Privacybeleid
Van Tilburg - Bastianen Groep

Inhoudsopgave

1 JURIDISCH EN STRATEGISCH KADER

1.1 Juridisch

Per 25 mei 2018 is in alle EU lidstaten de AVG (Algemene Verordening Gegevensbescherming) in werking getreden. Deze heeft tot doel de privacy van EU-ingezetenen te beschermen en de vrije uitwisseling van persoonsgegevens binnen de EU te borgen.

In dit beleid is onder meer uiteengezet hoe de verplichtingen uit hoofde van de AVG binnen de organisatie van Van Tilburg - Bastianen Groep (en alle onderliggende juridische entiteiten, hierna TB) worden toegepast en op welke manier wordt toegezien op een correcte naleving.

1.2 Strategisch

TB committeert zich altijd aan het zorgvuldig verwerken van persoonsgegevens. Dit betekent dat wij bescherming van de privacy van onze klanten, medewerkers en andere relaties serieus nemen. Wij verwachten van onze medewerkers en externe samenwerkingspartners dat zij zich bewust zijn van de vertrouwelijkheid van persoonsgegevens en hier zorgvuldig mee omgaan.

Bij het omgaan met persoonsgegevens zijn de volgende principes leidend:

1. Bewaar gegevens veilig;
2. Deel informatie bewust;
3. Respecteer ieders privacy;
4. Meld elk (mogelijk) datalek direct;
5. Zorg dat relaties van hun rechten gebruik kunnen maken.

2 DEFINITIES, ROLLEN EN VERANTWOORDELIJKHEDEN

2.1 Definities

- AP: De Nederlandse Autoriteit Persoonsgegevens.
- Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.
- Bijzondere persoonsgegevens: Persoonsgegevens betreffende iemands godsdienstovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke Persoonsgegevens en Persoonsgegevens over onrechtmatig dan wel hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- Datalek: een beveiligingsincident waarbij Persoonsgegevens verloren zijn gegaan, dan wel onrechtmatige verwerking redelijkerwijs niet is uit te sluiten.
- Leidende toezichthouder: De Nederlandse Autoriteit Persoonsgegevens die door TB is aangemerkt als leidende toezichthouder in het geval van overleg over datalekken binnen of buiten Nederland.
- Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

- Subverwerker: de door de Verwerker aangewezen partij die in opdracht van de Verwerker Persoonsgegevens verwerkt.

- Toezichthoudende Autoriteit: de AP, dan wel een andere toezichthoudende autoriteit van een EU-lidstaat die belast is met toezicht uit hoofde van de AVG.

- Verwerking van Persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder verzamelen, vastleggen, ordenen, bewaren, wijzigen, raadplegen, gebruiken, verstrekken en vernietigen.

- Verwerker: degene die ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt, zonder aan het gezag van de Verwerkingsverantwoordelijke te zijn onderworpen. De Verwerkingsverantwoordelijke is degene die de middelen voor de verwerking bepaalt.

- Verwerkingsverantwoordelijke: In ons geval TB

2.2 Rollen en verantwoordelijkheden

2.2.1 Directieverantwoordelijke Gegevensbescherming

Gegevensbescherming heeft bij TB nadrukkelijk de aandacht en is ingebed in de structuur van de organisatie. De eindverantwoordelijkheid voor de bescherming van persoonsgegevens ligt bij de CFO of in diens afwezigheid bij een door hem aangemerkte vervanger op directieniveau.

Taken

I. De CFO zorgt er voor dat de onderneming stuurt op adequate gegevensbescherming. Dit houdt in dat hij toeziet op het beheer, de periodieke toetsing en verantwoording op het gebied van gegevensbescherming.

II. Hij besluit of een (mogelijk) beveiligingsincident binnen de internationale onderneming moet worden gemeld bij de Nederlandse Privacy Autoriteit (AP). Hij is dan ook de woordvoerder.

III. De directieverantwoordelijke wordt altijd geïnformeerd wanneer betrokkenen hun rechten willen uitoefenen.

2.2.2 Privacy coördinator

Voor de totale onderneming en belanghebbenden buiten de organisatie wijst TB een privacy coördinator aan. Dit is een medewerker die privacy krijgt toegevoegd aan het bestaande takenpakket. De privacy coördinator is betrokken bij de dagelijkse (operationeel-/tactische) aspecten van privacy management bij TB. De privacy coördinator rapporteert aan de directieverantwoordelijke Gegevensbescherming.

Taken

I. De privacy coördinator is de contactpersoon indien betrokkenen een beroep doen op hun privacy rechten. Hij ziet toe op het adequaat inwilligen van deze rechten binnen de gestelde 'redelijke' termijn van vier weken (maximaal te verlengen met een extra periode van vier weken). De privacy coördinator doet dit eventueel na toestemming van de directieverantwoordelijke.

II. Ook zorgt de privacy coördinator bij een mogelijk beveiligingsincident dat de afgesproken procedure voor (mogelijke) datalekken wordt gevolgd. De privacy coördinator doet samen met, en eventueel als onderdeel van een team, onderzoek naar het incident om zo te achterhalen wat er exact is gebeurd en om de directieverantwoordelijke goed te kunnen informeren.

III. De privacy coördinator draagt zorg voor meldingen aan de Autoriteit Persoonsgegevens. Hij doet dit alleen na overleg met het privacy team en na toestemming van de directieverantwoordelijke Gegevensbescherming.

