

# Voorwaarden inzet SAAS toepassingen

|         |                                              |
|---------|----------------------------------------------|
| Datum   | 22 okt 2021                                  |
| Versie  | 1.4                                          |
| Auteurs | PO Beaubine Adriaansen, ISO Ruud Aarts       |
| Review  | FG Jill de Groot, CISO Peter van de Boogaard |

## Inhoud

|                                                                 |    |
|-----------------------------------------------------------------|----|
| Informatiebeveiliging .....                                     | 3  |
| Doel .....                                                      | 3  |
| Wat is SAAS.....                                                | 3  |
| SAAS, informatiebeveiliging en privacy.....                     | 3  |
| Dataclassificatie en verantwoording t.a.v. de organisatie ..... | 3  |
| Selectie eisen leverancier en product .....                     | 3  |
| Pakketselectie SAAS-dienst .....                                | 4  |
| SAAS en eisen vanuit de BIO .....                               | 4  |
| Maatregelen .....                                               | 5  |
| Privacy .....                                                   | 12 |
| Over Privacy.....                                               | 12 |
| De SAAS-dienst is volgens de AVG ‘verwerker’ .....              | 12 |
| AVG .....                                                       | 12 |
| Hulpmiddelen .....                                              | 12 |
| Bijlage: Originele artikelen vanuit de AVG .....                | 17 |

## Bronnen

BIO <https://bio-overheid.nl>

Forum Standaardisatie <https://www.forumstandaardisatie.nl/>

Autoriteit Persoonsgegevens <https://autoriteitpersoonsgegevens.nl>

# Informatiebeveiliging

## Doel

In de komende jaren zal de provincie haar ICT infrastructuur, data en applicaties omzetten naar cloudbased oplossingen. Cloud first en SAAS first zijn speerpunten die daarin worden gehanteerd. Onduidelijk is echter onder welke voorwaarden een SAAS applicatie kan worden ingezet.

## Wat is SAAS

SAAS is een afkorting voor Software As A Service. Een SAAS toepassing is veelal een webbased applicatie die wordt aangeboden vanaf een public of private cloudomgeving. De volgende kenmerken zijn van toepassing op SAAS diensten:

- SAAS applicaties draaien in de cloud
- Onderhoud en vernieuwing van een SAAS applicatie is centraal geregeld
- De configuratie van SAAS applicaties zijn eenduidig
- De applicatie is eenvoudig schaalbaar

## SAAS, informatiebeveiliging en privacy

Het gebruik van SAAS applicaties is niet zonder risico. De applicaties draaien in datacenters waarvan veelal onbekend is waar deze zijn gelokaliseerd. Het is niet onmogelijk dat de SAAS leverancier toegang heeft tot de data die wordt opgeslagen. Een SAAS applicatie is een online dienst die alleen functioneert met een werkende internetverbinding. Ook is het niet onmogelijk dat leveranciers diagnostische en gebruikersgegevens verzamelen.

## Dataclassificatie en verantwoording t.a.v. de organisatie

De BIO kent 3 dataclassificatie niveaus. Afhankelijk van het niveau zal er intern verantwoording moeten worden afgelegd. De provincie stelt in het algemeen dat alle data Basis Beveiliging Niveau 2 (BBN2) meekrijgt. **Voor BBN2 geldt dat er verantwoording moet worden afgelegd aan de CISO.** Meer informatie hierover is terug te lezen in hoofdstuk 4 van de BIO.

## Selectie eisen leverancier en product

De BIO hanteert de term Dienstenleverancier als het gaat over de levering, onderhoud en beheer van informatiediensten. Dit gaat over zowel interne als externe partijen en dus kan een leverancier van een SAAS-dienst worden gezien als een externe dienstenleverancier. De BIO stelt t.a.v. van de externe dienstenleverancier de volgende criteria op waar bij de selectie van een leverancier rekening moet worden gehouden:

1. **De aangeboden dienst is gecertificeert met de NEN ISO 27001 of gelijkwaardige norm en kan dit aantonen door het overleggen van een Statement of Compliance (of deel in control verklaring) afgegeven over de aangeboden dienst.**
2. De organisatie van de aanbieder van de dienst hoeft bij afname van de dienst niet gecertificeerd te zijn. Echter moet de opdrachtgever wel voldoen aan de eisen die worden gesteld vanuit de aanvrager en moeten die contractueel worden vastgelegd. Hoofdstuk 15 in de BIO gaat hierover.

## Pakketselectie SAAS-dienst

Om te kunnen voorzien in de pakketselectie zijn hieronder in het kort de criteria opgesteld t.a.v. het aangeboden pakket. Het is daarna aan de leverancier om aan te tonen dat ze voldoen aan deze criteria en de uitgebreide lijst en aanvullende omschrijvingen die daarin staan omschreven.

