# Privacybeleid VRT

B-01.02

VEILIGHEIDSREGIO TWENTE

| Versie | Wijzigingen |
|---|---|
| 1.0 | Initiële versie |
| | |
| | |
| | |

## Autorisatie

Eigenaar document: Privacy Officer

# Inhoudsopgave

Inhoudsopgave ..... 3

1 Inleiding ..... 4
1.1 Beleidsverklaring ..... 4
1.2 Managementsysteem voor informatiebeveiliging (ISMS) ..... 4
1.3 Continue verbeteren ..... 4

2 Beleidsregels ..... 5
2.1 Gedetailleerde beleidsregels ..... 5

3 Middelen en verantwoordelijkheden ..... 6
3.1 Middelen ..... 6
3.2 Verantwoordelijkheden ..... 6
Directie ..... 6
Functionaris gegevensbescherming ..... 6
Privacy Officer ..... 6

# 1 Inleiding

## 1.1 Beleidsverklaring

Het belangrijkste doel van het privacy beleid is het definiëren van de doelen en verantwoordelijkheden met betrekking tot privacy in overeenstemming met aanvaardbare privacy principes en toepasselijke wet- en regelgeving. De scope van dit beleid beperkt zich tot de verwerking van persoonsgegevens.

Veiligheidsregio Twente treedt, voor zover van toepassing, op als verwerkingsverantwoordelijke van persoonsgegevens met betrekking tot eigen medewerkers, medewerkers van derden, burgers, klanten [1]en externe partijen. Veiligheidsregio Twente wordt ook beschouwd als verwerker met betrekking tot de persoonsgegevens die in opdracht van derden worden verwerkt. Relevante verantwoordelijkheden met betrekking tot de bescherming van persoonsgegevens waarvoor Veiligheidsregio Twente verwerkingsverantwoordelijke of verwerker is worden vastgelegd in verwerkersovereenkomsten.

Vanuit de betrokkenen is er een verschillende mate van relevantie voor beveiliging van persoonsgegevens, afhankelijk van de soorten gegevens die worden verwerkt binnen de processen van de Veiligheidsregio Twente.

De belangrijkste belanghebbenden met betrekking tot de beveiliging van persoonsgegevens zijn:

- Burgers die veilige verwerking van persoonsgegevens eisen;
- Medewerkers Veiligheidsregio Twente en medewerkers van derden die veilige behandeling van hun persoonsgegevens verwachten;
- Externe partijen en klanten die veilige verwerking van persoonsgegevens eisen, maar ook verwachten;
- Overheid die naleving van wet- en regelgeving eist.

## 1.2 Managementsysteem voor informatiebeveiliging (ISMS)

Beheersmaatregelen met betrekking tot beveiliging van persoonsgegevens zijn geïmplementeerd in het Managementsysteem voor informatiebeveiliging (ISMS) op basis van ISO27701-principes. Het ISMS wordt periodiek gecontroleerd binnen de reikwijdte die is vastgesteld in de contextbeschrijving. Het ISMS ondersteunt de implementatie van vereisten voor de verwerking en beveiliging van persoonsgegevens die zijn afgeleid van relevante wet- en regelgeving. Bovendien dienen afspraken met leveranciers en samenwerkingsverbanden als basis voor de beveiliging van persoonsgegevens.

## 1.3 Continue verbeteren

Risicoanalyse dient als een belangrijke basis voor continue verbetering van de beveiliging van persoonsgegevens binnen Veiligheidsregio Twente. Het gewenste risiconiveau wordt vastgesteld door middel van periodieke risicobeoordeling. Nieuwe beheersmaatregelen worden geïmplementeerd waar nodig, of bestaande beheersmaatregelen worden aangescherpt dan wel herzien. Het afbakenen of verkleinen van beheersmaatregelen die niet langer relevant zijn, is ook mogelijk om overmatige controle te voorkomen.

[1] Bedrijven/organisaties die tegen betaling gebruik maken van de diensten van Twente Safety Campus

# 2 Beleidsregels

## 2.1 Gedetailleerde beleidsregels

De onderstaande gedetailleerde beleidsregels worden geïmplementeerd in de processen van het ISMS om te voldoen aan de wettelijke verplichtingen en het gewenste beveiligingsniveau van persoonsgegevens te bereiken:

- De actualiteit van het privacy beleid en de toepasselijke verantwoordelijkheden wordt jaarlijks geëvalueerd en indien van toepassing bijgesteld;
- Er is een actueel overzicht van alle verwerkingsactiviteiten binnen Veiligheidsregio Twente;
- Toepasselijke gegevensverwerkingsvoorwaarden worden gecommuniceerd naar externen middels de website en intern via de gedragsregels;
- Verwerkersovereenkomsten worden vastgesteld met leveranciers en samenwerkingsverbanden die persoonsgegevens verwerken (mede) namens de Veiligheidsregio Twente;
- Datalekken worden geregistreerd, verholpen, geanalyseerd en geëvalueerd volgens een formele procedure. Dit omvat ook het melden van datalekken aan relevante autoriteiten indien nodig.
- Privacyaspecten worden in overweging genomen bij (interne) projecten;
- Persoonsgegevens worden bewaard in lijn met de vastgestelde bewaartermijnen conform wet- en regelgeving;
- Verzoeken van betrokkenen met betrekking tot inzage, wijziging, verwijdering of overdracht van hun persoonsgegevens worden volgens vast protocol verwerkt een adequate wijze verwerkt.

# 3 Middelen en verantwoordelijkheden

## 3.1 Middelen

De directie van Veiligheidsregio Twente draagt zorg voor het beschikbaar stellen van voldoende middelen voor de uitvoering en waarborging van het privacy beleid. Met inbegrip van bijbehorende voorzieningen en menskracht.

## 3.2 Verantwoordelijkheden

**Directie**

De directie van Veiligheidsregio Twente draagt het belang van de beveiliging van persoonsgegevens en naleving van relevante beleidsrichtlijnen uit. Zij zijn tevens verantwoordelijk voor het vaststellen van de noodzakelijke rollen, verantwoordelijkheden en bevoegdheden met betrekking tot de beveiliging van persoonsgegevens.

**Functionaris gegevensbescherming**

Tot de taken van het FG behoren:
- Indien nodig adviseren over het resultaat van een DPIA aan de directie;
- Toezicht houden op de naleving van wet- en regelgeving met betrekking tot privacy en de verwerking van persoonsgegevens;
- Aanspreekpunt voor betrokkenen en toezichthoudende autoriteiten en samenwerken met deze autoriteit bij gegevensbeschermingsaangelegenheden;
- Het bijhouden van een verantwoordingsregister en hierover rapporteren en adviseren richting directie en dagelijks bestuur.

**Privacy Officer**

Tot de taken van het Privacy Officer behoren:
- Afhandelen van beveiligingsincidenten met betrekking tot privacy, in samenwerking met de CISO;
- Beheren van het datalekken register;
- Beheren, bewaken en onderhouden van het verwerkingsregister;
- Controleren van registraties in daarvoor bestemde systemen en archieven;
- Beoordelen bescherming persoonsgegevens bij het aanschaffen of implementeren van nieuwe bedrijfsmiddelen;
- Beoordelen van gegevensverwerking door middel van een DPIA;
- Onderhouden van het privacy beleid;
- Afstemmen met de CISO over activiteiten op het gebied van informatiebeveiliging en het uitvoeren van controles en risicoanalyses;
- Opleiden en bewustmaken van medewerkers met betrekking tot gegevensbescherming.