IV. De privacy coördinator is samen met het privacy team belast met het operationele beheer van het privacy managementsysteem van TB. Dit houdt in dat de administratieve organisatie waar onder andere dit beleid, de privacy verklaringen, verwerkersovereenkomsten, de procedure meldplicht datalekken en het verwerkingsregister onder valt, conform beheerafspraken op orde wordt gehouden. De privacy coördinator is de persoon die de operationele controles (laat) uitvoeren en die de rapportages opstelt op basis waarvan de onderneming kan aantonen *in control* te zijn op het gebied van gegevensbescherming.

V. De Privacy coördinator toetst periodiek of TB conform de beginselen gegevens verwerkt en brengt desgewenst verslag uit aan de directie. Tevens vraagt de Privacy coördinator aan de hand van de bevindingen aandacht bij de directie en medewerkers (indien relevant) voor de juiste toepassing van bovengenoemde beginselen.

2.2.3 Medewerkers

Alle medewerkers van TB zijn verplicht om op een zorgvuldige wijze en conform de beleidsregels en principes van TB én de verplichtingen uit de AVG met persoonsgegevens om te gaan.

Taken

I. De medewerkers zijn binnen het eigen taakgebied verantwoordelijk voor het naleven van deze principes.

II. Medewerkers herkennen en melden mogelijke incidenten die kunnen leiden tot een datalek.

III. Het bewust nalaten incidenten te melden is een reden voor (mogelijke) sancties.

2.2.4 De externe toezichthouder Autoriteit Persoonsgegevens

TB, alsmede de door haar ingeschakelde Verwerkers, zullen altijd de medewerking verlenen aan de AP, dan wel elke andere toezichthouder en binnen redelijke en gestelde termijnen ingaan op informatieverzoeken.

3 VERWERKING VAN PERSOONSGEGEVENS

3.1 Het begrip Persoonsgegeven

Bij TB worden alle gegevens die direct dan wel indirect herleidbaar zijn naar een natuurlijk persoon aangemerkt als Persoonsgegeven. Gegevens betreffende personenvennootschappen vallen onder het begrip natuurlijk persoon. Een rechtspersoon zelf valt niet binnen het begrip[1]. Indien de UBO (Ultimate Beneficial Owner), dan wel vertegenwoordiger van de rechtspersoon, een natuurlijk persoon is, valt deze onder het begrip. Alleen levende personen vallen onder het begrip.

De privacy coördinator draagt er zorg voor dat iedereen binnen TB voldoende bekend is met het begrip Persoonsgegeven.

3.2 Het begrip Verwerken

Persoonsgegevens worden binnen TB op diverse manieren op papier en digitaal verwerkt. In het verwerkingsregister staan de applicaties die voor de opslag en verwerking van Persoonsgegevens worden gebruikt.

3.3 Beginselen bij de verwerking van Persoonsgegevens

Binnen TB moeten Persoonsgegevens worden verwerkt volgens de in de AVG genoemde beginselen. Binnen de AVG worden de volgende beginselen beschreven[2]:

I. Persoonsgegevens worden door TB verwerkt op een manier die ten opzichte van de Betrokkene rechtmatig, behoorlijk en transparant zijn (rechtmatigheid, behoorlijkheid en transparantie);

II. Persoonsgegevens worden door TB voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare manier worden verwerkt (doelbinding);

III. Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (minimale gegevensverwerking);

IV. Persoonsgegevens zijn juist en worden door TB indien nodig geactualiseerd; alle redelijke maatregelen moeten worden genomen om de Persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen dan wel te rectificeren (juistheid);

V. Persoonsgegevens worden door TB bewaard in een vorm die het mogelijk maakt Betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen door TB voor langere periode worden opgeslagen (opslagbeperking);

[1] Een rechtspersoon wordt geacht vertrouwelijkheid te bedingen in een zogenaamde non-disclosure agreement dan wel een beding in de overeenkomst.

[2] Artikel 5 AVG.

VI. Persoonsgegevens worden door TB door het nemen van passende technische dan wel organisatorische maatregelen op een dusdanige manier verwerkt dat een passende beveiliging ervan geborgd is en dat de Persoonsgegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging dan wel beschadiging (integriteit en vertrouwelijkheid).

TB zorgt er voor dat deze beginselen worden nageleefd en is hier ook verantwoordelijk voor. Tevens dient TB aan te kunnen tonen dat deze beginselen worden nageleefd.

3.4 Rechtmatigheid van de verwerking

Het is binnen TB niet toegestaan om Persoonsgegevens te verwerken indien er geen grondslag voor verwerking aanwezig is. Binnen TB kunnen de volgende grondslagen voor verwerking van Persoonsgegevens worden toegepast:

I. Uitvoering van een overeenkomst: de verwerking van Persoonsgegevens is noodzakelijk om uitvoering te geven aan een overeenkomst waarbij Betrokkene partij is, dan wel wordt (pre-contractuele fase);

II. Voldoen aan wettelijke verplichting: de verwerking van Persoonsgegevens is noodzakelijk om aan een wettelijke verplichting te kunnen voldoen;

III. Gerechtvaardigd belang: de verwerking van Persoonsgegevens is noodzakelijk in geval van een voor TB zwaarwegend gerechtvaardigd belang, waarbij geldt dat het belang van TB zwaarder weegt dan het belang van de betrokkene;

IV. Toestemming: Betrokkene verleent toestemming voor het verwerken van Persoonsgegevens;

V. Vitaal belang.

3.4.1 Gerechtvaardigd belang:

De directie van TB is -eventueel op advies van de privacy coördinator- bevoegd om verwerkingen toe te staan op grond van gerechtvaardigd belang. Verwerkingen op deze grondslag worden nimmer toegestaan indien de belangen, de grondrechten dan wel de fundamentele vrijheden van de Betrokkene zwaarder wegen dan het belang van TB. Indien de Betrokkene nog minderjarig is zal TB deze grondslag niet gebruiken.

