

# Summ-IT



## Summ-IT en Europol Information System (EIS)

Met de introductie van Summ-IT binnen de Nederlandse politie werd tevens invulling gegeven aan de technische mogelijkheid om vanuit Summ-IT geautomatiseerd informatie aan te leveren aan het EIS. Hiermee wordt invulling gegeven aan de verplichting op basis van een Europol Raadbesluit en de wens de administratieve lastendruk terug te brengen. Om een ieder te informeren over EIS enerzijds en de procesinrichting vanuit Summ-IT naar EIS anderzijds hier een korte toelichting.

### **Wat is EIS?**

Het Europol Informatiesysteem (EIS) is een centrale **databank met informatie en intelligence** in relatie tot alle misdaad-gebieden waarvoor Europol gemandateerd is.

Deze databank bevat informatie met betrekking tot internationale zware criminaliteit over verdachte en veroordeelde personen, criminele netwerken en organisaties, misdrijven en de middelen die de criminelen in staat stellen ze te plegen.

Het EIS is een verwijzingssysteem dat de gebruiker in staat stelt te zien of informatie met betrekking tot een bepaalde persoon of een bepaald onderwerp beschikbaar is buiten de nationale of organisatorische jurisdictie.

Het EIS is ontwikkeld door Europol's eigen IT-afdeling en wordt gerund vanuit <sup>5.1.2</sup><sub>c</sub> . Het EIS is toegankelijk voor alle handhavingsinstanties in de EU en kan bevestigd worden in 21 talen.

### **Wie zijn de gebruikers?**

Het EIS kan door Europol en alle lidstaten van de EU gebruikt worden voor **de bevestiging en het opslaan van gegevens** met betrekking tot internationale zware criminaliteit en terrorisme. De gebruikers zijn functionarissen van Europol, de liaisons van de lidstaten en experts die door hun eigen land bij Europol zijn gedetacheerd, de medewerkers van de Nationale Europol Eenheden en medewerkers van bevestigde autoriteiten in de lidstaten. Tevens bestaat de mogelijkheid via <sup>5.1.2</sup><sub>c</sub> 

In het EIS worden de verschillende gegevens naar soort opgeslagen (personen, voertuigen, identiteitsbewijzen, etc.). <sup>5.1.2</sup><sub>c</sub> 

De eigenaar is verantwoordelijk voor de juistheid en betrouwbaarheid van de gegevens, zorgt ervoor dat de gegevens niet langer bewaard blijven dan is toegestaan, en zorgt dat de informatie actueel blijft.

Gebruikers behorende tot het bevestigd gezag in de lidstaten kunnen een zoekopdracht in het systeem invoeren om na te gaan of er informatie beschikbaar is die overeenkomt met hun zoekcriteria. In geval van een hit kan

aanvullende informatie worden aangevraagd via de gebruikers Nationale Europol Eenheid.

5.1.2.c

### **Waarom EIS?**

Door het EIS te raadplegen kan de gebruiker snel zien of de gezochte informatie beschikbaar is in een van de lidstaten van de EU of bij Europol (dus ook derde landen zoals Amerika, Canada en Australië).

5.1.2.c

### **Europol Nationale Eenheid.**

Het systeem wordt beheerd door Europol en staat ter beschikking van de aangewezen opsporingsinstanties in alle landen van de Europese Unie. Ieder land heeft een eigen Europol Nationale Eenheid, die zorgt voor de daadwerkelijke uitwisseling van opsporingsinformatie tussen de opsporingsdiensten en de EU-lidstaten. Het resultaat van de zoekopdracht in EIS geeft namelijk alleen aan dat de gezochte gegevens aanwezig zijn. De daadwerkelijke informatie kan verkregen worden via de Europol Nationale Eenheid. In Nederland is dat georganiseerd bij het LIRC van de Dienst DLIO.

### **Toegang tot informatie**

Alle EIS gebruikers kunnen (mits opgeleid en geautoriseerd) het systeem uitgebreid raadplegen, tenzij er een wettelijke beperking bestaat. 5.1.2.c

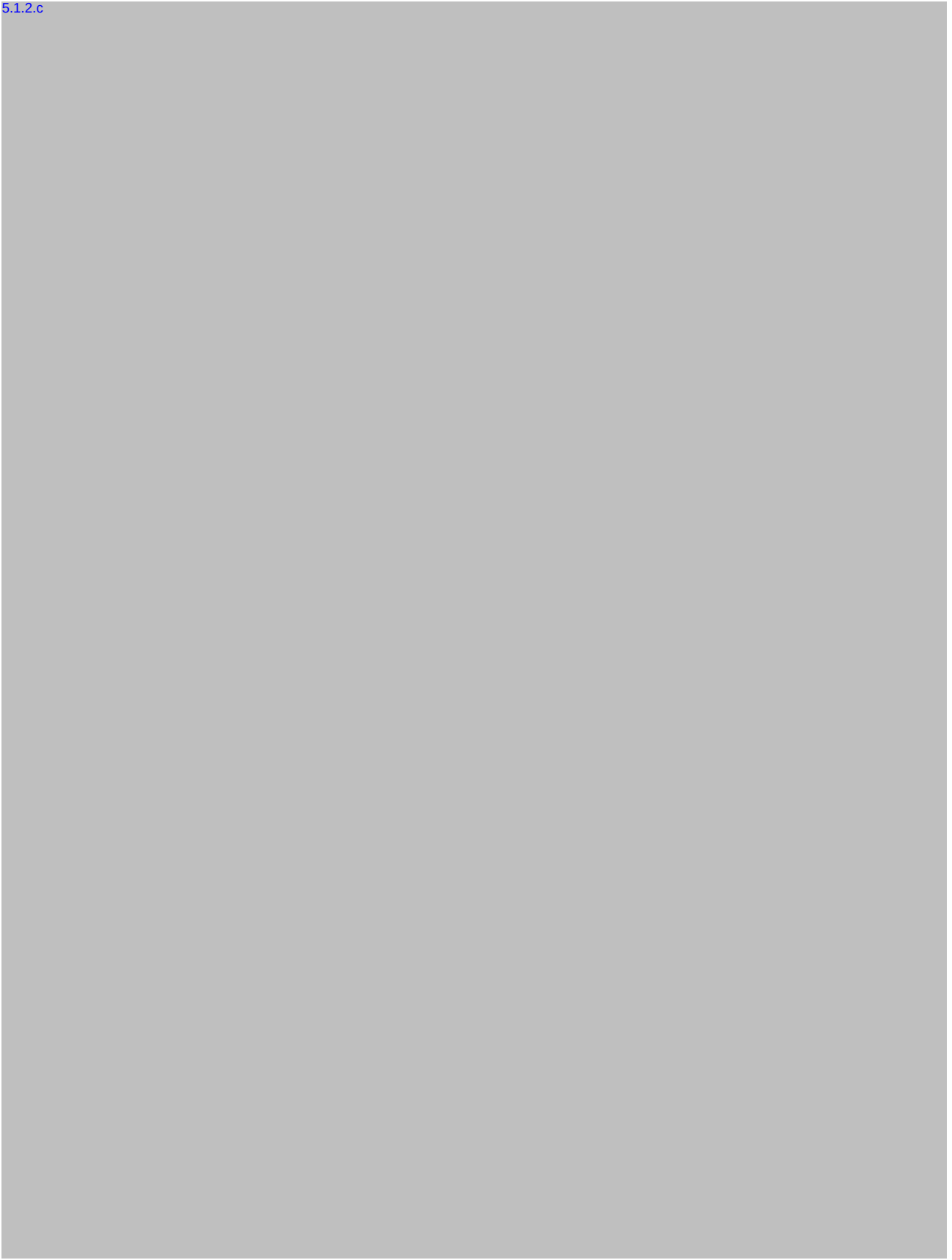
Nederland levert via Summ-IT gegevens aan EIS. Het toevoegen van foto en/of beeldmateriaal is handmatig mogelijk.

### **Eigendom van de informatie**

De Nationale Eenheid die de informatie voor opname in EIS heeft aangeleverd is voor Europol en de aangesloten lidstaten formeel de eigenaar. Europol, noch andere Europol-lidstaten kunnen op geen enkele wijze veranderingen aanbrengen in de informatie. De eigenaar (bron) is verantwoordelijk voor de juistheid en de betrouwbaarheid van de gegevens. Hij zorgt dat de informatie actueel is en bepaalt hoe lang deze bewaard moet worden.

## Summ-IT en EIS

5.1.2.c



5.1.2.c

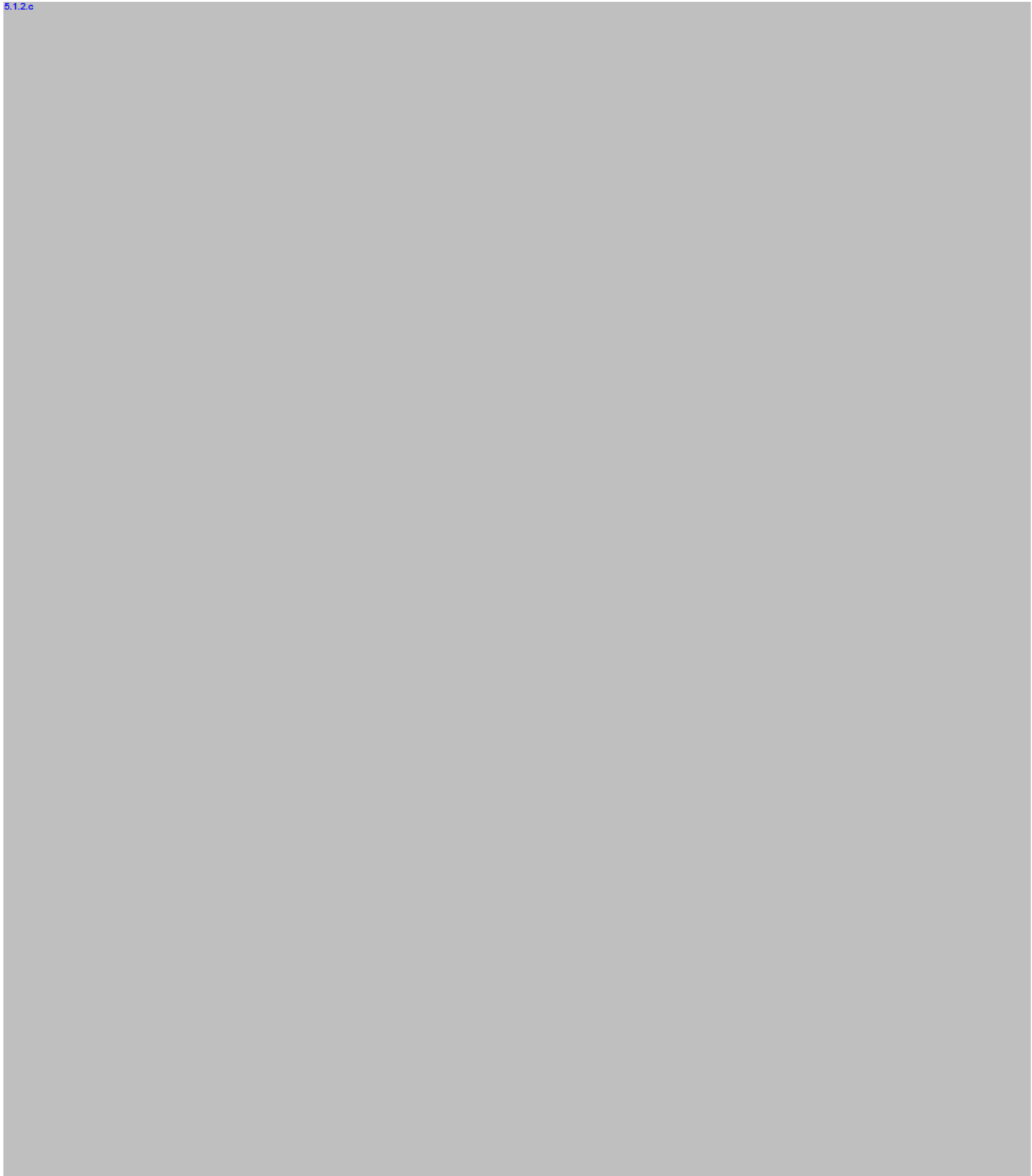


5.1.2.c



## Koppeling:

5.1.2.c



5.1.2.c



Voor algemene zaken over de uitwisseling met EIS kunt u contact opnemen met:

5.1.2.e

[@klpd.politie.nl](mailto:klpd.politie.nl)

5.1.2.e

5.1.2.e

Staf Korpsleiding  
Directie Strategie en Innovatie  
Bureau Managementinformatie

|                    |                                                              |                       |         |
|--------------------|--------------------------------------------------------------|-----------------------|---------|
| <b>Datum</b>       | 17 april 2025                                                | <b>Behandeld door</b> | 5.1.2.e |
| <b>Ons kenmerk</b> | #5335                                                        | <b>Kopie aan</b>      | n.v.t.  |
| <b>Uw kenmerk</b>  | Woo-verzoek inzake aandacht<br>vestigingen en OPS-coderingen | <b>Bijlage(n)</b>     | n.v.t.  |
| <b>Rubricering</b> | Openbaar                                                     |                       |         |

## Aanlevering data Nationale aandachtsvestigingen

### Achtergrond informatieverzoek

Bureau Managementinformatie (BMI) is door Woo-desk, 5.1.2.e verzocht om gegevens over Nationale aandachtsvestigingen te leveren ten behoeve van het Woo-verzoek van 5.1.2.e.

### Toelichting gegevens

Nationale aandachtsvestigingen is gedefinieerd als statistieken over het aantal actieve aandachtsvestigingen, hun duur en de voornaamste redenen voor verwijdering.

De cijfers zijn tot stand gekomen door het samenstellen van een query in Cognos op de database van het bronsysteem E&S (Executie & Signalering)

Daarbij is gebruik gemaakt van de volgende selecties: De aandachtsvestigingen die zijn opgemaakt bij personen met een instroomdatum vanaf 01 januari 2021 met een peildatum van 16 april 2025.

Deze cijfers zeggen iets over het aantal actieve en gesloten aandachtsvestigingen met een instroomdatum vanaf 01 januari 2021 t/m heden. In deze cijfers is echter geen informatie opgenomen over de reden voor verwijdering van de aandachtsvestiging. Deze gegevens zijn niet voorhanden.

### Kanttekeningen

Op de gegevens is een aantal kanttekeningen van toepassing.

De cijfers kennen een na-ijleffect, waardoor de cijfers op een later peilmoment hoger of lager uitvallen. Aantallen kunnen ook nog wijzigen als de status van de aandachtsvestiging wordt gewijzigd.



### Gegevens

Onderstaande tabellen weergeven het aantal actieve nationale aandachtsvestigingen met hierbij de periode vanaf de instroomdatum tot en met de peildatum. En het aantal afgehandelde aandachtsvestigingen uitgesplitst naar het instroomjaar op basis van de peildatum. De cijfers zijn verkregen uit E&S (Executie & signalering) op peildatum 16 april 2025. Het gaat om gegevens op landelijk niveau.

#### Actieve nationale aandachtsvestigingen:

| Vanaf peildatum                | Aantal       |
|--------------------------------|--------------|
| minder dan 1 jaar actief       | 4308         |
| tussen 1 jaar en 2 jaar actief | 2606         |
| tussen 2 jaar en 5 jaar actief | 4145         |
| <b>Eindtotaal</b>              | <b>11059</b> |

#### Afgehandelde nationale aandachtsvestigingen:

| Instroomdatum     | Aantal       |
|-------------------|--------------|
| 2021              | 2719         |
| 2022              | 3703         |
| 2023              | 2817         |
| 2024              | 2232         |
| 2025              | 154          |
| <b>Eindtotaal</b> | <b>11625</b> |

Bron: E&S (Executie & Signalering)

\*\*\*




---

**Instellingsprotocol voor het verder verwerken van politiegegevens  
ex artikel 13, eerste lid, onder d van de Wet politiegegevens (Wpg)  
Aandachtsvestigingen**

---

DE KORPSCHEF VAN POLITIE

GELET OP:

artikel 13, vierde lid, van de Wet politiegegevens (Wpg) en artikel 6:2 van het Besluit politiegegevens (Bpg);

OVERWEGENDE DAT:

het noodzakelijk is politiegegevens van **aandachtsvestigingen** verder te verwerken, ten behoeve van het onder de aandacht brengen van personen of zaken met het oog op het uitvoeren van een gevraagde handeling dan wel met het oog op een juiste bejegening van personen, binnen het zgn. Wpg-domein, door Politie, Koninklijke marechaussee, de vier (4) bijzondere opsporingsdiensten, de Rijksrecherche, alsmede de buitengewoon opsporingsambtenaren (boa's)

BESLUIT:

**Artikel 1 Begripsbepalingen**

In dit protocol wordt verstaan onder:

- a. de wet: de Wet politiegegevens (Wpg);
- b. het besluit: het Besluit politiegegevens (Bpg);
- c. de verwerking: de verwerking van politiegegevens als bedoeld in artikel 13, eerste lid, onder d van de Wet politiegegevens, die verband houdt met de in artikel 2 genoemde doelstelling;
- d. de verantwoordelijke: de korpschef, als bedoeld in artikel 27, Politiewet 2012;
- e. ambtenaar van politie: de ambtenaar, als bedoeld in artikel 2 van de Politiewet 2012, alsmede de ambtenaar van de Koninklijke marechaussee, voor zover werkzaam ter uitvoering van de politietaak, bedoeld in artikel 4, eerste lid, van de Politiewet 2012, alsmede de ambtenaar werkzaam bij een bijzondere opsporingsdienst, als bedoeld in artikel 2 van de Wet op de bijzondere opsporingsdiensten;
- f. buitengewoon opsporingsambtenaar (boa): de ambtenaar, als bedoeld in artikel 142, eerste lid, van het Wetboek van Strafvordering (WvSv), met een beperkte opsporingsbevoegdheid, afhankelijk van zijn taak- en functieomschrijving, zoals vermeld in de akte van opsporingsbevoegdheid en die werkzaam is in één van de zes (6) boa domeinen<sup>1</sup>;
- g. Wpg-domein: de ambtenaren van politie, als genoemd in dit artikel, onder e en f, die onderling politiegegevens kunnen delen (ter beschikking stellen);
- h. aandachtsvestiging: de registratie, voor interne berichtgeving (binnen het Wpg-domein), ten behoeve van het onder de aandacht brengen van personen of zaken met het oog op het uitvoeren van een gevraagde handeling dan wel met het oog op een juiste bejegening van personen;
- i. goed(eren): alle zaken en alle vermogensrechten, volgens artikel 3:1 Burgerlijk Wetboek;
- j. zaak: een voor menselijke beheersing tastbaar object, waarop men een recht kan hebben, volgens artikel 3:2 Burgerlijk Wetboek;
- k. handelingskader: een instructie, die het uitvoeren van een gevraagde handeling, dan wel een juiste bejegening van personen verwoord;
- l. looptijd: de verwerkingsperiode, met een begin- en einddatum, waarbinnen een aandachtsvestiging actief en actueel is en ter beschikking wordt gesteld.

---

<sup>1</sup> Regeling domeinlijsten buitengewoon opsporingsambtenaar



## Artikel 2 Doel

De verwerking heeft tot doel het ter ondersteuning van de (politie)taak verder verwerken van politiegegevens die worden verwerkt overeenkomstig artikel 8, 9 of 10 van de wet voor zover zij relevant zijn voor het onder de aandacht brengen van personen of zaken met het oog op het uitvoeren van een gevraagde handeling dan wel met het oog op een juiste bejegening van personen.

## Artikel 3 Categorieën van aandachtsvestigingen

Gelet op artikel 1, onder h van dit protocol worden de volgende categorieën van aandachtsvestigingen onderscheiden:

- a. **aandachtsvestiging op persoon (AOP):**  
voor het onder de aandacht brengen van één persoon of een groep van meerdere personen;
- b. **aandachtsvestiging op locatie (AOL):**  
voor het onder de aandacht brengen van een (geografische) locatie;
- c. **aandachtsvestiging op goed (AOG):**  
voor het onder de aandacht brengen van een goed of een zaak (als bedoeld in artikel 1 onder i en j);
- d. **aandachtsvestiging op werkwijze (AOW):**  
voor het onder de aandacht brengen van een bepaalde werkwijze of manier van handelen (modus operandi).

## Artikel 3a Categorieën van personen

Gelet op artikel 6b van de Wet politiegegevens en op artikel 2 van dit protocol, worden van de volgende categorieën van personen gegevens verwerkt:

- a. personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen gaan plegen;
  - b. slachtoffers van een strafbaar feit, of personen ten aanzien van wie op basis van bepaalde feiten wordt vermoed dat zij slachtoffer kunnen worden van een strafbaar feit;
  - c. derden, zoals getuigen of personen die anderszins informatie kunnen verstrekken over strafbare feiten of personen die contact hebben of banden onderhouden met één van de personen bedoeld onder a of d;
  - d. personen, die voor een strafbaar feit zijn veroordeeld;
- alsmede,
- e. vermiste personen (waaronder kinderen);
  - f. niet geïdentificeerde personen, waarvan herkenning wordt gevraagd;
  - g. ambtenaren van politie.

## Artikel 4 Soorten gegevens

Gelet op de in artikel 3, onder a genoemde categorie van **aandachtsvestigingen** en gelet op de in artikel 3a, onder a t/m f genoemde categorieën van personen, worden **ten hoogste** de volgende soorten gegevens verder verwerkt:

- a. relevante verwijzing naar bronregistraties waaruit de verdere verwerking afkomstig is;
- b. (slechts indien noodzakelijk) BSN, SKN, V-nummer, P-nummer;
- c. achternaam;
- d. voornamen/voorletters;
- e. geboorteplaats/-datum;
- f. woonplaats/postcode;
- g. woon-/verblijfadres;
- h. nationaliteit;
- i. geslacht;
- j. roepnaam/bijnaam/alias;

- k. burgerlijke staat;
- l. handelingskader;
- m. looptijd;
- n. gelet op artikel 5 van dit protocol,
  - i. fotografische afbeeldingen, beeld- en geluidmateriaal
  - ii. verwijzing naar dactyloscopische gegevens;
  - iii. verwijzing naar goederen- en zaak gegevens (als bedoeld in artikel 1 onder h en i);

Gelet op de in artikel 3a, onder g, genoemde categorieën van personen (ambtenaren van politie), worden **ten hoogste** de volgende soorten gegevens verder verwerkt:

- a. achternaam;
- b. voornamen/voorletters;
- c. dienstnummer, organisatieaanduiding, rang, functie;
- d. telecommunicatie-/contactgegevens;
- e. ambtseed/-belofte.

#### **Artikel 5 Bijzondere categorieën van (persoons)gegevens**

In aanvulling op artikel 4, onder n, worden slechts die gegevens verder verwerkt waaruit ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakbond blijkt, en de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, of gegevens over gezondheid, seksuele leven en seksuele gerichtheid wanneer dit onvermijdelijk is voor het doel en in aanvulling op de oorspronkelijke verwerking van politiegegevens betreffende de persoon/personen.

#### **Artikel 6 Beëindiging gegevensverwerking en vernietiging gegevens**

De gegevens worden

1. voortdurend getoetst op de noodzaak voor verdere verwerking;
2. vernietigd als:
  - a. de verdere verwerking wordt beëindigd en niet meer noodzakelijk is voor het in artikel 2 omschreven doel;
  - b. aan de verlangde uitvoering van de aandachtsvestiging gevolg is gegeven;
  - c. er zes (6) maanden zijn verstreken, na het overlijden van de persoon;
  - d. de looptijd van de aandachtsvestiging is verstreken;
  - e. uiterlijk **drie (3) jaar** na opmaking, tenzij verlenging noodzakelijk is, gelet op het nagestreefde doel.

#### **Artikel 7 Raadpleegbaarheid en ter beschikking stelling**

De gegevens als bedoeld in artikel 4 en 5 kunnen raadpleegbaar worden gesteld, aan daartoe geautoriseerde ambtenaren van politie en aan buitengewoon opsporingsambtenaren (boa's), werkzaam bij relevante partijen binnen het Wpg-domein, als bedoeld in artikel 1, onder g.

#### **Artikel 8 Beheer**

1. De verdere verwerking wordt gevoerd door, en onder verantwoordelijkheid van, de politiechefs van de eenheden;
2. Zij zien toe op:
  - a. de naleving van dit protocol;
  - b. de van toepassing zijnde wettelijke voorschriften en werkinstructies, door middel van:
    - i. het toezicht door de privacyfunctionaris;
    - ii. de controle door de interne audit, zoals bij of krachtens de wet bepaald;



3. Zij dragen zorg voor:

- a. de kwaliteit van de verwerkte gegevens;
- b. de raadpleegbaarheid en ter beschikking stelling van gegevens, als bedoeld in artikel 7.

#### **Artikel 9 Slotbepaling**

Dit instellingsprotocol wordt, in ieder geval, gepubliceerd via de interne communicatievoorziening(en) van de politie, onder verwijzing naar het opgestelde [Privacy Statement](#).

De korpschef van politie,

5.1.2.e

J.C. Knol MA

5.1.2.e



# Werkinstructie Summ-IT

Maart 2023



# Inhoudsopgave

|                                                        |   |
|--------------------------------------------------------|---|
| Werkdocument afspraken Summ - IT .....                 | 3 |
| Algemene afspraken .....                               | 3 |
| Invoer codering onderwerp regel Algemeen journaal..... | 3 |
| Invoer bericht Journaalgegevens .....                  | 3 |
| Invoer entiteiten .....                                | 4 |
| Documenten/Mails importeren .....                      | 4 |
| Gebruik label.....                                     | 5 |
| Voorbeeld invullen journaal.....                       | 6 |
| Indienen documenten.....                               | 6 |
| Overdragen journaalmutaties .....                      | 7 |

# Werkdocument afspraken Summ - IT

## Algemene afspraken

Voor wat betreft de invoer van de entiteiten gelden landelijke afspraken waar we ons aan te houden hebben.

De entiteit wordt altijd onder autorisatie 1 weggeschreven.

De journaalmutatie en de gekoppelde documenten worden onder autorisatie 7 weggeschreven.

Dit moet je handmatig aanpassen.

De entiteiten en het label (land) wordt gekoppeld aan het journaal.

De entiteiten worden ook gekoppeld aan het document die over die specifieke entiteit gaat.

In Summ-IT is het **Algemeen journaal** leidend. Dit houdt in dat elke vraag (P-Rhv) in Summ-IT opgestart wordt met een Algemeen journaalmutatie. [5.1.2.c](#)

[5.1.2.c](#), [5.2.1](#)

## Invoer codering onderwerp regel Algemeen journaal

De coderingen worden in HOOFDLETTERS in de onderwerp regel in onderstaande volgorde ingevoerd

[5.1.2.c](#)

[5.1.2.c](#)

[5.1.2.c](#)

Bij evt. vervolgcorrespondentie zal de journaalregel er als volgt uitzien:

[5.1.2.c](#)

## **BELANGRIJK:**

[5.1.2.c](#)

## Invoer bericht Journaalgegevens

Bij het aantekeningenveld vermeld je datum ontvangst / afzender / acties en een samenvatting van het verzoek



Zie afbeelding onderaan dit document.

### Invoer entiteiten

5.1.2.c



### PERSONEN:

5.1.2.c



### GEBEURTENIS:

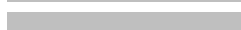
5.1.2.c



.



.



5.1.2.c



- 1.
- 2.
- 3.
- 4.
- 5.

### Documenten/Mails importeren

Importeer zoveel mogelijk het verzonden bericht tenzij je wijzigingen aanmaakt in het brondocument. Mocht dit gebeuren dan zal het brondocument en de uitzender apart geïmporteerd moeten worden.

Als het documenten of mails betreft die buiten Summ-it zijn opgemaakt, dan worden deze:

1. 5.1.2.c
- 

5.1.2.c

2.

3.

4.

5.

6.

7.

8.

9.

10.

11.

12.

13.

14.

15.

5.2.1

Onderwerpregel van het bronbericht is 5.1.2.c

Onderwerpregel van het uitgaande verzoek wordt 5.1.2.c

### Gebruik label

5.1.2.c

5.1.2.c

## Voorbeeld invullen journaal

5.1.2.c



## Indienen documenten

Wanneer je na het importeren en opmaken van een document van mening bent dat deze gereed is, kan het ter beoordeling aan een coördinator worden voorgelegd. Pas na het voltooien van een document is deze op vrije tekst in te lezen voor politie NL.

5.1.2.c



5.1.2.c



### **Overdragen journaalmutaties**

Verzoeken afkomstig van een Nederlandse Liaison Officer in het buitenland registreren we in Summit. Deze verzoeken worden als ze zijn geregistreerd in onze registratie overgedragen aan de registratie van de betreffende LO.

5.1.2.c



**Afzender**

5.1.2.e

Dienst Landelijke Informatie Organisatie (DLIO)  
Landelijk Internationaal Rechtshulp Centrum (LIRC)

5.1.2.e

@politie.nl

**Ontvanger(s)**

LIRC, IRC's

**Rubricering**

Politie INTERN - Politietaat

**Datum**

5 december 2023

**Behandeld door**

5.1.2.e

**Ons kenmerk**

5.1.2.e

**Kopie aan**

Landelijk Parket

**Uw kenmerk**

-

**Bijlage(n)**

1

**Onderwerp**

Handreiking internationale rechtshulp 2023

Beste collega's,

**Doel handreiking**

Deze handreiking is opgesteld om meer duiding te geven aan diverse (verouderde) aanwijzingen en wet- en regelgeving dat gaat over de internationale rechtshulp. Deze handreiking is bedoeld voor de uitvoerende praktijk met betrekking tot het verlenen van internationale rechtshulp. Deze handreiking is nadrukkelijk niet uitputtend bedoeld.

In deze handreiking wordt eerst het verschil uitgelegd tussen een politieel en een justitieel rechtshulpverzoek en in hoeverre de politie zelfstandig bevoegd is om een rechtshulpverzoek af te handelen. Hierbij wordt ook het proces kort beschreven. Ten tweede wordt ingegaan op het onderscheid tussen een veilig- en derde land. Tot slot wordt de derde landen toetsing besproken.

**1. Politieel of justitieel rechtshulpverzoek**

Er is diverse wet- en regelgeving van toepassing bij de vraag of een rechtshulpverzoek politieel of justitieel kan worden afgehandeld. De basis van internationale rechtshulp in het kader van strafzaken is gelegen in [het vijfde Boek van het Wetboek van Strafvordering: 'Internationale en Europese strafrechtelijke samenwerking.'](#) Voor de vraag of een rechtshulpverzoek door de politie zelfstandig afgehandeld kan worden, is [artikel 5.1.7.](#) van het Wetboek van Strafvordering (SV) relevant.

**Artikel 5.1.7. Wetboek van Strafvordering**

|              |                                                                                                                                                                                                                                                                                                                                                                               |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Lid 1</b> | Indien in het verzoek om rechtshulp uitsluitend om inlichtingen is gevraagd en voor het verkrijgen daarvan geen dwangmiddelen of bevoegdheden als bedoeld in de artikelen 126g tot en met 126z, 126zd tot en met 126zu en 126gg dan wel toepassing van artikel 126ff nodig zijn, kan de inwilliging en de uitvoering van het verzoek geschieden door een opsporingsambtenaar. |
| <b>Lid 2</b> | Uitvoering van verzoeken om rechtshulp krachtens het eerste lid vindt plaats onder gezag van de officier van justitie. Bij de afdoening van het verzoek worden de door de officier van justitie gegeven algemene en bijzondere aanwijzingen in acht genomen.                                                                                                                  |
| <b>Lid 3</b> | Van elke inwilliging van een verzoek om rechtshulp overeenkomstig het eerste lid wordt aantekening gehouden in een register waarvan het model door Onze Minister van Veiligheid en Justitie wordt vastgesteld. In de aantekening worden in ieder geval de aard van het verzoek, de hoedanigheid van de verzoeker en het gevolg dat aan het verzoek gegeven is opgenomen.      |

In artikel 5.1.7. SV is geregeld wanneer de politie zelfstandig bevoegd is om een rechtshulpverzoek uit te voeren en wanneer een officier van justitie betrokken moet worden bij de beslissing om informatie wel of niet te verstrekken.

In lid 1 staan twee voorwaarden waarbij het raadplegen van de officier van justitie achterwege gelaten kan worden. Dit zijn:

- ❖ Het verzoek tot rechtshulp gaat om het vragen van inlichtingen, en;
- ❖ Voor de verkrijging van deze inlichtingen zijn geen dwangmiddelen of bevoegdheden nodig.

Het eerste lid geeft een limitatieve opsomming van dwangmiddelen en bevoegdheden van met name bijzondere opsporingsbevoegdheden zoals stelselmatige observatie (126g Sv), het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel (126l Sv) of het vorderen van gegevens (126nc-126ni Sv).<sup>1</sup> Als deze bevoegdheden moeten worden ingezet om de gevraagde informatie te verkrijgen, dan is voorafgaand overleg met de officier van justitie noodzakelijk. In alle andere gevallen is de politie dus zelf bevoegd.

Lid 2 verwijst naar nadere algemene en bijzondere aanwijzingen. Een van deze aanwijzingen is de '[Aanwijzing inzake de informatie-uitwisseling in het kader van de wederzijdse rechtshulp in strafzaken \(552i Sv.\)](#)'. Deze aanwijzing verwijst nog naar het (oude) artikel 552i Sv, thans artikel 5.1.7 Sv. Aangezien de aanwijzing al sinds 1 januari 2009 van kracht is, en diverse (juridische) verwijzingen niet meer juist zijn, moet deze naar analogie worden toegepast. Dat betekent dat de tekst in de aanwijzing vertaald moet worden naar de bedoeling van de tekst. Daar wordt in de volgende paragraaf nader op ingegaan.

### 1.1. Zelfstandige bevoegdheid politie

In beginsel is alle informatie-uitwisseling tussen de nationale politie en een buitenlandse politiedienst politieke rechtshulp (pol-pol). Dit is alleen anders als door de wetgever of door het bevoegd gezag, het openbaar ministerie (OM), hierop uitzonderingen zijn gemaakt. In de '[Aanwijzing inzake de informatie-uitwisseling in het kader van de wederzijdse rechtshulp in strafzaken \(552i Sv.\)](#)' zijn in paragraaf 4.2 een aantal van deze uitzonderingen nader uitgewerkt. De grondslag van deze aanwijzing is artikel 5.1.7. lid 2 Sv.

De politie heeft de bevoegdheid om rechtshulpverzoeken zelfstandig af te handelen als de informatie al beschikbaar is in de politiesystemen. Het gaat dan om een **politeel rechtshulpverzoek**.

Het wordt **justitiële rechtshulp**,<sup>2</sup> of er is toestemming van een officier van justitie bij de afhandeling van een politiek verzoek nodig, als de gevraagde inlichtingen door het verzoekende land:

- ❖ Wordt gebruikt als bewijsmiddel in een strafrechtelijk onderzoek;
- ❖ Betrekking heeft op vervolging(en) in Nederland of in strijd is met het ne bis in idem-beginsel;<sup>3</sup>
- ❖ Een bijzondere opsporingsbevoegdheid<sup>4</sup> nodig is om die informatie te verkrijgen;
- ❖ Vrijheid ontnemende of -beperkende dwangmiddelen ingezet moet worden;
- ❖ Het gaat over verzoeken tot grensoverschrijdende observaties of gecontroleerde afleveringen;<sup>5</sup>
- ❖ Het verzoek betrekking heeft op TCI-informatie;<sup>6</sup>
- ❖ Het verzoek betrekking heeft op politieke of fiscale delicten;<sup>7</sup>
- ❖ Het gaat om justitiële gegevens, zoals een uitdraai van de Justitiële InformatieDienst (JustID).<sup>8</sup>

<sup>1</sup> Volledig: Bijzondere bevoegdheden tot opsporing (Titel IVA), bijzondere bevoegdheden tot opsporing voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband (Titel V), bijstand aan opsporing door burgers (Titel VA), bijzondere bevoegdheden tot opsporing van terroristische misdrijven (Titel VB), verkennend onderzoek (126gg Sv, Titel VE) en verbod op doorlaten (126ff Sv).

