

Privacyverklaring

Definities

In deze privacyverklaring wordt verstaan onder:

- **AVG:** Algemene Verordening Gegevensbescherming (EU) 2016/679;
- **Betrokkene:** natuurlijke persoon op wie persoonsgegevens betrekking hebben;
- **Verwerker:** partij die ten behoeve van een verwerkingsverantwoordelijke persoonsgegevens verwerkt;
- **Verwerkingsverantwoordelijke:** partij die het doel van en de middelen voor verwerking vaststelt;
- **Verwerkersovereenkomst:** overeenkomst ex artikel 28 AVG;
- **DPIA:** Data Protection Impact Assessment (gegevensbeschermingseffectbeoordeling).

Verwerkingsverantwoordelijke en verwerker

Deze verklaring is van toepassing op verwerkingen door:

- *Beleidsrendement B.V.;*
- *AEPB Onderzoek en Advies B.V.;*
- *AEPB Data en Info B.V.;*
- *Bank Check B.V..*

Vestigingsadres: Kribbestraat 42-II, 1079 WT Amsterdam.

Rollen

AEPB treedt op als:

- *Verwerker*, bij onderzoek, (data)analyses en ontwikkelen en aanbieden van informatieproducten in opdracht van bijvoorbeeld overheden, woningcorporaties, zorginstellingen, samenwerkingsverbanden en andere maatschappelijke organisaties;
- *Verwerkingsverantwoordelijke*, bij de verwerking van gegevens van eigen medewerkers, sollicitanten, leveranciers, zakelijke relaties en websitebezoekers.

Verwerkingen als verwerkingsverantwoordelijke

Categorieën, doeleinden en grondslagen

Nr.	Categorie	Gegevens	Doel	Grondslag	Bewaartermijn
1.	Medewerkers	NAW, BSN, salaris, functioneren	HR-administratie	Uitvoering overeenkomst, wettelijke plicht	7 jaar (fiscaal), 2 jaar (overig)
2.	Sollicitanten	NAW, CV, motivatie	Werving en selectie	Toestemming, gerechtvaardigd belang	4 weken na afronding procedure / 1 jaar met toestemming
3.	Leveranciers en relaties	Contact- en betaalgegevens	Inkoop, contractbeheer	Uitvoering overeenkomst	7 jaar na einde relatie
4.	Opdrachtgevers	Organisatie, contactpersonen, projectgegevens	Offertes, projectuitvoering	Uitvoering overeenkomst	Bewaard zolang nodig; daarna zo mogelijk ge(pseudo-)anonimiseerd. Bij blijvende bewaring gelden de waarborgen van art. 89 AVG.
5.	Websitebezoekers	IP-adres, cookies	Websiteoptimalisatie	Gerechtvaardigd belang	Sessie / max. 13 maanden

Ontvangers

- Belastingdienst, UWV (wettelijk);
- Accountant (wettelijk);
- IT-dienstverleners (verwerkers).

Er vindt geen doorgifte buiten de EER plaats, tenzij dit noodzakelijk is voor de uitvoering van onze dienstverlening. In dat geval worden passende waarborgen toegepast, zoals de door de Europese Commissie goedgekeurde standaardcontractbepalingen (SCC's).

Data Protection Impact Assessment (DPIA)

AEPB voert een DPIA uit wanneer een verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen, in het bijzonder bij:

- Systematische en uitgebreide beoordeling van persoonlijke aspecten, waaronder profilering;
- Grootchalige verwerking van bijzondere categorieën persoonsgegevens;
- Stelselmatige monitoring van openbaar toegankelijke ruimten.

Wij treffen passende technische en organisatorische maatregelen om geïdentificeerde risico's te mitigeren. Indien deze maatregelen de risico's onvoldoende kunnen beperken, raadplegen wij conform artikel 36 AVG de Autoriteit Persoonsgegevens voordat wij met de verwerking starten.

Verwerkingen als verwerker

Algemene bepalingen

Bij verwerking namens opdrachtgevers geldt dat AEPB uitsluitend handelt conform de verwerkersovereenkomst en instructies van de opdrachtgever. Medewerkers zijn gebonden aan geheimhouding. Subverwerkers worden alleen ingezet na toestemming van de opdrachtgever en ontvangen uitsluitend gepseudonimiseerde gegevens waar dat kan. Doelbinding geldt: gegevens worden nooit gebruikt voor andere doeleinden.

Specifieke verwerkingen

- **Onderzoeksdata** — beleidsonderzoek, evaluaties en data-analyses in de publieke sector.
- **Bijzondere persoonsgegevens** — gezondheidsgegevens, jeugdzorggegevens, justitiële gegevens en andere bijzondere categorieën worden alleen verwerkt indien één van de uitzonderingen van artikel 9 lid 2 AVG van toepassing is, zoals: uitdrukkelijke toestemming, arbeidsrechtelijke of sociale zekerheidsverplichtingen, bescherming vitale belangen, zwaarwegend algemeen belang, medische doeleinden, archivering/wetenschappelijk onderzoek met waarborgen, of openbaar gemaakte gegevens.
- **Bankgegevens (PSD2 en aangeleverde transacties)** — bij PSD2-koppelingen geeft de gebruiker toestemming aan de bank om transactiegegevens met AEPB te delen; deze toestemming wordt door ons direct na het ophalen ingetrokken. Bij handmatig aangeleverde bestanden uploadt de gebruiker zelf de gegevens. In beide gevallen is de verwerkingsgrondslag de uitvoering van de overeenkomst met de opdrachtgever. Gegevens worden uitsluitend gebruikt voor het uitvoeren van de overeenkomst en waar mogelijk gepseudonimiseerd.
- **Silent Party Data** — bij verschillende databronnen kunnen gegevens van derden voorkomen zonder dat deze hiervan op de hoogte zijn. Voorbeelden zijn: banktransacties (betaler/begunstigde), e-mailcorrespondentie (afzenders/ontvangers), sociale media posts (genoemde personen), enquêteantwoorden (waarin respondenten anderen noemen) of administratieve systemen (contactpersonen, relaties). Deze silent party data wordt verwerkt op grond van artikel 6 lid 1 sub f AVG (gerechtvaardigd belang) en uitsluitend voor de overeengekomen dienstverlening.

Maatregelen

- **Privacy by Design en by Default** — standaard pseudonisering en minimale gegevensverwerking;
- **Dataminimalisatie** — alleen noodzakelijke gegevens voor het specifieke doel;
- **Opslagbeperking** — verwijdering na projecteinde of overeengekomen bewaartermijn;
- **Integriteit en vertrouwelijkheid** — geen heridentificatie, beveiligde opslag en verwerking;
- **Transparantie** — duidelijke afspraken in verwerkersovereenkomst over bovenstaande maatregelen.

Beveiliging

Technische en organisatorische maatregelen: encryptie, multi-factor authenticatie, firewalls, security-updates, toegangscontrole, geheimhoudingsverklaringen, awareness-training, clean desk/clear screen en procedures voor incidenten.

Datalekken en incidenten

Bij een beveiligingsincident waarbij persoonsgegevens betrokken zijn, hanteert AEPB de volgende procedure:

- Interne melding: direct, uiterlijk binnen 12 uur na ontdekking;

- Beoordeling: vaststelling aard, omvang en risico voor betrokkenen;
- Melding Autoriteit Persoonsgegevens: binnen 72 uur indien het incident leidt tot een risico voor rechten en vrijheden van betrokkenen;
- Informeren betrokkenen: onverwijld bij hoog risico voor hun rechten en vrijheden;
- Documentatie: alle incidenten worden geregistreerd in ons incidentenregister;
- Evaluatie: na afhandeling analyseren wij het incident om herhaling te voorkomen.

Als verwerker melden wij incidenten onmiddellijk aan de verwerkingsverantwoordelijke.

Profilering en automatische besluitvorming

AEPB gebruikt algoritmes en analysemethoden om gegevens te verwerken tot indicatoren of patronen. Dit valt onder *profilering* (art. 4 lid 4 AVG). De resultaten dienen uitsluitend als ondersteuning bij onderzoek en beleidsadvies en worden altijd door mensen geïnterpreteerd.

AEPB neemt geen besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking zoals bedoeld in art. 22 AVG. Er is altijd menselijke tussenkomst en opdrachtgevers beslissen zelf over vervolgstappen.

Verwerking gegevens minderjarigen

AEPB verwerkt in beginsel geen persoonsgegevens van personen jonger dan 16 jaar, tenzij:

- Wij optreden als verwerker en de verwerkingsverantwoordelijke de rechtmatigheid heeft vastgesteld;
- De verwerking noodzakelijk is voor wetenschappelijk onderzoek met passende waarborgen;
- Het gaat om geaggregeerde data waarbij individuele minderjarigen niet identificeerbaar zijn.

Bij onderzoek waarbij gegevens van minderjarigen worden verwerkt:

- Worden extra beveiligingsmaatregelen toegepast;
- Vindt standaard pseudonimisering plaats;
- Worden geen individuele rapportages opgesteld;
- Geldt een striktere toegangscontrole.

Rechten van betrokkenen

Betrokkenen hebben recht op inzage, rectificatie, vergetelheid, beperking, dataportabiliteit, bezwaar en het recht om niet te worden onderworpen aan geautomatiseerde besluitvorming (art. 15-22 AVG).

Uitoefening rechten:

- Als AEPB verwerkingsverantwoordelijke is: verzoek via security@aepb.nl, met reactie binnen 4 weken.
- Als AEPB verwerker is: verzoek via de opdrachtgever; AEPB ondersteunt de afhandeling.

Klachten kunnen worden ingediend bij de Autoriteit Persoonsgegevens.

Contact

Voor algemene vragen of verzoeken over dit statement of ons privacybeleid kunt u contact opnemen via:

- E-mail: security@aepb.nl
- Postadres: Kribbestraat 42 2, 1079 WT Amsterdam

Voor rechtstreeks contact met onze Functionaris Gegevensbescherming kunt u mailen naar: fg@aepb.nl

Een toegankelijke, beknopte versie van deze verklaring is beschikbaar via onze website. Deze formele verklaring is leidend bij eventuele verschillen.