3.4.2 Toestemming:

De directie van TB is op advies van de privacy coördinator bevoegd om verwerkingen toe te staan op grond van toestemming van de klant. Indien de directie hiertoe besluit wordt erop toegezien dat aan de volgende eisen wordt voldaan:

I. Er kan worden aangetoond dat de Betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens op basis van deze grondslag;

II. Indien schriftelijk om toestemming wordt gevraagd in een verklaring die ook betrekking heeft op andere zaken dan wordt in eenvoudige taal duidelijk gemaakt waar de toestemming betrekking op heeft;

III. Een eenmaal gegeven toestemming kan worden ingetrokken. Een Betrokkene wordt hiervan voor het geven van de toestemming op de hoogte gebracht. Daarnaast is het intrekken van de toestemming net zo gemakkelijk als het geven ervan. Een ingetrokken toestemming heeft geen terugwerkende kracht;

IV. Een Betrokkene die de leeftijd van 16 jaar nog niet heeft bereikt is niet in staat om toestemming te verlenen. De toestemming dient te worden gegeven door de personen die de ouderlijke verantwoordelijkheden dragen. In een dergelijke geval wordt door TB, indien redelijkerwijze mogelijk, gecontroleerd of de persoon die het ouderlijk gezag uitoefent ook toestemming heeft gegeven.

3.5 Bijzondere Persoonsgegevens

Het is ons beleid geen bijzondere Persoonsgegevens te verwerken.

4 RECHTEN VAN BETROKKENEN

4.1 Rechten

Iedere Betrokkene heeft recht op:

1) inzage (artikel 15 AVG);
2) rectificatie (artikel16 AVG);
3) verwijdering (vergetelheid) (artikel 17 AVG);
4) beperking van de verwerking (artikel 18 AVG);
5) dataportabiliteit (artikel 20 AVG);
6) recht van bezwaar (artikel 21 AVG).

Indien de Betrokkene aangeeft één van de hierboven genoemde rechten te willen uitoefenen zal de privacy coördinator hier binnen de door de AVG gestelde voorwaarden en termijnen gevolg aan geven.

4.2 Betrokkenen informeren over hun rechten

De hierboven genoemde rechten worden door TB aan iedere Betrokkene schriftelijk via het Privacy statement voor kandidaten, medewerkers, leveranciers en klanten kenbaar gemaakt. Indien TB Persoonsgegevens van andere derde partijen ontvangt zal TB aan aanvullende informatieverplichtingen voldoen.

De tekst van dit statement is helder en begrijpelijk. Als alternatief verstrekt TB de informatie mondeling indien de Betrokkene hierom heeft verzocht en indien de identiteit van de Betrokkene is bewezen.

4.3 Ons privacy statement

Op de website van TB staat een actueel privacy statement, waarin TB aan al haar informatieverplichtingen uit hoofde van de AVG jegens de betrokkenen voldoet.

In het privacy statement wordt in ieder geval de volgende informatie opgenomen:

I. de entiteit en contactgegevens van TB;

II. (eventueel) de contactgegevens van de Privacy coördinator;

III. de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd en ook de rechtsgrond voor de verwerking;

IV. indien directie heeft besloten om gebruik te maken van de grond gerechtvaardigd belang, wordt aangegeven om welke gerechtvaardigde belangen het gaat;

V. de ontvangers of categorieën van ontvangers van de persoonsgegevens;

VI. de duur van de periode waarvoor de Persoonsgegevens zullen worden opgeslagen en, indien het voorgaande onmogelijk is, de criteria ter bepaling van die termijn;

VII. dat Betrokkene het recht heeft op:
1) inzage;
2) rectificatie;
3) verwijdering;
4) overdracht;
5) beperking van de verwerking;
6) het indienen van bezwaar tegen de verwerking;

VIII. de mogelijkheid tot het indienen van een klacht bij een AP;

IX. of de grondslag voor verstrekking van de Persoonsgegevens door de Betrokkene de nakoming van een overeenkomst betreft, dan wel wettelijke verplichting, of Betrokkene verplicht is deze gegevens te verstrekken en wat er gebeurt op het moment dat Betrokkene weigert de gegevens te verstrekken (art. 13 lid 2 sub e);

X. indien TB de verkregen Persoonsgegevens zal verwerken voor een andere doel dan waarvoor de Persoonsgegevens zijn verkregen, wordt voor verdere verwerking de Betrokkene geïnformeerd over het andere doel en wordt alle andere relevante informatie met betrekking tot die verwerking gedeeld.

Het Privacy statement wordt periodiek geëvalueerd en waar nodig geactualiseerd.

4.4 Verzoeken voor uitoefening van rechten

Een verzoek tot uitoefening van de hierboven genoemde rechten wordt altijd door TB uitgevoerd, tenzij TB onder bewijslast niet in staat is om de Betrokkene te identificeren. Indien getwijfeld wordt aan de identiteit van Betrokkene zal TB om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van Betrokkene.