1. Mogelijkheden tot toegangsbeveiliging
2. Biedt roll-based-access (onderscheid tussen beheer en gebruik)
3. Werkt met authenticatie en cryptografie
4. Heeft beveiligde verbindingen op web, app en/of andere verbindingen
5. Geen lokale opslag/download mogelijkheden op mobiele apparatuur
6. Biedt 2-factor authenticatie
7. Integratie van directory services o.b.v. Microsoft ADFS
8. Biedt maatregelen t.a.v. wetgeving zoals AVG om persoonsgegevens te verwerken en te beveiligen, m.a.w. is AVG-proof.
9. Waar mogelijk kan data versleuteld worden opgeslagen
10. Gesitueerd in gecertificeerde datacenters en redundant uitgevoerd
11. Data wordt beschermd door backup
12. Data en systeem bevinden zich binnen de Europese Unie
13. Biedt logging op gebied van security
14. Biedt eenvoudige mogelijkheden voor datamigratie bij contractbeëindiging.
15. De leverancier is zich bewust van de wet- en regelgeving bij de overheid waarvan het kader BIO de standaard is met verwijzingen naar bijvoorbeeld Forum Standaardisatie en NEN ISO27001/02.

De online module Inkoop Eisen Cybersecurity Overheid (ICO) geeft inzicht in **alle** abstracte maatregelen waar bijvoorbeeld een clouddienst aan moet voldoen:

<https://www.bio-overheid.nl/ico-wizard/>

## SAAS en eisen vanuit de BIO

Om een beter begrip te krijgen aan welke maatregelen een SAAS applicatie moet voldoen zijn de volgende uitgangspunten van toepassing.

- Een webbased toepassing any time, any place benaderbaar
- Web- of app based dus eenvoudig benaderbaar met een mobiel apparaat
- Draait binnen een public of private cloud
- Bereikbaar via het publieke internet
- Er is altijd sprake van verwerking van persoonsgegevens (in het geval van gebruikers accounts)

De maatregelen vanuit de BIO en de richtlijnen gegeven door PNB zijn verderop in dit document uitgewerkt.

**De in GROEN gestelde maatregelen zijn aspecten waar de SAAS toepassing c.q. leverancier minimaal aan moet voldoen.**

Daaromheen staan maatregelen die op orde moeten zijn, dus genoemd als randvoorwaarde voor een goede implementatie van de SAAS.

## Maatregelen

De volgende maatregelen vanuit de BIO zijn mogelijk voorwaardelijk of van belang bij aanschaf en inzet van een SAAS toepassing als het gaat om gegevensbescherming.

### 6.2 Mobiele apparatuur en telewerken

Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.

#### 6.2.1.1

2 Mobiele apparatuur is zo ingericht dat bedrijfsinformatie niet onbewust wordt opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn.

Résumé:

- **Uitgangspunt: De SAAS applicatie slaat lokaal geen gegevens op.**
- Lokaal opgeslagen gegevens worden beschermd door toegangsbeveiliging.
- **Lokaal opgeslagen gegevens zijn versleuteld opgeslagen.**
- Mobiel wissen op afstand van mobiele apparatuur moet mogelijk zijn.

#### 6.2.1.2

2 Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd:

- b. Het device maakt deel uit van patchmanagement en hardening.
- c. er wordt gebruik gemaakt van Mobile Device Management MDM of van Mobile Application Management (MAM)-oplossingen.

## 8.2 Informatieclassificatie

Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.

In principe wordt altijd **Basis Beveiligingsniveau 2** gehanteerd. Dit kan onder bepaalde voorwaarden teruggebracht worden naar BBN1 of verzaamd naar BBN3.

**Voor BBN2 geldt dat de proceseigenaar het informatiesysteem voor ingebruikname (bij voorkeur in ontwerp-/ontwikkelfase) ter consultatie voorlegt aan de CISO.**

Voor BBN1 en BBN3 gelden andere voorwaarden. Zie hiervoor het hoofdstuk 'Verantwoording over de BIO' in de BIO.

## 8.3 Behandelen van media

Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.

#### 8.3.2.3

2 Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is.

M.a.w. gegevens die door SAAS-toepassingen lokaal op mobiele apparatuur wordt opgeslagen, moet te allen tijde verwijderd kunnen worden.

## 9.2 Beheer van toegangsrechten van gebruikers

Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.

### 9.2.1.2

1 Het gebruiken van groepsaccounts is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar. M.a.w. toegang wordt verleend op persoonlijke, individuele basis.

### 9.2.2 1 Gebruikers toegang verlenen

Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.