<sup>2</sup> Bij justitiële rechtshulp gaat het er in de kern om dat de resultaten als bewijs worden gebruikt. Hier zal ook een justitieel verzoek (afkomstig van een justitiële autoriteit) aan ten grondslag moeten liggen.

<sup>3</sup> Het ne bis in idem-beginsel betekent in het strafrecht dat iemand niet twee keer voor hetzelfde feit kan terechtstaan en mag worden gestraft.

<sup>4</sup> Bevoegdheden die genoemd staan in Sv, zie voetnoot 1.

<sup>5</sup> Zie: 'Aanwijzing rechtshulpverzoeken voor grensoverschrijdende observaties.'

<sup>6</sup> Team Criminele Inlichtingen (TCI). Het verstrekken van TCI-informatie aan het buitenland vindt plaats met toestemming van de TCI-officier van justitie.

<sup>7</sup> Wanneer een rechtshulpverzoek betrekking heeft op politieke of fiscale delicten, moet een machtiging worden verkregen van het ministerie van Justitie en Veiligheid.

<sup>8</sup> Justitiële documentatie kan conform de Wet justitiële en strafvorderlijke gegevens (Wjsg) en het Besluit justitiële gegevens



Naast vorenstaande gevallen dient ook overleg met de (L)IRC-officier plaats te vinden als bij een politieel verzoek sprake is van een weigeringsgrond opgenomen in art. 5.1.5 Sv.

In bepaalde gevallen en in overleg met het openbaar ministerie kunnen politieke verzoeken soms ook justitieel afgehandeld worden. Gedacht kan worden aan een rijbewijsfoto die politieel is opgevraagd en waarvoor later via de politielijn toestemming voor gebruik als bewijs wordt gevraagd.

## 1.2 Proces

In geval van een politieel verzoek, kan de politie via het IRC of het LIRC direct contact leggen met het verzoekende land. Als het gaat om een justitieel verzoek, dan moet dit via het (L)IRC OM, of als er geen regionale duiding is of een specifieke zaak onder ligt, via de LIRC-officier (landelijk parket). Als het gaat om een verzoek van (of naar) derde landen, dan dient ook de Afdeling Internationale Rechtshulp in Strafzaken (AIRS) van het ministerie van Justitie en Veiligheid te worden betrokken. Dit geldt specifiek voor de gevallen waarin sprake is van verstrekking van politiegegevens aan landen waarbij mensenrechten- en veiligheidsrisico's kunnen spelen.

Dat proces ziet er dan als volgt uit.



Figuur 1: stroomproces politieel en justitieel rechtshulpverzoek (uitgaand)

Bij een derde landen toetsing gelden nadere eisen, zie hiervoor figuur 4

## 2. Veilige landen en derde landen

5.2.1

Hierin wordt onderscheid gemaakt tussen veilige landen en zogeheten derde landen. Bij een derde land dient altijd een derde landen toetsing te worden uitgevoerd. Dit gebeurt middels de '**Instructie doorgifte van politiegegevens aan derde landen**', deze is als bijlage toegevoegd. Deze instructie wordt binnen afzienbare tijd herzien, maar is tot die tijd gewoon van kracht.

### 2.1 Verschillend verstrektingsregime

Voor de veilige landen geldt een makkelijker verstrektingsregime dan voor derde landen. Voor veilige landen zijn voldoende (privacy)waarborgen vastgesteld dat de informatie die wij verstrekken ook veilig wordt verwerkt. Bij derde landen is dat niet vastgesteld en dient er altijd een derde landen toetsing te worden gedaan.<sup>9</sup> Nu wordt nader ingegaan op de vraag wat een veilig land is, welke categorieën derde landen er zijn en wat de derde landen toetsing inhoudt.

### 2.2 Veilige landen

Als veilige landen worden alle 27 lidstaten van de Europese Unie (EU) verstaan.<sup>10</sup> Dit is af te leiden uit artikel 15a lid 1 van de Wet politiegegevens (Wpg) (zie volgende pagina). Zolang het om politieke rechtshulp gaat, kan de politie de uitwisseling zelfstandig uitvoeren. Dit geldt ook voor diverse organen en instanties van de EU, zoals Europol en Eurojust.

(Bij) niet door de politie aan het buitenland verstrekt worden. Zo'n verzoek dient door het openbaar ministerie te worden afgehandeld.

<sup>9</sup> Zie hiervoor bijlage I 'Instructie doorgifte van politiegegevens aan derde landen'. De toetsing wordt uitgevoerd middels het derde landen formulier.

<sup>10</sup> Artikel 15a Wpg. De samenstelling van de Europese Unie per 1 februari 2020: België, Bulgarije, Duitsland, Cyprus, Denemarken, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Malta, Nederland, Oostenrijk, Polen, Portugal, Roemenië, Slowakije, Slovenië, Spanje, Tsjechië, en Zweden.



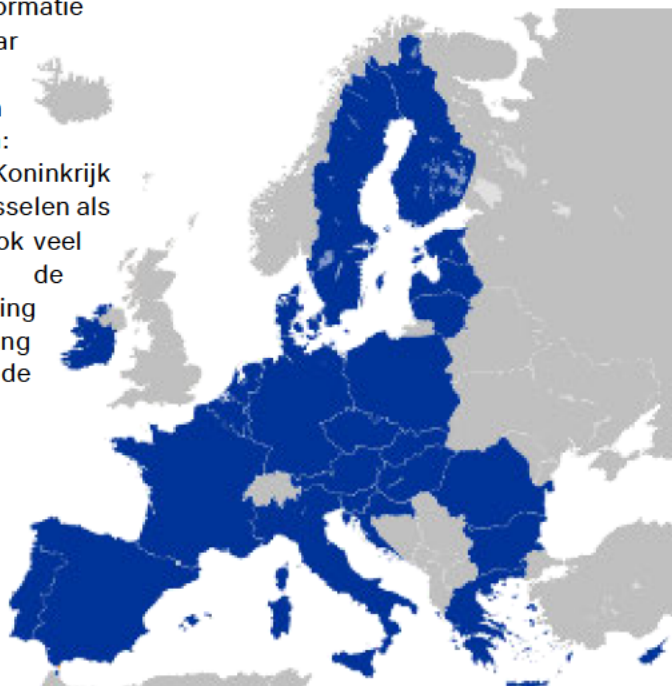
| Artikel 15a Wet politiegegevens |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Lid 1</b>                    | Politiegegevens worden of kunnen worden ter beschikking gesteld aan de bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties die zijn opgericht krachtens de hoofdstukken 4 en 5 van Titel V van het verdrag betreffende de werking van de Europese Unie, die zijn belast met de taken, bedoeld in artikel 1, onderdeel a, voor zover dat voortvloeit uit een rechtsinstrument op grond van het verdrag betreffende de werking van de Europese Unie. |

### 2.3. Derde landen die veilig zijn

Alle landen die buiten de 27 lidstaten van de EU vallen, zijn derde landen. Hoewel de wet niet expliciet spreekt van 'categorieën', zijn er wel drie soorten derde landen te onderscheiden die ook als veilig kunnen worden aangemerkt. De landen die buiten deze drie categorieën vallen, zijn overige derde landen waarbij een nadere toetsing op de waarborgen noodzakelijk is.

#### 2.3.1 Categorie 1: een adequaatheidsbesluit (art. 17a, lid 1, Wpg)

In eerste instantie kan de Europese Commissie (EC) een zogeheten adequaatheidsbesluit nemen. Dat betekent dat de EC een beslissing neemt dat voor één specifiek land er voldoende waarborgen zijn waardoor de lidstaten zonder toetsing informatie kunnen uitwisselen. Op dit moment is er maar één land waarvoor een adequaatheidsbesluit is genomen: het **Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland** (hierna: Verenigd Koninkrijk). Met het Verenigd Koninkrijk kunnen wij op dezelfde wijze informatie uitwisselen als met een veilig land. Let op: De EC neemt ook veel adequaatheidsbesluiten op grond van de Algemene verordening gegevensbescherming (Avg). Die beslissingen hebben geen betrekking op de informatie-uitwisseling op grond van de Wet politiegegevens (Wpg).



Figuur 2: de huidige lidstaten van de Europese Unie (2020)

#### 2.3.2 Categorie 2: Een juridisch bindend instrument (art. 17a, lid 2, sub a Wpg)

Bij ontstentenis van een besluit van de EC zijn er twee opties. De eerste optie is een juridisch bindend instrument, zoals een verdrag of (nationale) wetgeving in formele zin (door de Staten-Generaal vastgesteld). Er zijn op dit moment twee gevallen waarin dit van toepassing is.

Allereerst onze **BES-eilanden: Bonaire, Sint Eustatius en Saba**. De BES-eilanden maken deel uit van Europees Nederland en vallen dus onder het Koninkrijk der Nederlanden. De eilanden heten samen **Caribisch Nederland**. Ten opzichte van de EU heeft Caribisch Nederland de status van 'landen en gebieden overzee' (LGO). Hierdoor geldt EU-regelgeving niet voor de BES-eilanden. Daarom was het noodzakelijk om extra regels voor de BES-eilanden in de Wpg op te stellen (§ 5a. Bonaire, Sint Eustatius en Saba). Met deze eilanden kunnen we dus gewoon informatie uitwisselen zoals dat op nationaal niveau gebeurt. Dit geldt niet voor de onafhankelijke landen binnen het Koninkrijk: de CAS-eilanden Curaçao en Aruba. (Voor Sint-Maarten zie paragraaf 2.3.3). De CAS-eilanden zijn namelijk niet ondergeschikt aan onze wetten in formele zin.

Het tweede voorbeeld zijn de landen binnen het Schengen acquis<sup>11</sup>: **IJsland, Noorwegen, Zwitserland en Liechtenstein**. Ook met deze landen kunnen we uitwisselen alsof het een veilig land is.

<sup>11</sup> Het akkoord en alle aanverwante overeenkomsten die gaan over het vervallen van de controles op de binnengrenzen van landen, vormen samen het zogeheten 'Schengen-acquis.'



### 2.3.3 Categorie 3: Goedgekeurd door Wpg-partijen (art. 17a, lid 2, sub b Wpg)

Als een juridisch bindend instrument ontbreekt, kan een lidstaat er zelf ook voor kiezen om een besluit te nemen dat een land voldoende waarborgen biedt. In Nederland is afgesproken dat een gezamenlijke beslissing van een commissie van de Wpg-partijen hiertoe kan leiden. Naast de nationale politie en het landelijk parket (OM) zijn er ook nog de Koninklijke Marechaussee, de rijksrecherche<sup>12</sup>, de vier bijzondere opsporingsdiensten<sup>13</sup> en de werkgevers van de bijzondere opsporingsambtenaren.<sup>14</sup> Op dit moment (december 2023) is er één derde land dat door de commissie op de nominatie staat om beoordeeld te worden als een land dat voldoende waarborgen heeft: **Sint Maarten**. De verwachting is dat Sint Maarten medio 2024 ook als veilig land kan worden aangemerkt.

### 2.4 Conclusie derde landen als veilige landen

5.2.1

Met deze landen kan dus gewoon informatie worden uitgewisseld alsof het een EU-land is. Dit geldt dus voor het Verenigd Koninkrijk (art. 17a lid 1 Wpg), voor IJsland, Noorwegen, Zwitserland en Liechtenstein en onze BES-eilanden Bonaire, Sint Eustatius en Saba (art. 17a lid 2 sub a Wpg) en (vanaf medio 2024) ook Sint Maarten (art. 17a lid 2 sub b Wpg).

### 2.5 Restcategorie: overige derde landen (artikel 17a, lid 3 Wpg)

Als geen van de voorgenoemde situaties zich voordoen, is een land een zogeheten derde land en moet er altijd een derde landen toetsing gedaan worden volgens de 'Instructie doorgifte van politiegegevens aan derde landen.'<sup>15</sup>



Figuur 3: overzicht veilige (en derde) landen in Europa  
*Alle overige landen ter wereld die niet op deze kaart staan zijn derde landen*

<sup>12</sup> Artikel 1, sub f, Wpg.

<sup>13</sup> De vier bijzondere opsporingsdiensten: de Fiscale Inlichtingen- en Opsporingsdienst (FIOD), de Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport (ILT), de Inlichtingen- en Opsporingsdienst van de Nederlandse Voedsel- en Warenautoriteit (NVW) en de Directie Opsporing van de Nederlandse Arbeidsinspectie (NA) (artikel 1, sub c, Besluit politiegegevens bijzondere opsporingsdiensten).

<sup>14</sup> Artikel 1, sub c Besluit politiegegevens buitengewoon opsporingsambtenaren (zoals gemeenten).

<sup>15</sup> Zie bijlage I.

### 3. Derde landen toetsing

Als er sprake is van een derde land, dan is niet vooraf vastgesteld of er voldoende waarborgen zijn die ervoor zorgen dat de informatie die wij verstrekken goed en veilig worden verwerkt. Ook spelen de mogelijke veiligheidsrisico's mee voor de persoon waarvan de informatie wordt verstrekt. Voorkomen moet worden dat wij als Nederlandse politie informatie aan een land verstrekken, waardoor vervolgens personen geschonden worden in hun mensenrechten (zoals de doodstraf). Hierin vindt een belangenafweging plaats tussen enerzijds de privacy van de betrokkene en anderzijds het doel en belang van de verstrekking. Hierin wordt de proportionaliteit en subsidiariteit van de verstrekking getoetst, evenals het in kaart brengen van mogelijke negatieve neveneffecten.

De toetsing geschiedt door toepassing van de 'Instructie doorgifte van politiegegevens aan derde landen'.<sup>16</sup> In geval van het verstrekken van politiegegevens, is de politie in alle gevallen verantwoordelijk om de toets op grond van de Wpg uit te voeren. De toets wordt uitgewerkt en nagelopen met het 'derde landen formulier'. Als er sprake is van een politieel of justitieel rechtshulpverzoek, dient het openbaar ministerie de eisen van rechtshulpverzoeken uit het Wetboek van Strafvordering na te lopen, zoals nagaan of er sprake is van mogelijk collusiegevaar met (lopende) onderzoeken. De toets van de politie en het openbaar ministerie gebeurt gelijktijdig. De politie draagt te allen tijde zorg voor het invullen en verwerken van deze derde landen formulieren, volgens de documentatieplicht van de Wpg (art. 32 Wpg).

Zoals eerder gezegd dient bij een justitieel rechtshulpverzoek ook de Afdeling Internationale Rechtshulp in Strafzaken (AIRS) van het ministerie van Justitie te worden betrokken. Dit geldt specifiek voor de gevallen waarin sprake is van verstrekking van politiegegevens aan landen waarbij mensenrechten- en veiligheidsrisico's kunnen spelen.



Figuur 4: Stroomschema politieel en justitieel (uitgaand) rechtshulpverzoek bij derde landen

Deze handreiking dient alleen als basis te worden gebruikt. Elke verstrekking, of dit nu aan een veilig land of een derde land is, dient altijd op zijn merites te worden beoordeeld.

5.1.2.e

Jurist 5.1.2.e

<sup>16</sup> Zie bijlage I.







Reeds openbaar

















**Afzender**

5.1.2.e

Dienst Landelijke Informatie Organisatie (DLIO)  
Landelijk Internationaal Rechtshulp Centrum (LIRC)  
@politie.nl

**Ontvanger(s)**

LIRC, IRC's

**Rubricering**

Politie INTERN - Politietaak

**Datum** 5 december 2023**Ons kenmerk**

5.1.2.e

**Uw kenmerk**

-

**Behandeld door**

5.1.2.e

**Kopie aan**

Landelijk Parket

**Bijlage(n)**

2

**Onderwerp** Handreiking verstrekking politie-antecedenten

Beste collega's,

Regelmatig komen er bij het LIRC vragen binnen over het wel of niet verstrekken van antecedenten aan het buitenland. Er is onduidelijkheid over het begrip antecedent, wie antecedenten aan het buitenland mag verstrekken en binnen hoeveel tijd na eerste verwerking deze antecedenten nog mogen worden verstrekt. Ook is het niet duidelijk of er een onderscheid moet worden gemaakt tussen een EU-land (art. 15a Wpg) en een derde land (art. 17a Wpg). Deze handreiking is geschreven voor medewerkers van het LIRC (Interpol, Europol, Sirene en Team Liaisons) en de regionale IRC's om hier duidelijkheid over te scheppen en om hier eenduidig in te gaan werken en te gaan verstrekken.

In deze handreiking wordt opeenvolgend besproken:

1. Onderscheid tussen justitiële documentatie (antecedenten) en politie-antecedenten;
2. Onderscheid tussen veilige landen en derde landen;
3. Verstrekken politie-antecedenten aan veilige landen;
4. Verstrekken politie-antecedenten aan derde landen;
5. Aanvullende disclaimer bij verstrekking van politie-antecedenten;
6. Verstrekken van gevarenclassificaties.

## **1. Onderscheid tussen justitiële documentatie (antecedenten) en politie-antecedenten**

Als er over antecedenten wordt gesproken, dan wordt bedoeld een uitdraai van een specifiek persoon uit het systeem van de Justitiële InformatieDienst (JustID). Hierop staan alle (onherroepelijke) vervolgingen die door de rechtbank (of een hoger/ander rechtsorgaan) zijn uitgesproken of bepaalde (beleids)sepots. Deze informatie is justitiële informatie. Dat betekent dat alleen justitie en dus het openbaar ministerie (functioneel/landelijk parket) deze informatie mag verstrekken aan het buitenland.<sup>1</sup>

<sup>1</sup> Justitiële informatie valt niet onder de Wet politiegegevens, maar onder de Wet justitiële en strafvorderlijke gegevens (Wjsg).

Politie-antecedenten zijn registraties die door de politie<sup>2</sup> zijn aangemaakt en verwerkt. Deze zijn terug

5.1.2.c

Figuur 1: een voorbeeld van een overzicht van politie-antecedenten

## 2. Onderscheid tussen veilige landen en derde landen

Voor de veilige landen geldt een makkelijker verstrekingsregime dan voor derde landen. <sup>5.2.1</sup>

Bij derde landen dient er altijd een derde landen toetsing te worden gedaan.<sup>3</sup> Er zijn ook een aantal derde landen die op een andere wijze als veilig land zijn aangemerkt. In deze handreiking scharen we deze derde landen ook onder de definitie van veilig land.

Als veilige landen worden aangemerkt:

- Alle EU-lidstaten;<sup>4</sup>
- Het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland (hierna het VK);<sup>5</sup>
- De landen binnen het Schengen acquis: IJsland, Noorwegen, Zwitserland en Liechtenstein;<sup>6</sup>
- De bijzondere gemeenten van Caribisch Nederland: Bonaire, Sint-Eustatius en Saba.<sup>7</sup>

Alle andere landen worden aangemerkt als een derde land.



Figuur 2: Overzicht veilige landen in Europa (d.d. 5 december 2023)  
Alle overige landen ter wereld die niet op deze kaart staan zijn derde landen

<sup>2</sup> Of in het kader van hun politietaak, de Koninklijke Marechaussee (Kmar).

<sup>3</sup> Zie hiervoor de 'Tijdelijke instructie doorgifte van politiegegevens aan derde landen en internationale organisaties'.

<sup>4</sup> Artikel 15a Wpg. De samenstelling van de Europese Unie per 1 februari 2020: België, Bulgarije, Duitsland, Cyprus, Denemarken, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Malta, Nederland, Oostenrijk, Polen, Portugal, Roemenië, Slowakije, Slovenië, Spanje, Tsjechië, en Zweden.

<sup>5</sup> Artikel 17a, eerste lid Wpg. Voor het VK is door de Europese Commissie een adequaatheidsbesluit genomen.

<sup>6</sup> Artikel 17a, tweede lid, sub a Wpg. Het akkoord en alle aanverwante overeenkomsten die gaan over het vervallen van de controles op de binnengrenzen van landen, vormen samen het zogeheten 'Schengen acquis'.

<sup>7</sup> Artikel 17a, tweede lid, sub a Wpg. De regels over de BES-eilanden is nader geregeld in § 5a van de Wpg. Let op: Aruba, Curaçao en Sint Maarten vallen hier niet onder en zijn dus een derde land. Sint Maarten wordt in 2024 wel een veilig land.

### 3. Verstrekken politie-antecedenten aan veilige landen

Een informatieverzoek van een veilig land naar politie-antecedenten kan op grond van het Zweeds Kaderbesluit<sup>8</sup> worden verstrekt. Een van de hoofddoelstellingen van de Europese Unie (EU) is namelijk om haar burgers een hoog niveau van veiligheid te bieden in een ruimte van vrijheid, veiligheid en recht. De uitwisseling van informatie en inlichtingen over criminaliteit en strafbare activiteiten vormt daarmee de grondslag voor samenwerking inzake rechtshandhaving. Informatie wordt versterkt op grond van artikel 15a Wpg<sup>9</sup> en op grond van de politietaak volgens artikel 3 Politiewet.

Als je een overzicht van politie-antecedenten erbij pakt van een veelpleger die al langer bekend is bij de politie, dan is te zien dat de registraties soms (fors) verder teruggaan dan de vaak gehanteerde 5 jaar.<sup>10</sup> Dit klopt. Voor politie-antecedenten is namelijk een apart protocol opgesteld: het *Protocol Herkenningsdienst Systeem d.d. 20 september 2010* (Protocol HKS). Hierin is vastgesteld dat politie-antecedenten in ieder geval na verloop van 30 jaar moeten worden vernietigd.<sup>11</sup>

#### Wat mag ik dan verstrekken aan veilige landen?

Als een veilig land een concreet verzoek doet voor een persoon 'komt hij voor?', dan kunnen relevante politie-antecedenten worden gedeeld met de verzoeker. Met een concreet verzoek wordt bedoeld, een specifieke vraag over een persoon (of personen). Een *fishing expedition*<sup>12</sup> valt hier dus niet onder. Als dus wordt gevraagd 'komt hij voor in jullie systemen voor geweldsdelicten', dan worden alleen de relevante geweldsdelicten gedeeld.<sup>5.1.2.c</sup>

. Voor misdrijven geldt een verjaringstermijn van 6, 12 of 20 jaar. Ernstige misdrijven verjaren niet. Zie voor de termijnen bijlage 1.

5.1.2.c

### 4. Verstrekken politie-antecedenten aan derde landen

Voor het verstrekken van informatie aan een derde land geldt dat de derde landen toetsing gedaan moet worden.<sup>13</sup> Daar moet dus altijd een derde landen formulier voor worden opgemaakt, waarbij getoetst is of de verstrekking proportioneel is, subsidiair is en of er sprake is van mogelijke negatieve neveneffecten.<sup>5.1.2.c</sup>

<sup>8</sup> Kaderbesluit 2006/960/JBZ van de Raad van 18 december 2006 betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de rechtshandavingsautoriteiten van de lidstaten van de Europese Unie.

<sup>9</sup> In geval van het VK is de grondslag artikel 17a, eerste lid Wpg, en de grondslag voor de vier (overige) Schengenlanden + BES is artikel 17a, lid 2 Wpg. Hoewel het een andere grondslag betreft, heeft dat geen gevolgen voor de verstrekking.

<sup>10</sup> De standaard termijn is 5 jaar op grond van artikel 8 Wpg (informatieverwerking op grond van de politietaak). Er zijn echter ook andere gronden mogelijk, waardoor de termijn kan afwijken (zoals artikel 9 of 10 Wpg). Voor antecedenten is echter een langere termijn vastgesteld conform artikel 13 Wpg, namelijk 30 jaar.

<sup>11</sup> Artikel 6, tweede lid Protocol HKS

<sup>12</sup> Een *fishing expedition* is een algemene zoektocht tot bewijsgaring zonder een duidelijk afgebakend, rechtmatig doel.

<sup>13</sup> Tijdelijke instructie doorgifte van politiegegevens aan derde landen en internationale organisaties.



5.1.2.c

5.1.2.c

5.1.2.c

## 5. Verstrekken van gevarenclassificaties

5.1.2.c

5.1.2.c Deze handreiking dient alleen als basis te worden gebruikt. Elke verstrekking, of dit nu aan een veilig land of een derde land is, dient altijd op zijn merites te worden beoordeeld.

5.1.2.e

Jurist 5.1.2.e





## Bijlage 1 – Verjaringstermijnen

| Overzicht verjaringstermijnen misdrijven <sup>14</sup> |                                                                                                                                                                                                        |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verjaringstermijn                                      | Soort misdrijf                                                                                                                                                                                         |
| <b>6 jaar</b>                                          | Misdrijven waarop een boete, hechtenis of gevangenisstraf staat van maximaal 3 jaar. Zoals stroperij en het niet opvolgen van een ambtelijk bevel.                                                     |
| <b>12 jaar</b>                                         | Misdrijven waarop een gevangenisstraf staat van meer dan 3 jaar. Bijvoorbeeld diefstal, oplichting en vervalsing van documenten.                                                                       |
| <b>20 jaar</b>                                         | Misdrijven waarop een gevangenisstraf staat van 8 jaar of meer. Bijvoorbeeld afpersing, aanranding en samenspanning tot bepaalde misdrijven.                                                           |
| <b>Geen</b>                                            | Misdrijven waarop een gevangenisstraf staat van 12 jaar of meer. Zoals moord, doodslag, verkrachting en mensenhandel.<br>Bepaalde zedenmisdrijven waarop een gevangenisstraf staat van 8 jaar of meer. |

## Bijlage 2 – Gevarenclassificaties

5.1.2.e

<sup>14</sup> Zie hiervoor artikel 70 van het Wetboek van Strafrecht.



**Rubricering**

Niet Vertrouwelijk

**Datum** 11 maart 2024  
**Ons kenmerk** 2024-0014468

**Behandeld door** 5.1.2.e - Gegevensautoriteit politie  
**Bijlage(n)** 2

**Onderwerp** Besluit vaststellen passende waarborgen Sint-Maarten ex. artikel 17a tweede lid onder b Wpg

De korpschef,

Overwegende dat:

- Het voor de goede samenwerking in het kader van criminaliteitsbestrijding en het handhaven van de rechtsorde van essentieel belang is dat politiegegevens kunnen worden doorgegeven;
- Sint-Maarten op grond van het gegevensbeschermingsrecht kwalificeert als derde land (artikel 1 onder v Wpg jo. artikel 355 Verdrag Werking EU);
- Voor de doorgifte van politiegegevens naar derde landen een strenger regime geldt (artikel 17a Wpg);
- Er voor Sint-Maarten geen adequaatheidsbesluit (ex. artikel 17a eerste lid Wpg) is;
- Structurele doorgifte mogelijk is als er passende waarborgen ter bescherming van persoonsgegevens zijn;

Heeft vastgesteld dat:

- Sint-Maarten een Landsverordening Politiegegevens (A.B. 2014, no 50) heeft;
- Deze Landsverordening wat inhoud betreft overeenkomt met de Wpg BES;
- Van de Wpg BES is, bij de implementatie van Richtlijn (EU)2016/680, vastgesteld dat dit een voldoende passende waarborging ter bescherming van persoonsgegevens, ex. artikel 17a tweede lid onder a Wpg, bevat;
- Sint-Maarten daarmee in de nationale wetgeving waarborgen biedt ter bescherming van persoonsgegevens en voorwaarden stelt voor voldoende technische en organisatorische maatregelen ter beveiliging van deze gegevens;
- Betrokkenen in Sint-Maarten het recht hebben kennis te nemen van de over hun verwerkte politiegegevens en deze kunnen laten verbeteren, aanvullen of af laten schermen;
- De verwerkingsverantwoordelijke verplicht is audits uit te laten voeren en een privacyfunctionaris aan te laten stellen die namens hem toezicht houdt;
- De Raad voor de rechtshandhaving, als onafhankelijke toezichtsorgaan, toezicht houdt op de verwerking van politiegegevens (artikel 3 vijfde lid Rijkswet raad voor de rechtshandhaving jo. artikel 37 Landsverordening politiegegevens);
- De Raad voor de rechtshandhaving daadwerkelijke toezichtsacties uitvoert, waarbij het toezicht op de verwerking van politiegegevens op Sint-Maarten voor 2023 staat gepland;
- De Franse Republiek en het Koninkrijk der Nederlanden een verdrag over de politieke samenwerking op Sint-Maarten hebben gesloten, waarbij ook is gekeken naar de uitwisseling van politiegegevens;

- Frankrijk, als lidstaat van de EU, zich net als Nederland moet houden aan de Europese regels met betrekking tot doorgifte naar derde landen;
- Sint-Maarten vanwege de aanwezigheid van nationale wetgeving en het onafhankelijke toezicht hierop voldoende passende waarborgen ter bescherming van persoonsgegevens heeft;

Er op Sint-Maarten voldoende passende waarborgen ter bescherming van politiegegevens zijn en dat het daarom mogelijk is om ten behoeve van de criminaliteitsbestrijding en het handhaven van de rechtsorde in Sint-Maarten op structurele wijze politiegegevens door te geven, ex. artikel 17a tweede lid onder b Wpg. Gezien de omstandigheden op Sint-Maarten wordt er geen onderscheid gemaakt tussen de verschillende categorieën politiegegevens, onverminderd de eventuele extra eisen die aan bepaalde categorieën politiegegevens in de Wpg worden opgelegd.

J.C. Knol MA  
korpschef

Bijlage:

- Uitwerking beoordeling passende waarborgen Sint-Maarten ex. artikel 17a tweede lid onder b Wpg.
- Brief om de Autoriteit Persoonsgegevens te informeren over het vaststellen van de passende waarborgen op Sint-Maarten ex. artikel 17a tweede lid onder b Wpg.



## Bijlage - Uitwerking beoordeling passende waarborgen Sint-Maarten ex. Artikel 17a tweede lid onder b Wpg

### Richtlijn (EU) 2016/680 creëert minimumbeschermingsniveau binnen de EU

De Richtlijn (EU) 2016/680 ('Richtlijn') creëert een minimumbeschermingsniveau voor gegevensverwerking door rechtshandavingsinstanties binnen de Europese Unie. Hierdoor zullen alle betrokkenen binnen de EU een minimaal beschermingsniveau kennen. Dit geldt niet voor landen die geen lidstaat zijn van de EU en zich dus niet aan deze wetgeving hoeven te houden. De zogenaamde derde landen. Om te voorkomen dat er politiegegevens naar landen gaan waar het beschermingsniveau niet voldoende is, is doorgifte aan derde landen door de Richtlijn beperkt. Slechts in bepaalde omstandigheden kunnen politiegegevens worden doorgegeven.

Deze notitie werkt de belangrijkste randvoorwaarden rondom het besluit van de passende waarborgen voor structurele gegevensuitwisseling met Sint-Maarten verder uit.

### Derde landen binnen het gegevensbeschermingsrecht

Alle landen die geen lidstaat zijn of gebieden die geen onderdeel zijn van een lidstaat worden gekwalificeerd als derde land. Er zijn enkele bijzonderheden. Zo zijn Bonaire, Sint-Eustatius en Saba ('BES') als openbare lichamen van Nederland wel onderdeel van een lidstaat, maar hebben zij als LGO<sup>1</sup> een bijzondere status. Zij zijn geen derde landen, maar maken ook geen onderdeel uit van de interne markt. Hierdoor vallen zij voor het gegevensbeschermingsrecht onder de categorie derde landen. De overige Koninkrijkslanden, Aruba, Curaçao en Sint-Maarten kwalificeren ook als derde land. En deze notitie beperkt zich tot het land Sint-Maarten.

### Passende waarborgen Sint-Maarten

Voor het structureel doorgeven van politiegegevens aan derde landen zijn er drie mogelijkheden. Allereerst is er het adequaatheidsbesluit dat door Europese Commissie wordt genomen (artikel 17a eerste lid Wet politiegegevens). Op dit moment is er alleen voor het Verenigd Koninkrijk een adequaatheidsbesluit genomen. Verder kunnen er politiegegevens worden doorgegeven indien er een juridisch bindend instrument is waarin passende waarborgen ter bescherming van persoonsgegevens zijn vastgelegd (artikel 17a tweede lid onder a Wpg). Dat is het geval voor Caribisch Nederland (BES) vanwege de Wpg BES (paragraaf 6a Wpg), waarvan bij de implementatie van de Richtlijn is vastgesteld dat dit een juridisch bindend instrument met passende waarborgen is, ex. artikel 17a tweede lid onder a Wpg<sup>2</sup>. Tot slot, bij het ontbreken van een adequaatheidsbesluit of een juridisch bindend instrument, kan de verwerkingsverantwoordelijke alle omstandigheden beoordelen en vaststellen dat er passende waarborgen zijn (artikel 17a tweede lid onder b Wpg). De beoordeling van Sint-Maarten heeft in dit kader plaatsgevonden.

### Structurele doorgifte houdt geen open kraan in

Artikel 17a Wpg biedt alleen een *grondslag* voor de doorgifte naar een derde land. Voor de structurele doorgifte op basis van het eerste of tweede lid betekent dat niet in elke situatie apart hoeft te worden vastgesteld of het ontvangende land een voldoende beschermingsniveau voor gegevensbescherming heeft. Het betekent echter **niet** dat gegevens altijd kunnen worden doorgegeven. Voorafgaand aan elke verwerking zal, net als een verwerking binnen de EU of binnen NL, moeten worden vastgesteld of het noodzakelijk, proportioneel en subsidiair is. Ook zullen alle gegevensbeschermingsbeginselen zoals dataminimalisatie in acht genomen moeten worden.

<sup>1</sup> Landen en gebieden overzee (LGO) zijn gebieden binnen de Europese Unie een speciale status, ex. Artikel 52 tweede lid VEU jo. 355 VWEU.

<sup>2</sup> TK 2017/18, 33889, nr. 3, p. 70-71.



### **Categorieën politiegegevens**

Gezien de omstandigheden op Sint-Maarten wordt er geen onderscheid gemaakt tussen verschillende categorieën politiegegevens. Wel blijven alle voorwaarden uit de Wpg met betrekking tot verschillende soorten politiegegevens gelden. Zo blijven de zwaardere eisen om bijzondere categorieën politiegegevens (ex artikel 5 Wpg) ook gelden als deze moeten worden doorgegeven naar derde landen en is ook nog steeds instemming van het bevoegd gezag nodig om TCI of TOOI informatie door te geven. Dit boven op de gewone voorwaarden van subsidiariteit, proportionaliteit en noodzakelijkheid.

### **Artikel 3 EVRM**

Een doorgifte naar derde landen kan daarnaast alleen indien de rechtsstatelijkheid en eerbiediging van de van mensenrechten en fundamentele vrijheden naar behoren zijn. Indien een doorgifte een risico inhoudt voor deze rechten van de betrokkene kunnen de politiegegevens niet worden doorgegeven. Het Comité ter voorkoming van foltering, onmenselijke of vernederende behandelingen en bestraffing<sup>3</sup> ('CPT') heeft in 2022 een bezoek gebracht aan het Koninkrijk der Nederlanden en heeft een rapport uitgebracht<sup>4</sup>. Uit het rapport volgt dat er in alle landen van het Koninkrijk verbeterpunten zijn. Deze geven echter geen aanleiding om aan te nemen dat er op Sint-Maarten sprake is van onmenselijke of vernederende behandelingen en bestraffingen. Er is dus geen aanleiding om aan te nemen dat de eerbiediging van fundamentele vrijheden en mensenrechten op Sint-Maarten in het geding komt.

### **Verdrag tussen de Franse Republiek en het Koninkrijk der Nederlanden**

Het eiland waarop Sint-Maarten ligt wordt gedeeld met het Franse overzeese gebied Saint-Martin. Dit houdt in dat er op het eiland een buitengrens van de Europese Unie loopt. In 2010 is er een verdrag gesloten tussen de Franse Republiek en het Koninkrijk der Nederlanden inzake de eilandbrede samenwerking op politiegebied op het eiland Sint-Maarten<sup>5</sup>. Frankrijk moet zich als lidstaat van de Europese Unie net als Nederland houden aan de EU-regelgeving omtrent de uitwisseling van politiegegevens. De afspraken in dit verdrag, die met een andere EU-lidstaat zijn gemaakt, kunnen niet gelden voor de uitwisseling van politiegegevens tussen landen *binnen* het Koninkrijk. De inrichting van het Koninkrijk staat het onderling sluiten van Verdragen niet toe.