Een verzoek dient binnen vier weken na ontvangst te zijn uitgevoerd door het privacy team. Indien TB, gezien de complexiteit dan wel de veelvoud van het verzoek, niet in staat is om deze binnen de reeds genoemde termijn uit te voeren, kan deze termijn door de directie met acht weken worden verlengd. De Betrokkene wordt binnen vier weken na ontvangst van het verzoek hiervan in kennis gesteld.

Een verzoek tot informatie dat via elektronische weg is ontvangen mag via dezelfde weg worden beantwoord, tenzij de Betrokkene heeft verzocht om een afschrift in hard copy.

Indien de directie van TB, eventueel op advies van de privacy coördinator, heeft besloten om geen gevolg te geven aan het verzoek van Betrokkene, wordt dit binnen vier weken na ontvangst van het verzoek aan Betrokkene gemotiveerd medegedeeld. Tevens wordt Betrokkene geïnformeerd over de mogelijkheid om een klacht bij de Autoriteit Persoonsgegevens in te dienen, dan wel een geschil aanhangig te maken bij de rechter.

Het uitoefenen van de rechten van Betrokkene wordt kosteloos mogelijk gemaakt, tenzij de directie - onder bewijslast- bepaalt:

I. dat vanwege het repetitieve karakter, dan wel de buitensporigheid van het verzoek, redelijk gemaakte kosten in rekening mogen worden gebracht; of

II. het verzoek dient te worden afgewezen aangezien het verzoek van Betrokkene ongegrond zou zijn.

4.4.1 Verzoek tot inzage

Betrokkene heeft het recht om uitsluitsel te krijgen over de vraag of zijn Persoonsgegevens worden verwerkt en indien dit het geval is, inzage te krijgen in de verwerkte Persoonsgegevens en:

I. de verwerkingsdoeleinden;

II. de betrokken categorieën van Persoonsgegevens;

III. de ontvangers of categorieën van Persoonsgegevens;

IV. de bewaartermijn, dan wel de criteria ter bepaling van de bewaartermijn;

V. recht van Betrokkene om Persoonsgegevens te wissen, de verwerking te beperken, dan wel bezwaar te maken tegen de verwerking;

VI. dat de Betrokkene het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

TB geeft bij inzage een afschrift af van de Persoonsgegevens die worden verwerkt.

4.4.2 Verzoek tot rectificatie

Indien Betrokkene aan TB verzoekt om de bij TB bekende Persoonsgegevens te rectificeren wordt van een gehonoreerd verzoek tot rectificatie mededeling gedaan aan de Betrokkene.

4.4.3 Verzoek tot verwijdering (vergetelheid)

Betrokkene heeft het recht om TB te verzoeken alle van hem bij TB verwerkte Persoonsgegevens te laten verwijderen. Indien TB dit verzoek honoreert, zal hier onverwijld gevolg aan worden gegeven. In ieder geval wordt aan een dergelijk verzoek gevolg gegeven indien:

I. de Persoonsgegevens niet langer noodzakelijk zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins zijn verwerkt;

II. de Betrokkene zijn toestemming heeft ingetrokken en er is geen andere grondslag voor verwerking meer aanwezig;

III. Betrokkene heeft bezwaar gemaakt tegen de verwerking en er zijn geen andere prevalerende belangen om tot verwerking over te gaan;

IV. de Persoonsgegevens zijn onrechtmatig verwerkt;

V. de Persoonsgegevens moeten op basis van Unierecht dan wel wettelijk voorschrift worden gewist.

Indien de Betrokkene, wiens Persoonsgegevens worden bewaard, verzoekt om verwijdering van zijn Persoonsgegevens, is het de directie toegestaan om de verwijdering te weigeren op grond van een voor de instelling uitoefening, dan wel onderbouwing, van een rechtsvordering.

Van een gehonoreerd verzoek tot verwijdering wordt mededeling gedaan aan de Betrokkene.

4.4.4 Verzoek tot beperking van de verwerking

De betrokkene heeft het recht beperking van de verwerking te verkrijgen indien:

I. de juistheid van de Persoonsgegevens wordt betwist. In een dergelijk geval wordt de beperking gehonoreerd voor de periode voor onderzoek;

II. de verwerking is onrechtmatig en de Betrokkene verzoekt niet om verwijdering van de onrechtmatige gegevens;

III. Betrokkene van oordeel is dat TB de gegevens niet meer nodig heeft voor verwerking, maar Betrokkene heeft de gegevens nodig voor de instelling van een rechtsvordering;

IV. Betrokkene bezwaar heeft gemaakt tegen de verwerking en Betrokkene in afwachting is van het antwoord van TB of de gerechtvaardigde gronden zwaarder wegen.

4.4.5 Verzoek tot overdracht van Persoonsgegevens

Indien de Betrokkene een verzoek doet tot overdraagbaarheid van Persoonsgegevens wordt dit verzoek door het privacy team conform de procesbeschrijving verwerking van Persoonsgegevens in behandeling genomen indien het verzoek:

I. betrekking heeft op door de Betrokkene (in) actief verstrekte Persoonsgegevens;

II. de verwerking berust op toestemming dan wel uitvoering van de overeenkomst[3].

TB zorgt er voor dat de gegevens in een gestructureerde, gangbare en voor computers leesbare wijze worden verstrekt (PDF of Excel).