Voor SAAS toepassingen geldt dat voor gebruikerstoegang op basis van een koppeling met directory services de beste oplossing is. Waarbij alleen gebruikers toegewezen aan de groep voor de specifieke SAAS toepassing toegang hebben.

Er is geen sprake van lokale accounts binnen de SAAS applicatie als er op basis van directory services toegang wordt geboden.

### 9.2.2.2

1 Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.

Dat betekent dat er verschil is tussen gebruikersaccounts en beheeraccounts binnen de toepassing. Verschillende rollen mogen ook niet binnen één account worden ondergebracht. Sommige SAAS oplossingen bieden een uitgebreid spectrum aan rollen die kunnen worden ingezet. In elk geval moet er duidelijk onderscheid zijn tussen de rechten en de rollen die kunnen worden ingezet. De aanbeveling is om beheerrollen te laten landen binnen een team Functioneel Beheer.

De dienstenleverancier heeft in het dagelijks beheer géén toegang tot de gegevens inhoudelijk van de provincie die worden verwerkt in de dienst c.q. SAAS-toepassing die wordt geleverd.

Als er situaties optreden waarbij dit op de een of andere manier nodig of onoverkomelijk is, denk aan calamiteiten, data- of systeem migratie, dan gaat dit altijd in overleg en met toestemming van de provincie.

### 9.2.6 1 Toegangsrechten intrekken of aanpassen

De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.

De toegangsrechten op een SAAS applicatie vervallen met het beëindigen van het dienstverband of wijzigen van functie binnen de organisatie. Afhankelijk van de inzet van een koppeling met directory services gebeurt dit automatisch.

## 9.4 Toegangsbeveiliging van systeem en toepassing

Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.

#### 9.4.1.1

2 Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.

MDM ondersteunt dat lokaal opgeslagen informatie ontoegankelijk is voor andere toepassingen.

#### 9.4.2

##### 1 Beveiligde inlogprocedures

Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.

##### 9.4.2.1

1 Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.

Het benaderen van een SAAS toepassing via het publieke internet wordt altijd gezien als toegang vanuit een onvertrouwde zone.

De SAAS applicatie ondersteunt minimaal 2-factor authenticatie. Dit kan bijvoorbeeld door het gebruik van Google of Microsoft Authenticator.

#### 9.4.3

##### 1 Systeem voor wachtwoordbeheer

Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.

Voor een koppeling met directory services geldt dat gebruikersaccounts automatisch al zijn voorzien van het wachtwoordbeleid zoals de Provincie dit heeft gesteld.

Indien de SAAS toepassing geen gebruik kan maken van een koppeling met directory services zal voor de wachtwoorden van gebruikersaccounts de richtlijn DOC-BB-01L Richtlijn Wachtwoordbeheer van de Provincie van toepassing zijn.

#### 10.1 Cryptografische beheersmaatregelen

Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

Data wordt waar mogelijk versleuteld opgeslagen.

De overdracht van data wordt gedaan op basis van een bewezen versleutelingsprotocol. De minimale eisen hiervoor zijn vastgelegd bij het Forum Standaardisatie. <https://www.forumstandaardisatie.nl/>

### 11.1 Beveiligde gebieden

Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen.

De SAAS toepassing is gelokaliseerd in gecertificeerde datacenters als het gaat om informatiebeveiliging. Het hebben van een ISO 27001 certificering en implementatie van de maatregelen vanuit ISO 27002 is daarvoor een minimale eis.

De inrichting en opslag van de SAAS applicatie bevindt zich binnen de grenzen van de Europese Unie.

### 11.2 Apparatuur

Doelstelling: Verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.

#### 11.2.9.2

2 Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screenlock na een inactiviteit van maximaal 15 minuten.

#### 11.2.9.3

2 Sessies op remote desktops worden op het remote platform vergrendeld na een vastgestelde periode.

De SAAS toepassing biedt de mogelijkheid om na een termijn van inactiviteit de actieve sessie te beëindigen zodoende dat informatie niet meer zichtbaar is. De gebruiker zal na deze periode opnieuw moeten inloggen.

Het maken van screenshots moet waar mogelijk niet zijn toegestaan.

De export van data vanuit een SAAS toepassing moet voor gewone gebruikers beperkt zijn tenzij de rol het toelaat.

## 12.1 Bedieningsprocedures en verantwoordelijkheden

Doelstelling: Correcte en veilige bediening van informatie verwerkende faciliteiten waarborgen.

### 12.1.4 1 Scheiding van ontwikkel-, test- en productieomgevingen

Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.

## 12.2 Bescherming tegen malware

Doelstelling: Waarborgen dat informatie en informatie verwerkende faciliteiten beschermd zijn tegen malware.

### 12.2.1

#### 1 Beheersmaatregelen tegen malware

Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.