### **Voorwaarden**

Zoals hiervoor aangegeven betekent het vaststellen van voldoende passende waarborgen door de verwerkingsverantwoordelijke niet dat alle gegevens altijd verstrekt mogen worden. In elk specifiek geval zal moeten worden vastgesteld of de doorgifte voldoet aan subsidiariteit, proportionaliteit en noodzakelijkheid. Daarnaast zal ook voldaan moeten worden naar de voorwaarden zoals verder gesteld in de Wpg en het bijbehorende Besluit politiegegevens.

---

<sup>3</sup> Het CPT vloeit voort uit het Europees Verdrag ter voorkoming van foltering en onmenselijke of vernederende behandeling (Raad van Europa) en onderzoekt of de verdragspartijen zich houden aan de eisen uit het Verdrag.

<sup>4</sup> Het rapport en de reactie van het Koninkrijk der Nederlanden zijn te vinden op:

<https://www.coe.int/en/web/cpt/-/council-of-europe-anti-torture-committee-cpt-publishes-report-on-its-2022-periodic-visit-to-the-netherlands>.

<sup>5</sup> Verdrag tussen de Regering van het Koninkrijk der Nederlanden en de Regering van de Franse Republiek inzake eilandbrede samenwerking op politiegebied op Sint-Maarten, Tractatenblad 2010 nr. 311.



## Motivering verstrekking derde landen (art. 17a Wpg)

### Motivering

In overeenstemming met artikel 17a, derde lid Wpg zijn de volgende politiegegevens aan het betreffende derde land vertrekt.

|                               |                                                                     |
|-------------------------------|---------------------------------------------------------------------|
| <b>Verstrekkende land</b>     | Nederland                                                           |
| <b>Ontvangende derde land</b> | <a href="#">Klik om een land in te voeren (alleen derde landen)</a> |
| <b>Datum verstrekking</b>     | Zie datum en tijdstip van uploaden DIAS                             |

### Context

Omschrijf hier bondig wat de aanleiding van het verzoek is, welke informatie wordt verstrekt en de reden van verstrekking:

[Klik hier om een beknopte uitleg te geven van de verstrekking](#)

|                                                |                                                                  |
|------------------------------------------------|------------------------------------------------------------------|
| <b>Datum toestemming officier van justitie</b> | <a href="#">Klik om een datum in te voeren</a>                   |
| <b>Naam officier van justitie</b>              | mr. <a href="#">Klik om de naam van de officier in te voeren</a> |

### Grondslag (doelbinding) (artikel 17a, lid 3, Wpg) (minimaal één mogelijkheid aanvinken)

- ☐ Om een vitaal belang van de betrokkene of van een andere persoon te beschermen (**sub a**)
- ☐ Bescherming van gerechtvaardigde belangen van de betrokkene (**sub b**)
- ☐ Ter voorkoming van onmiddellijk en ernstig gevaar voor de openbare veiligheid van een lidstaat of derde land (**sub c**)
- ☐ Er is sprake van een afzonderlijk geval met het oog op de uitvoering van de politietaak (**sub d**)
- ☐ Het instellen, uitoefenen of verdedigen van rechtsvorderingen in verband met de politietaak (**sub e**)

### Toetsing (alle opties zijn verplicht)

- ☐ Het gestelde doel van deze verstrekking staat in verhouding tot de (mogelijke) privacy inbreuk van betrokkene(n) waarbij de grondrechten en fundamentele vrijheden van de betrokkene niet prevaleren boven het algemeen belang van de doorgifte (**proportionaliteitstoets**) (verplicht)  
[Klik hier om een beknopte uitleg te geven](#)
- ☐ Voor deze verstrekking zijn geen minder ingrijpende middelen beschikbaar om het gestelde doel te bereiken (**subsidiariteitstoets**) (verplicht)  
[Klik hier om een beknopte uitleg te geven](#)
- ☐ Er is voldoende rekening gehouden met **negatieve neveneffecten** (verplicht)  
[Klik hier om een beknopte uitleg te geven](#)

# Gegevensbeschermings- effectbeoordeling (PIA)

## Dutch International Assistance System (DIAS)

Opgesteld in samenwerking met JenV, OM-LP-DVOM, NP, AIRS, Justid en DJI

Rotterdam, november 2021



Vaststelling verwerkersverantwoordelijke: 25 oktober 2021

Naam: 5.1.2.e [redacted] Openbaar Ministerie

Advies functionaris voor gegevensbescherming: Selecteer/typ datum

Naam: 5.1.2.e [redacted]

Advies CIO: Selecteer/typ datum

Naam: 5.1.2.e [redacted], Openbaar Ministerie



# **Gegevensbeschermingseffect- beoordeling (PIA) Dutch International Assistance System (DIAS)**

**Opgesteld in samenwerking met JenV, OM-LP-DVOM, NP, AIRS, Justid  
en DJI**

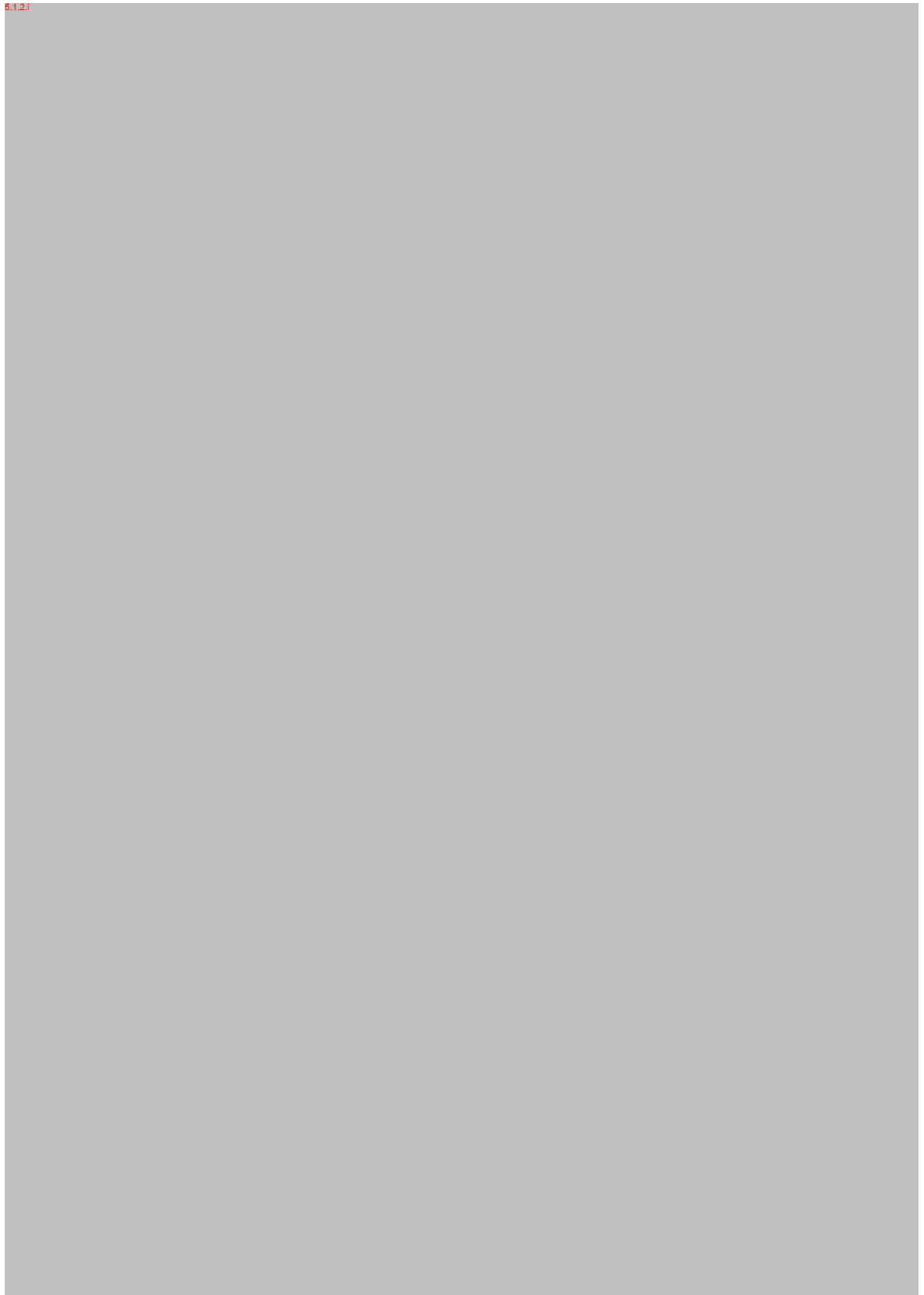
## **Contact:**

5.12.e , Openbaar Ministerie

Versie: 0.27 november 2021

## Colofon

5.1.2.1





# Inhoudsopgave

|                                                                   |    |
|-------------------------------------------------------------------|----|
| Inleiding .....                                                   | 8  |
| A. Beschrijving kenmerken gegevensverwerkingen .....              | 9  |
| 1.    Voorstel .....                                              | 9  |
| 2.    Persoonsgegevens .....                                      | 11 |
| 3.    Gegevensverwerkingen .....                                  | 11 |
| 4.    Verwerkingsdoeleinden .....                                 | 11 |
| 5.    Betrokken partijen.....                                     | 12 |
| 6.    Belangen bij de gegevensverwerking .....                    | 14 |
| 7.    Verwerkingslocaties .....                                   | 14 |
| 8.    Techniek en methode van gegevensverwerking .....            | 14 |
| 9.    Juridisch en beleidsmatig kader.....                        | 15 |
| 10.   Bewaartermijnen .....                                       | 17 |
| B. Beoordeling rechtmatigheid gegevensverwerkingen.....           | 21 |
| 11.   Rechtsgrond .....                                           | 21 |
| 12.   Bijzondere persoonsgegevens .....                           | 27 |
| 13.   Doelbinding .....                                           | 27 |
| 14.   Noodzaak en evenredigheid .....                             | 28 |
| 15.   Rechten van de betrokkene .....                             | 28 |
| C. Beschrijving en beoordeling risico's voor de betrokkenen ..... | 29 |
| 16.   Risico's.....                                               | 29 |
| D. Beschrijving voorgenomen maatregelen .....                     | 33 |
| 17.   Maatregelen.....                                            | 33 |

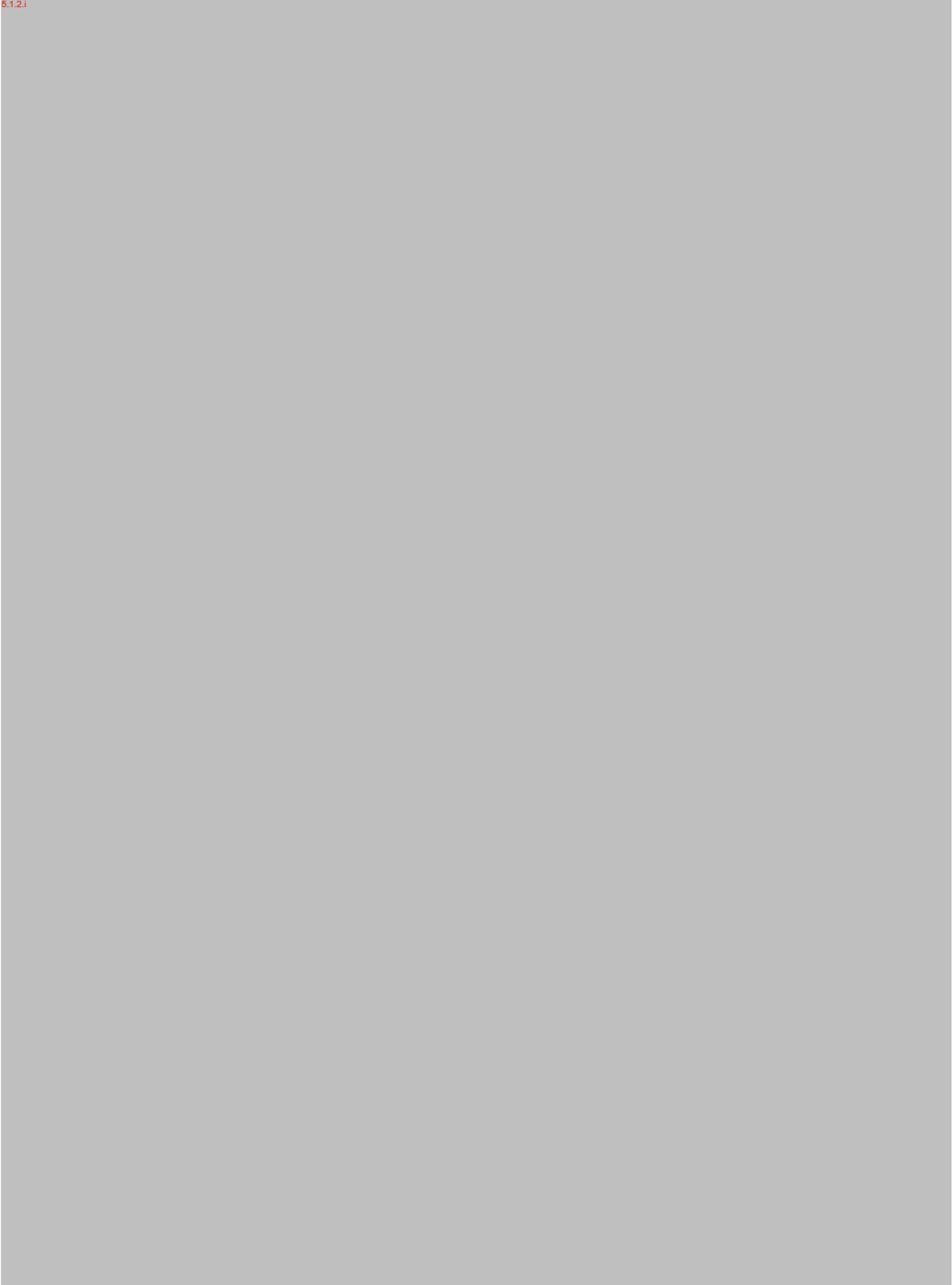
## Bijlagen:

|         |                                                                           |
|---------|---------------------------------------------------------------------------|
| Bijlage | 1. Gegevensverwerkingen                                                   |
| Bijlage | 2. Protocol Samenwerking bij Internationale Rechtshulp                    |
| Bijlage | 3a. Quickscan Informatiebeveiliging                                       |
|         | 3b. Dreigingen en kwetsbaarheden analyse TVA dreigingen en kwetsbaarheden |
|         | 3c. Specifieke DIAS Informatiebeveiliging maatregelen                     |
| Bijlage | 4a. Autorisatiebeleid DIAS                                                |
|         | 4b. Autorisatiematrix DIAS                                                |
|         | 4c. Overzicht IRChoofden,                                                 |
|         | 4d. Autorisatieformulier DIAS                                             |
|         | 4e. Invoerprotocol                                                        |
| Bijlage | 5. Logging en Monitoring Keuzes DIAS                                      |
| Bijlage | 6. Template verwerkersafpraak v0.5                                        |

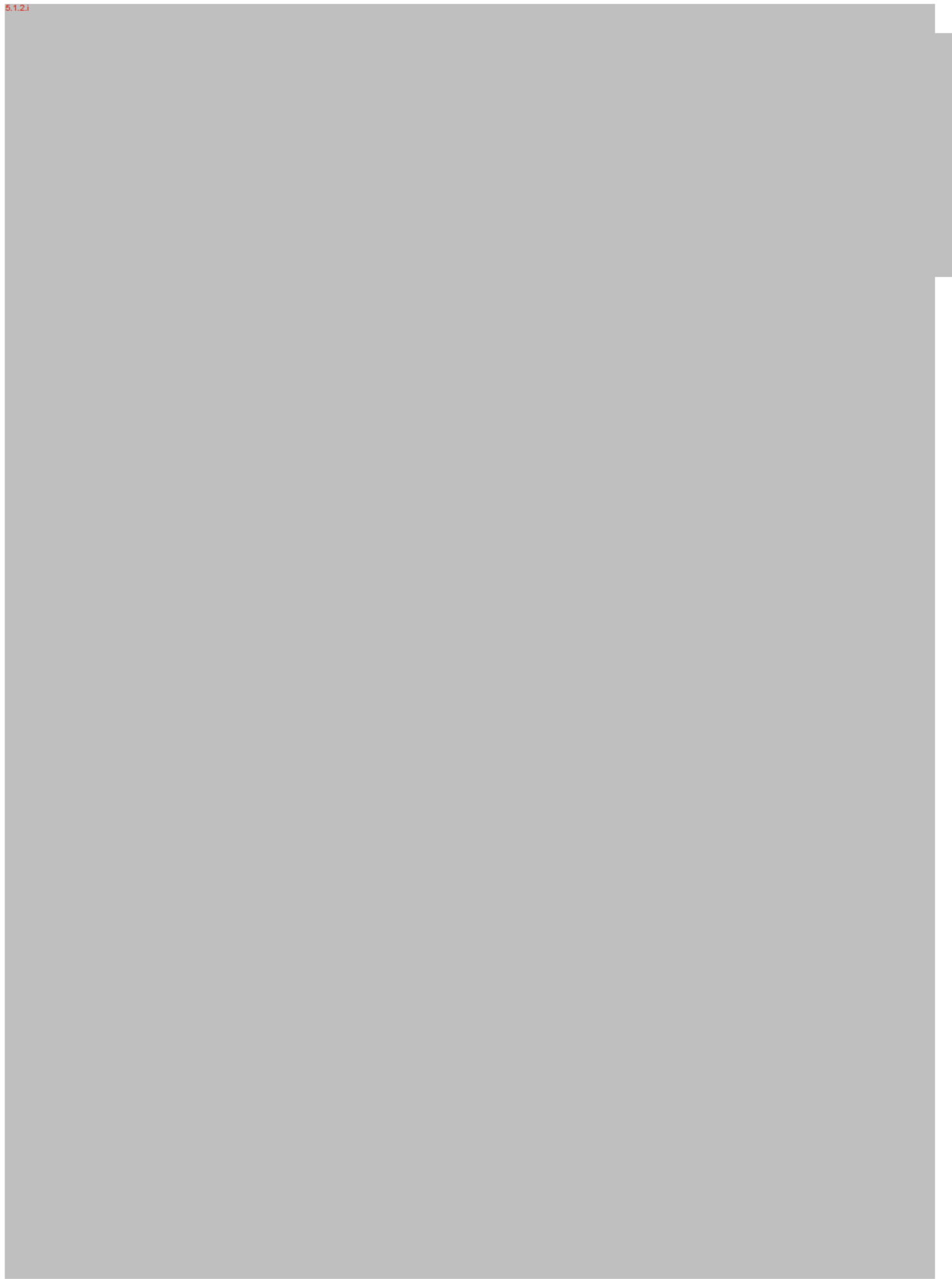
5.1.2.1



5.1.2.i

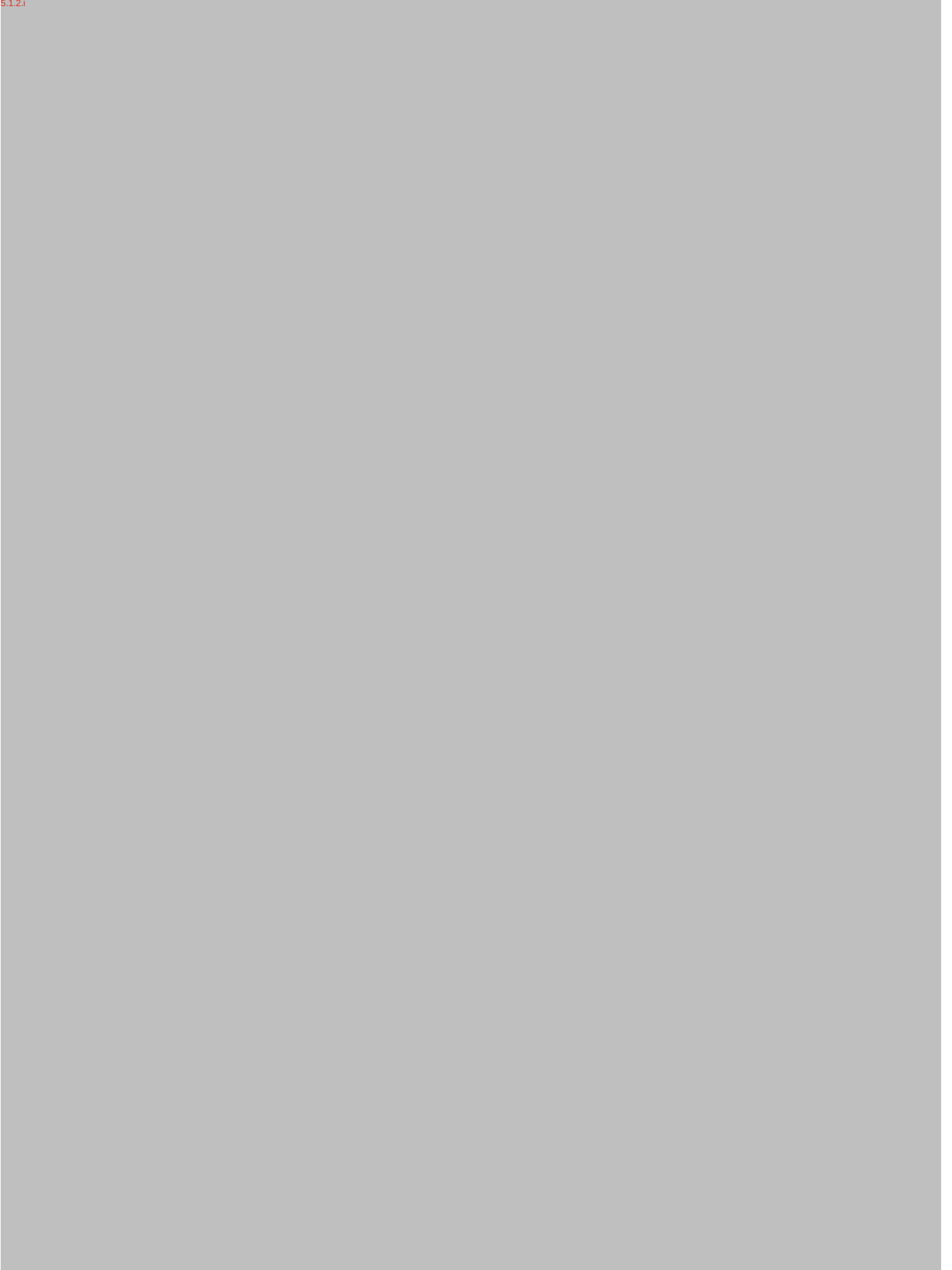


5.1.2.i





5.1.2.1



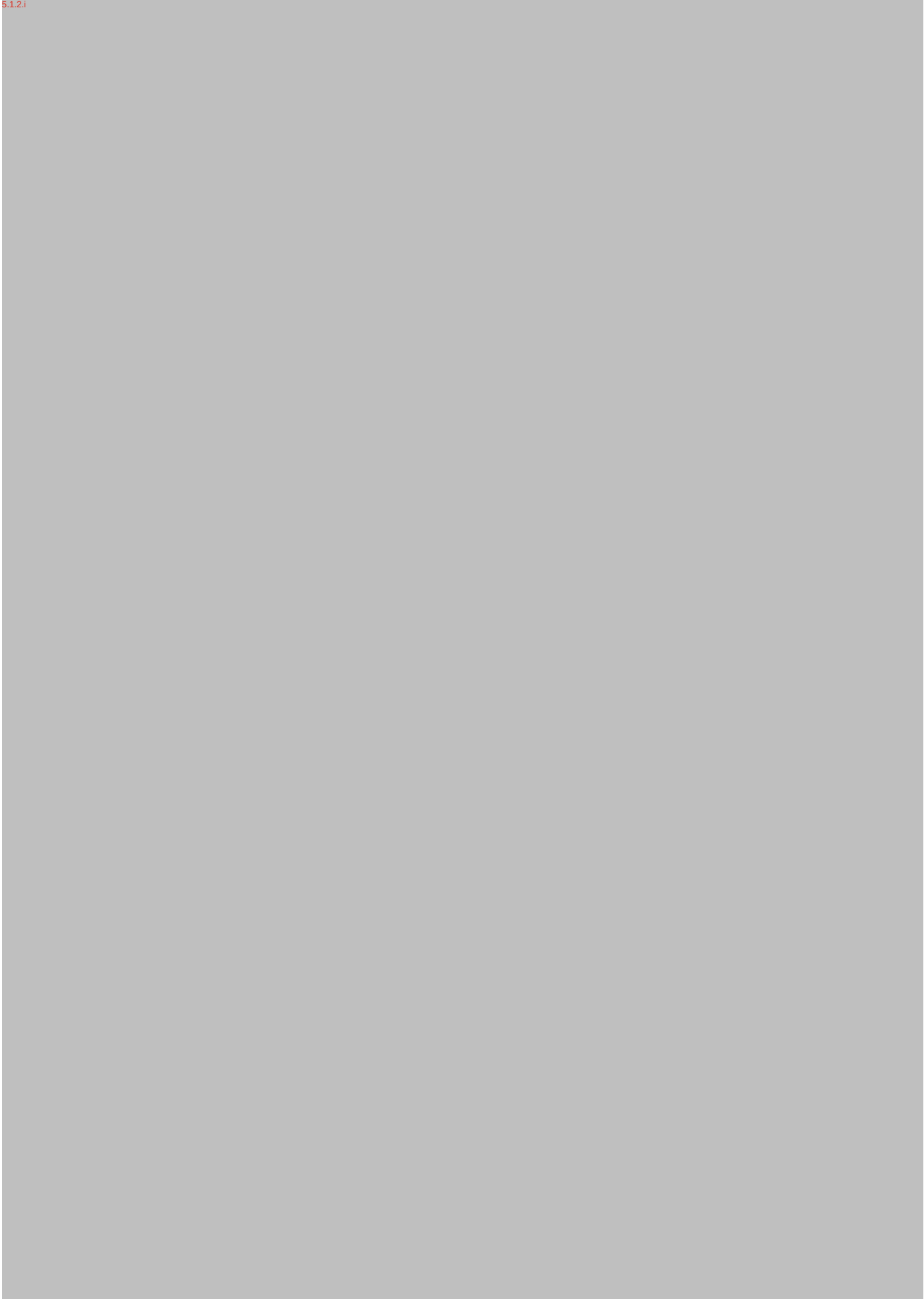
5.1.2.i



5.1.2.i



5.1.2.1



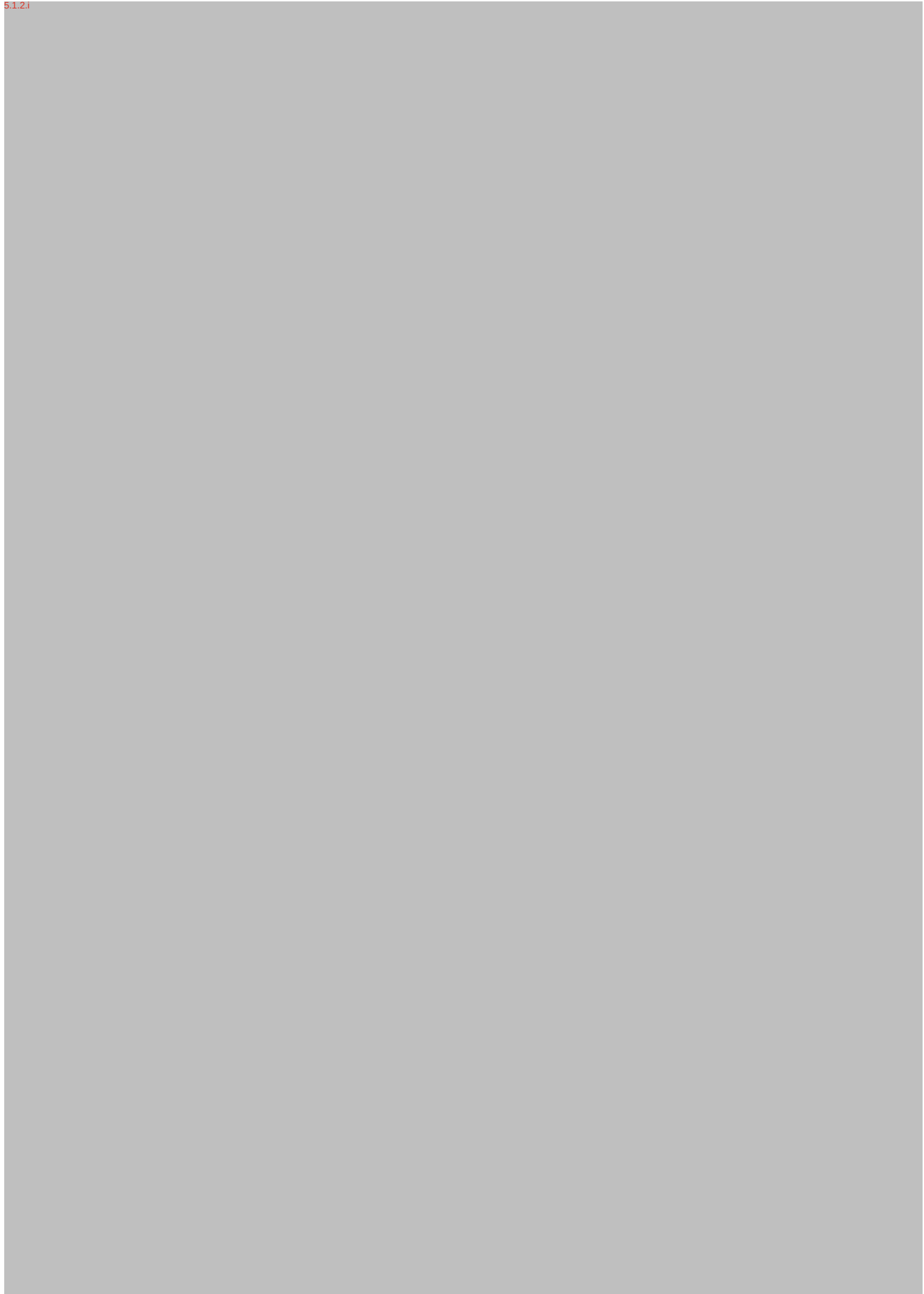
5.1.2.]