4.4.6 Recht van bezwaar

Een Betrokkene heeft altijd het recht om bezwaar te maken tegen de verwerking van zijn Persoonsgegevens indien dit Persoonsgegevens betreffen die op basis van de grondslag gerechtvaardigd belang zijn verwerkt. Indien TB Persoonsgegevens op basis van deze grondslag verwerkt is directie bevoegd om na advies van de privacy coördinator het bezwaar tegen de verwerking ongegrond te verklaren indien naar het oordeel van directie er binnen TB een zwaarder belang aanwezig is. In ieder geval honoreert de directie het verzoek van Betrokkene om de verwerking van Persoonsgegevens in het kader van direct marketing te staken.

5 BEVEILIGING

5.1 Inleiding

TB zorgt er voor, rekening houdend met de stand van de techniek, de kosten van de tenuitvoerlegging, de risico's die de uitvoering met zich mee brengt en de aard van de Persoonsgegevens, dat passende technische en organisatorische maatregelen worden genomen om Persoonsgegevens te beveiligen tegen verlies, vernietiging, vervalsing, ongewenste toegang en verspreiding, dan wel enige andere vorm van misbruik.

5.2 Systeem autorisaties

Autorisatieverzoeken dienen door de aanvrager digitaal aangeleverd te worden. Registratie van het verzoek vindt plaats in het incidentregistratiesysteem van IT. Daarbij wordt vastgelegd: de manager van de aanvrager en gedetailleerde omschrijving van het autorisatieverzoek. De wijziging wordt door de dienstdoende helpdeskmedewerker uitgevoerd, controle vindt plaats door de functioneel beheerder bij afronden van de werkzaamheden. Deze controle wordt vastgelegd in het incidentregistratiesysteem. Er vindt nadien door de helpdeskmedewerker verificatie plaats met de aanvrager om juiste toepassing te verifiëren.

[3] TB is derhalve niet verplicht om Persoonsgegevens over te dragen die worden verwerkt op de grondslag wettelijke verplichting.

5.3 Privacy by design

TB draagt er zorg voor dat mede gezien de:

I. stand van de techniek;

II. uitvoeringskosten;

III. aard, omvang, de context en doel van de verwerking;

IV. waarschijnlijkheid en de ernst van de risico's voor de rechten en vrijheden van natuurlijke personen.

bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen zijn opgesteld met als doel de gegevensbeschermingsbeginselen op een doeltreffende wijze uit te voeren en de nodige waarborgen in te bouwen ter naleving van de wettelijke voorschriften.

5.4 Privacy by default

De directie van TB zorgt, in samenspraak met de Privacy coördinator, voor passende technische en organisatorische maatregelen om te voorkomen dat niet meer persoonsgegevens worden verwerkt voor een bepaald doel dan nodig, dan wel een te lange periode worden bewaard.

6 DATALEKKEN

6.1 Behandeling datalekken

Een datalek wordt behandeld en gedocumenteerd conform de procesbeschrijvingen zoals opgenomen in de procedure meldplicht datalekken.

Indien zich een inbreuk bij TB heeft voorgedaan verband houdende met Persoonsgegevens zal door TB deze gebeurtenis bij de Autoriteit Persoonsgegevens worden gemeld binnen 72 uur nadat de inbreuk bij TB bekend is geworden, behalve wanneer het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Indien een melding niet binnen 72 uur bij de Autoriteit Persoonsgegevens is gedaan, zal de latere melding aan de Autoriteit Persoonsgegevens worden gemotiveerd.

6.2 Datalek bij Verwerker

Indien het datalek zich bij de Verwerker heeft voorgedaan zal deze de Privacy coördinator bij TB onverwijld moeten informeren, waarbij de benodigde informatie wordt gegeven over:

I. de aard van de inbreuk van de Persoonsgegevens;

II. de naam van de privacy coördinator dan wel contactpersoon waarmee contact opgenomen kan worden;

III. gevolgen van de inbreuk;

IV. de maatregelen zoals door de verwerkingsverantwoordelijke zijn voorgesteld.

Indien het onmogelijk is alle informatie ineens te verstrekken is het mogelijk om de reeds beschikbare informatie door te geven (voormelding). TB draagt er zorg voor dat alle gegevens met betrekking tot de inbreuk worden gedocumenteerd en geregistreerd[4] zodat toezicht van de Autoriteit altijd mogelijk is.

6.3 Informeren betrokkenen

TB draagt er zorg voor dat Betrokkene onverwijld wordt geïnformeerd indien de inbreuk een hoog risico inhoudt voor de rechten en vrijheden van Betrokkenen. Indien een in de AVG genoemde uitzonderingsgrond voor melding aan betrokkene aan de orde is, zal melding achterwege blijven. Hiertoe beslist de directie conform de procedure zoals uiteengezet in paragraaf 9.4.

6.4 Procedure datalekken

De directie bepaalt op advies van de privacy coördinator in welk geval sprake is van een datalek en wanneer Betrokkenen dienen te worden geïnformeerd. In ieder geval wordt de gebeurtenis geregistreerd, en indien er sprake is van een datalek wordt een melding gedaan aan de Autoriteit Persoonsgegevens

Daarnaast is op basis van de procedure omgaan met media en publiciteit alleen de (algemeen) directeur bevoegd om de pers te woord te staan.