#### 12.2.1.3

1 De gebruikte antimalware software en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.

#### 12.2.1.4

1 Computers en media worden als voorzorgsmaatregel routinematig gescand.

## 12.3 Back-up

Doelstelling: Beschermen tegen het verlies van gegevens.

### 12.3.1 1 Back-up van informatie

Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.

Van alle gegevens die binnen de SAAS applicatie worden opgeslagen, wordt een backup gemaakt.

Met de SAAS leverancier worden afspraken gemaakt over hersteltijden na een incident (maximaal 16 uur over twee aaneengesloten werkdagen van 8 uur verspreid) en het dataverlies met een maximale tijd van 28 uur.

## 12.4 Verslaglegging en monitoren

Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.

De SAAS applicatie registreert de toegang van alle gebruikers.

### 12.4.1

#### 1 Gebeurtenissen registreren

Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

#### 12.4.1.1

1 Een logregel bevat minimaal:

- a. de gebeurtenis;
- b. de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon;
- c. het gebruikte apparaat;
- d. het resultaat van de handeling;
- e. een datum en tijdstip van de gebeurtenis.

### 13.2 Informatietransport

Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.

#### 13.2.3

1 Elektronische berichten

Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.

##### 13.2.3.1

1 Voor de beveiliging van elektronische (e-mail)berichten gelden de vastgestelde open standaarden tegen phishing en afluisteren op de 'pas toe of leg uit'-lijst van het Forum<sup>1</sup>. Voor beveiliging van websiteverkeer gelden de open standaarden tegen afluisteren op de 'pas toe of leg uit'-lijst van het Forum.

<sup>1</sup> het Forum verwijst naar Forum Standaardisatie

##### 13.2.3.3

2 Maak gebruik van PKI overheid-certificaten<sup>1</sup> bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlelen.

<sup>1</sup> Het gebruikte certificaat moet herleidbaar zijn naar de eigenaar van het domein. Inzet van zelf gegenereerde certificaten of aangekochte of verkregen certificaten die dat niet kunnen zijn niet toegestaan.

### 16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen

Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.

#### 16.1.2

1 Rapportage van informatiebeveiligingsgebeurtenissen

Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.

##### 16.1.2.1

1 Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.

### 17.2 Redundante componenten

Doelstelling: Beschikbaarheid van informatie verwerkende faciliteiten bewerkstelligen.

### 17.2.1

#### 1 Beschikbaarheid van informatie verwerkende faciliteiten

Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.

De SAAS toepassing moet redundant zijn uitgevoerd. Dat impliceert dat de toepassing en opgeslagen data op minimaal twee fysieke locaties bestaat.

#### Beëindiging SAAS contract

Vooraf aan de beëindiging van het SAAS contract is er de mogelijkheid om alle data en gegevens te exporteren naar bruikbare gegevenssets, bestanden of database.

Na beëindiging van het SAAS contract worden alle gegevens in productie, backup of uitwijklocatie verwijderd.

# Privacy

## Over Privacy

De volgende artikelen vanuit de AVG zijn minstens van belang bij aanschaf en inzet van een SAAS-toepassing als het gaat om gegevensbescherming bij de verwerking van persoonsgegevens binnen de SAAS-oplossing c.q. dienst van de leverancier onder verantwoordelijkheid van de Provincie Noord-Brabant. In de beschreven artikelen wordt soms verwezen naar andere artikelen of hoofdstukken uit de AVG. Deze zijn te raadplegen in de AVG zelf.

Bij de inzet van een SAAS-toepassing is het van belang onderscheid te maken tussen de verantwoordelijkheden van de verschillende partijen. Daarin maken we onderscheid tussen:

1. Verwerkingsverantwoordelijke: de verwerkingsverantwoordelijke is degene die het doel en de middelen bepaalt voor een verwerking van persoonsgegevens. Bij de inzet van een SAAS-toepassing door de Provincie, heeft deze de rol van Verwerkingsverantwoordelijke.
2. Verwerker: de verwerker is degene die persoonsgegevens verwerkt ten behoeve van de verwerkingsverantwoordelijke. Bij de inzet van een SaaS-toepassing door de Provincie Noord-Brabant, heeft de leverancier van de SaaS-toepassing de rol van verwerker.
3. Betrokkene: de betrokkene is de persoon van wie persoonsgegevens wordt verwerkt binnen de SAAS-oplossing.

## De SAAS-dienst is volgens de AVG ‘verwerker’

Het is belangrijk om te begrijpen dat alle partijen vanuit de AVG gezien een bepaalde verantwoordelijkheid dragen als het gaat over de verwerking van persoonsgegevens. Op het moment dat er een SAAS-dienst wordt overeengekomen waarin vervolgens persoonsgegevens worden verwerkt, dan is de SAAS-leverancier niet enkel leverancier van een software product maar volgens de AVG ook ‘verwerker’. De SAAS-leverancier is daarmee mede verantwoordelijk voor een goed beheer volgens alle wet- en regelgeving op het gebied van privacy- en informatiebeveiliging.