5.1.2.i



5.1.2.f



5.1.2.1

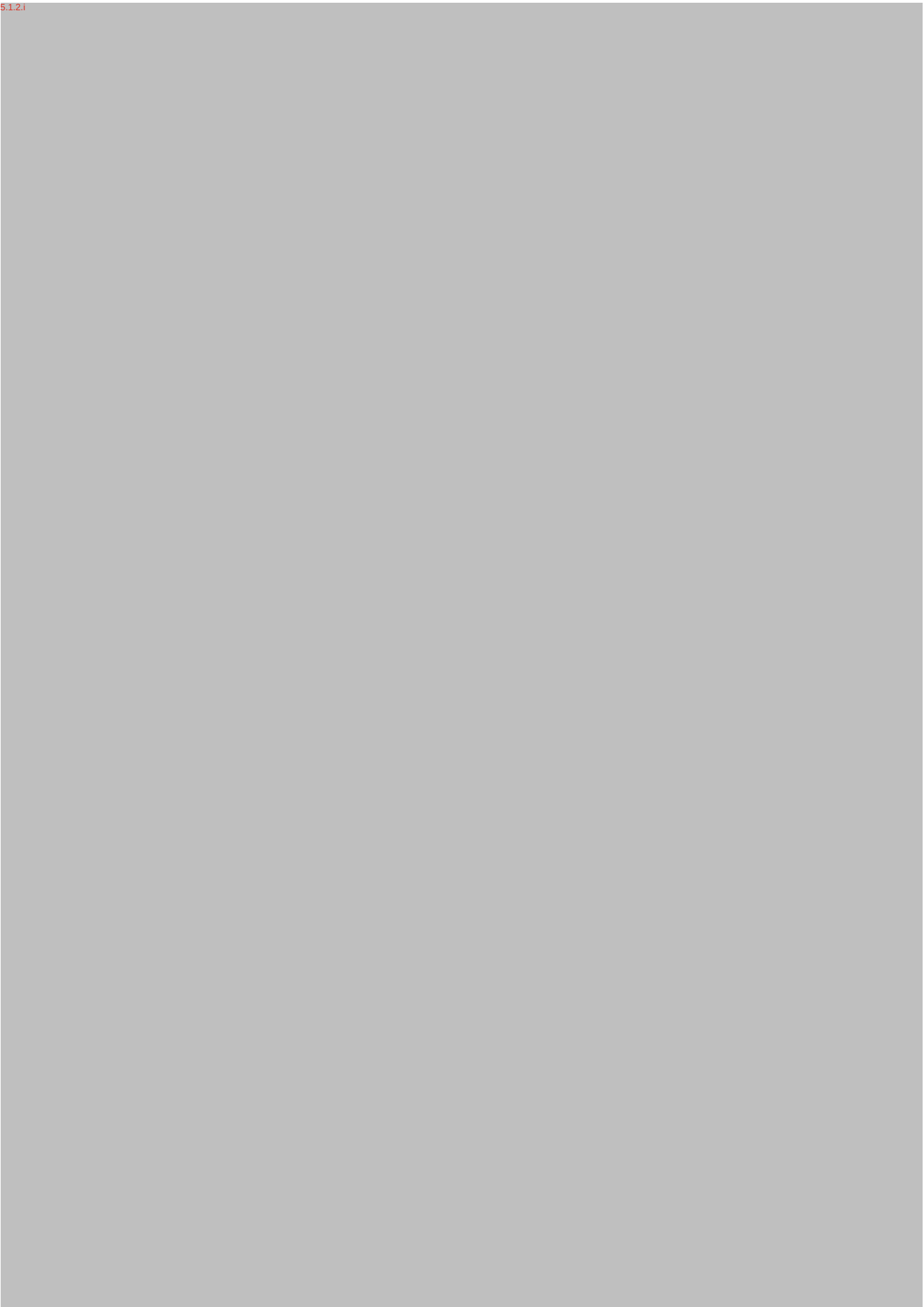




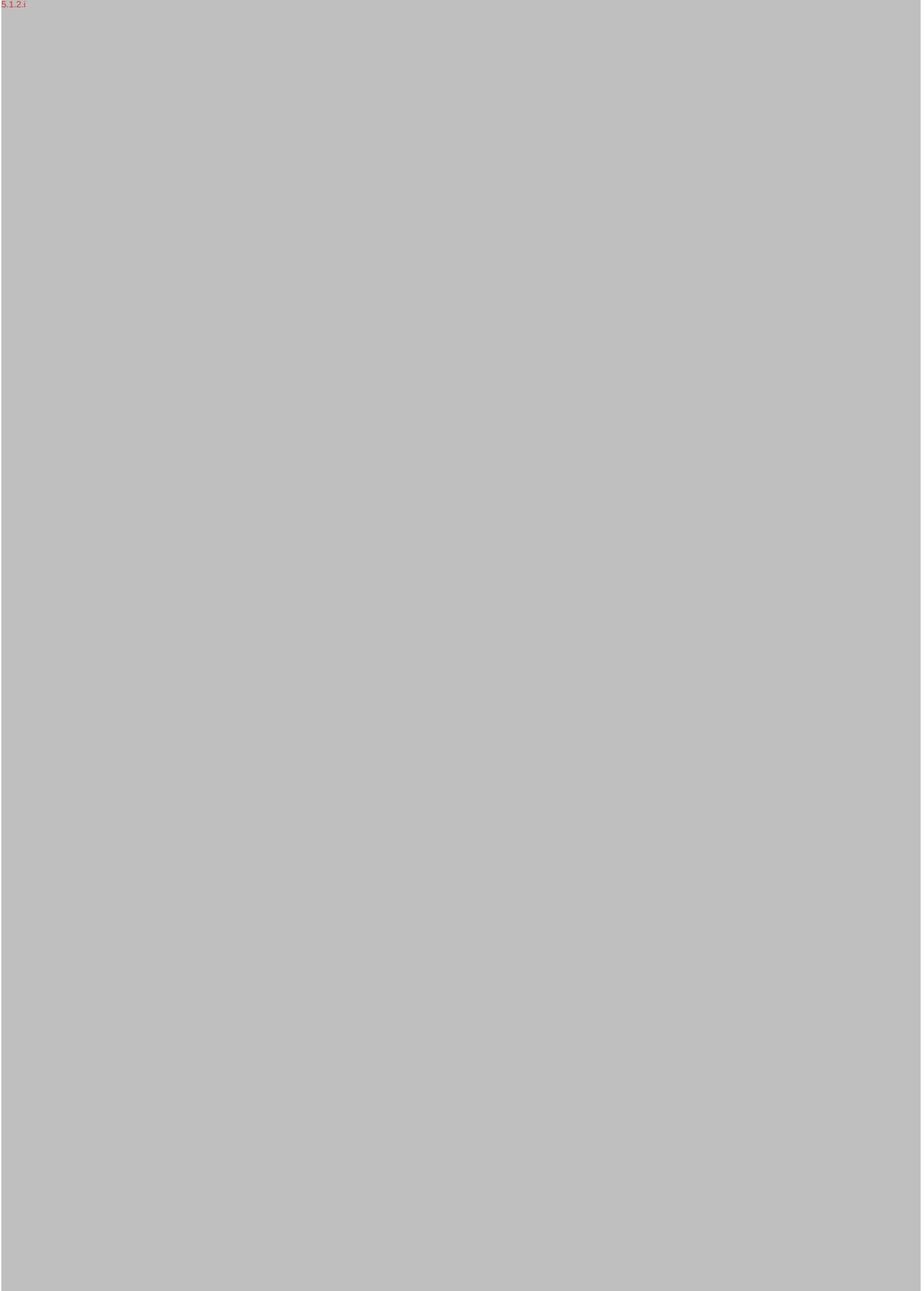
5.1.2.1



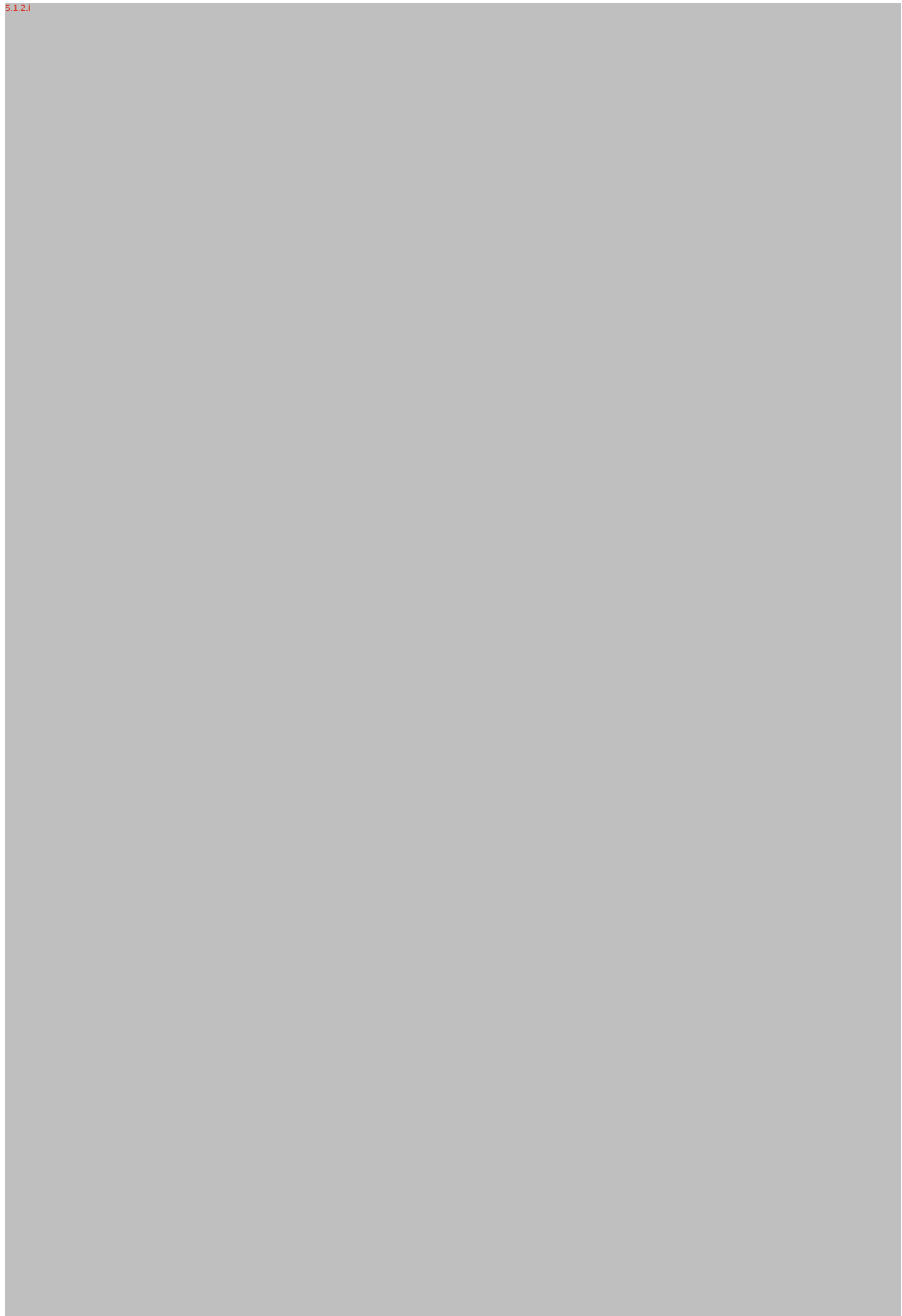
5.1.2.1



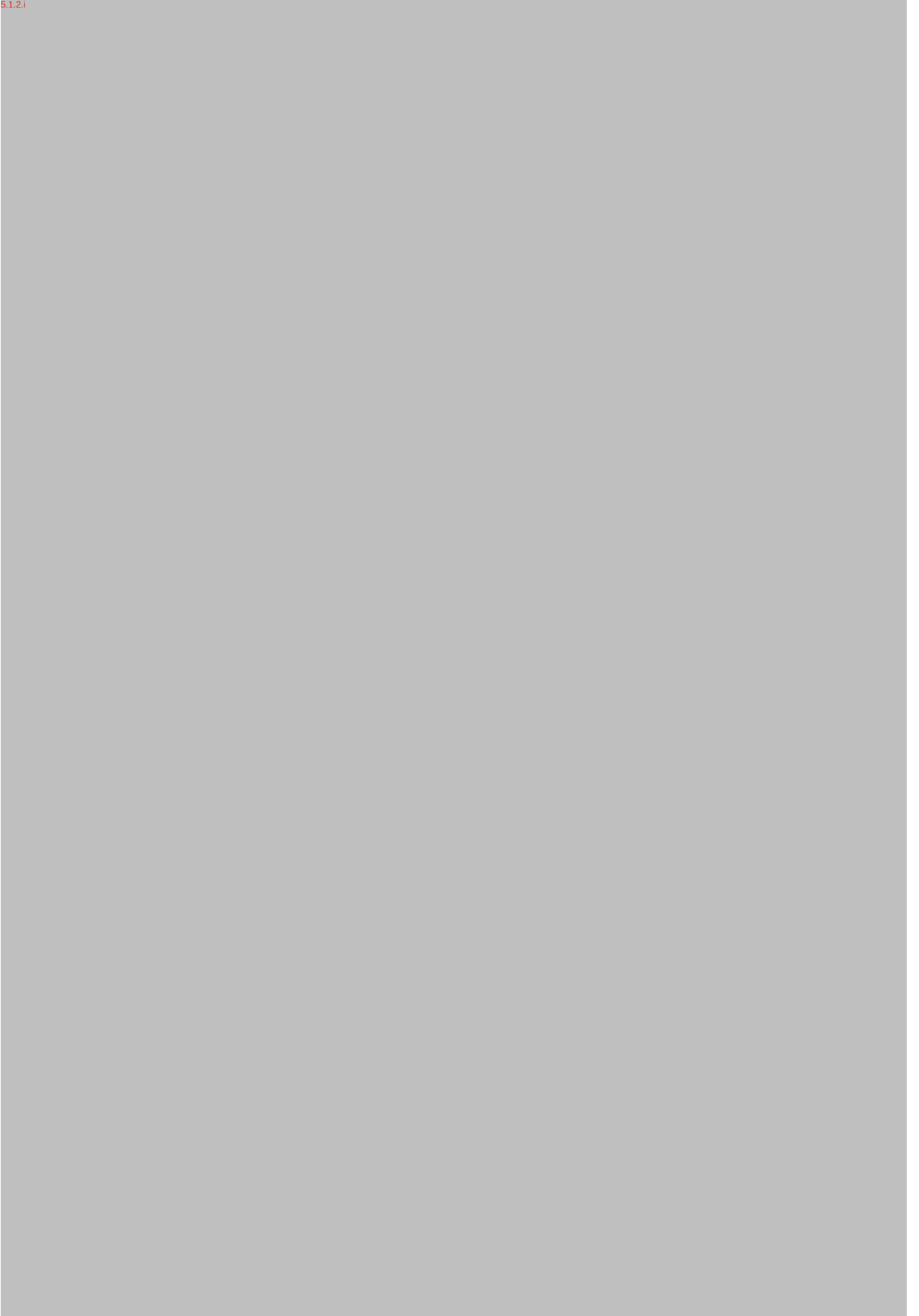
5.1.2.1



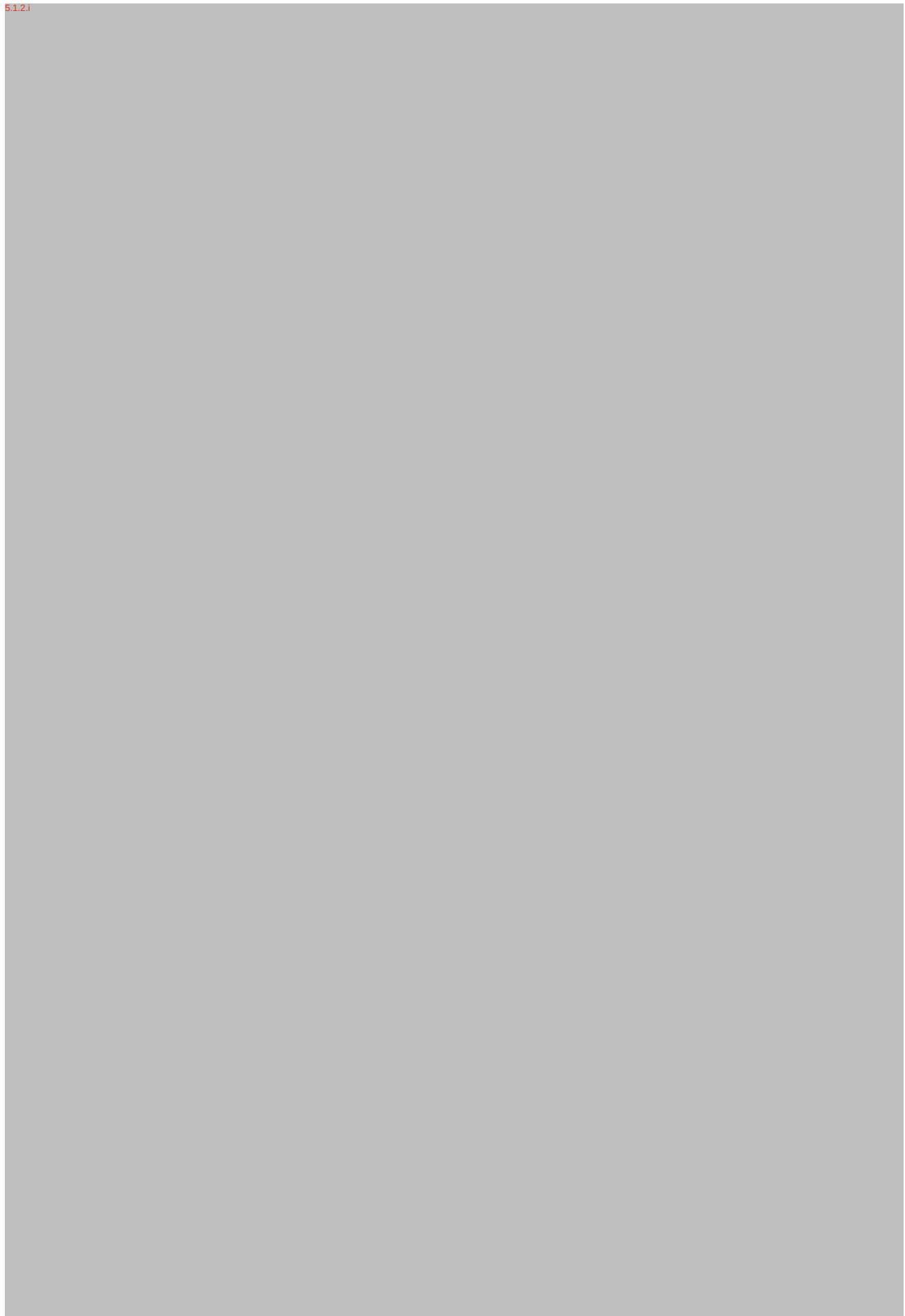
5.1.2.i



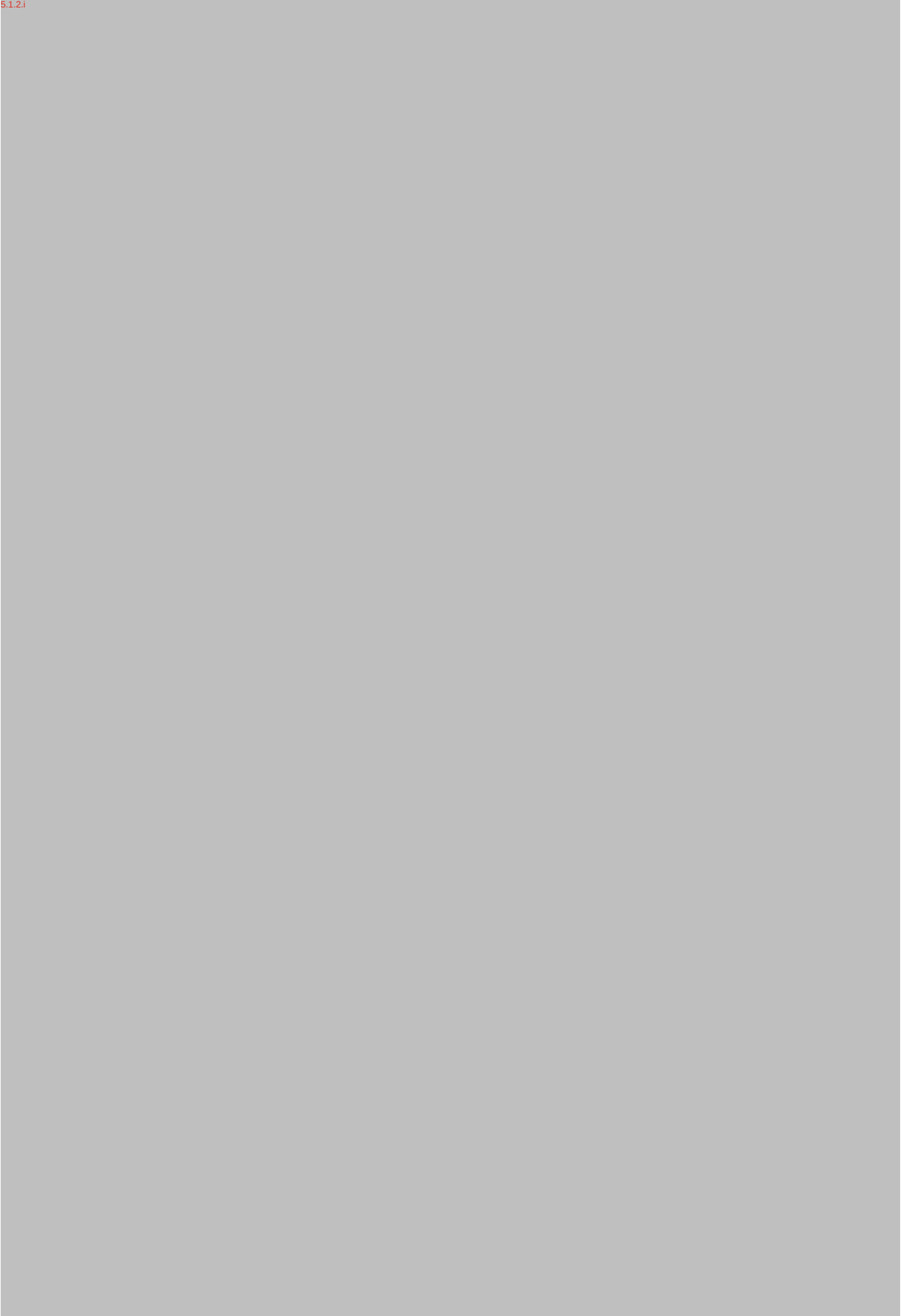
5.1.2.i



5.1.2.1



5.1.2.i



5.1.2.i

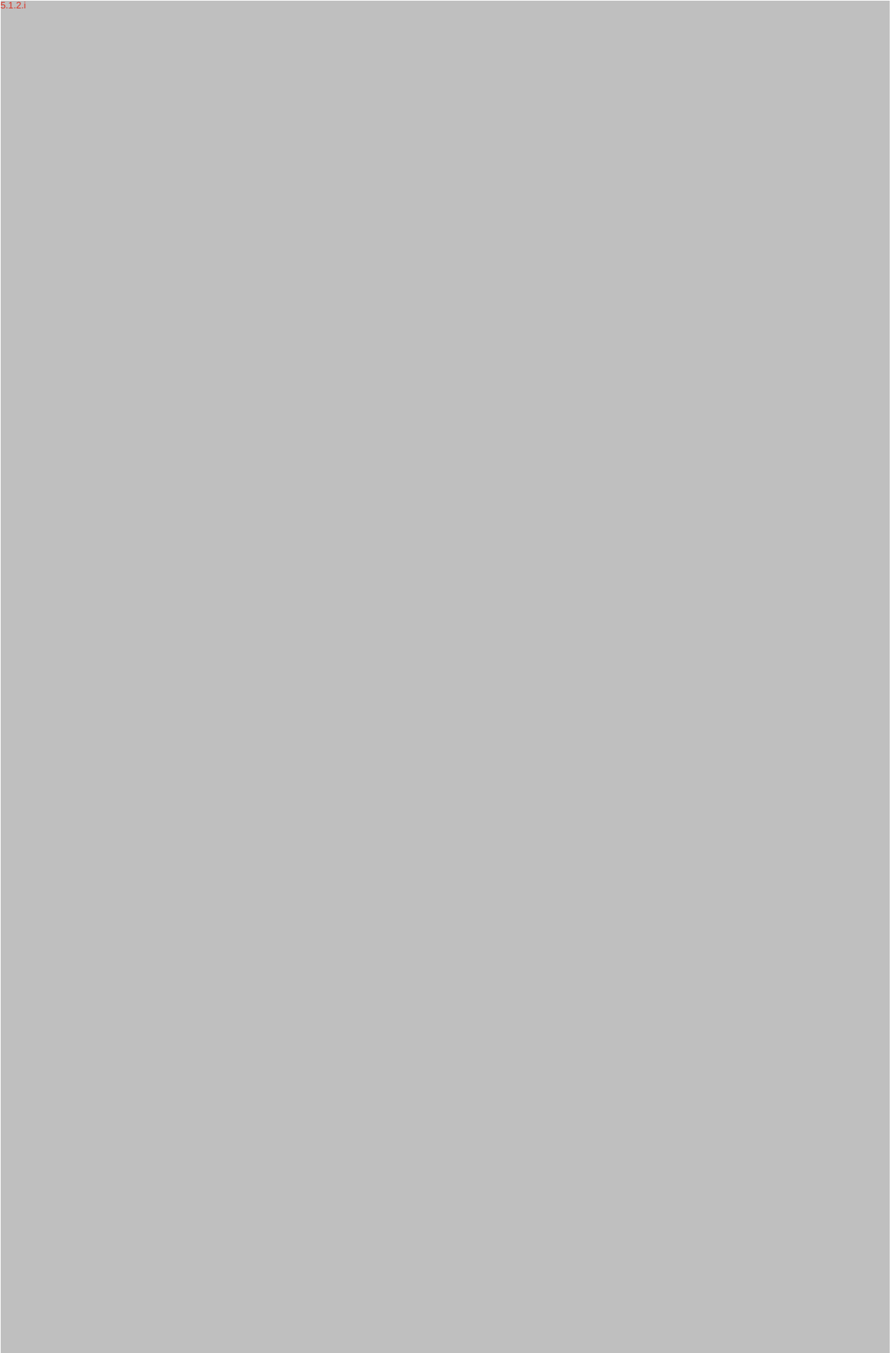




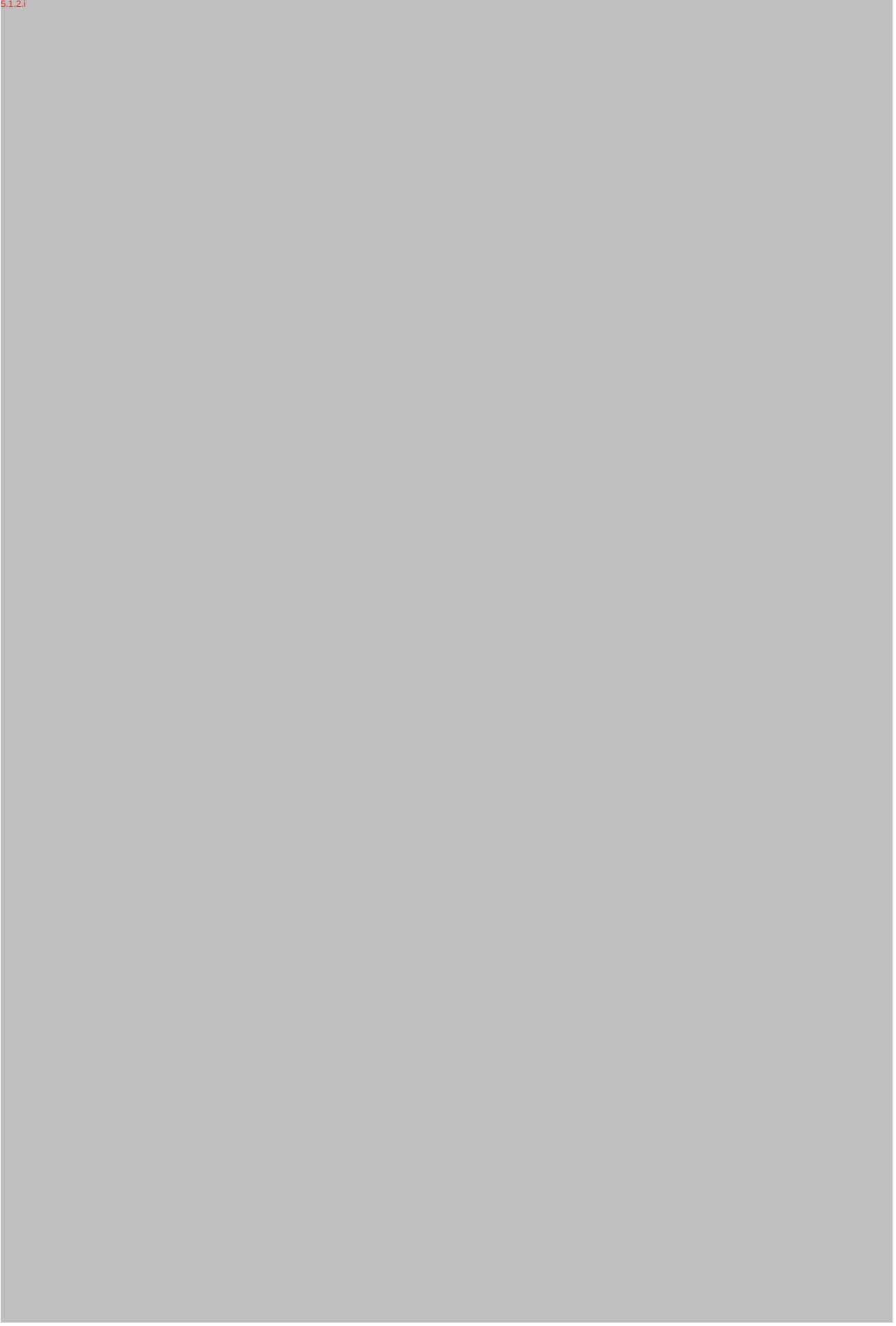
5.1.2.1



5.1.2.1



5.1.2.i

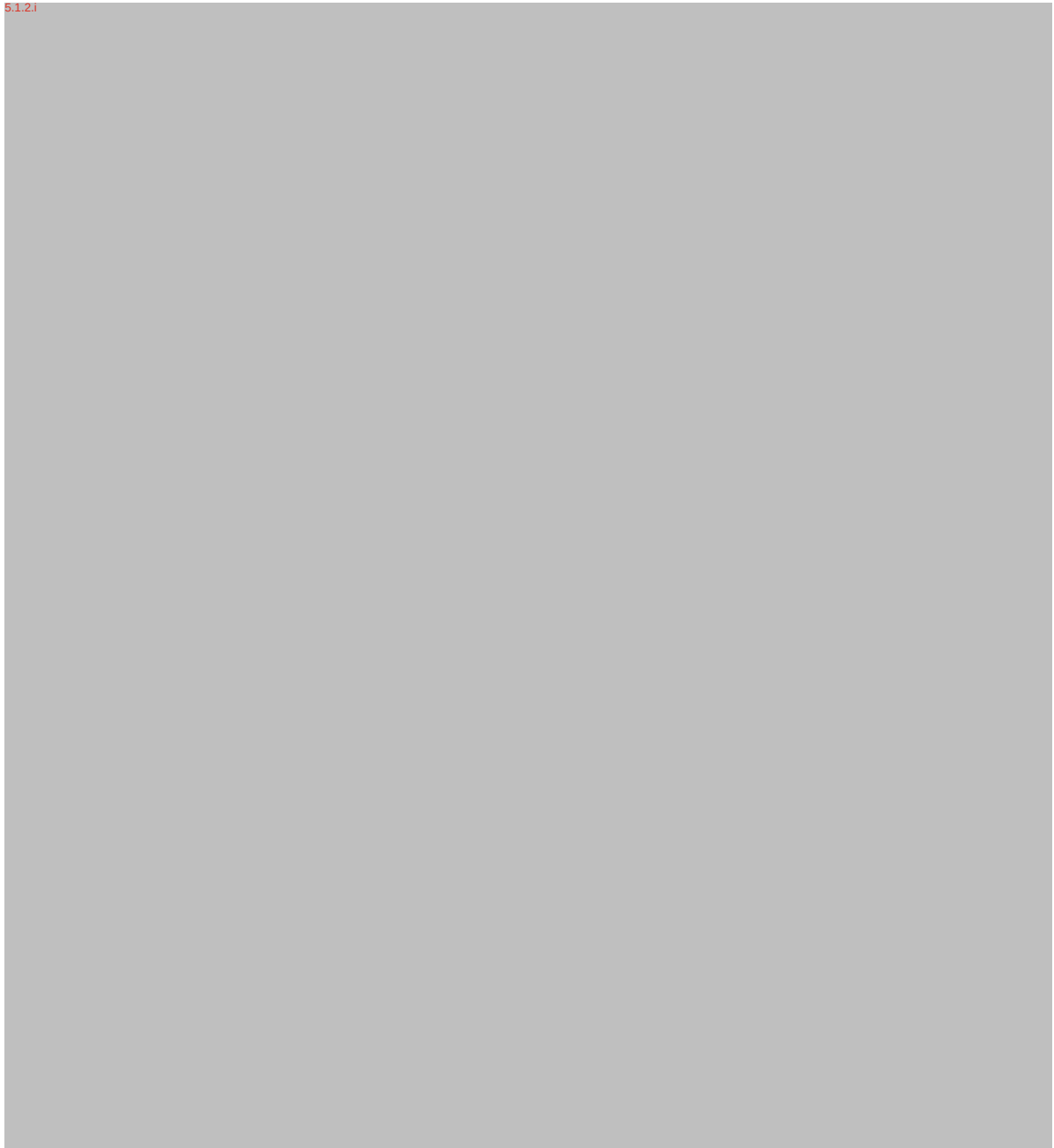


5.1.2.i

5.1.2.1



5.1.2.1

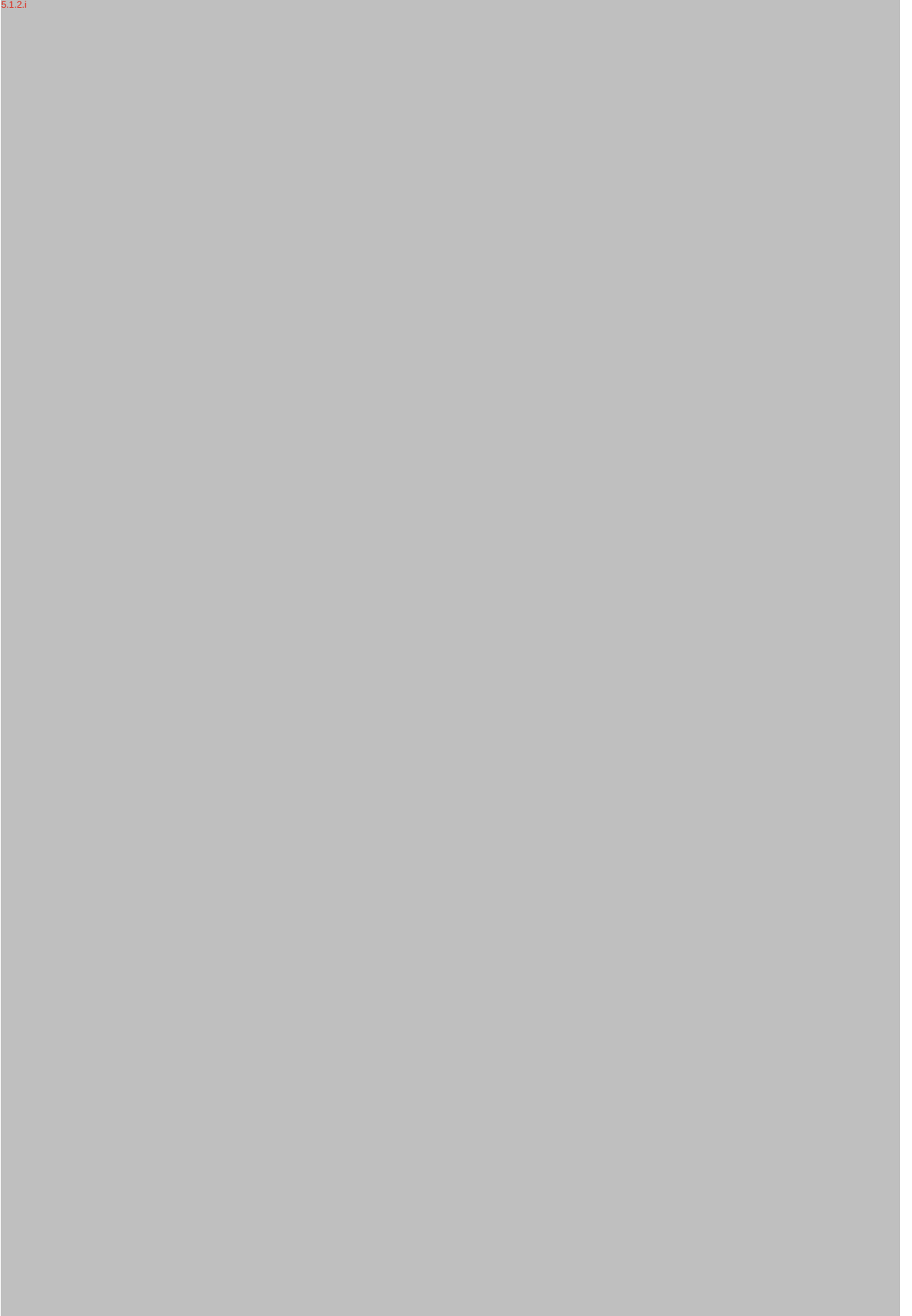


|  |
|--|
|  |
|--|

5.1.2.i



5.1.2.1





5.1.2.1

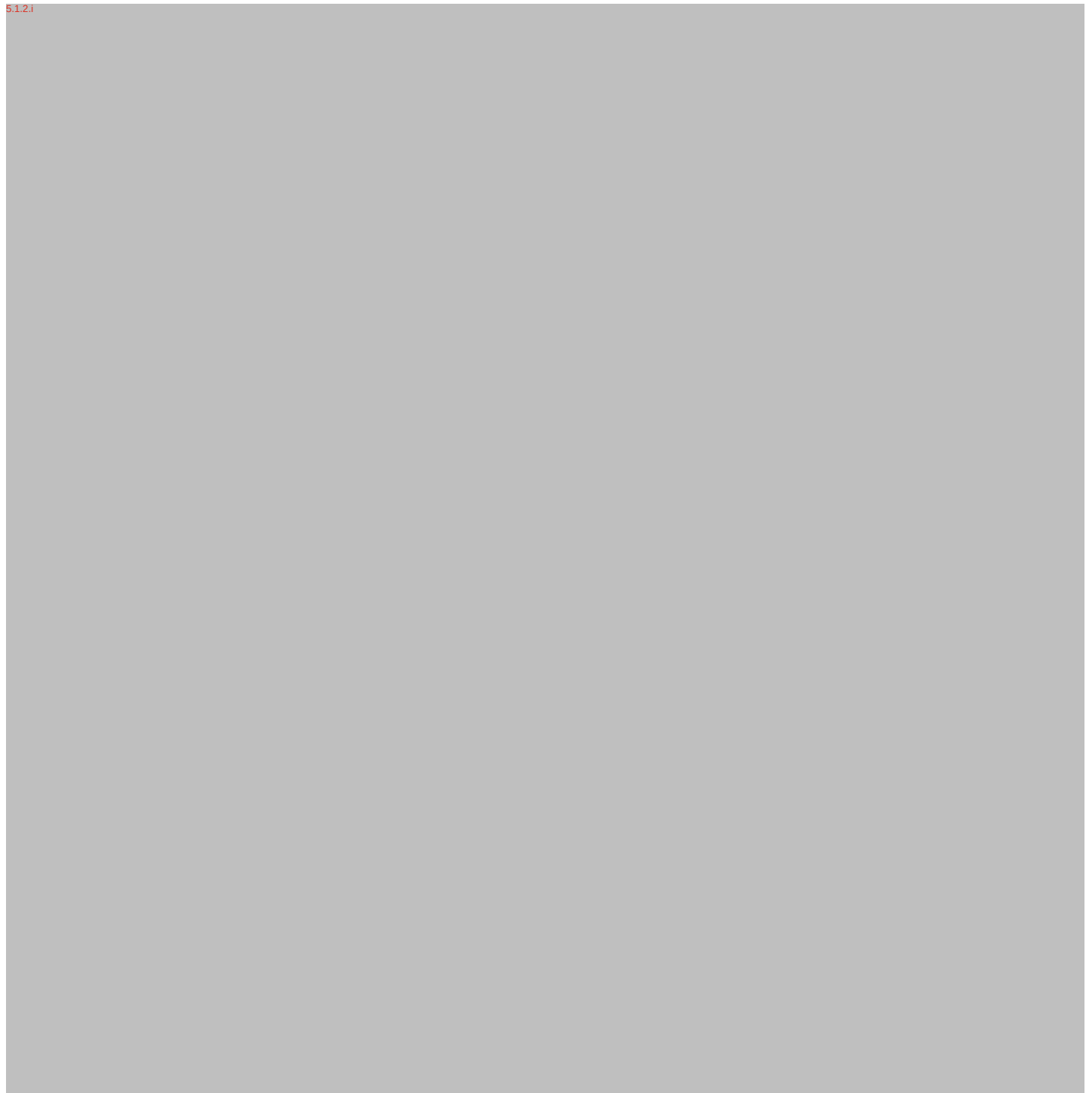


Maatregelen  
nemen  
Privacybewustwording  
PIA  
Doelbinding  
Noodzaak  
Effecten in kaart  
Bescherming van  
persoonsgegevens  
Risico's  
minimaliseren  
Richtinggevend  
Rechtsgrond.  
Met open vizier