7 VERWERKERS

7.1 Aanstelling van Verwerkers

TB maakt in de bedrijfsvoering gebruik van een aantal Verwerkers die in geval van een uitbestedingsrelatie worden aangesteld op basis van de uitgangspunten voor uitbesteding binnen TB. In dit beleid is een aantal processen en eisen geformuleerd die moeten borgen dat TB de juiste partij selecteert. Uit hoofde van dit beleid geldt voor TB de verplichting om alleen die Verwerkers te selecteren die voldoende garanties kunnen bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen zodat de verwerking conform de eisen uit hoofde van de AVG voldoet en de bescherming van de rechten van Betrokkenen is gewaarborgd.

[4] Ook niet-gemelde datalekken dienen te worden geregistreerd en gedocumenteerd.

7.2 Overeenkomsten met Verwerkers

TB is in het bezit van een standaard verwerkingsovereenkomst, die dient als basis. Afhankelijk van de situatie kan of de overeenkomst van TB of die van de verwerker ingezet worden. De directie van TB draagt er in samenwerking met het privacy team zorg voor dat de opdracht tot Verwerking van bepaalde Persoonsgegevens in een (afzonderlijke) overeenkomst is geregeld waarin in ieder geval de volgende onderwerpen worden opgenomen:

I. de Verwerker is slecht gerechtigd Persoonsgegevens te verwerken op basis van schriftelijke instructies van TB, waarbij in ieder geval TB bepaalt of er sprake is van doorgifte aan derde landen dan wel internationale organisaties, tenzij de Verwerker hier op basis van wettelijke regels verplicht toe is, in dat geval is de Verwerker verplicht dit aan TB te melden, tenzij de wettelijke verplichting dit verbiedt;

II. de Verwerker dient te waarborgen dat tot de verwerking van Persoonsgegevens gemachtigde personen de vertrouwelijkheid in acht nemen, dan wel door een passende wettelijke verplichting tot vertrouwelijkheid zijn gebonden;

III. de Verwerker de in artikel 32 van de AVG genoemde passende maatregelen neemt om de Persoonsgegevens te beveiligen;

IV. de Verwerker de in dit beleid genoemde maatregelen neemt in geval van benoeming van een andere Verwerker;

V. de Verwerker, voor zover redelijkerwijs mogelijk, bijstand verleent in geval van een verzoek tot uitoefening van de rechten van Betrokkene zoals uiteengezet in hoofdstuk 4 van dit beleid;

VI. de Verwerker, voor zover redelijkerwijs mogelijk, bijstand verleent tot nakoming van de verplichtingen uit hoofde van de AVG die zien op beveiliging van Persoonsgegevens, meldplicht aan de AP/ Betrokkene in geval van een datalek en tot slot het uitvoeren van een DPIA. In ieder geval is Verwerker verplicht om TB onmiddellijk - doch uiterlijk binnen 24 uur - te informeren in geval van een datalek;

VII. de Verwerker na afloop van de dienstverlening over zal gaan tot vernietiging van de Persoonsgegevens en kopieën verwijdert, tenzij Verwerker op basis van wettelijke verplichtingen gehouden is deze te bewaren;

VIII. de Verwerker zijn medewerking zal verlenen om de accountability te bewijzen en audits dan wel andere inspecties door TB dan wel een derde mogelijk te maken en daar ook aan bijdraagt;

IX. de Verwerker werkt onder gezagsverhouding van TB, hetgeen inhoudt dat de Verwerker niet meer gegevens verwerkt dan strikt noodzakelijk is in het kader van de opdracht;

X. de Verwerker meewerkt aan alle redelijke verzoeken van TB dan wel de AP, zoals het verzoek om het register van verwerkingsactiviteiten te overleggen.

7.3 Benoeming Subverwerker

Indien de Verwerker het voornemen heeft om (een gedeelte van) de werkzaamheden door een (andere) Subverwerker te laten uitvoeren, zal deze eerst schriftelijk aan TB toestemming dienen te vragen. Indien de Verwerker bij het aangaan van de overeenkomst al gebruik maakt van Subverwerkers wordt op verzoek van TB met naam aangegeven om welke partijen dit gaat. De Verwerker draagt er zorg voor dat de in paragraaf 7.2 genoemde afspraken in de overeenkomst zullen worden vastgelegd en dat in voornoemde overeenkomst is geregeld dat de Verwerker aansprakelijk blijft ondanks het aanstellen van andere Subverwerkers.

8 REGISTER VAN VERWERKINGEN

8.1 Eisen aan het register

TB draagt er zorg voor dat alle verwerkingen van Persoonsgegevens worden geregistreerd in een verwerkingsregister. In het register wordt in ieder geval de volgende informatie opgenomen:

I. de naam en contactgegevens van TB, de initialen van de lokale privacy verantwoordelijke dan wel privacy teamlid;

II. de verwerkingsdoeleinden;

III. een beschrijving van de categorieën van Betrokkenen en categorieën van Persoonsgegevens;

IV. de categorieën van ontvangers aan wie Persoonsgegevens zullen worden doorgeven en indien relevant ontvangers in derde landen;

V. indien relevant: of er sprake is van doorgifte van Persoonsgegevens aan derde landen;

VI. indien mogelijk, de bewaartermijn;

VII. indien mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen die genomen zijn om de Persoonsgegevens te beveiligen.