## AVG

De Europese richtlijn GDPR is naar het Nederlands vertaald als AVG. Het is Europese wetgeving om de privacy van personen binnen de EU beter te waarborgen en volgt hiermee o.a. de Wet bescherming Persoonsgegevens. Omdat de AVG een verordening is, wordt hier veel jargon gebruikt, om die reden zijn hieronder de belangrijkste artikelen omgezet naar begrijpbare taal. De artikelen zijn als bijlage toegevoegd aan dit document om misvatting of verschil van inzicht op basis van perceptie te voorkomen. Mocht er op de een of andere manier toch een geschil optreden over de inhoud dan is het raadzaam de Privacy Officer of Functionaris Gegevensbescherming hierover te raadplegen.

## Hulpmiddelen

### [AVG in een notendop](#)

### [Checklist AVG](#)

### [Autoriteit Persoonsgegevens](#)

Opsomming AVG artikelen voor een SAAS-dienst

**1. De verwerkingsverantwoordelijke (PNB) en verwerker (SAAS-dienst) waarborgen dat alle maatregelen zijn getroffen op het gebied van informatiebeveiliging om te voldoen aan de uitvoering van de AVG.**

De voor de AVG ingezette maatregelen worden van tijd tot tijd geëvalueerd en geactualiseerd.

In de praktijk betekent dit voor een SAAS-dienst dat die zich conformeert aan de actuele standaarden en technieken die voorhanden zijn als het gaat over bijvoorbeeld toegangsbeveiliging, encryptiemogelijkheden en antivirusdetectie.

**Resumé**

- De provincie Noord-Brabant heeft de rol van verwerkingsverantwoordelijke en blijft verantwoordelijk voor de persoonsgegevens, ook wanneer die verwerking is uitbesteedt aan een verwerker (verwerker is hier de leverancier van de SAAS-toepassing).
- Het is aan PNB als verwerkingsverantwoordelijke in afstemming met de verwerker om passende technische en organisatorische maatregelen te nemen om te waarborgen en te kunnen aantonen dat de verwerking van persoonsgegevens in de SaaS-oplossing in overeenstemming is met de AVG en het privacy beleid van PNB. **Maatregelen zijn beschreven in de BIO of NEN ISO27001/02.**
- Er dient een eigenaar van de SaaS-applicatie te worden aangewezen binnen PNB. Daarvoor is de budgethouder of programmamanager binnen de provincie Noord-Brabant de meest aangewezen persoon. In sommige gevallen wordt het eigenaarschap bij Functioneel Beheer belegd.

**AVG Artikel 24**

**2. De verwerkingsverantwoordelijke bepaalt welke beveiligingsmaatregelen er worden ingezet om te voldoen aan de AVG. Passende technische en organisatorische maatregelen staan onder andere beschreven in de BIO. SAAS-diensten die niet kunnen voldoen aan de gestelde maatregelen zoals die zijn beschreven in de BIO en aanvullende bepalingen beschreven in provinciale richtlijnen komen niet in aanmerking.**

- a. Alleen noodzakelijke persoonsgegevens worden verwerkt
- b. Persoonsgegevens zijn niet onbeperkt en voor iedereen toegankelijk. De SAAS-toepassing biedt de mogelijkheid dat gegevens op basis van het principe need-to-know kunnen worden aangeboden.
- c. De persoonsgegevens die verwerkt zullen worden in de SaaS-applicatie dienen beschermt te worden door middel van ontwerp (privacy by design) en door standaardinstellingen (privacy by default). Privacybescherming moet een integraal deel uitmaken van de ontwerpkeuzes en inrichting van de SaaS-oplossing.
- d. Belangrijk om privacy by design te bereiken zijn de beveiligingsmaatregelen (zie eisen uit de BIO).
- e. In de architectuur moet vastgelegd worden dat niet meer gegevens worden verwerkt in de SaaS-oplossing dan noodzakelijk voor het doel. Dit wordt gedocumenteerd in een DPIA en aan de hand van de DPIA zal worden beoordeeld of de gegevensverwerking gewenst is en of er eventuele aanvullende maatregelen moeten worden genomen.

- f. Bewaartermijnen moeten door de verwerkingsverantwoordelijke zorgvuldig worden bepaald en vastgelegd.
- g. Het moet voor betrokkenen mogelijk zijn hun persoonsgegevens in te zien, te corrigeren en te wissen.

