” en “expliciete toestemming”.
  - Het onderscheid maken is niet nodig, aangezien de toestemming in beide gevallen vrij, specifiek, geïnformeerd en ondubbelzinnig moet zijn. De toestemming moet ook blijken uit een actieve indicatie van akkoord. M.a.w. de toestemming kan niet worden afgeleid uit een stilzwijgen, een vooraf aangevinkt vakje of uit een niet-handelen.
  - Indien je rekent op de toestemming van de betrokkene om diens gegevens te verwerken, zorg dan zeker dat die toestemming voldoet aan de vereisten van de AVG. Noteer dat de toestemming controleerbaar moet zijn en dat de betrokkene doorgaans meer rechten heeft wanneer je vertrouwt op toestemming als grondslag voor de gegevensverwerking.
  - De nieuwe privacywetgeving verduidelijkt dat de verwerkingsverantwoordelijke in staat moet zijn om aan te tonen dat toestemming werd gegeven. Evalueer dus je systemen die toestemming registreren, teneinde te verzekeren van een effective audit trail (controlespoor).

8 Kinderen

- De nieuwe privacywetgeving laat in één bepaalde context kinderen vanaf 16 jaar toe om zelf toe te stemmen met gegevensverwerking, namelijk in de context van commerciële internetdiensten die zich rechtstreeks richten tot kinderen.
  - De Belgische wetgever mag de groep 13 - 16-jarigen hetzelfde privilege geven dus hou de berichtgeving van de Autoriteit in het oog. Let wel op, kinderen die zelf toestemden mogen eisen dat hun gegevens op elk moment gewist worden, ook na hun meerderjarigheid!
  - Bekijk of je gegevens verwerkt van minderjarige kinderen en of je de leeftijd van de betrokkene moet nagaan. Ga na hoe je met de ouder(s) of voogd(en) in contact kan treden, bijvoorbeeld om toestemming te vragen of een contract aan te gaan.

9 Gegevenslekken

- Voorzie adequate procedures om persoonlijke gegevenslekken op te sporen, te rapporteren en te onderzoeken. Beoordeel hiervoor de verscheidene types van persoonsgegevens die je bijhoudt en documenteer welke binnen de meldingsplicht zouden vallen, ingeval zich een gegevenslek zou voordoen.
  - Let op – de Belgische wetgever mag de groep 13 - 16-jarigen hetzelfde privilege geven – hou de berichtgeving van de Autoriteit in het oog. Let wel op, kinderen die zelf toestemden mogen eisen dat hun gegevens op elk moment gewist wor den, ook na hun meerderjarigheid!
  - Bekijk of je gegevens verwerkt van minderjarige kinderen en of je de leeftijd van de betrokkene moet nagaan. Ga na hoe je met de ouder(s) of voogd(en) in contact kan treden, bijvoorbeeld om toestemming te vragen of een contract aan te gaan.

10 Gegevensbescherming door ontwerp en gegevensbeschermingseffectbeoordeling (GEB)

- Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling", beter gekend als Privacy by design en Data Protection Impact Assessment (DPIA).
  - Ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren. Deze kunnen worden gelinkt aan andere organisatorische processen zoals risicobeheer en projectbeheer. Beoordeel de situaties waarin het nodig is dergelijke analyses uit te voeren.
    Wie zal dit doen? Wie moet hierbij worden betrokken? Gebeurt de analyse centraal of lokaal? Het behoorde altijd al tot de "good practices" van een bedrijf of organisatie om gegevensbescherming van bij de start in te bouwen en als onderdeel hiervan een effectbeoordeling uit te voeren. De nieuwe privacywetgeving maakt hiervan een duidelijke wettelijke vereiste.
  - Noteer dat je niet steeds een GEB moet uitvoeren. Deze is enkel vereist in hoge risicosituaties, bijv. wanneer een nieuwe technologie wordt geïmplementeerd of wanneer een profileringsoperatie een aanzienlijk effect kan teweegbrengen voor de betrokkenen. Wanneer de GEB aangeeft dat de gegevensverwerking een "hoog risico" inhoudt en dit ondanks maatregelen genomen ter beheersing van het "hoog risico" (met andere woorden er is een "hoog residueel risico"), is het noodzakelijk het advies in te winnen van de toezichthoudende autoriteit omtrent de wetmatigheid van de verwerking in het licht van de nieuwe privacywetgeving.

11 Functionaris voor gegevensbescherming

- Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de gegevensbeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.
  - De nieuwe privacywetgeving vereist voor sommige bedrijven en organisaties dat zij een functionaris voor gegevensbescherming aanwijzen, bijvoorbeeld voor openbare overheden of verwerkers wiens kerntaak bestaat uit het regelmatig en stelselmatig observeren op grote schaal van betrokkenen of een grootschalige verwerking van gevoelige gegevens.
  - Het is van belang dat, hetzij iemand in de organisatie, hetzij een externe adviseur, verantwoordelijkheid neemt voor het naleven van de gegevensbeschermingsprincipes en dat iemand de kennis, medewerking en bevoegdheid heeft om dit te doen. Daarom moet je nu reeds beoordelen of op jouw bedrijf of organisatie de plicht rust een dergelijke functionaris aan te stellen. Zo ja, evalueer of de huidige aanpak in lijn is met de vereisten van de nieuwe privacywetgeving.

12 Internationaal

- Indien jouw bedrijf of organisatie internationaal actief is, dien je te bepalen onder welke toezichthoudende autoriteit je valt.
  - De nieuwe privacywetgeving voorziet een enigszins complexe regeling om te bepalen welke toezichthoudende autoriteit de leiding neemt bij het onderzoek naar een klacht met een internationaal karakter, bijv. wanneer een gegevensverwerking betrekking heeft op inwoners van meerdere lidstaten. De leidende autoriteit wordt bepaald naargelang waar het bedrijf of de organisatie haar hoofdvestiging heeft of de vestiging waar de beslissingen omtrent de gegevensverwerkingen worden genomen. Voor een traditionele hoofdzetel is dit vrij eenvoudig vast te stellen. Moeilijker wordt het voor complexe, multi-site bedrijven of organisaties waarbij beslissingen omtrent diverse verwerkingsactiviteiten op verschillende plaatsen worden genomen.
  - Om duidelijkheid te krijgen over welke toezichthoudende autoriteit de leiding heeft over jouw bedrijf of organisatie kan het raadzaam zijn in kaart te brengen waar jouw organisatie haar meest belangrijke beslissingen omtrent gegevensverwerkingen neemt. Dit zal je helpen bij het bepalen van jouw "hoofdvestiging" en dus ook van de bevoegde toezichthoudende autoriteit.

13 Bestaande contracten

- Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng indien nodig veranderingen aan.
  - De nieuwe privacywetgeving creëert een intelligent systeem die de verhouding tussen de verwerkingsverantwoordelijke en de verwerkers behelst. Het bepaalt zelfs de voorwaarden die van toepassing zijn op onder-aanneming activiteiten. Opdat je deze voorwaarden zou aantreffen, moet je bestaande contracten beoordelen en de nodige wijzigingen aanbrengen.
  - De nieuwe privacywetgeving benadrukt het belang van op databanken toepasselijke veiligheidsmaatregelen. Ook in het geval van outsourcing is het belangrijk te beoordelen of de veiligheidsmaatregelen die werden voorzien in de bestaande contracten nog steeds toereikend zijn en voldoen aan de vereisten van de nieuwe privacywetgeving.