8.2 Register bij Verwerkers

TB draagt er zorg voor dat Verwerkers aan de verplichting voldoen om een register bij te houden van alle verwerkingen in opdracht van TB. In het register van de Verwerker wordt in ieder geval de volgende informatie opgenomen:

I. de naam en contactgegevens van de Verwerkers en van TB in de hoedanigheid van Verwerkingsverantwoordelijke, alsmede van de contactgegevens van de vertegenwoordiger en/of de Privacy coördinator van TB;

II. de categorieën van verwerkingen die voor rekening van TB worden uitgevoerd;

III. indien van toepassing, of er sprake is van doorgifte van Persoonsgegevens aan een derde land onder vermelding van dat land en de (gedocumenteerde) passende waarborgen;

IV. indien van toepassing, een beschrijving van de passende technische maatregelen om de Persoonsgegevens te beschermen.

TB draagt er zorg voor dat het verwerkingsregister in schriftelijke dan wel elektronische vorm wordt opgezet.

9 GEGEVENS EFFECTBEOORDELING

9.1 Gegevens effectbeoordeling

Directie kan op advies van de Privacy coördinator beslissen dat een gegevens effectbeoordeling (DPIA) plaats zal vinden op bepaalde door directie aan te wijzen verwerkingen die, gelet op de aard, de omvang, context en doeleinden daarvan waarschijnlijk een hoog risico inhouden voor de Betrokkenen.

De Privacy coördinator neemt in ieder geval de richtlijnen zoals gepubliceerd door het comité (art. 68 AVG) en de Autoriteit Persoonsgegevens in beschouwing bij de beantwoording van de vraag of een gegevens effectbeoordeling op bepaalde verwerkingen vereist is.

Hoewel er binnen TB geen gegevens worden verwerkt die op basis van de AVG een DPIA behoeven, zal er binnen TB conform de aanbevelingen van de WP29 periodiek een DPIA worden verricht. Directie wijst op advies van de Privacy coördinator de medewerker aan die de DPIA uit dient te voeren. Daarnaast ziet de Privacy coördinator erop toe dat een DPIA actueel is en minimaal eens in de drie jaar wordt uitgevoerd.

9.2 Melding risicoverwerkingen aan Autoriteit

Indien uit een gegevens effectbeoordeling blijkt dat een verwerking een hoog risico meebrengt, zonder dat hier doeltreffende beheersmaatregelen tegenover staan, dient TB in de persoon van de Privacy coördinator in overleg te treden met de Autoriteit Persoonsgegevens. Bij de raadpleging worden in ieder geval de volgende gegevens door TB aan de Autoriteit Persoonsgegevens
verstrekt:

I. de verantwoordelijkheden van TB jegens de bij de verwerking betrokken Verwerkers;

II. de doeleinden en de middelen voor de voorgenomen verwerking;

III. de maatregelen en waarborgen die worden genomen om de rechten van Betrokkenen te beschermen;

IV. de contactgegevens van de Privacy coördinator;

V. de gegevens effectbeoordeling;

VI. alle informatie waar de AP nog om verzoekt.

10 BEWAARTERMIJNEN

10.1 Bewaartermijn

Binnen TB geldt het beleid dat Persoonsgegevens naar hun aard niet langer dan noodzakelijk worden bewaard. In het verwerkingsregister wordt steeds per verwerking vastgelegd wat de bewaartermijnen zijn.

Binnen TB geldt voor persoonsgegevens dat deze in ieder geval minimaal de wettelijk vereiste bewaartermijn vanaf afwikkeling van het dossier worden bewaard.

Gezien het feit dat de kans bestaat dat een partij een rechtsvordering instelt, worden deze dossiers gedurende de extinctieve verjaringstermijn bewaard. De directie is bevoegd om aanvullende maatregelen te nemen om deze gegevens extra te beveiligen.

10.2 Verwerkingen

Een sollicitant wordt conform bestaand beleid (VOG) gescreend op betrouwbaarheid. Bij indiensttreding zullen Persoonsgegevens worden verwerkt teneinde te waarborgen dat de indiensttreding correct wordt afgehandeld.

Gedurende de looptijd van de arbeidsovereenkomst zullen Persoonsgegevens van medewerkers door TB worden verwerkt om aan verplichtingen uit hoofde van de arbeidsovereenkomst te voldoen. Het gaat in ieder geval om de volgende verwerkingen:

I. salarisoverboeking, declaraties;

II. ziek- en betermelding;

III. uitvoering van pensioenverplichtingen;

IV. opleidingen en trainingen;

V. tijdregistratie;

VI. deurwaarders, overheidsinstanties;

VII. toezenden nieuwsbrief;

VIII. het aangaan van verzekeringen namens de werknemers.

Daarnaast worden reguliere Persoonsgegevens verwerkt in het kader van het plannen, coachen en beoordelen van medewerkers.

De grondslag voor deze verwerkingen kan als volgt zijn:

I. uitvoering arbeidsovereenkomst;

II. naleving wettelijke verplichting;

III. indien er sprake is van een gerechtvaardigd belang aan de zijde van TB waarbij het belang van TB zwaarder weegt dan het belang van de werknemer.

TB communiceert duidelijk aan haar medewerkers op welke wijze Persoonsgegevens worden verwerkt. Op intranet is de AVR gepubliceerd, waarin de door TB gehanteerde verwerkingen worden benoemd.