## **AVG Artikel 25**

3. Het is de taak van de verwerkingsverantwoordelijke om toe te zien op de verwerker. Als de verwerker een derde partij betreft kan deze waarborgen dat alle technische en organisatorische maatregelen zijn gegarandeerd.

De verwerker mag de verwerkingwerkzaamheden niet zomaar zondermeer uitbesteden zonder de verwerkingsverantwoordelijke daarover op de hoogte te stellen en daarover schriftelijke toestemming te hebben ontvangen.

Tussen de verwerkingsverantwoordelijke en de verwerker wordt een verbintenis getekend in de vorm van een verwerkingsovereenkomst.

Resumé:

PNB dient een verwerkersovereenkomst af te sluiten met de leverancier van de SaaS-applicatie waarin over alle onderwerpen zoals van toepassing zijnde en beschreven in art. 28 afspraken worden gemaakt.

Indien mogelijk, is daarbij de standaard ICT-verwerkersovereenkomst van PNB leidend.

Bij de keuze voor leverancier (verwerker) dient zorgvuldig gekozen te worden voor een leverancier die afdoende garanties biedt m.b.t. het toepassen van passende technische en organisatorische beveiligingsmaatregelen.

## **AVG Artikel 28**

**4. De verwerkingsverantwoordelijke is verplicht om een verwerkingsregister bij te houden.**

**De verwerker houdt een overzicht bij van alle verwerkingsactiviteiten die ze doet in opdracht van de verwerkingsverantwoordelijke.**

Resumé:

Bij aanschaf van een SaaS-applicatie, dient de Provincie deze op te nemen in het verwerkingsregister. Het is de verantwoordelijkheid van de eigenaar van de applicatie dat dit gebeurt volgens de 'Procedure Verwerkingsregister' van de Provincie.

**5.**

**AVG Artikel 30**

**6. Verwerkingsverantwoordelijke en verwerker bepalen aan de hand van het risico welke passende maatregelen worden ingezet om persoonsgegevens te beschermen.**

- a. de pseudonimisering en versleuteling van persoonsgegevens;
- b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking

**De risicoafweging die wordt gemaakt wordt gedaan op basis van de verwerkingsrisico's waarbij verlies, vernietiging, diefstal, wijziging, ongeoorloofde toegang of verstrekking van gegevens een rol speelt.**

**Het dient de voorkeur als een dienst is gecertificeerd bijvoorbeeld ISO 27001**

**Personen die persoonsgegevens verwerken vallen onder het gezag van de verwerkingsverantwoordelijke en handelen in opdracht.**

Resumé:

- Er zal een risico-analyse (BBN-toets?) moeten worden gedaan om te bepalen wat voor passende technische en organisatorische maatregelen er door zowel PNB als de leverancier genomen moeten worden om een op het risico afgestemd beveiligingsniveau te waarborgen.
- De beveiligingsmaatregelen die de verwerker treft, dienen getoetst te worden door de Information Security Officer van PNB. Deze worden vervolgens vastgelegd in de verwerkersovereenkomst.

**AVG Artikel 32**

**7. De verwerker is verplicht alle incidenten van inbreuk van persoonsgegevens te melden bij de verwerkingsverantwoordelijke en te documenteren.**

**De verwerker heeft een proces ingericht omtrent het melden en documenteren van datalekken.**

Resumé:

Met dit artikel wordt bedoeld dat de provincie Noord-Brabant een meldingsplicht heeft wanneer er zich een datalek voordoet binnen een verwerking waarbij de Provincie de rol van verwerkingsverantwoordelijke is. Indien het een meldenswaardig datalek betreft, dient deze binnen 72 uur gemeld te worden bij de Autoriteit Persoonsgegevens.

Indien de leverancier van de SAAS-toepassing een datalek constateert in de verwerking die hij doet in opdracht van provincie Noord-Brabant.

Met de leverancier dienen in de verwerkersovereenkomst afspraken worden gemaakt over een inbreuk in verband met persoonsgegevens. De afspraken dienen in lijn te zijn met art. 33 AVG en de datalek procedure van PNB.

### **AVG Artikel 33**

**8. Voorafgaand aan de aanschaf van een systeem (applicatie of SAAS-dienst) zal er een DPIA (Data Protection Information Assessment of een zogenaamd Gegevensbeschermingseffectbeoordeling) worden opgesteld in samenwerking met de Privacy Officer en onder toezicht van de Functionaris Gegevensbescherming.**

Resumé:

Voorafgaand aan de aanschaf van een SaaS-oplossing dienen de privacy risico's daarvan in kaart worden gebracht in een risicobeoordeling in de vorm van een DPIA. Hiermee voldoet PNB tevens aan de documentatieplicht en privacy by design.

