

AVG & Privacyverklaring

TrueScope Onderzoeksbureau

Ashok Bachoe
1-7-2026

Inhoudsopgave

1. Privacyverklaring	4
2. Verwerkingsregister	7
3. Datalekprotocol	8
4. AVG/PPO Werkprotocol	9
5. DPIA-template	11
6. Verwerkersoverzicht	12

1. Privacyverklaring

Privacyverklaring – TrueScope Onderzoeksbureau

1. Wie zijn wij

TrueScope Onderzoeksbureau verwerkt persoonsgegevens in het kader van feitenonderzoek, toedrachtonderzoek, schadeonderzoek, aansprakelijkheidsonderzoek, fraudeonderzoek, mediation en aanverwante dienstverlening.

Verantwoordelijke:

Naam : TrueScope Onderzoeksbureau
Adres : Roemer Visscherhof 40, 3341 GK Hendrik Ido Ambacht
KvK-nummer : 98965271
E-mail : info@truescope.nl
Telefoon : 06-57940031

2. Welke persoonsgegevens verwerken wij

Afhankelijk van de opdracht kunnen wij onder andere de volgende persoonsgegevens verwerken:

- Naam- en adresgegevens
- Contactgegevens
- Geboortedatum
- Polis- en schadedossiers
- Verklaringen van betrokkenen en getuigen
- Correspondentie
- Foto's en documentatie
- Financiële gegevens voor facturatie
- Onderzoeksbevindingen

Bijzondere persoonsgegevens worden uitsluitend verwerkt indien dit noodzakelijk en juridisch toegestaan is.

3. Waarom verwerken wij persoonsgegevens

Wij verwerken persoonsgegevens voor:

- Uitvoering van onderzoeksopdrachten
- Vaststelling van feiten en omstandigheden
- Schade- en aansprakelijkheidsbeoordeling
- Fraudeonderzoek
- Mediation en conflictbemiddeling
- Wettelijke verplichtingen
- Facturatie en administratie
- Beveiliging en kwaliteitsbewaking

4. Op basis van welke grondslag

Wij verwerken persoonsgegevens op basis van:

- Uitvoering van overeenkomst
- Wettelijke verplichting
- Gerechtvaardigd belang
- Toestemming (indien vereist)

Het gerechtvaardigd belang kan bestaan uit:

- fraudepreventie

- bescherming van financiële belangen
- waarheidsvinding
- juridische bewijsvoering
- risicobeheersing

5. Hoe lang bewaren wij gegevens

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor het doel waarvoor zij zijn verzameld, tenzij een wettelijke verplichting of lopende juridische procedure een langere bewaartermijn noodzakelijk maakt.

Indicatieve bewaartermijnen:

- Onderzoeksdossiers: maximaal 5 jaar na afronding
- Financiële administratie: 7 jaar
- Correspondentie: maximaal 5 jaar

6. Delen van persoonsgegevens

Persoonsgegevens kunnen uitsluitend worden gedeeld indien dit noodzakelijk is voor de uitvoering van de opdracht of op grond van wet- en regelgeving.

Denk hierbij aan:

- opdrachtgevers
- advocaten
- verzekeraars
- experts
- IT-dienstverleners
- toezichthouders

Met verwerkers worden waar nodig verwerkersovereenkomsten gesloten.

7. Beveiliging

TrueScope Onderzoeksbureau treft passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies, onbevoegde toegang of onrechtmatige verwerking.

Onder meer:

- versleutelde apparatuur
- sterke wachtwoorden
- multi-factor authenticatie
- beveiligde cloudopslag
- beperkte toegangsrechten

8. Rechten van betrokkenen

Betrokkenen hebben het recht om:

- persoonsgegevens in te zien
- gegevens te laten corrigeren
- gegevens te laten verwijderen
- bezwaar te maken
- verwerking te beperken
- gegevens over te dragen

Verzoeken kunnen worden gericht aan:

info@truescope.nl

Deze rechten kunnen worden beperkt indien wet- en regelgeving of een gerechtvaardigd onderzoeksbelang daaraan in de weg staan.

9. Klachten

Indien een betrokkene van mening is dat persoonsgegevens onjuist worden verwerkt, kan een klacht worden ingediend bij de:

Autoriteit Persoonsgegevens

<https://www.autoriteitpersoonsgegevens.nl>

10. Wijzigingen

TrueScope Onderzoeksbureau behoudt zich het recht voor deze privacyverklaring te wijzigen.

2. Verwerkingsregister

Verwerking	Doel	Grondslag	Categorie gegevens
Onderzoeksdossier	Uitvoering onderzoek	Gerechtvaardigd belang / overeenkomst	NAW, verklaringen, correspondentie, bewijsstukken
Facturatie	Financiële administratie	Wettelijke verplichting	Naam, adres, factuurgegevens
E-mailverkeer	Communicatie	Overeenkomst / gerechtvaardigd belang	Contactgegevens
Websitecontactformulier	Contactafhandeling	Toestemming / gerechtvaardigd belang	Naam, e-mail, telefoon
Mediation dossiers	Conflict-bemiddeling	Conflict-bemiddeling	Gespreksinformatie
Beelden/documentatie	Bewijsvoering	Gerechtvaardigd belang	Foto's/video's

3. Datalekprotocol

Datalekprotocol – TrueScope Onderzoeksbureau

1. Doel

Dit protocol beschrijft hoe wordt gehandeld bij een mogelijk datalek.