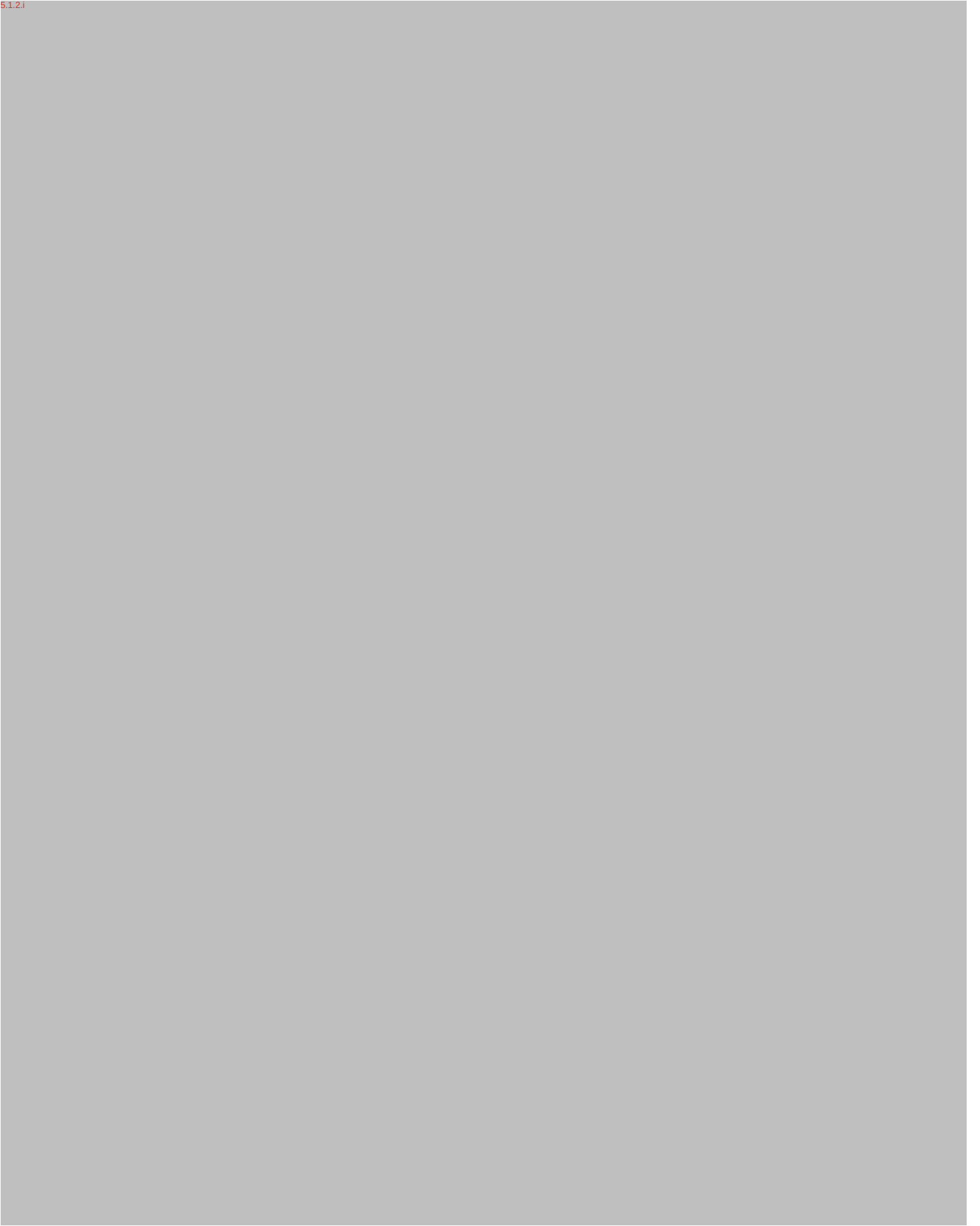
**Bijlage 1 - Gegevensverwerkingen**

(Bron: Project Startarchitectuur DIAS, auteur Justid, versie 1.0a, 1 oktober 2020)





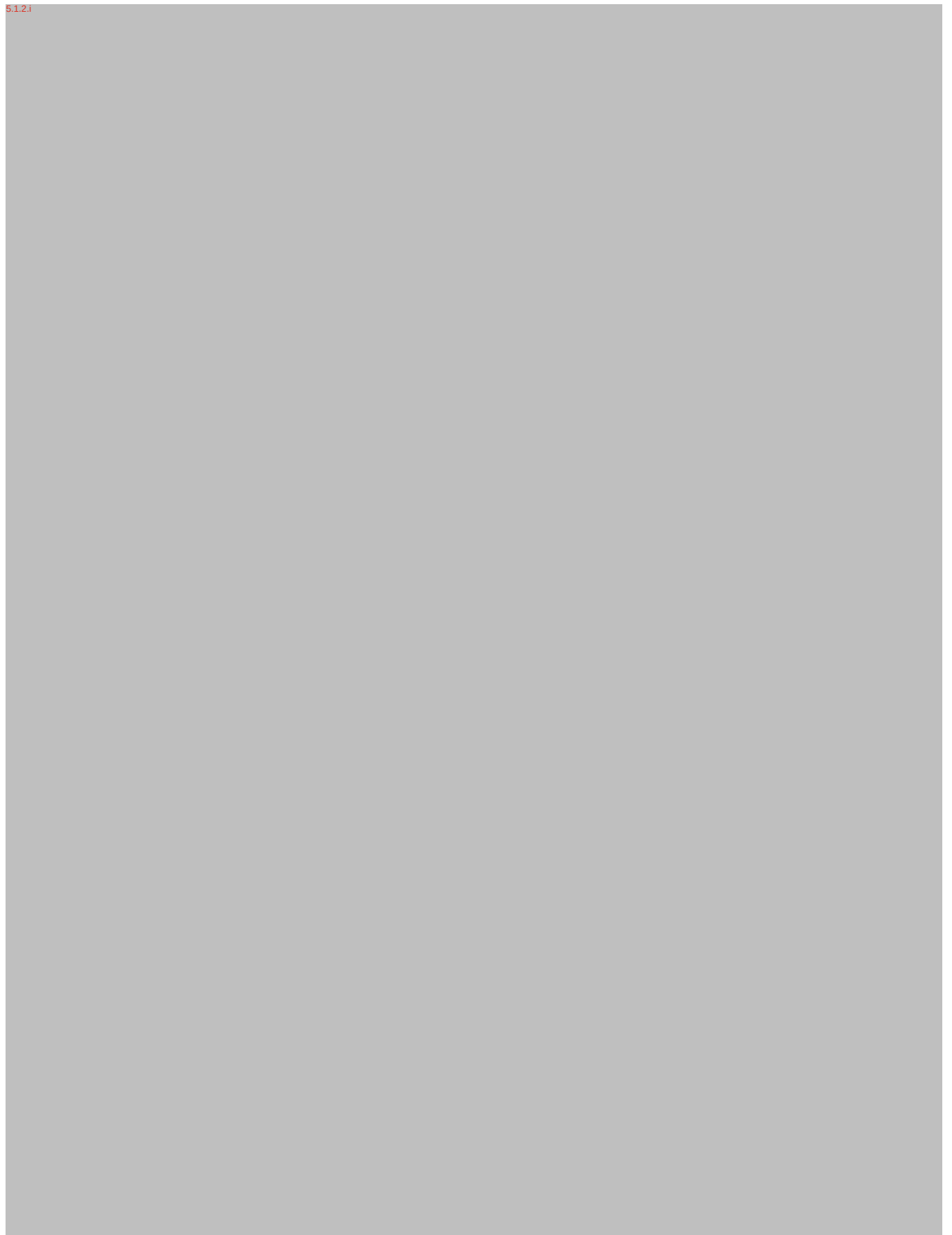
5.1.2



5.1.2.i



5.1.2.i

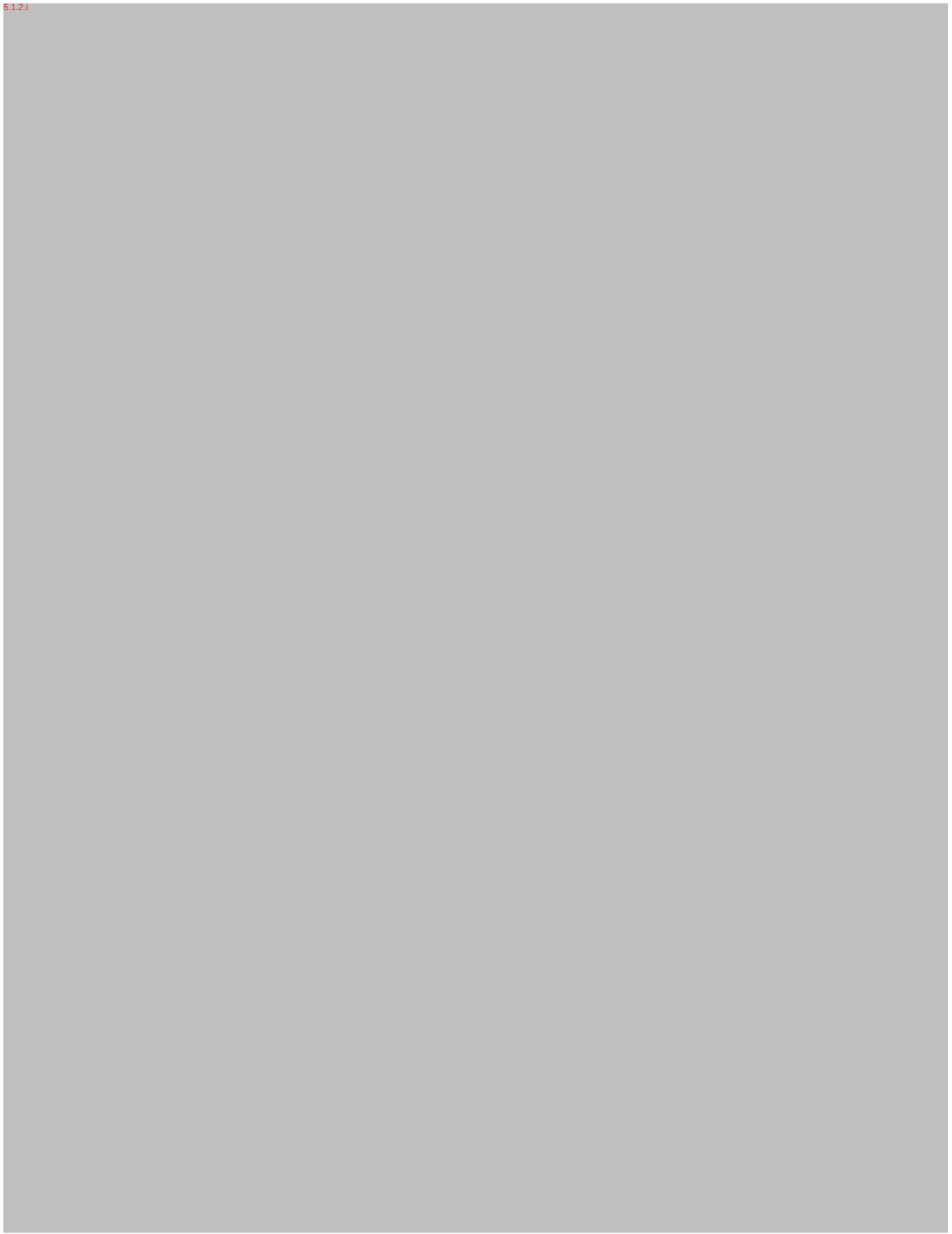


5.1.2.i

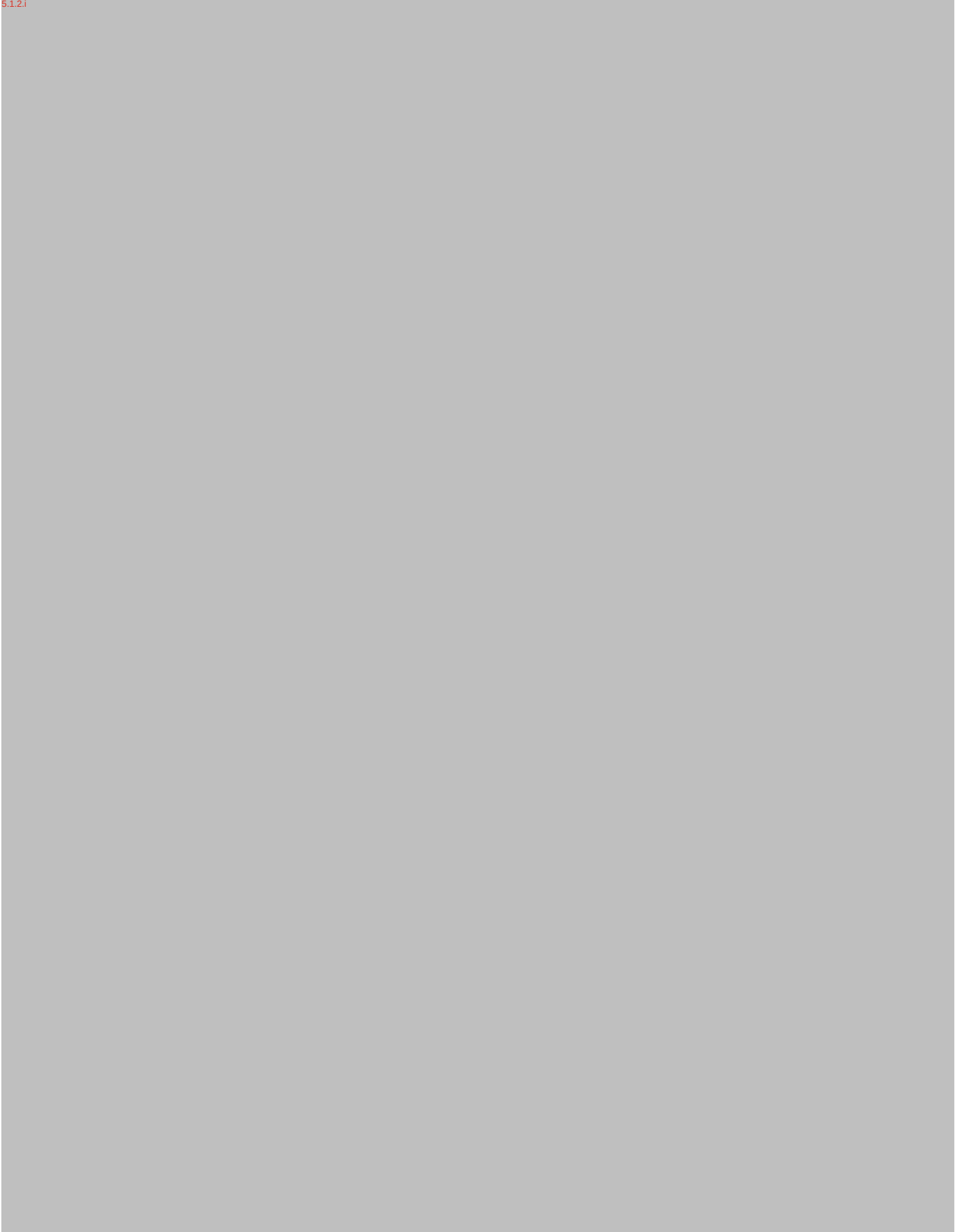




5.1.2.i

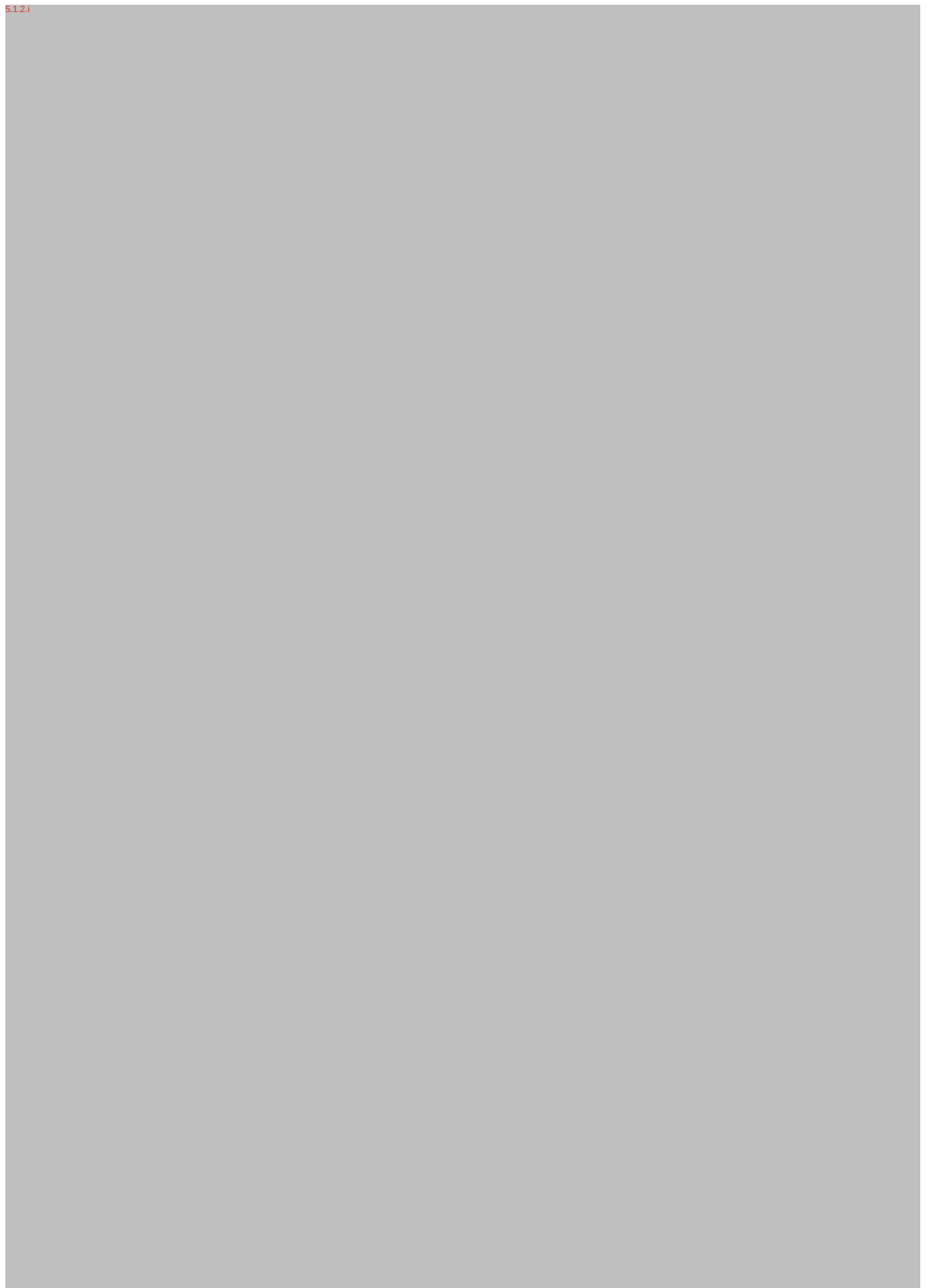


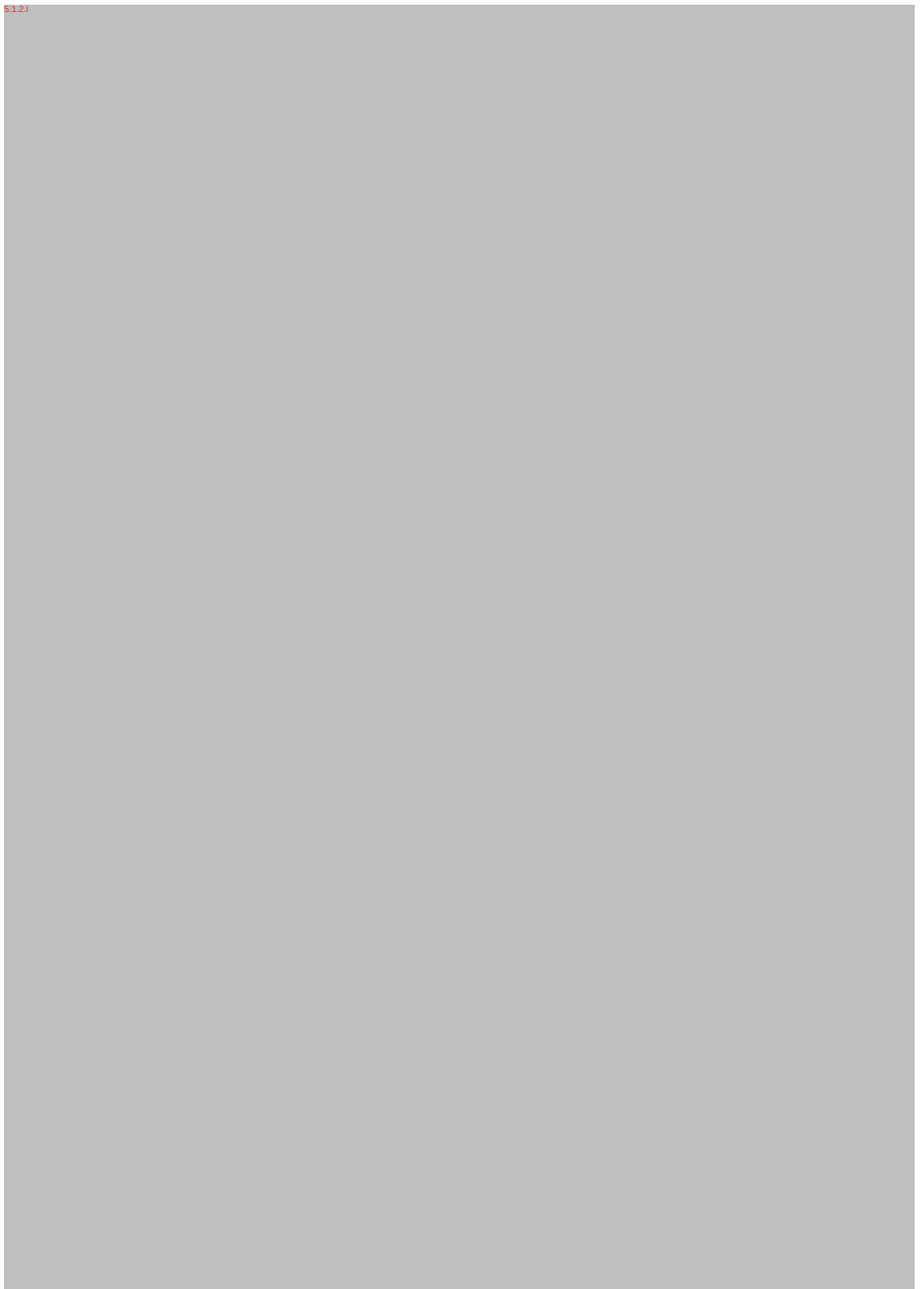
5.1.2.1



5.1.2.i









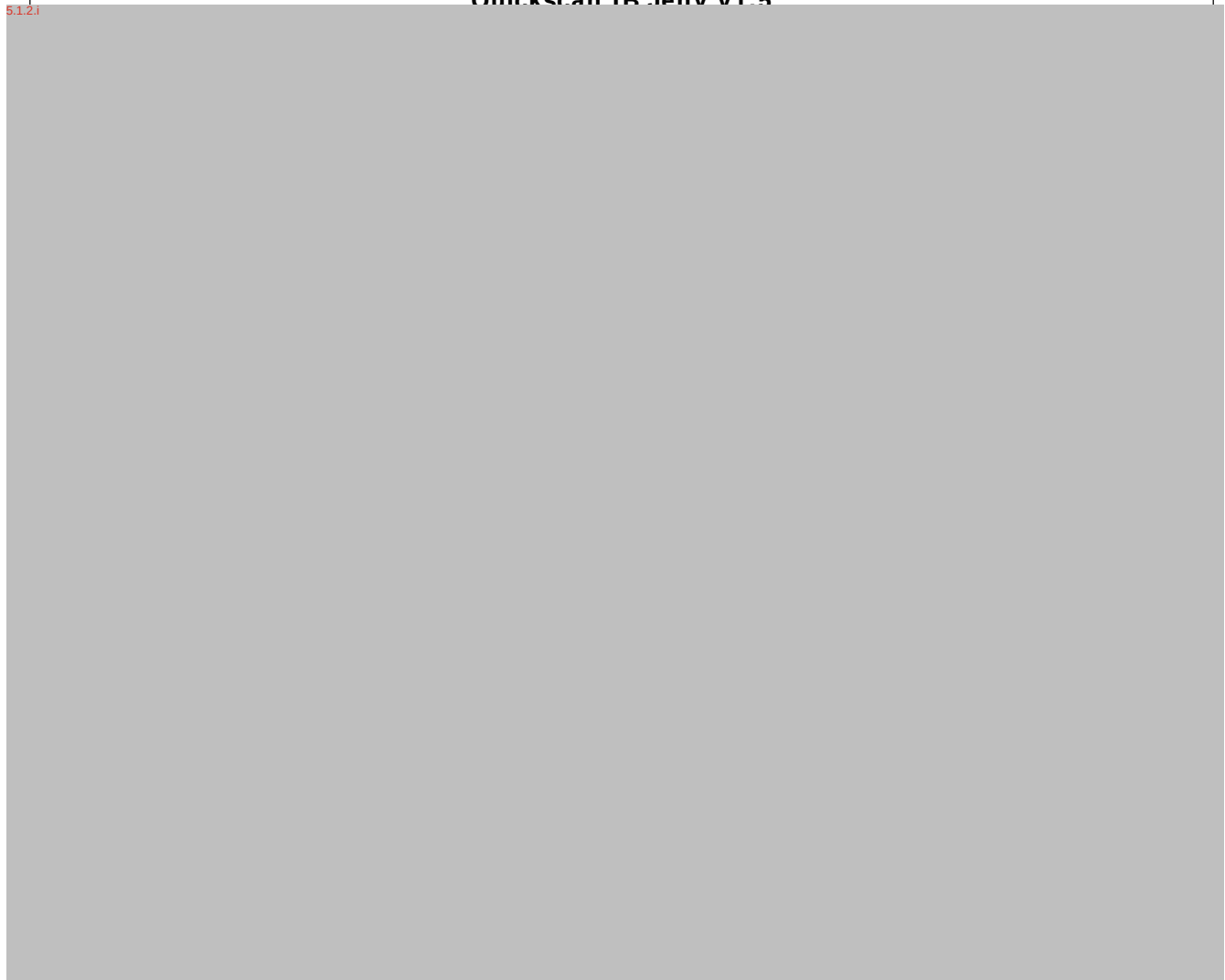






5.1.2.1

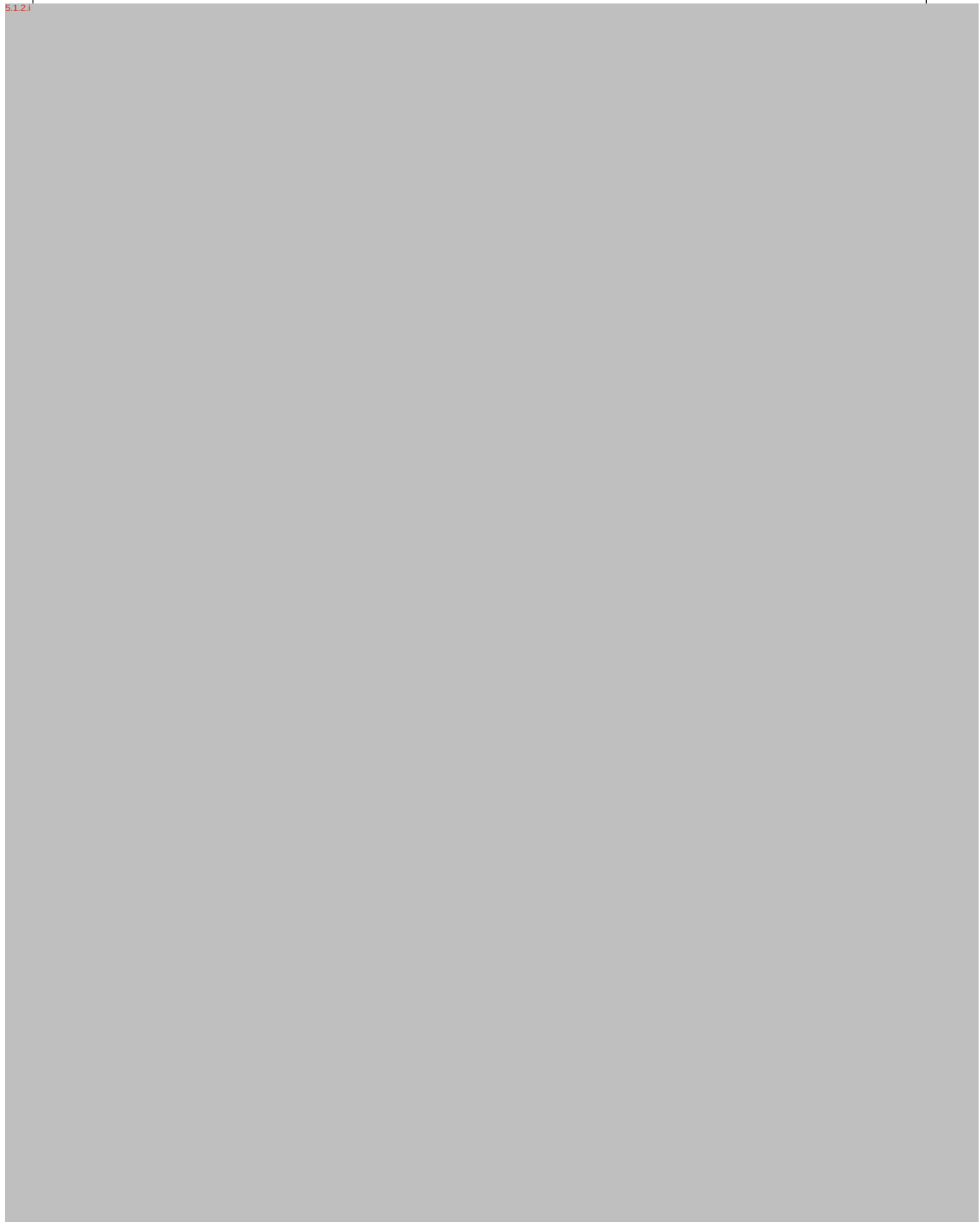




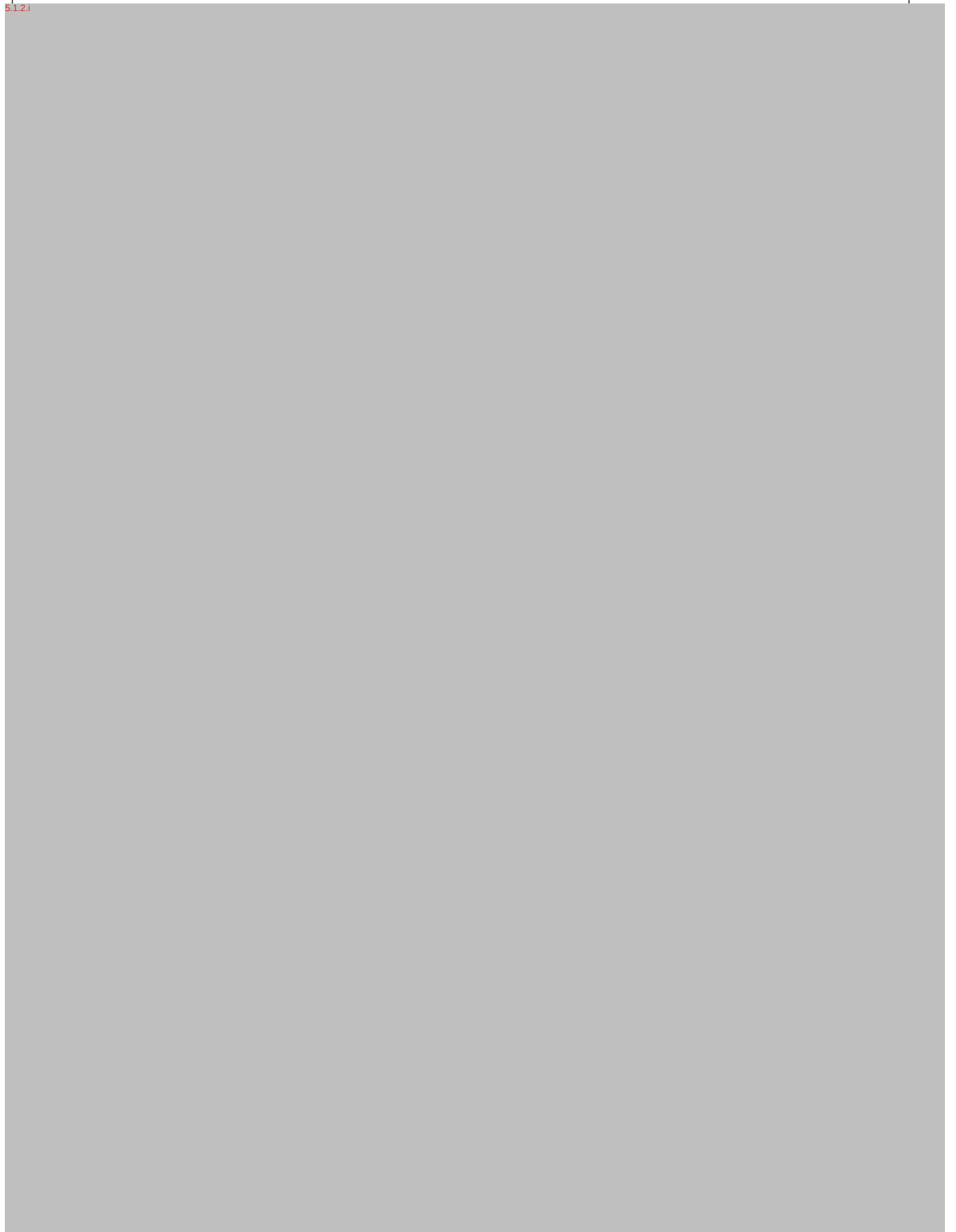




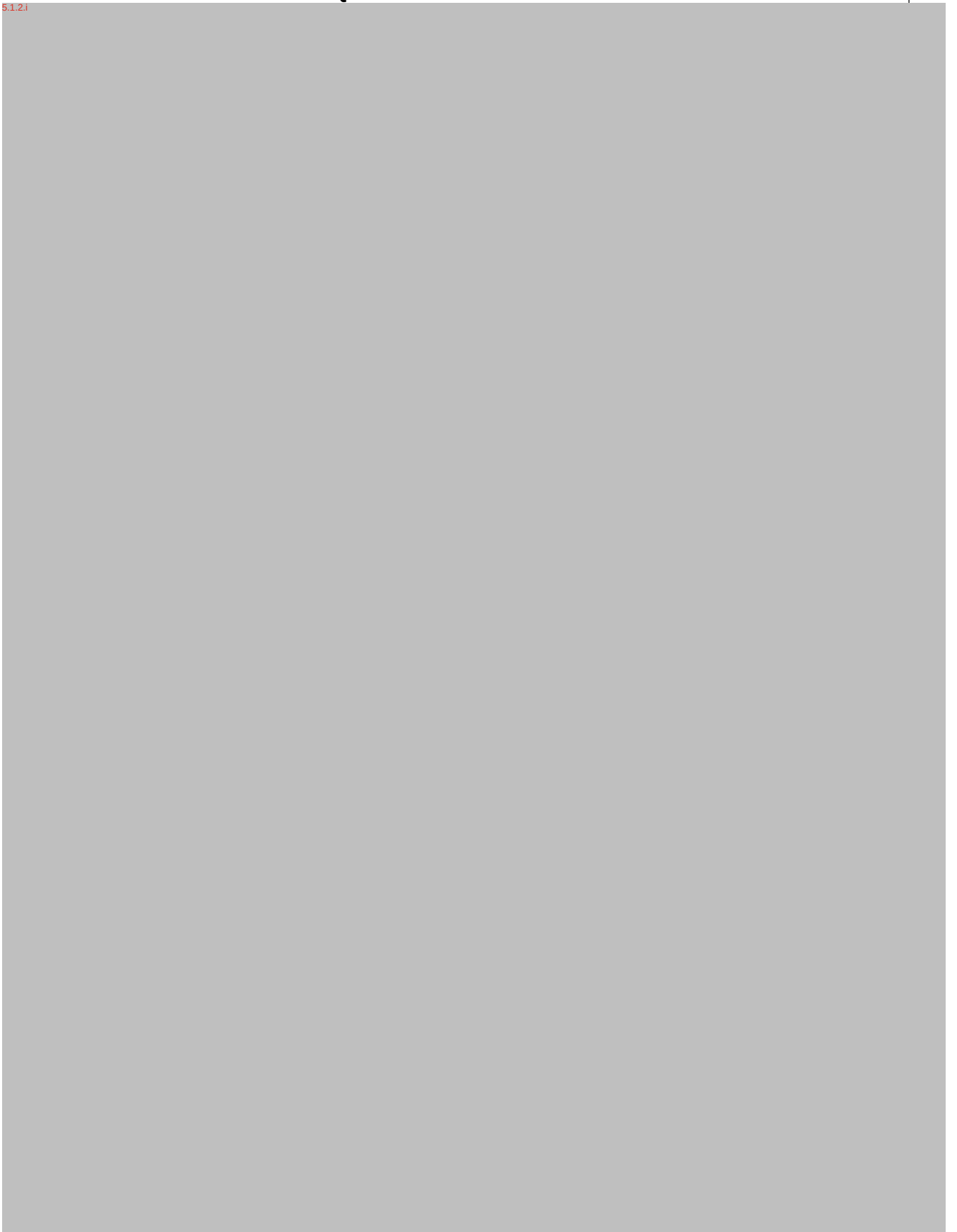




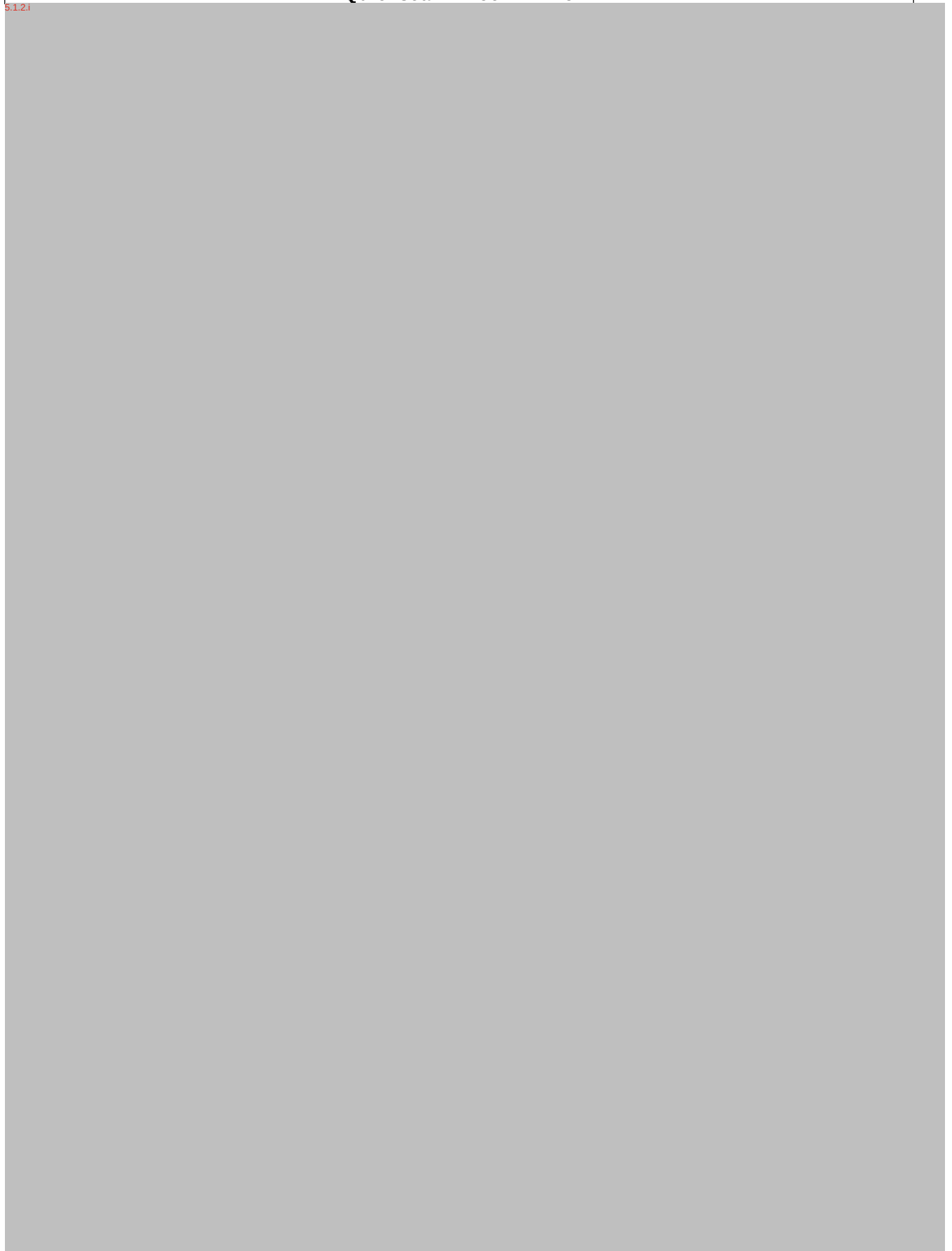
5.12.1

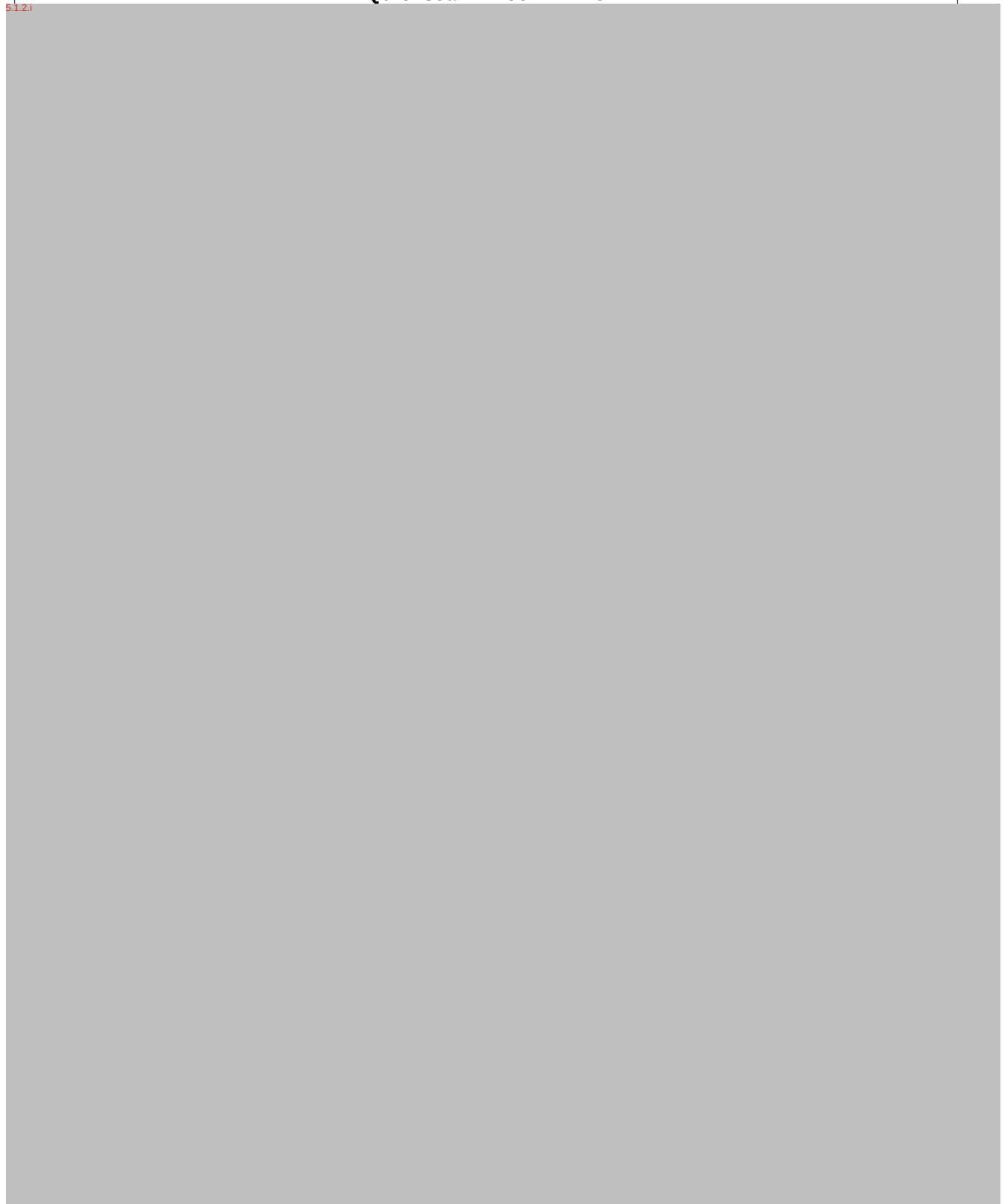






5.1.2.1





5.1.2.i





|  |
|--|
|  |
|--|

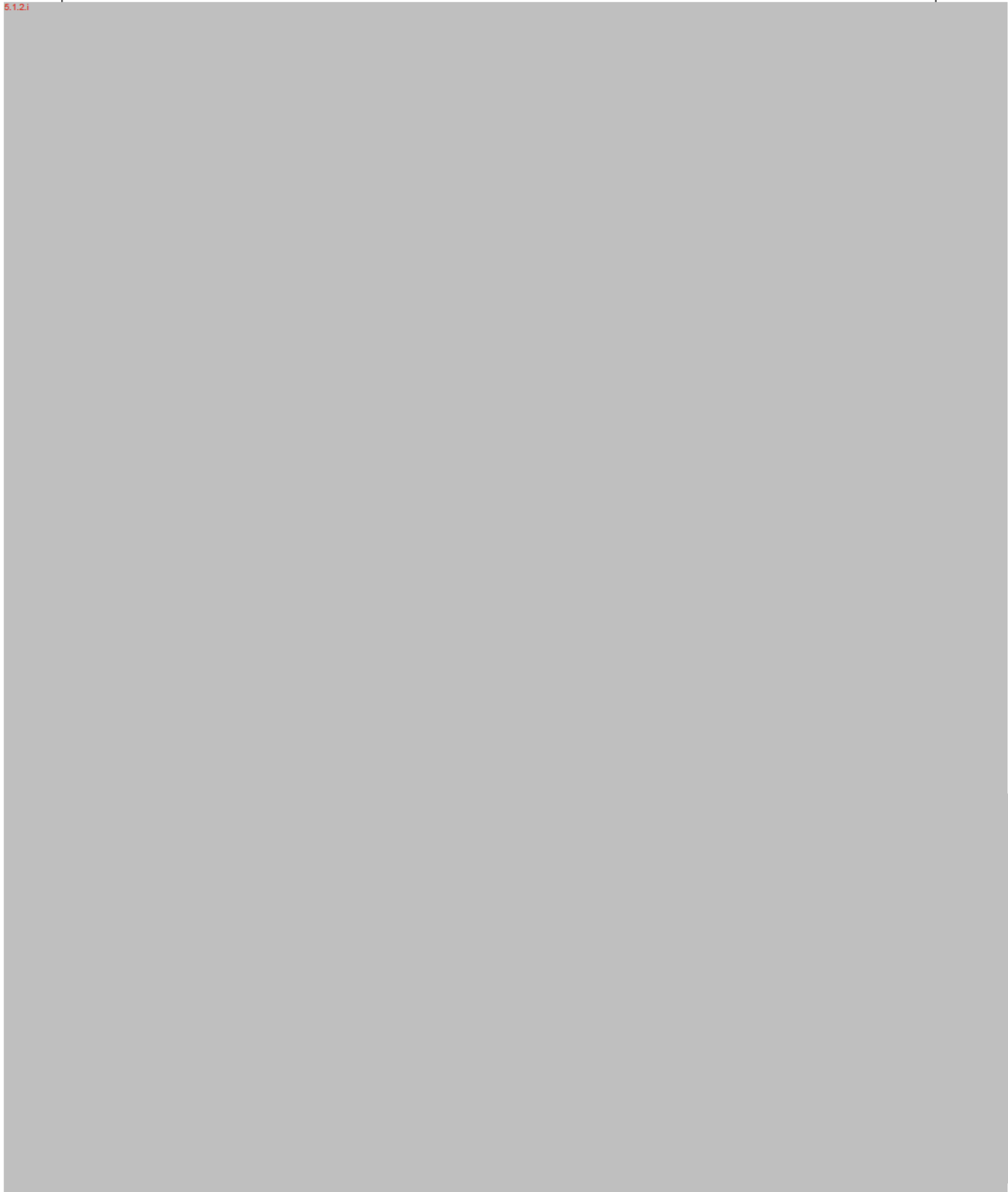








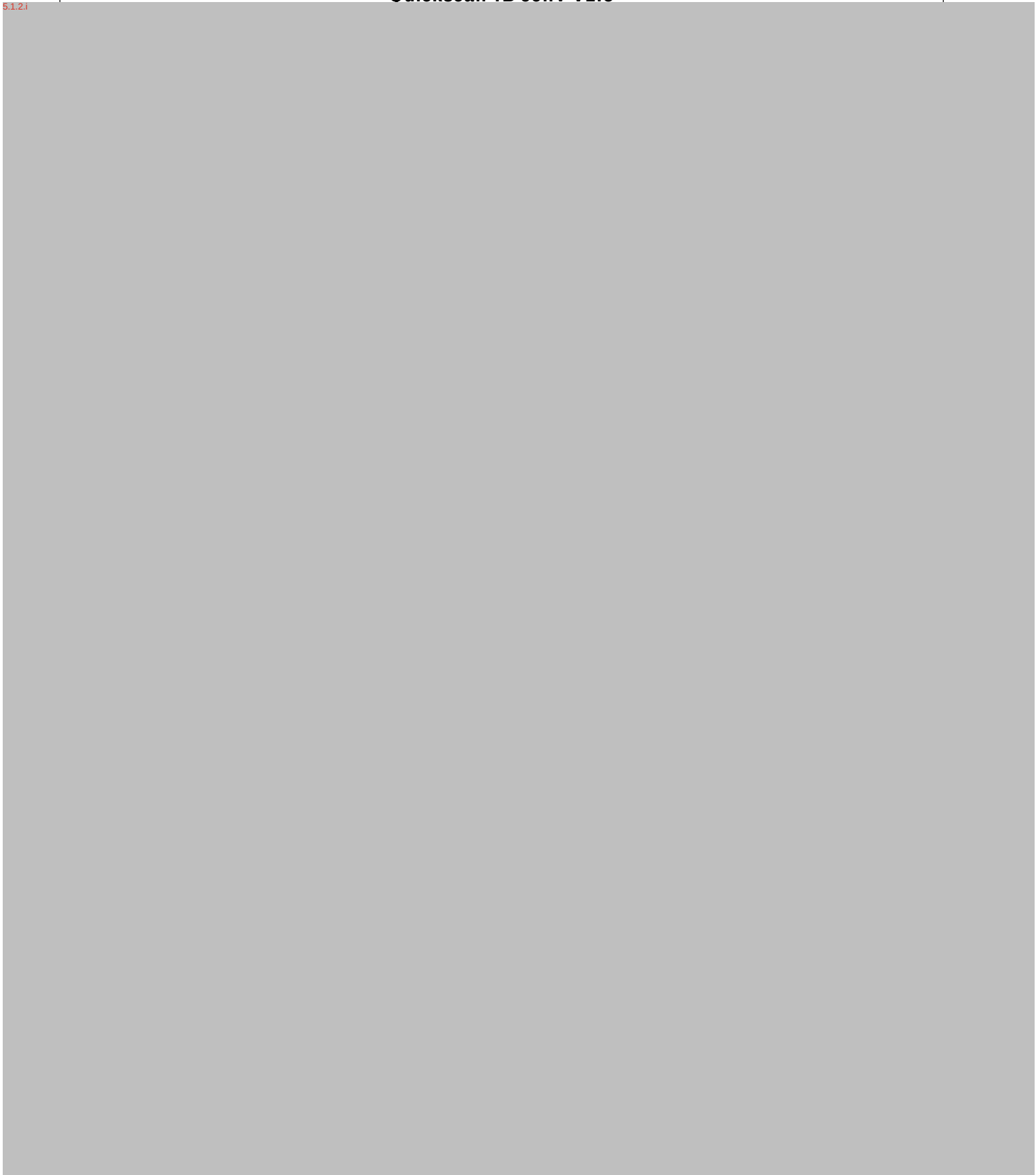




5.1.2.1









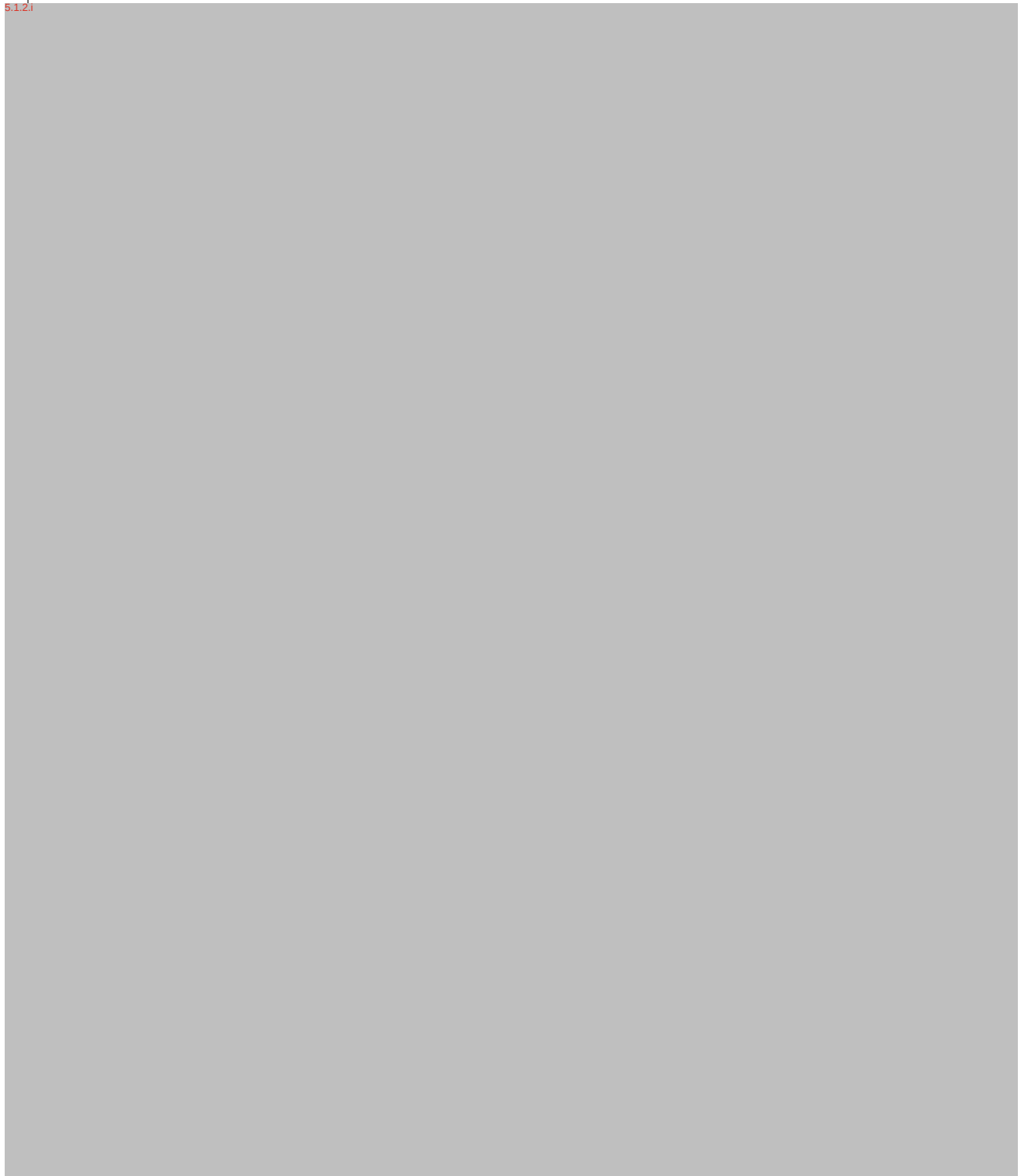




## **Bijlage 2: Samenhang QS-IB en PIA**

---

5.1.21

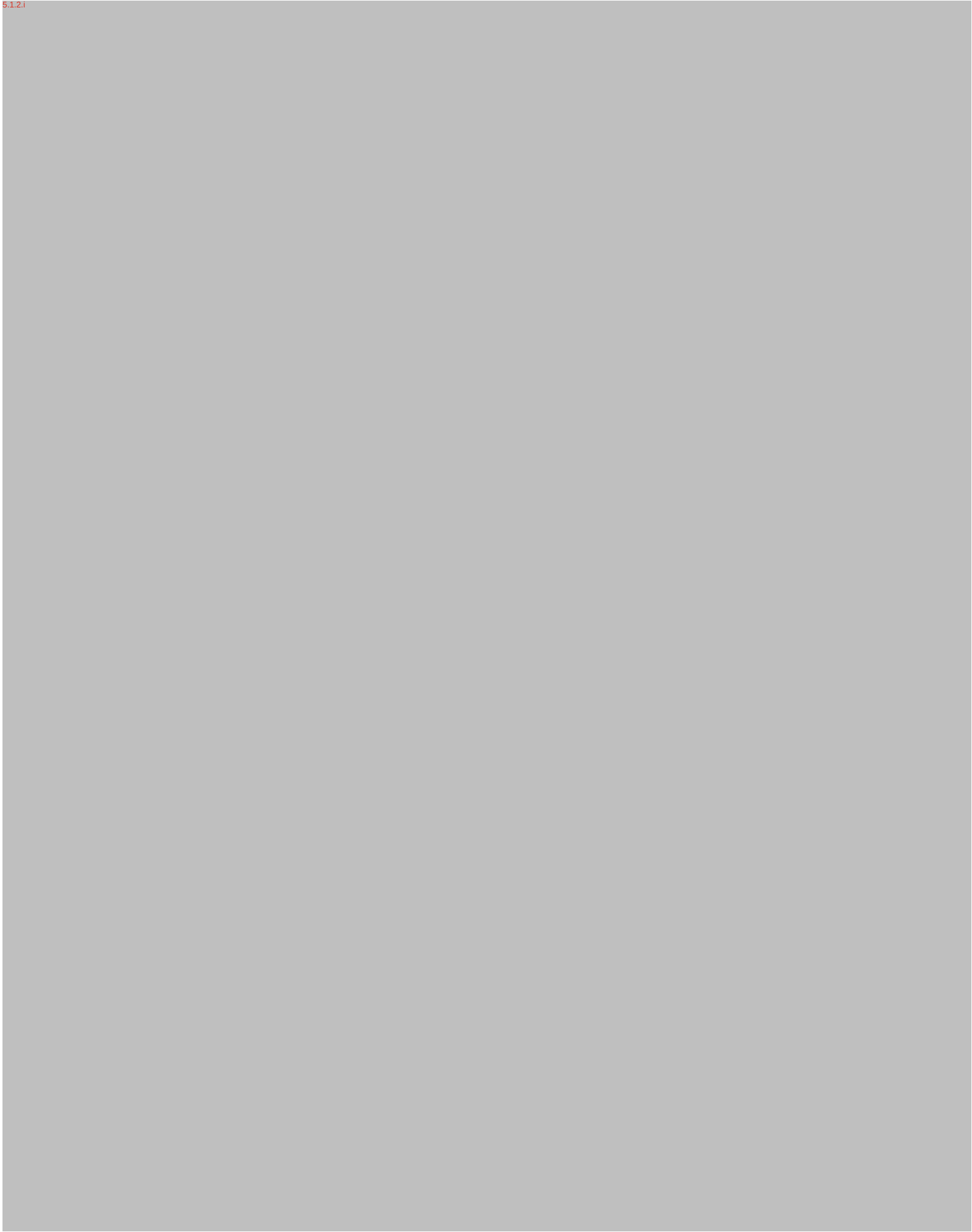




5.1.2.1

5.1.2.1









5.1.2.i

5.1.2.i

5.1.2.i







# Autorisatiebeleid DIAS

**OPENBAAR MINISTERIE**

Dienstverleningsorganisatie Openbaar Ministerie

## Autorisatiebeleid DIAS

Datum 28 oktober 2021

Auteur 

Versie V1.0

Op 11 oktober heeft het tactisch projectoverleg DIAS positief geadviseerd.  
Op 28 oktober heeft de stuurgroep DIAS dit document vastgesteld.

# Inhoud

|     |                                                           |    |
|-----|-----------------------------------------------------------|----|
| 1   | Leeswijzer                                                | 4  |
| 2   | Autorisatiemodel DIAS                                     | 4  |
| 2.1 | Rubricering van gegevens                                  | 4  |
| 2.2 | Toelichting Autorisatiematrix DIAS                        | 4  |
| 2.3 | Toelichting werking Attribute-based Access Control (ABAC) | 6  |
| 3   | Procedures                                                | 8  |
| 3.1 | Procedure Autorisatieaanvraag DIAS gebruiker              | 8  |
| 3.2 | Procedure Intrekken autorisatie van DIAS gebruiker        | 8  |
| 3.3 | Procedure Periodieke controle DIAS gebruikers             | 8  |
| 3.4 | Procedure Aanpassingen autorisatiebeleid DIAS             | 8  |
| 4   | Eisen aan autorisatie                                     | 9  |
| 4.1 | Gestelde eisen door informatiebeveiliging                 | 9  |
|     | Bijlagen Autorisatiebeleid DIAS                           | 10 |
|     | Bijlage A. Autorisatiematrix DIAS                         | 10 |
|     | Bijlage B. Hoofden IRC                                    | 10 |
|     | Bijlage C. Autorisatieformulier DIAS                      | 10 |
|     | Bijlage D. Invoerprotocol                                 | 10 |

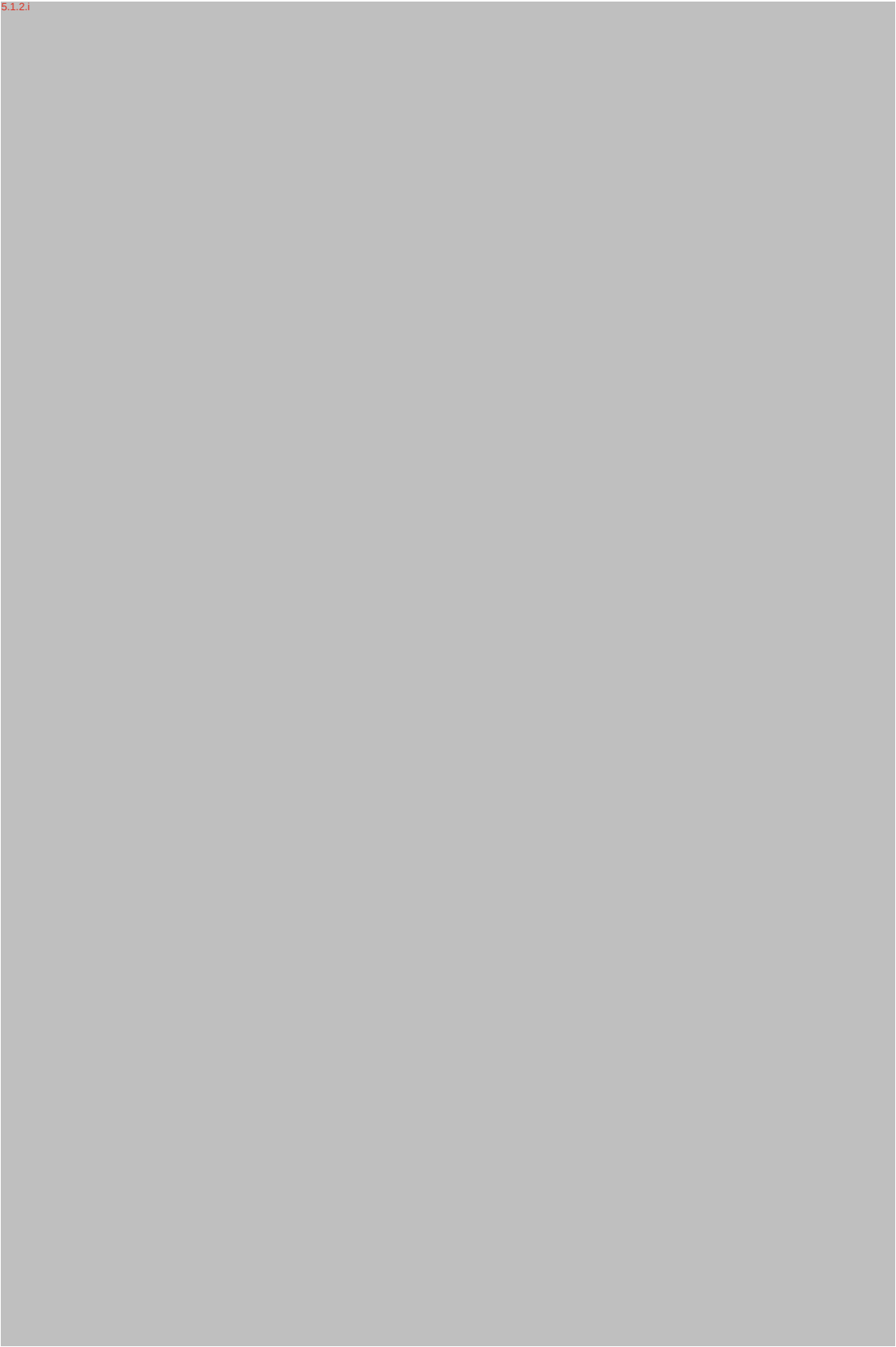
5.1.2.i



5.1.2.i



5.1.2.1



5.1.2.1





5.1.2.1



5.12.1



5.1.2.1









# Overzicht IRC hoofden

In dit overzicht staan de personen vermeld die aan het hoofd van een IRC staan, zij dienen het autorisatieformulier voor LURIS te ondertekenen.

Zie ook de procedure [autorisaties](#).

| IRC                  | Hoofd   | e-mailadres |
|----------------------|---------|-------------|
| Amsterdam            | 5.1.2.e |             |
| Den Haag             |         |             |
| IRC-LE               |         |             |
| Limburg              |         |             |
| Midden-Nederland     |         |             |
| Noord-Holland        |         |             |
| Noord-Nederland      |         |             |
| Oost-Brabant         |         |             |
| Oost-Nederland       |         |             |
| Rotterdam            |         |             |
| Zeeland-West Brabant |         |             |
| IRC IOS              |         |             |
| LIRC - Politie       |         |             |
| LIRC - LP (OM)       |         |             |
| IRC FP               |         |             |
| AIRS                 |         |             |



## Aanvraag Autorisatie LURIS

### Formulier

Hiermee kunt u autorisatie(s) voor LURIS aanvragen, wijzigen of opheffen.

### Voorwaarden

De werkplek waarop LURIS gebruikt gaat worden voldoet aan de eisen zoals gesteld in de Voorschriften Informatiebeveiliging Rijksoverheid.

### Opsturen of mailen

Stuur het formulier naar de Justitiële Informatiedienst, Postbus 337, 7600 AH Almelo, of mail het formulier als bijlage naar [info@justid.nl](mailto:info@justid.nl).

### Meer informatie

[www.justid.nl](http://www.justid.nl); Frontoffice: (088) 998 90 00 / [info@justid.nl](mailto:info@justid.nl)

## 1 Gegevens aanvragende instantie

|                               |                          |  |
|-------------------------------|--------------------------|--|
| Naam instantie                |                          |  |
| Naam IRC                      |                          |  |
| Naam en voorletters           |                          |  |
| Contactpersoon                |                          |  |
| Telefoonnummer contactpersoon | Mailadres contactpersoon |  |
| Telefoonnummer en mailadres   |                          |  |

## 2 Te autoriseren personen

|           |                                   |                                   |                     |                     |                                    |                                   |                                   |
|-----------|-----------------------------------|-----------------------------------|---------------------|---------------------|------------------------------------|-----------------------------------|-----------------------------------|
| Persoon 1 | Gegevens te autoriseren personen  |                                   |                     |                     |                                    |                                   |                                   |
|           | Achternaam                        |                                   | Voornaam            |                     | Mailadres                          |                                   |                                   |
|           |                                   |                                   |                     |                     |                                    |                                   |                                   |
|           | Telefoonnummer                    | Gebbruikersnaam <sup>1</sup>      | Status <sup>2</sup> | Rollen <sup>3</sup> | Autorisatie                        |                                   |                                   |
|           |                                   |                                   |                     |                     | <input type="checkbox"/> Aanvragen | <input type="checkbox"/> Wijzigen | <input type="checkbox"/> Opheffen |
|           | Ruimte voor eventuele toelichting |                                   |                     |                     |                                    |                                   |                                   |
|           |                                   |                                   |                     |                     |                                    |                                   |                                   |
| Persoon 2 | Achternaam                        |                                   | Voornaam            |                     | Mailadres                          |                                   |                                   |
|           |                                   |                                   |                     |                     |                                    |                                   |                                   |
|           | Telefoonnummer                    | Gebbruikersnaam <sup>1</sup>      | Status <sup>2</sup> | Rollen <sup>3</sup> | Autorisatie                        |                                   |                                   |
|           |                                   |                                   |                     |                     | <input type="checkbox"/> Aanvragen | <input type="checkbox"/> Wijzigen | <input type="checkbox"/> Opheffen |
|           |                                   | Ruimte voor eventuele toelichting |                     |                     |                                    |                                   |                                   |
|           |                                   |                                   |                     |                     |                                    |                                   |                                   |



# Aanvraag

Autorisatie LURIS

Persoon 3

|                                   |                             |                      |                      |                                                                                                        |
|-----------------------------------|-----------------------------|----------------------|----------------------|--------------------------------------------------------------------------------------------------------|
| Achternaam                        | Voornaam                    |                      | Mailadres            |                                                                                                        |
| <input type="text"/>              | <input type="text"/>        |                      | <input type="text"/> |                                                                                                        |
| Telefoonnummer                    | Gebruikersnaam <sup>1</sup> | Status <sup>2</sup>  | Rollen <sup>3</sup>  | Autorisatie                                                                                            |
| <input type="text"/>              | <input type="text"/>        | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> Aanvragen <input type="checkbox"/> Wijzigen <input type="checkbox"/> Opheffen |
| Ruimte voor eventuele toelichting |                             |                      |                      |                                                                                                        |
| <input type="text"/>              |                             |                      |                      |                                                                                                        |

Persoon 4

|                                   |                             |                      |                      |                                                                                                        |
|-----------------------------------|-----------------------------|----------------------|----------------------|--------------------------------------------------------------------------------------------------------|
| Achternaam                        | Voornaam                    |                      | Mailadres            |                                                                                                        |
| <input type="text"/>              | <input type="text"/>        |                      | <input type="text"/> |                                                                                                        |
| Telefoonnummer                    | Gebruikersnaam <sup>1</sup> | Status <sup>2</sup>  | Rollen <sup>3</sup>  | Autorisatie                                                                                            |
| <input type="text"/>              | <input type="text"/>        | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> Aanvragen <input type="checkbox"/> Wijzigen <input type="checkbox"/> Opheffen |
| Ruimte voor eventuele toelichting |                             |                      |                      |                                                                                                        |
| <input type="text"/>              |                             |                      |                      |                                                                                                        |

Persoon 5

|                                   |                             |                      |                      |                                                                                                        |
|-----------------------------------|-----------------------------|----------------------|----------------------|--------------------------------------------------------------------------------------------------------|
| Achternaam                        | Voornaam                    |                      | Mailadres            |                                                                                                        |
| <input type="text"/>              | <input type="text"/>        |                      | <input type="text"/> |                                                                                                        |
| Telefoonnummer                    | Gebruikersnaam <sup>1</sup> | Status <sup>2</sup>  | Rollen <sup>3</sup>  | Autorisatie                                                                                            |
| <input type="text"/>              | <input type="text"/>        | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> Aanvragen <input type="checkbox"/> Wijzigen <input type="checkbox"/> Opheffen |
| Ruimte voor eventuele toelichting |                             |                      |                      |                                                                                                        |
| <input type="text"/>              |                             |                      |                      |                                                                                                        |

Persoon 6

|                                   |                             |                      |                      |                                                                                                        |
|-----------------------------------|-----------------------------|----------------------|----------------------|--------------------------------------------------------------------------------------------------------|
| Achternaam                        | Voornaam                    |                      | Mailadres            |                                                                                                        |
| <input type="text"/>              | <input type="text"/>        |                      | <input type="text"/> |                                                                                                        |
| Telefoonnummer                    | Gebruikersnaam <sup>1</sup> | Status <sup>2</sup>  | Rollen <sup>3</sup>  | Autorisatie                                                                                            |
| <input type="text"/>              | <input type="text"/>        | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> Aanvragen <input type="checkbox"/> Wijzigen <input type="checkbox"/> Opheffen |
| Ruimte voor eventuele toelichting |                             |                      |                      |                                                                                                        |
| <input type="text"/>              |                             |                      |                      |                                                                                                        |

## 3 Ondertekening

U dient het volledig ingevulde formulier af te drukken en vervolgens te ondertekenen; digitale ondertekening is niet toegestaan.

Naam en handtekening

Functie

Datum

Naam en handtekening hoofd IRC

<sup>1</sup> Uitsluitend invullen indien er een voorkeur is voor een gebruikersnaam.

<sup>2</sup> Geef hier de status aan: **N** = Normaal, **V** = Vertrouwelijk en **B** = Bijzonder

<sup>3</sup> Geef hier de rol aan:

1 = Registratie medewerker

2 = Raadpleger rapportage

3 = Coördinator

4 = Lokaal applicatiebeheerder

5 = Raadpleger

6 = "Full-Text" zoeken Zylab (alleen in combinatie met de status "vertrouwelijk")

7 = DJI medewerker



Justitiële Informatiedienst  
*Ministerie van Justitie*

**Afsprakenet LURIS en Zylab –  
Invoerprotocol voor de registratie in  
LURIS en digitale archivering in Zylab**

|        |                  |
|--------|------------------|
| Datum  | 21 november 2013 |
| Status | Definitief       |



## Colofon

### Afzendgegevens

### **Justitiële Informatiedienst**

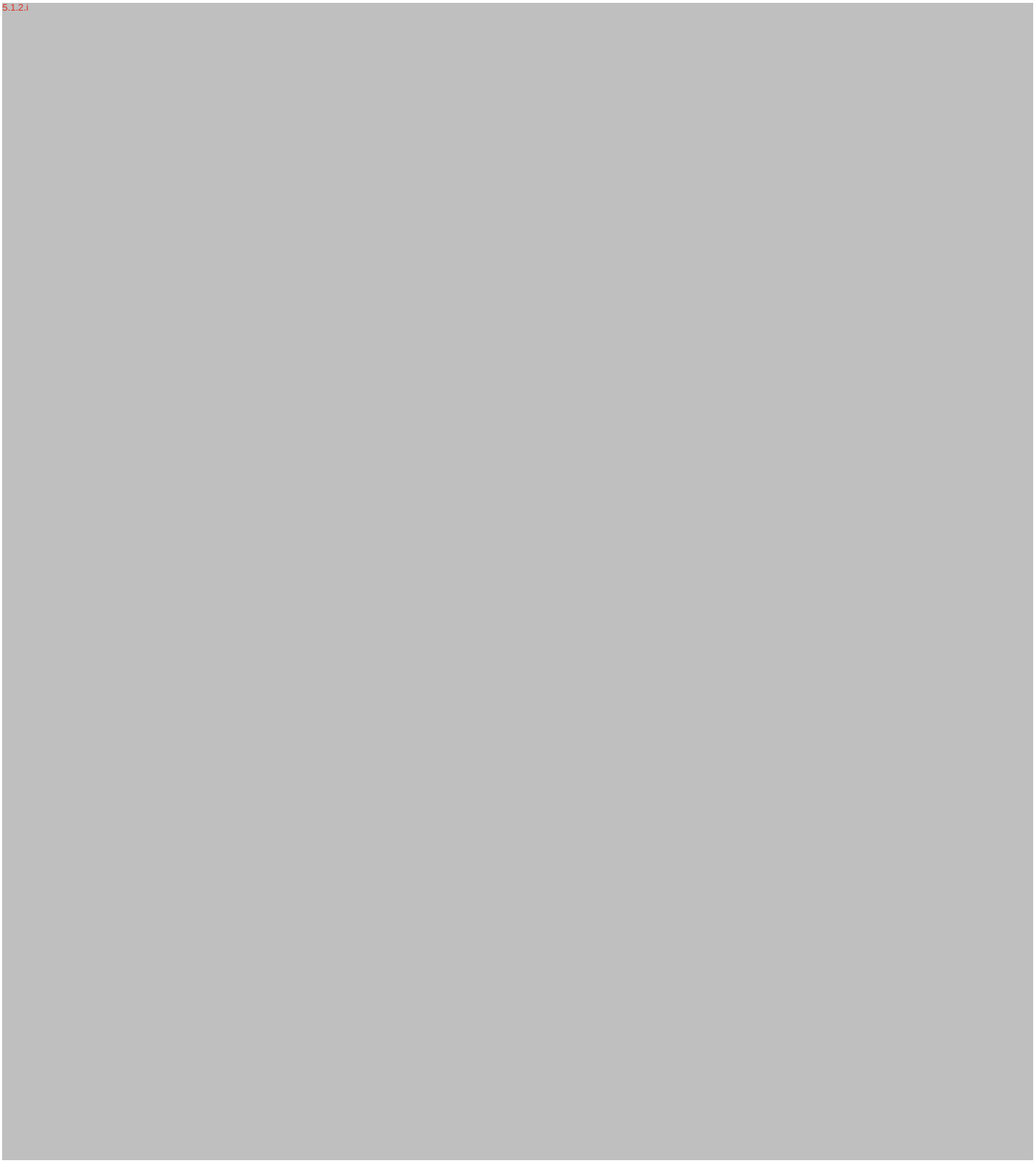
Egbert Gorterstraat 6  
7607 GB Almelo  
Postbus 337  
7600 AH Almelo  
[www.justid.nl](http://www.justid.nl)

### Auteurs

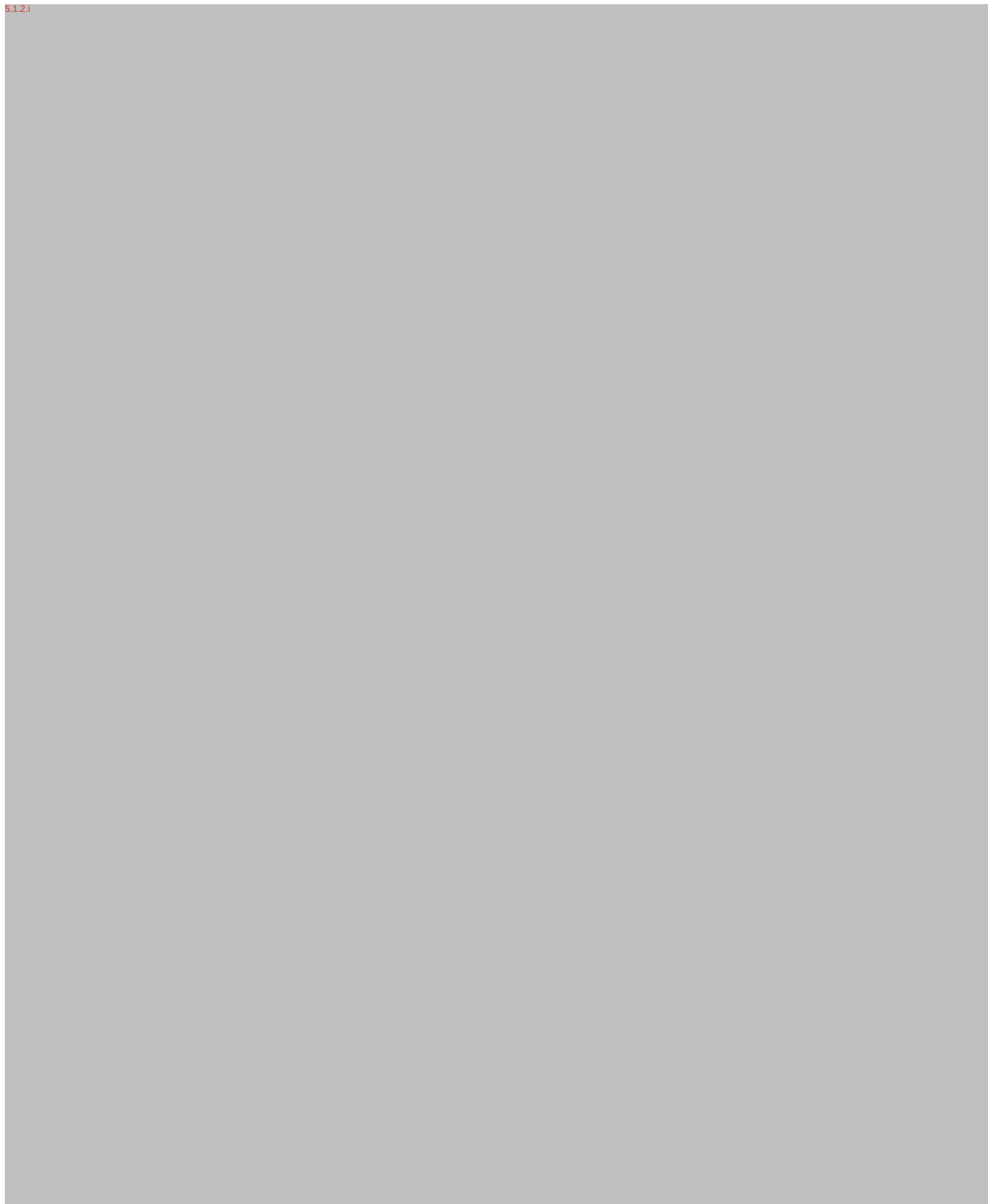
Functioneel beheer



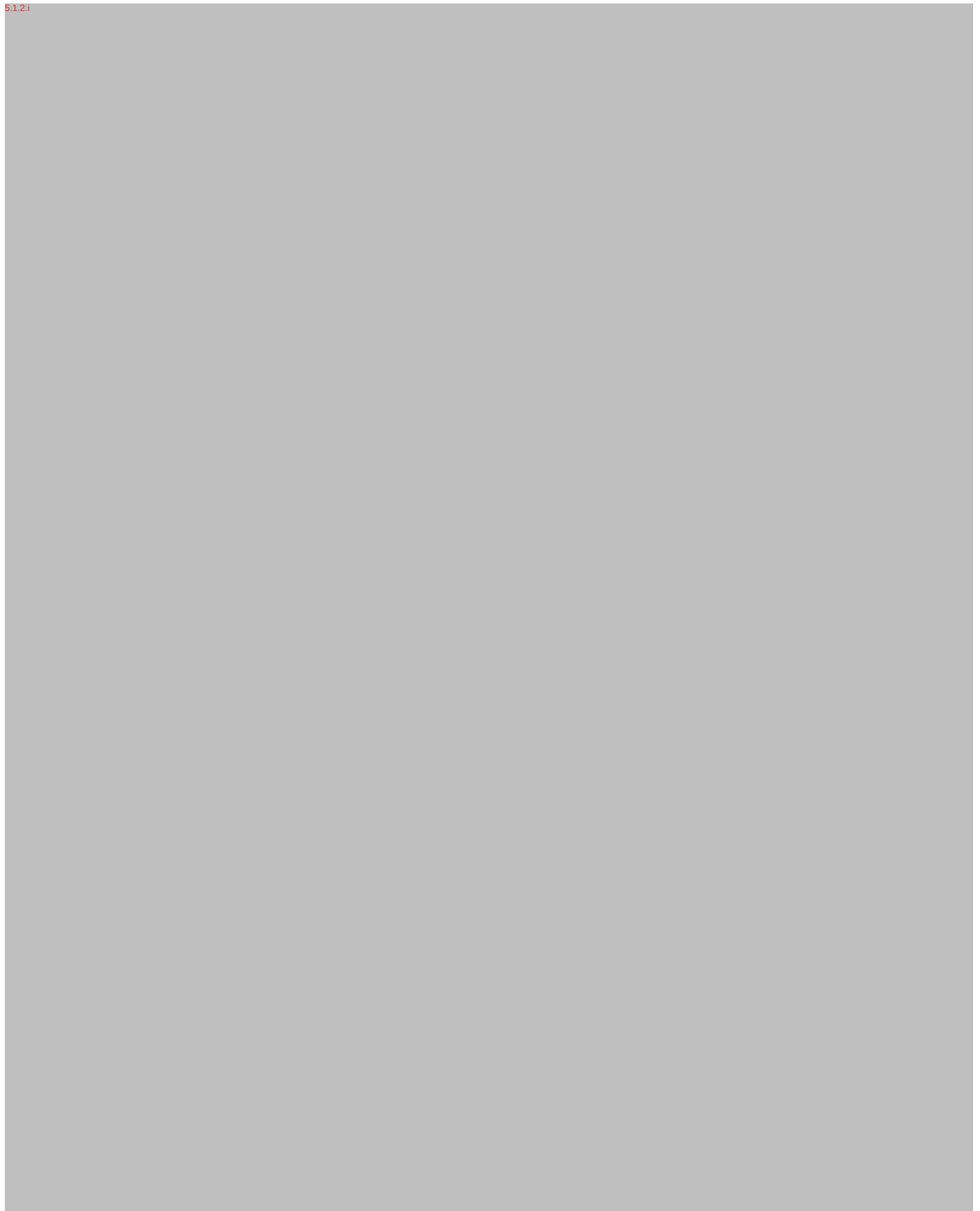
5.1.2.i



5.1.2.1



5.1.2.1





5.1.2.1



5.1.2.i



# Logging & Monitoring keuzes DIAS

**OPENBAAR MINISTERIE**

Dienstverleningsorganisatie Openbaar Ministerie

# OPENBAAR MINISTERIE

Dienstverleningsorganisatie Openbaar Ministerie

## Logging & Monitoring keuzes DIAS

Datum 15 september 2021

Auteur 5.12e 

Versie V0.81

# Inhoud

|     |                                                                       |    |
|-----|-----------------------------------------------------------------------|----|
| 1   | Leeswijzer                                                            | 4  |
| 2   | Doel logging & monitoring keuzes DIAS                                 | 4  |
| 3   | Logging binnen DIAS                                                   | 5  |
| 3.1 | Vormen van logging                                                    | 5  |
| 3.2 | Loggegevens                                                           | 6  |
| 3.3 | Bewaartermijnen loggegevens                                           | 7  |
| 3.4 | Eisen aan oplossing                                                   | 7  |
| 3.5 | Synchronisatie van systeemklokken                                     | 9  |
| 4   | Procedures                                                            | 9  |
| 4.1 | Procedure “Inzageverzoeken”                                           | 9  |
| 4.2 | Procedure “Verdachte handelingen van gebruikers”                      | 9  |
| 4.3 | Procedure “Inzicht in verwerking RHV middels tijdlijn DIAS”           | 10 |
| 4.4 | Procedure “Borging goed functionerend systeem DIAS”                   | 11 |
| 4.5 | Procedure “Controle technische logbestanden op security issues”       | 11 |
| 4.6 | Procedure “Communicatie aan DIAS gebruiker over Logging & Monitoring” | 11 |
| 4.7 | Procedure “Vermoede van onrechtmatig gebruik”                         | 12 |
|     | Bijlagen Logging & Monitoring keuzes DIAS                             | 13 |
|     | Bijlage A. Informatie over logging DIAS                               | 13 |

5.1.2.i





5.1.2.1





5.1.2.i



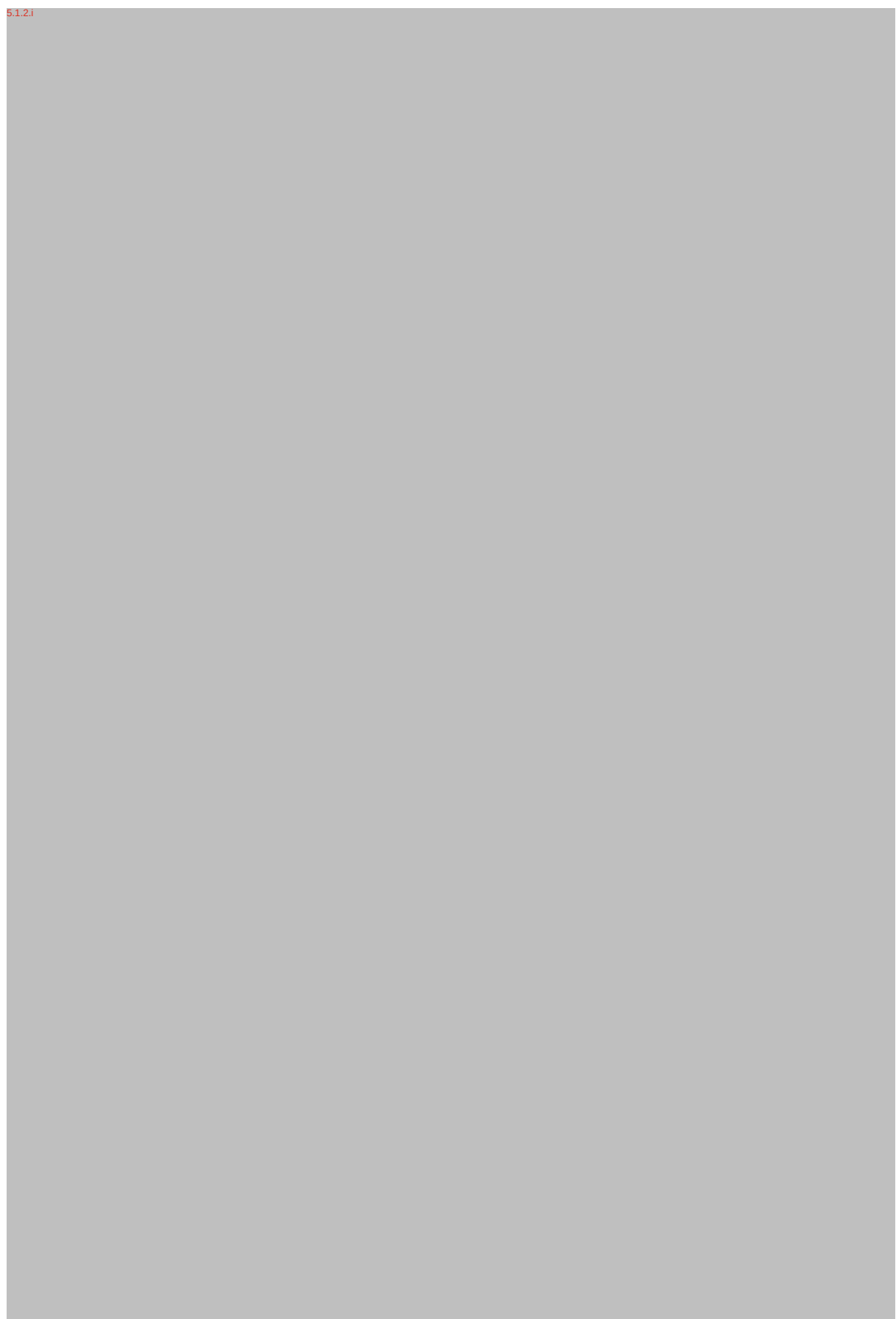
5.1.2.1



5.1.2.1



5.1.2.i



5.1.2.1



5.12.1



5.1.2.1

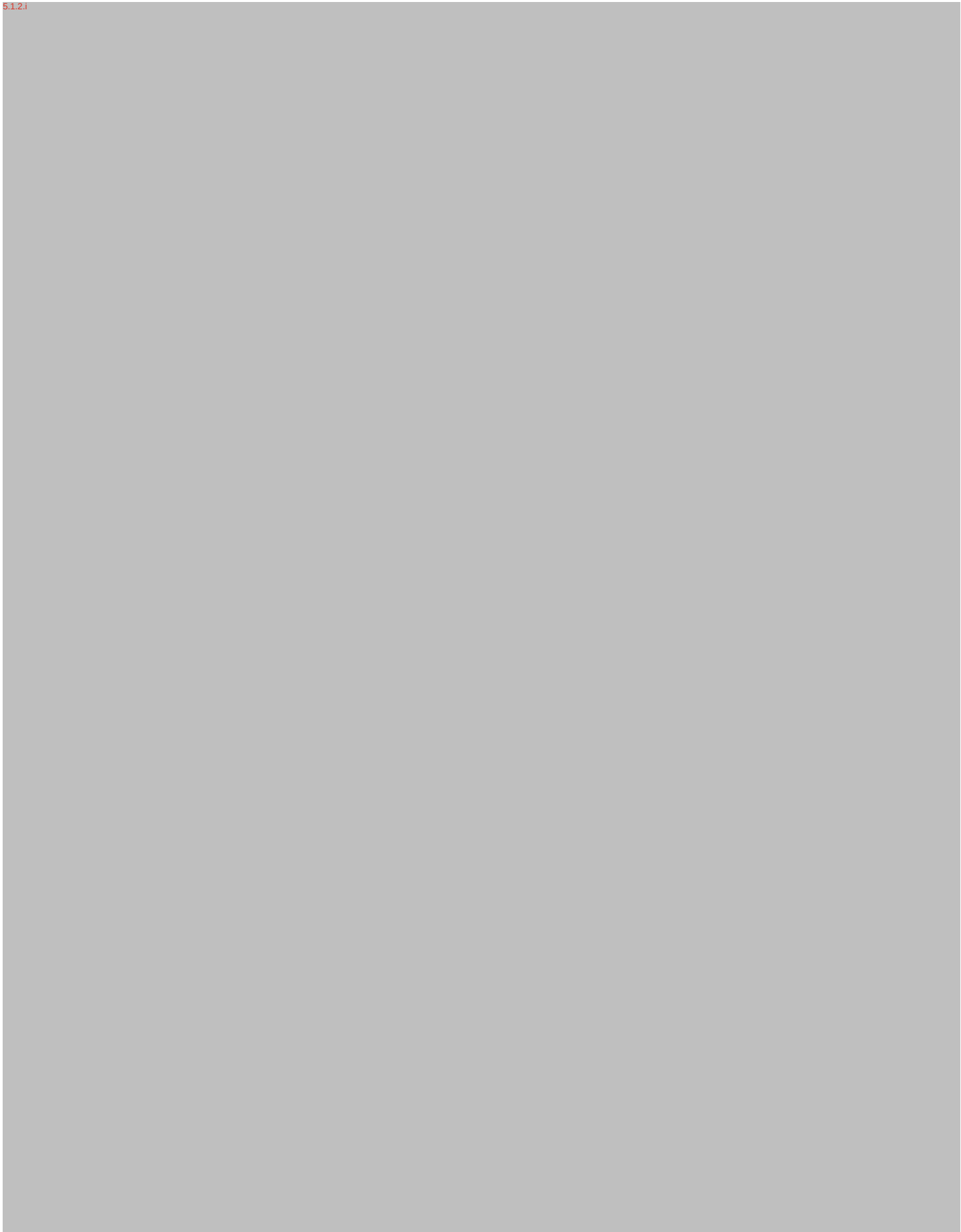


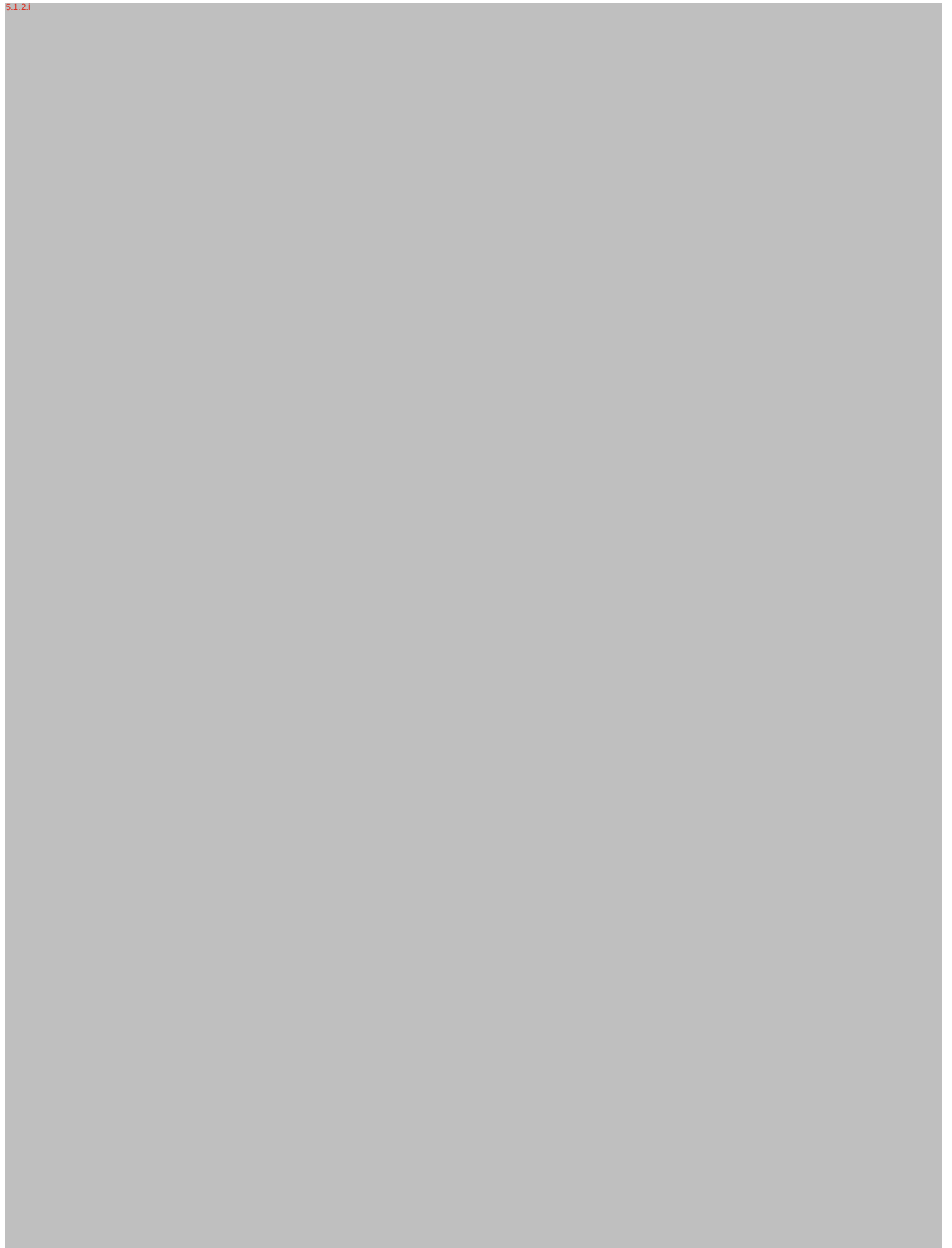
5.1.2.i

























# Beleidskader registerplicht en GEB

Bescherming van persoons- en  
politiegegevens

Gegevensautoriteit

Definitief

Versie 2.0

Versie datum 8 november 2019

Rubricering politie intern

# Documentinformatie

## Versiegeschiedenis

| Versie | Versie datum     | Samenvatting van de aanpassing                                                                                                                                                                                                                                    | Gemarkeerde wijzigingen |
|--------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| 0.1    | 26 november 2018 | Eerste opzet door <a href="#">5.1.2.e</a>                                                                                                                                                                                                                         |                         |
| 0.2    | 11 december 2018 | Reacties GA verwerkt ( <a href="#">5.1.2.e</a> , <a href="#">5.1.2.e</a> , <a href="#">5.1.2.e</a> ). Invulling H4 AVG door <a href="#">5.1.2.e</a>                                                                                                               |                         |
| 0.3    | 14 januari 2019  | Reacties Registerwerkgroep ( <a href="#">5.1.2.e</a> , <a href="#">5.1.2.e</a> , <a href="#">5.1.2.e</a> ) verwerkt. Opzet iets gewijzigd naar verantwoordingsplicht                                                                                              |                         |
| 0.4    | 5 februari 2019  | Tussenversie met aanpassingen n.a.v. plenaire bespreking registerwerkgroep 24 februari 2019 .                                                                                                                                                                     |                         |
| 0.5    | 22 februari      | Reacties verwerkt van <a href="#">5.1.2.e</a> (kwartiermaker privacy PDC) <a href="#">5.1.2.e</a> , <a href="#">5.1.2.e</a> , <a href="#">5.1.2.e</a> , <a href="#">5.1.2.e</a>                                                                                   |                         |
| 0.6    | 7 maart 2019     | Paragraaf. over GEB uitgebreid en structuur aangepast n.a.v. reacties GA en Verbeterprogramma                                                                                                                                                                     |                         |
| 0.7    | 11 maart 2019    | Reacties verwerkt van <a href="#">5.1.2.e</a> over uitvoering control-functie, redactieslag van <a href="#">5.1.2.e</a> , <a href="#">5.1.2.e</a> , <a href="#">5.1.2.e</a> , reactie <a href="#">5.1.2.e</a> , <a href="#">5.1.2.e</a> , <a href="#">5.1.2.e</a> |                         |
| 1.0    | 14 maart 2019    | Versie voor stuurgroep Verbeterprogramma Wpg en IB en stuurgroep AVG                                                                                                                                                                                              |                         |
| 1.1    | 28 maart 2019    | Versie goedgekeurd door stuurgroep Verbeterprogramma Wpg en IB, reactie <a href="#">5.1.2.e</a> <a href="#">5.1.2.e</a> verwerkt                                                                                                                                  |                         |
| 1.2    | 28 mei 2019      | Enkele reacties nav stuurgroep verwerkt                                                                                                                                                                                                                           |                         |
| 1.3    | 1 augustus 2019  | Reactie <a href="#">5.1.2.e</a> verwerkt                                                                                                                                                                                                                          |                         |
| 1.3    | 3 oktober 2019   | Akkoord Hoofden Bedrijfsvoering Overleg HBVO                                                                                                                                                                                                                      |                         |
| 2.0    | 8 november 2019  | Akkoord Breed Bedrijfsvoering Overleg BBVO                                                                                                                                                                                                                        |                         |

## Distributie

| Versie | Verzend datum | Naam | Afdeling / Functie |
|--------|---------------|------|--------------------|
|        |               |      |                    |
|        |               |      |                    |

## Review commentaar

| Versie | Wanneer | Wie | Functie |
|--------|---------|-----|---------|
|        |         |     |         |
|        |         |     |         |

© Politie, all rights reserved.

Niets uit deze uitgave mag worden verveelvoudigd, op geautomatiseerde wijze opgeslagen of openbaar gemaakt in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de Politie.

# Inhoudsopgave

|                                                        |    |
|--------------------------------------------------------|----|
| Documentinformatie .....                               | 2  |
| Inhoudsopgave.....                                     | 2  |
| 1. Inleiding.....                                      | 4  |
| 1.1 Verantwoordingsplicht .....                        | 4  |
| 1.2 Registerplicht en GEB .....                        | 4  |
| 1.3 Dit beleidskader.....                              | 4  |
| 2. Verwerkingen, de GEB en het register.....           | 6  |
| 2.1 Relevante wetgeving .....                          | 6  |
| 2.2 Verwerkingen en verwerkingsverantwoordelijke ..... | 6  |
| 2.2.1 Juridisch kader.....                             | 6  |
| 2.2.1.1 Verwerken van persoonsgegevens.....            | 6  |
| 2.2.1.2 Verwerken van politiegegevens .....            | 6  |
| 2.2.1.3 Verwerkingsverantwoordelijke .....             | 7  |
| 2.2.2 Keuze verwerking politie.....                    | 7  |
| 2.2.3 Eisen aan verwerkingen .....                     | 8  |
| 2.3 GEB.....                                           | 8  |
| 2.3.1 Juridisch kader.....                             | 8  |
| 2.3.2 GEB bij politie .....                            | 9  |
| 2.4 Verwerkingsregister .....                          | 10 |
| 2.4.1 Juridisch kader.....                             | 10 |
| 2.4.2 Verwerkingsregister bij politie .....            | 10 |
| 2.5 Samenwerkingsverbanden .....                       | 11 |
| 2.6 Ondersteunende tool .....                          | 11 |
| 2.7 Eisen aan verwerkingen .....                       | 12 |
| 3. Rollen en verantwoordelijkheden .....               | 13 |
| 5.1 De korpschef .....                                 | 13 |
| 5.2 Landelijke portefeuillehouders .....               | 13 |
| 5.2.1 Portefeuillehouder AVG .....                     | 13 |
| 5.2.2 Portefeuillehouder Wpg .....                     | 13 |
| 5.3 Lijnmanagement .....                               | 13 |
| 5.4 FG.....                                            | 13 |
| 5.5 Team informatiebeveiliging .....                   | 14 |
| 5.6 Privacyfunctionarissen .....                       | 14 |
| 5.7 Gegevensautoriteit.....                            | 14 |
| 5.8 Directie Operatiën.....                            | 14 |
| 5.9 Directeur PDC.....                                 | 14 |
| 5.10 De Centrale Ondernemingsraad .....                | 14 |
| 5.11 AP.....                                           | 14 |
| Bijlage 1 .....                                        | 15 |
| Bijlage 2 .....                                        | 16 |

# 1. Inleiding

## 1.1 Verantwoordingsplicht

Allerlei technologische ontwikkelingen hebben ertoe geleid dat vanuit de samenleving meer aandacht is gekomen voor privacy en het belang van bescherming van persoonsgegevens. Organisaties die gegevens verwerken moeten daarom veel meer dan vroeger transparant zijn over de gegevens die zij verwerken, en hierover verantwoording afleggen: de verantwoordingsplicht.

De politie staat voor de bescherming van de grondrechten en dus ook het recht dat de privacy beschermt. En ook voor de politie geldt dat het verwerken van persoonlijke gegevens veel meer in de spotlights is komen te staan. De samenleving en de politiek verlangen meer dan vroeger inzicht in en rekenschap over de verwerking van persoonlijke gegevens. De aandacht voor de bescherming van persoonlijke data heeft uiteindelijk geleid tot wijzigingen in de privacyregelgeving, waarin deze verantwoordingsplicht ook wettelijk is vastgelegd. Per 25 mei 2018 is de Algemene verordening gegevensbescherming (hierna: AVG) in werking getreden. Met ingang van 1 januari 2019 is in Nederland de vergelijkbare Europese Richtlijn gegevensbescherming opsporing en vervolging (2016/680) geïmplementeerd in de aldus gewijzigde Wet politiegegevens (hierna: Wpg).

Er zijn diverse instrumenten om uitvoering te geven aan de verantwoordingsplicht. Zo geldt bijvoorbeeld de loggingverplichting, de verplichting om een functionaris voor gegevensbescherming (hierna: FG) aan te stellen, en het verplicht bijhouden van een register van verwerkingen en een register van datalekken. Dit beleidskader gaat over de registerplicht, als onderdeel van de verantwoordingsplicht en de bijkomende verplichting om indien noodzakelijk een gegevensbeschermingseffectbeoordeling (hierna: GEB) uit te voeren. De andere onderdelen van de verantwoordingsplicht vallen buiten scope en zijn elders belegd.

## 1.2 Registerplicht en GEB

De belangrijkste verplichting onder de AVG en aangepaste Wpg is dat verwerkingen van persoons- en politiegegevens voldoen aan belangrijke beginselen zoals rechtmatigheid, transparantie, doelbinding en juistheid. Het register is een manier om verantwoording af te leggen over gegevensverwerkingen. Dat geldt naar de verwerkingsverantwoordelijke, maar ook naar de interne toezichthouder de FG, en de Autoriteit Persoonsgegevens (hierna: AP). Ook kan het register in de toekomst behulpzaam zijn bij het inzichtelijk maken van verwerkingen richting betrokkenen.

De basismaatregel om te voldoen aan de verantwoordingsplicht is het inzichtelijk maken van het effect van een verwerking op de privacy van betrokkene. In het geval er mogelijk een hoog risico is voor de rechten en vrijheden van natuurlijke personen moet er voorafgaande aan de verwerking een GEB worden uitgevoerd. Alle verwerkingen van persoonlijke gegevens zijn beschreven en opgenomen in het register van verwerkingsactiviteiten, oftewel het register. In het register moet worden aangetoond dat er maatregelen zijn genomen ter beveiliging van de persoonsgegevens. Er zijn organisaties die het register of delen daarvan online publiceren, om zo de verwerkingen aan betrokkenen zichtbaar te maken. Dat is voor de politie op dit moment niet aan de orde. Wel kunnen op termijn delen van het register gebruikt worden om betrokkenen en andere stakeholders inzicht te geven in verwerkingen.

## 1.3 Dit beleidskader

Dit beleidskader beschrijft hoe de politie invulling geeft aan verplichting om verwerkingen te beschrijven en op te nemen in een register en een GEB uit te voeren. Dit beleidskader maakt onderdeel uit van het privacy beleid van de politie.

Dit beleidskader is gericht aan:

- personen die een verantwoordelijkheid hebben in de plan- of ontwerpfase van processen, waaronder werkprocessen, projecten en programma's, proeftuinen, pilots, innovaties en andere verandertrajecten waarin persoons- of politiegegevens worden verwerkt. Dit beleidskader geldt ook wanneer deze plannen gewijzigd worden, bijvoorbeeld wanneer de noodzaak hiertoe blijkt in de uitvoeringsfase.
- personen die de autorisaties verzorgen conform het autorisatiemodel. Tot hun taak behoort het autoriseren van juiste personen voor de tool die de politie ondersteunt bij het uitvoeren van verantwoordingsplicht, zoals het register, de quick scan en de GEB.

- personen die zorgen voor de uitvoering van de control-functie: controllers en auditors. Zij kunnen mede op basis van een (automatische) selectie van gegevens uit het register inzicht krijgen in de stand van zaken met betrekking tot de vulling van het register met verwerkingen en het uitvoeren van GEB's.
- de veranderteams, waaronder de bouwers en beheerders van het verwerkingsregister.

De daadwerkelijke operationele uitvoering van werkprocessen, projecten, programma's, pilots, proeftuinen, innovaties en dergelijke moet in overstemming zijn met dit beleidskader. Voordat met de uitvoering mag worden gestart behoort deze eerst getoetst te worden aan dit beleidskader of aan processen/procedures/uitvoeringskaders die conform dit beleidskader zijn opgesteld.

**Eigenaar**

De Gegevensautoriteit (hierna: GA) is eigenaar van dit beleidsdocument. De GA ziet ook toe op de juiste uitvoering van dit beleid. De FG ziet toe op de rechtmatige uitvoering van de beschreven verwerkingen.

## 2. Verwerkingen, de GEB en het register

Dit hoofdstuk beschrijft de verplichtingen ten aanzien van verwerkingen, de GEB en het register.

### 2.1 Relevante wetgeving

De verplichting om verwerkingen te beschrijven in een register en op hoog risicoverwerkingen een GEB uit te voeren, volgt uit de AVG en de Wpg. De Wpg is van toepassing op de verwerkingen van politiegegevens door een bevoegde autoriteit. Hieronder vallen de verwerkingen in het kader van de politietaak, zoals genoemd in artikel 3 van de Politiewet 2012, uitgezonderd de korpschef-, vreemdelingen-, - en burgemeesterstaken. Deze laatst genoemde taken vallen onder het toepassingsbereik van de AVG. De AVG is van toepassing op alle verwerkingen van persoonsgegevens die niet vallen onder het toepassingsbereik van de Wpg.

De vuistregel binnen de politie is dat de AVG geldt voor de bedrijfsvoeringprocessen, korpscheftaken, vreemdelingenzaken en burgemeesterstaken, en een groot deel van de processen van de afdeling Veiligheid, Integriteit en Klachten, en de Wpg voor de operationele politietaak.

De AVG en Wpg sluiten elkaar uit: op een verwerking is óf de Wpg óf de AVG van toepassing.

### 2.2 Verwerkingen en verwerkingsverantwoordelijke

Deze paragraaf beschrijft wat een verwerking is en welke verplichtingen er gelden.

#### 2.2.1 Juridisch kader

Alles wat je doet met een persoons- en/of politiegegeven is een verwerking. Het juridisch kader luidt als volgt:

##### 2.2.1.1 Verwerken van persoonsgegevens

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”)<sup>1</sup>

Verwerken van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens<sup>2</sup>;

##### 2.2.1.2 Verwerken van politiegegevens

Politiegegevens: elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4 van de Politiewet 2012, met uitzondering van:

- de uitvoering van wettelijke voorschriften anders dan de Wet administratiefrechtelijke handhaving verkeersvoorschriften;
- de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, bedoeld in artikel 1, eerste lid, onderdeel i, onder 1° en artikel 4, eerste lid, onderdeel f, van de Politiewet 2012<sup>3</sup>;

Verwerken van politiegegevens: elke bewerking of elk geheel van bewerkingen met betrekking tot politiegegevens of een geheel van politiegegevens, al dan niet uitgevoerd op geautomatiseerde wijze, zoals het verzamelen, vastleggen,

---

<sup>1</sup> Artikel 4 sub 1 AVG

<sup>2</sup> Artikel 4 sub 2 AVG

<sup>3</sup> Artikel 1 sub a Wpg

ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen of vernietigen van politiegegevens<sup>4</sup>.

Een verwerking omvat dus alle handelingen met betrekking tot een persoons- en/of politiegegeven:

- geautomatiseerde vormen van deze handelingen vallen onder het begrip verwerking
- één verwerking kan bestaan uit een geheel van onderliggende verwerkingen
- een verwerking van persoons- en/of politiegegevens staat los van de applicatie waarin dit plaatsvindt
- een verwerking kan in één of meerdere systemen plaatsvinden
- één applicatie kan meerdere verwerkingen van gegevens betreffen
- een verwerking die volledig op papier of buiten de kernsystemen- of applicaties (ongestructureerde verwerkingen) wordt uitgevoerd kan onder de reikwijdte van de AVG of Wpg vallen.

Het begrip verwerking is wettelijk gezien ruim gedefinieerd, wat de verwerkingsverantwoordelijke enige speelruimte geeft bij de keuze voor een verwerking in zijn organisatie. Variërend van een zeer abstract niveau tot aan een gedetailleerd inzicht per verwerking. Het gekozen niveau moet aan de verwerkingsverantwoordelijke en de toezichthouders voldoende inzicht bieden in de eventuele risico's van de verwerking.

### 2.2.1.3 Verwerkingsverantwoordelijke

Alle verwerkingen vinden plaats onder de verantwoordelijkheid van een verwerkingsverantwoordelijke. Dat is degene die alleen of samen met anderen, doel en middelen voor de verwerking vaststelt<sup>5</sup>. De korpschef is verwerkingsverantwoordelijke voor de politie. Deze verantwoordelijkheid is via een mandatenstelsel gemandateerd aan de lijnorganisatie. Overal waar in dit stuk staat 'verwerkingsverantwoordelijke' wordt ook bedoeld de gemandateerde verwerkingsverantwoordelijke.

Wanneer partijen gezamenlijk doel en middelen van de AVG verwerking bepalen zijn zij gezamenlijk verantwoordelijk voor deze verwerking<sup>6</sup>. Bijvoorbeeld in een samenwerkingsverband als het RIEC. Deelnemende partijen hebben een gezamenlijke verwerkingsverantwoordelijkheid voor de verwerking waarvoor gezamenlijk doel en middelen zijn bepaald. Iedere partij is mede-verantwoordelijke. Partijen blijven wel zelfstandig verantwoordelijk voor hun 'eigen' verwerkingen, waaronder het verstrekken van informatie aan het samenwerkingsverband.

De Wpg kent geen gezamenlijke verwerkingsverantwoordelijkheid, maar wel een gemeenschappelijke verwerking. Wanneer uitsluitend Wpg partijen<sup>7</sup> gezamenlijk een Wpg verwerking uitvoeren wordt altijd één verwerkingsverantwoordelijke aangewezen<sup>8</sup>.

### 2.2.2 Keuze verwerking politie

Een bedrijfsfunctiemodel beschrijft de functies (ook wel: doelen) van een organisatie. De politie heeft een bedrijfsfunctiemodel voor de operationele processen en één voor de bedrijfsvoering. Functies worden gerealiseerd door werkprocessen. De relatie tussen functies en werkprocessen is als volgt: functies beschrijven 'wat de politie doet, en de werkprocessen hoe de politie dat doet. Werkprocessen en functies zijn aan elkaar gekoppeld. Een werkproces kan bijdragen aan de realisatie van meerdere functies. Een functie wordt gerealiseerd door meerdere werkprocessen. Het bedrijfsfunctiemodel en de werkprocessen zijn vastgesteld door de Korpsleiding t.b.v. de vorming van de nationale politie. De functies en werkprocessen zijn opgehaald uit de eenheden, het is een beschrijving op tactisch niveau wat alle politie-eenheden doen.

De werkprocessen die de functies in het bedrijfsfunctiemodel realiseren worden gelijkgesteld aan een verwerking in de zin van zowel de AVG als de Wpg<sup>9</sup>. Deze werkprocessen geven inzicht in de huidige verwerkingen van persoons- en politiegegevens. Het bedrijfsfunctiemodel politie omvat echter niet alle verwerkingen, want ook innovaties, een proeftuin of pilot, projecten, nieuwe applicaties, wijzigingen van een bestaande applicatie, een

---

<sup>4</sup> Artikel 1 sub c Wpg

<sup>5</sup> Artikel 4 sub 7 AVG en artikel 1 sub f onder 1 Wpg

<sup>6</sup> Artikel 26 lid 1 AVG

<sup>7</sup> Bevoegde autoriteit die gegevens verwerkt voor de strafrechtspleging: politie, Rijksrecherche en KMAR

<sup>8</sup> Artikel 1 sub f onder 4 Wpg: gemeenschappelijke verwerking

<sup>9</sup> Uiteraard voor zover hier persoons- of politiegegevens in voorkomen.

samenwerkingsverband, een nieuwe werkstroom, en nieuw werkprocessen zijn allemaal verwerkingen waarop de registerplicht en de GEB-verplichting van toepassing zijn.

#### Voorbeelden van verwerkingen

- het werkproces 'Aanhouden verdachte'
- de proeftuin 'ANPR Roermond'
- DNA eliminatie-database politiemedewerkers
- personeelsadministratie
- screening politiesollicitanten

Er bestaat altijd een relatie tussen de werkprocessen en overige verwerkingen, zoals projecten en pilots. Voor alle verwerkingen geldt dat zij één of meerdere relaties met elkaar kunnen hebben. Deze relaties kunnen hiërarchisch zijn, maar dit hoeft niet.

### 2.2.3 Eisen aan verwerkingen

Voor alle verwerkingen geldt dat zij moeten voldoen aan de eisen uit de AVG of de Wpg. Paragraaf 2.6 beschrijft de wat nodig is om specifiek te voldoen aan de wettelijke registerplicht en de verplichting een GEB uit te voeren op hoog risico verwerkingen<sup>10</sup>.

## 2.3 GEB

### 2.3.1 Juridisch kader

Wanneer een verwerking van persoon- of politiegegevens een hoog risico oplevert voor de rechten en vrijheden van personen, dan moet voorafgaand aan deze verwerking een beoordeling van het effect van de voorgenomen activiteiten op de bescherming van persoonsgegevens uitgevoerd worden<sup>11</sup>. Het doel van de GEB is om al bij het initiatief van een verwerking waarbij het risico mogelijk hoog is, te beoordelen welk effect de verwerkingsactiviteiten op de betrokkene(n) hebben en hoe de betreffende gegevens het beste kunnen worden beschermd. Aan de hand daarvan kunnen privacy en informatiebeveiligingsrisico's worden ingeschat en maatregelen worden genomen.

Een GEB moet in ieder geval de volgende elementen bevatten<sup>12</sup>:

- een algemene beschrijving van de beoogde verwerking of verwerkingen
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen
- de beoogde maatregelen ter beperking van de risico's
- de voorzorgs- en beveiligingsmaatregelen en mechanismen om de persoons- of politiegegevens te beschermen en aan te tonen dat aan het bij of krachtens deze wet bepaalde is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere betrokken personen beoordeling.

Bij het uitvoeren van een GEB op een AVG verwerking 'wint de verwerkingsverantwoordelijke het advies in van de FG'<sup>13</sup>. Deze adviserende taak van de FG is belegd bij de privacyfunctionarissen<sup>14</sup>.

Wanneer uit een GEB blijkt dat de verwerking een hoog risico oplevert als de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de toezichthoudende autoriteit<sup>15</sup>.

---

<sup>10</sup> Voor een volledig overzicht van alle eisen aan een verwerking i.v.m. privacywet- en regelgeving ontwikkelt de GA een checklist

<sup>11</sup> Artikel 35 lid 1 AVG en artikel 4c lid 1 Wpg

<sup>12</sup> Artikel 35 lid 7 AVG en artikel 4c lid 2 Wpg

<sup>13</sup> Artikel 35 lid 2 AVG

<sup>14</sup> Functionaris Gegevensbescherming (kwartiermaken), versie 1.0 definitief van 6 maart 2019

<sup>15</sup> Artikel 36 AVG en artikel 33b lid 1 sub b Wpg



Voor een GEB uitgevoerd op een Wpg verwerking is voorafgaande raadpleging van de AP<sup>16</sup> ook noodzakelijk wanneer de aard van de verwerking, in het bijzonder met gebruikmaking van nieuwe technologieën, mechanismen of procedures, een hoog risico voor de rechten en vrijheden van de betrokkene met zich meebrengt<sup>17</sup>.

### 2.3.2 GEB bij politie

De politie maakt gebruik van één centraal verwerkingen registratieproces, waarin twee soorten GEB's zijn opgenomen: één voor de Wpg verwerkingen en één voor AVG verwerkingen. Beide modellen zijn gebaseerd op het rijksmodel Privacy Impact Assessment, maar zijn toepasbaar gemaakt voor de specifieke politiesituatie.

Om na te gaan of er sprake is van een hoog risico voor de privacy is een quick scan ontwikkeld. Er is één quick scan die van toepassing is op zowel AVG als Wpg verwerkingen. Voor de start van een verwerking moet een quick scan worden uitgevoerd op de voorgenomen verwerking. Blijkt hieruit een hoog risico, dan is de volgende stap het uitvoeren van een GEB vóór de start van de voorgenomen verwerking.

Een GEB kan betrekking hebben op een individuele gegevensverwerking, maar kan ook zien op een reeks vergelijkbare verwerkingen die vergelijkbare risico's inhouden. Een GEB hoeft zich dus niet te beperken tot een enkel proces, product of verwerkingsverantwoordelijke, bijvoorbeeld wanneer de politie op meerdere plaatsen een vergelijkbare verwerking uitvoert of met andere instanties een gemeenschappelijke verwerking wil opzetten. Het in kaart brengen van de risico's door middel van een GEB is ook nodig wanneer er nieuwe applicaties of toepassingen worden ontwikkeld.

Het is aan de persoon die verantwoordelijk is voor de verwerking om ervoor te zorgen dat tijdig een quick scan en eventueel een GEB wordt uitgevoerd op de verwerking. Hij zorgt er ook voor dat de juiste expertise aanwezig is om een GEB te kunnen uitvoeren, waaronder deskundigheid op het gebied van privacy en informatiebeveiliging.

Een uitgevoerde GEB geeft inzicht in de risico's voor betrokkene en de informatiebeveiligingsrisico's voor de organisatie. Daar kan de verwerkingsverantwoordelijke op de volgende manieren mee omgaan:

1. aanvullende (informatiebeveiligings-)maatregelen nemen, bijvoorbeeld het anonimiseren of pseudonimiseren van de gegevens, deze maatregelen worden dan beschreven in een actieplan
2. de voorgenomen verwerking aanpassen zodat het risico omlaag gaat, bijvoorbeeld door minder of andere persoons- of politiegegevens te gebruiken
3. de voorgenomen verwerking kan geen doorgang vinden omdat de risico's te hoog zijn in relatie tot het doel van de verwerking, tenzij er een wettelijke uitzonderingsgrond van toepassing is die de verwerking alsnog toestaat.

In principe kan een voorgenomen verwerking niet van start gaan als er nog hoge risico's zijn. Dat betekent dat vóór de start van de verwerking de maatregelen uit het actieplan zijn uitgevoerd. Of de verwerking is zodanig aangepast dat alleen laag- risico's overblijven, waarvan duidelijk is dat deze op een acceptabele manier worden weggewerkt. Er zijn situaties waarin de voorgenomen verwerking toch moet plaatsvinden, ondanks de (hoge) risico's.

Alleen degene die op dat moment verantwoordelijk is voor de verwerking kan besluiten dat deze toch mag starten zonder dat aan alle eisen is voldaan. Voorafgaand aan dit besluit vindt overleg plaats met de FG, GA en de CISO. Welke lijnmanager of portefeuillehouder verantwoordelijk is voor de verwerking volgt uit het mandaatstelsel, zie ook para 5.3 Lijnmanagement.

Een verwerking waar nog een hoog risico van toepassing is moet worden aangemeld bij de AP, dit verloopt altijd via de FG<sup>18</sup>.

---

<sup>16</sup> De Gegevensautoriteit is de contactpersoon

<sup>17</sup> Artikel 33b lid 1 sub a Wpg.

<sup>18</sup> Functionaris Gegevensbescherming (kwartiermaken), versie 1.0 definitief van 6 maart 2019

## 2.4 Verwerkingsregister

### 2.4.1 Juridisch kader

Iedere verwerkingsverantwoordelijke is verplicht beschrijvingen van alle verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden in een register bij te houden<sup>19</sup>. De registerplicht dwingt organisaties inzichtelijk te maken hoe met persoonsgegevens en politiegegevens wordt omgaan en dit ook te kunnen verantwoorden.

Het register is ook bedoeld als toezichtinstrument voor zowel de interne toezichthouder, de FG, als de externe toezichthouder, de AP.

De AVG en de Wpg<sup>20</sup> schrijven voor welke informatie in het register beschreven moet worden:

- contactgegevens van de verwerkingsverantwoordelijke en indien van toepassing de gezamenlijke verwerkingsverantwoordelijken
- het doel van de verwerking
- de categorieën van betrokkenen, dat wil zeggen de personen op wie de gegevens betrekking hebben
- of het persoonsgegevens dan wel politiegegevens betreft
- hoe men aan de gegevens is gekomen; direct van de betrokkene, of anderszins
- aanwijzing van rechtsgrondslag van de verwerking waarvoor de persoons of politiegegevens bedoeld zijn, de verwerkingsgrondslag. Ook bij een eventuele doorgifte moet dit worden geregistreerd
- een algemene beschrijving van technische en organisatorische beveiligingsmaatregelen
- de beoogde termijnen voor verwijdering en vernietiging
- de categorieën van ontvangers aan wie gegevens worden verstrekt, of beschikbaar worden gesteld (zowel intern, als extern)
- toekenning van de juiste autorisaties
- of gebruik wordt gemaakt van (geautomatiseerde) profilering
- de doorgifte van persoonsgegevens (of politiegegevens aan een derde land of internationale organisatie buiten de EU.
- documenten waaruit blijkt dat het derde land passende waarborgen heeft getroffen omtrent de bescherming van de persoonsgegevens.

### 2.4.2 Verwerkingsregister bij politie

Er is één register van verwerkingen, waarin alle Wpg en AGV verwerkingen van de politie staan. Op termijn zal ook de Politieacademie<sup>21</sup> (hierna: PA) gebruik maken van de registertool. De verwerkingen van de PA worden door middel van autorisaties afgescheiden van de politieverwerkingen, want de PA is geen onderdeel van de politie en kent een eigen verwerkingsverantwoordelijke. Het register is de enige authentieke bron voor AVG en Wpg verwerkingen en zal dus moeten voldoen aan kwaliteitseisen<sup>22</sup>. Dat betekent dat wanneer de verwerkingsverantwoordelijke of een toezichthouder op zoek is naar een verwerking, zij daarvoor het register moeten raadplegen.

In het register wordt zoveel mogelijk gebruik gemaakt van referentiegegevens en informatie uit bronbestanden. Het register bevat geen bestanden of documenten maar verwijst hier zoveel mogelijk naar middels een dynamische link. Bijvoorbeeld naar een verwerkersovereenkomst bij de Dienst Verwerving of naar een convenant in het convenantenregister. Dergelijke dynamische verwijzingen kunnen alleen naar interne opslaglocaties binnen de politie verwijzen. Bestanden van externen moeten wél in het register te worden opgenomen.

Het register is een referentie- en toezichtinstrument voor zowel de eigen organisatie als de AP, en kan daarom niet in zijn geheel worden gerubriceerd of geheim worden verklaard. Specifieke onderdelen van het register kunnen wel degelijk vertrouwelijke informatie bevatten. Via autorisaties wordt de inzage op dergelijke vertrouwelijke informatie beperkt.

Van bepaalde verwerkingen is het mogelijk niet wenselijk dat zij in het register worden geregistreerd, omdat informatie hierover te zeer de opsporings- en vervolgingsbelangen van de politie zou schaden. Dit geldt bijvoorbeeld

---

<sup>19</sup> Artikel 30 AVG en Artikel 31d Wpg

<sup>20</sup> Artikel 30 lid 1 AVG en artikel 31d lid 1 Wpg

<sup>21</sup> De Politieacademie is een zelfstandig bestuursorgaan, een ZBO

<sup>22</sup> Dit volgt ook uit §5.7.2 van het Uitvoeringskader Privacy & Security by Design, versie 2.0

voor de verwerking van gegevens over informanten, ook wel 'artikel 12 Wpg –verwerking', of de verwerking van gegevens over medewerkers in de bijzondere bedrijfsvoering. De verwerkingsverantwoordelijke beslist hierover in overleg met de FG.

Vanwege het vertrouwelijke karakter van de informatiebeveiliging risicoanalyses binnen de politie worden deze niet centraal in het register opgenomen. Wel wordt aangegeven of een dergelijke analyse is uitgevoerd, wanneer, door wie en waar deze te vinden is. De te nemen privacy- en informatiebeveiligingsmaatregelen worden wel in het register opgenomen.

### **Verwerkingen in register**

De hierna volgende verwerkingen worden in het verwerkingsregister opgenomen, waarbij bij iedere verwerking de verwerkingsverantwoordelijke wordt aangegeven:

- verwerkingen waarvoor de korpschef de verwerkingsverantwoordelijke is
- verwerkingen waarvoor de korpschef de mede-verantwoordelijke is in geval van samenwerkingsverbanden. Bijvoorbeeld bij de gemeenschappelijke meldkamer, waar alle partijen gezamenlijk verantwoordelijk zijn. Het gaat dan vaak om een AVG-verwerking.
- verwerkingen die de politie uitvoert als verwerker, bijvoorbeeld de verwerkingen die de politie voor de Koninklijke Marechaussee (KMAR) en de Immigratie- en Naturalisatie Dienst (IND) uitvoert.
- de verwerkingen van de Politieacademie, die als ZBO, ten behoeve van het geven van opleidingen met betrekking tot de uitvoering van de politietaak formeel een zelfstandige verwerkingsverantwoordelijkheid heeft.

Verwerkingen van persoons- of politiegegevens waar de politie geen enkele verantwoordelijkheid heeft, worden niet in het register opgenomen. Zo worden verwerkingen van boa's die niet werkzaam zijn bij de politie, niet in het register opgenomen.

Door middel van autorisaties wordt de toegang tot de registertool geregeld. Autorisaties worden uitgegeven op basis van functionele noodzaak, conform het vastgestelde autorisatiebeleid. De registertool levert rapportages met betrekking tot de status van alle in het register opgenomen verwerkingen. Rapportages met managementinformatie verlopen via de reguliere rapportagelijnen. Daarbij wordt de cyclus van de 4-, 8- en 12-maandsrapportages gevolgd. De informatie uit het register kan ook worden gebruikt voor het uitvoeren van de control-functie.

## **2.5 Samenwerkingsverbanden**

Bij deelname aan een verwerking in samenwerkingsverbanden registreert de politie deze in het verwerkingsregister en voert een GEB uit. Daarbij noteert zij de rol ten aanzien van die specifieke verwerking: zelfstandig of mede verantwoordelijk. Voor de gegevens die de politie verstrekt ten behoeve van de gezamenlijke verwerking is de politie zelfstandig verwerkingsverantwoordelijke. Alleen ten aanzien van gezamenlijke verwerkingen<sup>23</sup> is de politie mede-verantwoordelijk.

Bij het uitvoeren van een GEB voor de eigen verwerking in het samenwerkingsverband kan de politie gebruik maken van een al uitgevoerde GEB. Bijvoorbeeld een GEB op een ketenverwerking of een nieuwe wet. Deze moet dan wel naar het oordeel van de politie voldoende inzicht bieden in de risico's voor de politie-verwerking. In de meeste gevallen zal de politie zelf een (aanvullende) GEB moeten uitvoeren.

## **2.6 Ondersteunende tool**

Ter ondersteuning van de uitvoering van de registerplicht en de GEB is een tool aangeschaft. In de tool kan een verwerking worden geregistreerd, en een quick scan en een GEB worden uitgevoerd.

De uitgangspunten voor het gebruik van deze tool zijn als volgt:

- het Politiedienstencentrum (hierna: PDC) zorgt voor het functioneel en technisch beheer van de tool
- de verwerkingsverantwoordelijken zorgen er zelf voor dat verwerkingen in de tool worden geregistreerd, en dat een GEB wordt uitgevoerd en in de tool wordt geregistreerd.
- uit doelmatigheidsoverwegingen worden sommige bedrijfsvoering processen nog geclusterd.

- het Verbeterprogramma Wpg en IB zorgt voor een initiële vulling van het register in de tool met de huidige Wpg verwerkingen, oftewel de werkprocessen uit het BRM politie.
- uit informatiebeveiligingsoverwegingen heeft het MT van het PDC besloten dat de tool in gebruik én beheer wordt genomen binnen het politiedomein. De applicatie wordt lokaal geïnstalleerd op servers van de politie. De applicatie mag niet worden afgenomen als zogenaamde Software as a service (Saas) oplossing, waarbij de applicatie in beheer blijft bij de leverancier en deze door de afnemers benaderbaar is via internet.
- vanuit de tool kunnen naast rapportages ten behoeve van de (status) van de verwerkingen en het toezicht, ook rapportages met management informatie worden gegenereerd. De verwerkingsverantwoordelijke kan deze informatie gebruiken om te sturen op onder andere compliance, voortgang, juistheid en volledigheid van de verwerking die onder zijn verantwoordelijkheid wordt uitgevoerd.
- de tool kan ook gebruikt worden voor het registreren en documenteren van documenten, zoals de toestemming indien een verwerking van persoonsgegevens hierop berust.

## 2.7 Eisen aan verwerkingen

De hiervoor beschreven verplichtingen en uitgangspunten leiden tot de volgende eisen aan een verwerking:

1. Er is sprake van een voornemen tot een nieuwe verwerking, óf een voornemen tot aanpassing van een bestaande verwerking.
2. De voorgenomen verwerking wordt geregistreerd in het register met behulp van de tool.
3. Op de voorgenomen verwerking wordt een quick scan uitgevoerd om een indicatie te krijgen van de risico's voor betrokkenen. Hierbij wordt gebruik gemaakt van de tool.
4. Een informatiebeveiliging specialist voert op de voorgenomen verwerking een informatiebeveiliging analyse uit. In het register wordt geregistreerd of en door wie een dergelijke analyse is uitgevoerd.
5. Wanneer uit de quick scan een hoog risico blijkt, wordt een GEB uitgevoerd en gedocumenteerd vóór de start van de verwerking met behulp van de tool.
6. Voer een GEB uit met een team van deskundigen van de betreffende verwerking, en deskundigen op het gebied van privacy en informatiebeveiliging. Vraag advies aan de PF.
7. Mitigeer de risico's die volgen uit de GEB, en stel daarvoor een actieplan op met per risico de mitigerende maatregelen. Neem dit plan op in de tool.
8. Raadpleeg de AP als blijkt dat alsnog een hoog risico overblijft. Dit moet vóór de start van de verwerking en verloopt altijd via de FG.
9. De FG en de GA hebben een rol in het toezicht op registratie van verwerkingen in het register en het uitvoeren van een GEB. De GA vanuit een systeemverantwoordelijkheid, de FG vanuit zijn verantwoordelijkheid als wettelijke toezichthouder en adviseur. Desgevraagd geeft de FG advies over de GEB.

Iedere voorgenomen verwerking moet voldoen aan bovenstaande vereisten. Wanneer dat niet het geval is mag de verwerking (het project, de proeftuin, de pilot, de innovatie) niet starten. Alleen de verwerkingsverantwoordelijke kan besluiten dat deze toch mag starten zonder dat aan alle eisen is voldaan. Voorafgaand aan dit besluit vindt overleg plaats met de FG, GA en de CISO.

## 3. Rollen en verantwoordelijkheden

De korpsbrede taken, rollen en verantwoordelijkheden met betrekking tot privacy in de politie organisatie worden beschreven in het privacy beleid. In dit hoofdstuk worden specifieke rollen, taken en verantwoordelijkheden in relatie tot het verwerkingsregister en de GEB verder uitgewerkt.

### 5.1 De korpschef

De korpschef is als verwerkingsverantwoordelijke eindverantwoordelijk voor het wetsconform gebruik van persoonsgegevens.

Via een stelsel van mandaten en ondermandaten is deze verantwoordelijkheid gemandateerd. Iedere verwerking heeft daardoor altijd een verwerkingsverantwoordelijke namens de korpschef.

### 5.2 Landelijke portefeuillehouders

De portefeuilles zijn gericht op planvorming en monitoring van de uitvoering. De landelijke portefeuillehouder is verantwoordelijk voor de beleidsvorming op zijn portefeuille, en voorbereiding van besluitvorming inclusief impactanalyse op de eenheden en het PDC. Hierbij zorgt de portefeuillehouder er voor dat het beleid voldoet aan de eisen uit dit beleidskader.

#### 5.2.1 Portefeuillehouder AVG

De portefeuillehouder AVG is verantwoordelijk voor de beleidsontwikkeling op het gebied van de AVG. Dat betreft verwerkingen inzake de bedrijfsvoering, vreemdelingenzaken en korpscheftaken. Hij ziet erop toe dat de voor de uitvoering verantwoordelijken (resp. directeur PDC, portefeuillehouder vreemdelingenzaken en portefeuillehouder korpscheftaken) zijn beleid implementeren met inachtneming van de verplichtingen uit dit beleidskader.

De portefeuillehouder is daarnaast eigenaar van de ondersteunende tool. Hij zorgt ervoor dat de organisatie gebruik kan maken van de tool voor het uitvoeren van de verplichtingen in dit beleidskader. Ook zorgt de portefeuillehouder voor technische en functionele ondersteuning bij het gebruik van de tool.

#### 5.2.2 Portefeuillehouder Wpg

De portefeuillehouder Wpg is verantwoordelijk voor de beleidsontwikkeling op het gebied van de Wpg. Dat zijn verwerkingen in het kader van de politietaak, zoals genoemd in artikel 3 van de Politiewet 2012, uitgezonderd de korpschef-, vreemdelingen-, - en burgemeesterstaken. Hij ziet erop toe dat de voor de uitvoering verantwoordelijken zijn beleid implementeren met inachtneming van de verplichtingen uit dit beleidskader.

### 5.3 Lijnmanagement

Het lijnmanagement is verantwoordelijk voor de implementatie en uitvoering van privacybeleid, waaronder dit beleidskader. Het lijnmanagement voor de operationele taakuitvoering bestaat uit de korpschef, eenheidschef, sectorhoofd (waaronder een districtschef) en teamchef (waaronder een basisteamchef). Voor de bedrijfsvoering zijn dit korpschef, directeur van het PDC, diensthoofd en afdelingshoofd. Het lijnmanagement besluit over de start van een verwerking, en is ervoor verantwoordelijk dat deze voldoet aan de verplichtingen uit dit beleidskader. Besluit het lijnmanagement te starten met een verwerking die niet voldoet, dan is daarover vóóraf overleg met de FG, GA en CISO.

### 5.4 FG

De FG houdt onafhankelijk toezicht op de toepassing en naleving van de verplichtingen in dit beleidskader. De FG rapporteert rechtstreeks aan de korpschef. Daarnaast heeft de FG een wettelijke adviesrol. De advisering aangaande de uitvoering van een GEB is door de FG belegd bij de privacyfunctionaris. Op grond van de Wpg heeft de privacyfunctionaris een zelfstandige adviseringsrol.

## **5.5 Team informatiebeveiliging**

Het team Informatiebeveiliging voert op verzoek van de verwerkingsverantwoordelijke een informatiebeveiligingsanalyse uit op voorgenomen verwerking en adviseert over te nemen beveiligingsmaatregelen.

## **5.6 Privacyfunctionarissen**

De privacyfunctionarissen adviseren over de verplichtingen in dit beleidskader. Naast advisering hebben privacyfunctionarissen ook een toezichhoudende taak. Dat is een wettelijk omschreven taak voor wat betreft Wpg verwerkingen. Voor AVG verwerkingen is deze taak ontleend aan de bevoegdheden van de FG, dat geldt ook t.a.v. het verwerkingsregister.

## **5.7 Gegevensautoriteit**

De GA is verantwoordelijk voor de ontwikkeling van privacybeleid. Vanuit een systeemverantwoordelijkheid monitort de GA de uitvoering van dit beleid.

## **5.8 Directie Operatiën**

De directie en het PDC zijn gezamenlijk verantwoordelijk voor het bedrijfsreferentiemodel. De bedrijfsarchitect van deze directie toetst periodiek of de in het register opgevoerde verwerkingen leiden tot een wijziging in de werkprocessen. De bedrijfsarchitect van de Staf PDC doet het zelfde met betrekking tot de verwerkingen ten behoeve van de bedrijfsvoering.

## **5.9 Directeur PDC**

De directeur van het PDC is verantwoordelijk voor de uitvoering van verwerkingen ten behoeve van de bedrijfsvoering. Een deel daarvan vindt plaats in de eenheden, maar altijd onder verantwoordelijkheid van het PDC.

## **5.10 De Centrale Ondernemingsraad**

Instemming of advies van de COR is nodig voor het uitvoeren van verwerkingen van persoonsgegevens op bepaalde onderwerpen. Welke dit zijn staat in artikel 27 van de Wet op de ondernemingsraden. Periodiek bespreekt de GA dergelijke verwerkingen met de COR commissie AVG.

## **5.11 AP**

De AP is de externe toezichthouder met de bijbehorende wettelijke toezicht bevoegdheden. Zo is de AP bevoegd tot inzage in het verwerkingsregister en kunnen zij documenten en informatie opvragen. De AP kan boetes en een last onder dwangsom opleggen. De AP moet voor de start van een verwerking worden geraadpleegd als daaraan risico's zijn verbonden die niet gemitigeerd kunnen worden.

# Bijlage 1

## Processen en werkstromen Bedrijfsvoering (AVG)

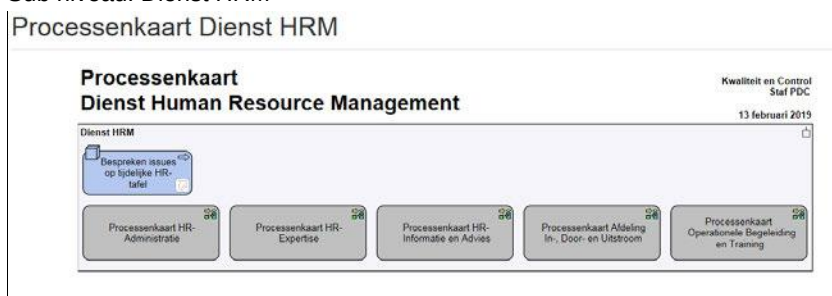
Hierin zijn beschreven de processenkaarten per dienst van het PDC, de integrale werkstromen én de werkstromen van de diensten. Op een processenkaart staan per organisatieonderdeel (afdeling, sector of team) de processen welke binnen dit organisatieonderdeel worden uitgevoerd. Van deze processen zijn een definitie, de beschrijving en de versie weergegeven.

Ten aanzien van de bedrijfsvoering is dit gelaagd ingericht:

Hoofdniveau (PDC)



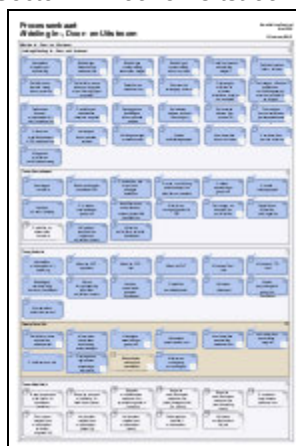
Sub niveau: Dienst HRM



Detail niveaus: Sector: HR-Administratie



Sector In- Door en Uitstroom (IDU)



Bron: Staf PDC, Kwaliteit en Control, 13 februari 2019

- Relevante artikelen uit de AVG en de gewijzigde Wpg
- Het BRM 2018, inclusief de werkprocessen en de toelichting



## Bijlage 2

### Referentiemodel Politiewerk 2018