In het bijzonder moet aandacht besteed worden aan:

- a. Waar staat de data opgeslagen? Binnen of buiten de EER?
- b. Indien buiten de EER: de hoofdregel is dat een organisatie persoonsgegevens alleen mag doorgeven naar derde landen met een passend beschermingsniveau. Dus als de SaaS-oplossing buiten de EER staat, dient bekeken te worden of er sprake is van een derde land met een passend beschermingsniveau. Meer specifiek komt dat neer op art. 44t/m 47 AVG. Let op: Doorgifte op basis van Privacy Shield is in juli 2020 ongeldig verklaard
- c. Als er geen sprake is van een derde land met een passend beschermingsniveau, is doorgifte slechts toegestaan op grond van een van de wettelijke bepalingen uit de AVG.
- d. Wie heeft er toegang tot de data?
- e. Nader aan te vullen.

### **AVG Artikel 35**

## Bijlage: Originele artikelen vanuit de AVG

Bron: [https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening\\_2016\\_-\\_679\\_definitief.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf)

### HOOFDSTUK IV

#### Verwerkingsverantwoordelijke en verwerker

##### Afdeling 1

#### Algemene verplichtingen Artikel 24

##### Verantwoordelijkheid van de verwerkingsverantwoordelijke

1. Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.
2. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de in lid 1 bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd.
3. Het aansluiten bij goedgekeurde gedragscodes als bedoeld in artikel 40 of goedgekeurde certificeringsmechanismen als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat de verplichtingen van de verwerkingsverantwoordelijke zijn nagekomen.

## Artikel 25

### Gegevensbescherming door ontwerp en door standaardinstellingen

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.
2. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.
3. Een overeenkomstig artikel 42 goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften van de leden 1 en 2 van dit artikel is voldaan.

## Artikel 28

### Verwerker

1. Wanneer een verwerking namens een verwerkingsverantwoordelijke wordt verricht, doet de verwerkingsverantwoordelijke uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.
2. De verwerker neemt geen andere verwerker in dienst zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke. In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.
3. De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven. Die overeenkomst of andere rechtshandeling bepaalt met name dat de verwerker:
  - a. de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, tenzij een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt;
  - b. waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;
  - c. alle overeenkomstig artikel 32 vereiste maatregelen neemt;
  - d. aan de in de leden 2 en 4 bedoelde voorwaarden voor het in dienst nemen van een andere verwerker voldoet;
  - e. rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van de in

hoofdstuk III vastgestelde rechten van de betrokkene te beantwoorden;

- f. rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36;
- g. na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht;
- h. de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de nakoming van de in dit artikel neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk maakt en eraan bijdraagt

Waar het gaat om de eerste alinea, punt h), stelt de verwerker de verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op deze verordening of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming.

- 4. Wanneer een verwerker een andere verwerker in dienst neemt om voor rekening van de verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst of een andere rechtshandeling krachtens Unierecht of lidstatelijk recht dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in de in lid 3 bedoelde overeenkomst of andere rechtshandeling tussen de verwerkingsverantwoordelijke en de verwerker zijn opgenomen, met name de verplichting afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen te bieden opdat de verwerking aan het bepaalde in deze verordening voldoet. Wanneer de andere verwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de eerste verwerker ten aanzien van de verwerkingsverantwoordelijke volledig aansprakelijk voor het nakomen van de verplichtingen van die andere verwerker.
- 5. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat voldoende garanties als bedoeld in de leden 1 en 4 van dit artikel worden geboden.
- 6. Onverminderd een individuele overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker kan de in de leden 3 en 4 van dit artikel bedoelde overeenkomst of andere rechtshandeling geheel of ten dele gebaseerd zijn op de in de leden 7 en 8 van dit artikel bedoelde standaardcontractbepalingen, ook indien zij deel uitmaken van de certificering die door een verwerkingsverantwoordelijke of verwerker uit hoofde van de artikelen 42 en 43 is verleend.

7. De Commissie kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure standaardcontractbepalingen vaststellen.
8. Een toezichthoudende autoriteit kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens het in artikel 63 bedoelde coherentiemechanisme standaardcontractbepalingen opstellen.
9. De in de leden 3 en 4 bedoelde overeenkomst of andere rechtshandeling wordt in schriftelijke vorm, waaronder elektronische vorm, opgesteld.
10. Indien een verwerker in strijd met deze verordening de doeleinden en middelen van een verwerking bepaalt, wordt die verwerker onverminderd de artikelen 82, 83 en 84 met betrekking tot die verwerking als de verwerkingsverantwoordelijke beschouwd.