2. Wat is een datalek

Een datalek is een inbreuk op de beveiliging van persoonsgegevens.

Voorbeelden:

- verloren laptop
- verkeerd verzonden e-mail
- hack of malware
- onbevoegde toegang
- verlies van documenten

3. Interne melding

Een datalek wordt direct intern geregistreerd.

Minimaal vastleggen:

- datum
- aard van het incident
- betrokken gegevens
- mogelijke gevolgen
- genomen maatregelen

4. Beoordeling

Er wordt beoordeeld:

- welke persoonsgegevens betrokken zijn
- hoeveel personen geraakt zijn
- of risico bestaat voor betrokkenen
- of melding aan de Autoriteit Persoonsgegevens noodzakelijk is

5. Melding AP

Indien vereist wordt een datalek binnen 72 uur gemeld bij de Autoriteit Persoonsgegevens.

6. Melding betrokkenen

Indien het lek waarschijnlijk een hoog risico oplevert voor betrokkenen, worden betrokkenen geïnformeerd.

7. Evaluatie

Na ieder incident worden maatregelen genomen om herhaling te voorkomen.

4. AVG/PPO Werkprotocol

Werkprotocol – Privacy & Onderzoek - TrueScope Onderzoeksbureau

1. Uitgangspunten

TrueScope Onderzoeksbureau handelt conform:

- AVG
- proportionaliteit
- subsidiariteit
- doelbinding
- noodzakelijkheid
- zorgvuldigheid

2. Verzameling van gegevens

Persoonsgegevens worden uitsluitend verzameld indien noodzakelijk voor het onderzoek.

Er wordt gewerkt volgens het principe van minimale gegevensverwerking.

3. Observatie en onderzoek

Observatie of aanvullende onderzoekshandelingen worden uitsluitend ingezet indien:

- een legitiem onderzoeksdoel bestaat
- minder ingrijpende middelen onvoldoende zijn
- de maatregel proportioneel is

4. Dossiervorming

Onderzoeksdossiers bevatten:

- opdrachtschrijving
- onderzoeksdoel
- bevindingen
- gebruikte bronnen
- belangenafweging
- verslaglegging

5. Toegang tot dossiers

Toegang wordt beperkt tot personen die betrokken zijn bij de uitvoering van het onderzoek.

6. Beveiliging

Onderzoeksinformatie wordt beveiligd opgeslagen.

Minimaal:

- MFA
- apparaat versleuteling
- sterke wachtwoorden
- beperkte toegang
- beveiligde cloudopslag

7. Verstrekking aan derden

Gegevens worden uitsluitend gedeeld indien:

- noodzakelijk voor de opdracht
- wettelijk toegestaan

- passend binnen het onderzoeksdoel

8. Bewaartermijnen

Dossiers worden niet langer bewaard dan noodzakelijk.

9. Integriteit

Onderzoeksbevindingen worden feitelijk, objectief en controleerbaar vastgelegd.

5. DPIA-template

DPIA – Gegevensbeschermingseffect beoordeling - TrueScope Onderzoeksbureau

1. Omschrijving verwerking

- Wat is het doel van het onderzoek?
- Welke persoonsgegevens worden verwerkt?
- Welke betrokkenen zijn betrokken?

2. Noodzaak

- Waarom is deze verwerking noodzakelijk?
- Kan hetzelfde doel met minder ingrijpende middelen worden bereikt?

3. Proportionaliteit

- Staat de verwerking in verhouding tot het doel?
- Is de verwerking passend en verdedigbaar?

4. Subsidiariteit

- Zijn minder ingrijpende alternatieven overwogen?
- Waarom zijn deze onvoldoende?

5. Risicoanalyse

Mogelijke risico's:

- reputatieschade
- privacyschending
- datalekken
- onjuiste conclusies
- ongeautoriseerde toegang

6. Maatregelen

- MFA
- Encryptie
- Toegangsbeperking
- Logging
- Beveiligde opslag
- Dossiervalidatie

7. Eindafweging

Conclusie:

- verwerking toegestaan / niet toegestaan
- aanvullende maatregelen noodzakelijk ja/nee

6. Verwerkersoverzicht

Leverancier	Dienst	Verwerkersovereenkomst aanwezig	Locatie opslag
Microsoft 365	E-mail/cloud	Ja	EU
Apple iCloud	Apparaten/back-up	Ja	EU / VS
Boekhoudsoftware	Administratie	Ja	EU
Hostingprovider	Website/e-mail	Ja	EU
OneDrive	Bestandsopslag	Ja	EU

Aanvullende praktische aanbevelingen

Minimale beveiligingsbasis

Aanbevolen:

- FileVault inschakelen op MacBook
- MFA op alle accounts
- Passwordmanager gebruiken
- Geen privé en zakelijke dossiers mengen
- Regelmatige back-ups
- Apparaten automatisch vergrendelen
- Geen openbare USB-sticks gebruiken

Praktische waarschuwing

Vermijd in de opstartfase:

- onnodig verzamelen van persoonsgegevens
- WhatsApp als structureel dossierarchief
- onbeveiligde externe harde schijven
- verzending van gevoelige dossiers zonder beveiliging
- observaties zonder duidelijke belangenafweging

Slotopmerking

Deze basisset vormt een praktische AVG-basis voor een startend onderzoeksbureau. Afhankelijk van de aard van opdrachten kunnen aanvullende verplichtingen of sectorspecifieke eisen gelden.