10.3 Verwerking in geval van ziekmelding

Indien een werknemer zich ziek meldt is het TB niet toegestaan om gegevens te verwerken dan voor zover redelijkerwijs gerechtvaardigd om onder meer vast te stellen of er sprake is van een loondoorbetalingsverplichting en op welke termijn de werkzaamheden weer zouden kunnen worden hervat. Het is anderzijds wel toegestaan om gegevens vast te leggen omtrent eventuele chronische aandoeningen (maar niet het medicijngebruik), die relevant zouden kunnen zijn voor het verlenen van (eerste) hulp. Daarnaast is het toegestaan gegevens vast te leggen omtrent de periode van ziekte, alsmede gegevens die noodzakelijk zijn om vast te stellen of de ziekte verband houdt met het werk.

In geen geval wordt gevraagd of de ziekte gerelateerd is aan het werk. Daarnaast zal TB nimmer vragen naar de aard en oorzaak van de ziekte. Indien de betreffende werknemer uit vrije wil over de ziekte praat zal deze informatie in beginsel niet worden opgenomen in het personeelsdossier dan wel op enige andere manier worden vastgelegd.

Het is TB toegestaan om te controleren of werknemer daadwerkelijk ziek is en derhalve of er voldoende grond is om het loon door te betalen. Een dergelijk nader onderzoek vindt alleen plaats indien TB duidelijke aanwijzingen heeft dat werknemer mogelijk niet ziek is en wel in staat is om te werken. In dat geval is het HR medewerker en leidinggevende toegestaan om een vervroegde oproep van de Arbodienst te doen verzenden. In geen geval wordt een rechercheburau dan wel een andere dienstverlener ingeschakeld, tenzij een zeer zwaarwegend belang bestaat. In dat geval zal directie, alvorens tot een dergelijke beslissing te komen, de Privacy coördinator raadplegen.

Aan de Arbodienst worden de volgende gegevens doorgegeven:

- identificerende Persoonsgegevens van de betreffende werknemer;
- indien van toepassing: informatie van werknemer bij ziekmelding en eigen waarneming.

Indien de werknemer na langdurige ziekte gaat re-integreren zullen TB en de medewerker van de Arbodienst een probleemanalyse alsmede een advies voor een plan van aanpak ontvangen. Mede op basis van deze stukken zullen TB en de medewerker overgaan tot het maken van een plan van aanpak. Dit plan van aanpak wordt in het personeelsdossier opgeslagen. Dit dossier wordt niet langer dan voor de duur van twee jaar nadat de medewerker uit dienst is opgeslagen.

De directie draagt er zorg voor dat slechts een enkele medewerker toegang heeft tot het (extern) verzuimsysteem, te weten HR medewerkers als ook direct leidinggevenden. In dit (extern) systeem wordt het verzuim geregistreerd.

10.4 Bewaartermijn personeelsdossiers

TB heeft personeelsdossiers waarin relevante gegevens van personeel is opgeslagen. TB zal deze gegevens bewaren zolang als redelijkerwijs noodzakelijk, maar niet langer dan voor de duur van de verjaringstermijn na beëindiging van het dienstverband. Directie is bevoegd (om voor bepaalde gegevens) een kortere termijn te bepalen. In ieder geval worden gegevens die niet langer noodzakelijk zijn om te bewaren gewist.

10.5 Rechten werknemers en andere betrokkenen

Aan alle werknemers komt in ieder geval het recht tot inzage, correctie, verwijdering en beperking van de verwerking toe. Elk verzoek dient te worden gedaan bij de Privacy coördinator en indien relevant in overleg met de directie, die het verzoek in beginsel honoreert, dan wel gemotiveerd afwijst[5].

10.6 Beveiliging gegevens personeel

Alle Persoonsgegevens worden op adequate wijze bewaard, verwezen wordt naar hoofdstuk 5 van dit beleid. Alleen leden van directie en HR afdeling hebben toegang tot deze gegevens. Managers kunnen alleen toegang verkrijgen van de onder hen ressorterende medewerkers voor zover dit strikt noodzakelijk is voor de uitoefening van de aan hen opgedragen leidinggevende functie.

Voor zover de Persoonsgegevens op papier zijn opgeslagen worden zij opgeborgen in een brandwerende kluis waartoe alleen leden van directie toegang hebben.

10.7 Doorgifte van Persoonsgegevens aan derde landen

TB draagt er steeds zorg voor dat Persoonsgegevens niet aan derde landen[6] worden verstuurd die geen adequaat niveau van bescherming bieden. Indien persoonsgegevens aan derde landen worden doorgestuurd dan wel door verwerkers verder worden doorgestuurd, wordt steeds de Privacy coördinator vergewist naar welk land de gegevens worden doorgestuurd. De Privacy coördinator bepaalt of en welke aanvullende maatregelen getroffen dienen te worden.

In ieder geval is het de privacy coördinator toegestaan doorgifte op basis van adequaatheidsbesluiten, op basis van passende waarborgen, dan wel op basis van bindende bedrijfsvoorschriften onder voorwaarden toe te laten.

11 VASTSTELLING

11.1 Vaststelling en inwerkingtreding

Dit beleid is vastgesteld door de directie van TB in het bestuursoverleg van 8 juli 2022 en treedt per gelijke datum in werking. Hiermee worden alle voorgaande beleidsstukken met betrekking tot verwerking van persoonsgegevens en privacy vervangen.

[5] Een verzoek tot verwijdering ligt niet altijd voor toewijzing gereed.

[6] Te weten landen die buiten de EER zijn gevestigd dan wel landen die niet op basis van het adequaatheidbesluit door de Europese Commissie zijn aangewezen