## Artikel 30

### Register van de verwerkingsactiviteiten

1. Elke verwerkingsverantwoordelijke en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat alle volgende gegevens:
  - a) de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;
  - b) de verwerkingsdoeleinden;
  - c) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
  - d) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
  - e) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;
  - f) indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
  - g) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.
2. De verwerker, en, in voorkomend geval, de vertegenwoordiger van de verwerker houdt een register van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht. Dit register bevat de volgende gegevens:
  - a) de naam en de contactgegevens van de verwerkers en van iedere verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker en van de functionaris voor gegevensbescherming;
  - b) de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd;
  - c) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1,

tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;

d) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.

3. Het in de leden 1 en 2 bedoelde register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld.
4. Desgevraagd stellen de verwerkingsverantwoordelijke of de verwerker en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker het register ter beschikking van de toezichthoudende autoriteit.
5. De in de leden 1 en 2 bedoelde verplichtingen zijn niet van toepassing op ondernemingen of organisaties die minder dan 250 personen in dienst hebben, tenzij het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen, de verwerking niet incidenteel is, of de verwerking bijzondere categorieën van gegevens, als bedoeld in artikel 9, lid 1, of persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10 betreft.

## Artikel 32

### Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:
  - a) de pseudonimisering en versleuteling van persoonsgegevens;
  - b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
  - c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
  - d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.
2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.
3. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.
4. De verwerkingsverantwoordelijke en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de verwerkingsverantwoordelijke verwerkt, tenzij hij daartoe Unierechtelijk of lidstaatrechtelijk is gehouden.

### Artikel 33

#### Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit

- 1) Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.
- 2) De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.
- 3) In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld:
  - a) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
  - b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
  - c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
  - d) de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.
- 4) Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.
- 5) De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.

## Afdeling 3

### Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging

#### Artikel 35

##### Gegevensbeschermingseffectbeoordeling

- 1) Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.
- 2) Wanneer een functionaris voor gegevensbescherming is aangewezen, wint de verwerkingsverantwoordelijke bij het uitvoeren van een gegevensbeschermingseffectbeoordeling diens advies in.
- 3) Een gegevensbeschermingseffectbeoordeling als bedoeld in lid 1 is met name vereist in de volgende gevallen:
  - a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
  - b) grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10; of
  - c) stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.
- 4) De toezichthoudende autoriteit stelt een lijst op van het soort verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling overeenkomstig lid 1 verplicht is, en maakt deze openbaar. De toezichthoudende autoriteit deelt die lijsten mee aan het in artikel 68 bedoelde Comité.
- 4) De toezichthoudende autoriteit kan ook een lijst opstellen en openbaar maken van het soort verwerking waarvoor geen gegevensbeschermingseffectbeoordeling is vereist. De toezichthoudende autoriteit deelt deze lijst mee aan het Comité.
- 5) Wanneer de in de leden 4 en 5 bedoelde lijsten betrekking hebben op verwerkingen met betrekking tot het aanbieden van goederen of diensten aan betrokkenen of op het observeren van hun gedrag in verschillende lidstaten, of op verwerkingen die het vrije verkeer van persoonsgegevens in de Unie wezenlijk

kunnen beïnvloeden, past de bevoegde toezichhoudende autoriteit voorafgaand aan de vaststelling van die lijsten het in artikel 63 bedoelde coherentiemechanisme toe.

- 6) De beoordeling bevat ten minste:
- 7) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
  - a) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
  - b) een beoordeling van de in lid 1 bedoelde risico's voor de rechten en vrijheden van betrokkenen; en
  - c) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.
  - d) Bij het beoordelen van het effect van de door een verwerkingsverantwoordelijke of verwerker verrichte verwerkingen, en met name ter wille van een gegevensbeschermingseffectbeoordeling, wordt de naleving van de in artikel 40 bedoelde goedgekeurde gedragscodes naar behoren in aanmerking genomen.
- 8) De verwerkingsverantwoordelijke vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking, met inachtneming van de bescherming van commerciële of algemene belangen of de beveiliging van verwerkingen.
- 9) 10. Wanneer verwerking uit hoofde van artikel 6, lid 1, onder c) of e), haar rechtsgrond heeft in het Unierecht of in het recht van de lidstaat dat op de verwerkingsverantwoordelijke van toepassing is, de specifieke verwerking of geheel van verwerkingen in kwestie daarbij wordt geregeld, en er reeds als onderdeel van een algemene effectbeoordeling in het kader van de vaststelling van deze rechtsgrond een gegevensbeschermingseffectbeoordeling is uitgevoerd, zijn de leden 1 tot en met 7 niet van toepassing, tenzij de lidstaten het noodzakelijk achten om voorafgaand aan de verwerkingen een dergelijke beoordeling uit te voeren.
- 10) 11. Indien nodig verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden