Protocol IZB en databeveiliging

Versie 6 december 2017.

Deze versie staat ter beschikking van leden van MissieNederland, onder de voorwaarde dat *vertrouwelijk* met de inhoud van dit document zal worden omgegaan.

IZB houdt zich niet verantwoordelijk/aansprakelijk voor de inhoud van dit document jegens derden als derden dit gebruiken als basis voor een eigen document.

Organisaties die lid zijn van MissieNederland kunnen dit protocol gebruiken als voorbeeld respectievelijk als basis voor een eigen protocol; het document dient dan wel bewerkt te worden en specifiek gemaakt te worden voor de eigen organisatie.

Inhoud

1. Algemeen

1.1. Totstandkoming protocol

Het protocol is in juli 2017 tot stand gekomen na raadplegen van medewerkers, ICT-adviseur en brancheorganisaties. Er is mede gebruik gemaakt van een stappenplan om te komen tot een protocol, zoals aangereikt door het CBF.
Op grond van de verzamelde informatie zijn technische en organisatorische maatregelen voorgesteld, die in de loop van 2017 geïmplementeerd dienen te zijn.

1.2. Van toepassing zijnde regelgeving

Als ondergrens voor de maatregelen die de IZB neemt, geldt dat voldaan wordt aan de wettelijke voorschriften, te weten:

1. Richtlijn Databescherming 1995 (in Nederland: Wet bescherming persoonsgegevens (Wbp) en
2. General Data Protection Regulation van de EU (Algemene Verordening Gegevensbescherming), die op 25 mei 2018 van kracht wordt. De regelgeving van deze AVG, die opgesteld is i.v.m. technologische ontwikkelingen, gaat verder dan de regelgeving in de huidige Wbp.

Daarnaast dient de IZB, als een erkend goed doel, zich te houden aan de voorschriften van het CBF m.b.t. beveiliging van informatie. Databeveiliging is een van de normen, die van toepassing zijn voor de toekenning van een erkenning. De voorschriften luiden als volgt:
1. De organisatie heeft een actueel beleid met betrekking tot de beveiliging van informatie.
2. De organisatie zorgt voor een afdoende beveiliging van de haar ter beschikking staande informatie, zodanig dat de privacywetgeving, waaronder de Wet Bescherming Persoonsgegevens, wordt nageleefd.
De ICT en databeveiliging sluiten aan bij de aard van de ter beschikking staande informatie.

1.3. Data bij de IZB

In het kader van de werkzaamheden verzamelt en registreert de IZB persoonsgegevens. Leden, begunstigers, gemeenten en anderen moeten er op kunnen vertrouwen dat de persoonsgegevens op een toereikende wijze beveiligd zijn.
Op grond van de wet is de IZB zelfs verplicht deze gegevens te beveiligen door passende technische en organisatorische maatregelen te nemen. Dit speelt des te meer omdat bepaalde gegevensbestanden ook uitgewisseld worden met derden.

1.4. Datalek

Er is sprake van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens. Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking, dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Onder een datalek valt niet alleen het vrijkomen (lekken) van gegevens, maar ook de onrechtmatige verwerking van gegevens.

1.5. Voorbeelden en gevaren van datalekken

Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens (tenzij met encryptie), een gestolen laptop, een inbraak in een databestand door een hacker, besmetting met malware, verzenden van een e-mail waarin alle persoonlijke e-mailadressen zichtbaar zijn, of een calamiteit in een datacentrum.

Een van de *gevaren* van datalekken is het misbruik van persoonsgegevens in het kader van identiteitsfraude[1].

[1] Bij identiteitsfraude maken criminelen misbruik van valse of gestolen identiteitsgegevens. Ze kopen bijvoorbeeld op naam van iemand anders spullen zonder te betalen.

2. Wettelijke bepalingen

In dit hoofdstuk is een overzicht van de belangrijkste wettelijke bepalingen opgenomen, zoals deze vanaf 25 mei 2018 gelden:

2.1. Persoonsgegevens

Persoonsgegevens zijn gegevens die direct over een natuurlijk persoon gaan of tot een natuurlijk persoon zijn te herleiden. Dat betekent dat gegevens over overleden personen en organisaties geen persoonsgegevens zijn.
De wet onderscheidt gewone persoonsgegevens (naam, adres, woonplaats, postcode, telefoonnummer, e-mailadres) en bijzondere persoonsgegevens.

Tot de categorie 'bijzondere persoonsgegevens' behoren:

- Gegevens m.b.t. godsdienst of levensovertuiging.
- Ras of afkomst.
- Politieke voorkeur.
- Gezondheid.
- Seksuele leven.
- Lidmaatschap van een vakbond.
- BSN-nummer.

Bijzondere persoonsgegevens mogen niet vastgelegd worden, tenzij de wet daarvoor een uitzondering heeft gemaakt.

Recente informatie d.d. 30 november 2017: Autoriteit Persoonsgegevens zou hebben vastgesteld dat BSN-nummers niet langer aangemerkt worden als bijzondere persoonsgegevens. De website van AP maakt hiervan echter nog geen melding.

2.2. Verwerken van persoonsgegevens

Verwerken van persoonsgegevens is een breed begrip; het omvat alles van verzamelen, vastleggen, raadplegen tot en met vernietigen van de gegevens. Kopiëren naar een USB-stick of lezen van een Excel-bestand is ook 'verwerken'.

2.3. Verwerken en rechtmatige grondslag

Verwerking moet behoorlijk (eerlijk, rekening houdend met de wet, juist en nauwkeurig), rechtmatig (is er een grondslag) en transparant (realiseer je zelf wat je doet) geschieden.

Verwerken van gegevens mag alleen (en vindt daarom alleen plaats) als er een grondslag is; voor de IZB is hierbij het volgende van belang:

- Toestemming
  (bijvoorbeeld zijn door op een te tekenen formulier, incasso-opdracht, invulveld op een website expliciet te vermelden: 'ik geef hierbij toestemming dat mijn gegevens vastgelegd worden in het systeem van de IZB').
- Uitvoering overeenkomst
- Wettelijke verplichting
  (bijvoorbeeld vastleggen van persoonsgegevens van personen die een betaling ontvangen, die aan de Belastingdienst moet worden opgegeven; gegevens in personeels- en salarisadministratie).
- Gerechtvaardigde belangen
  (bijvoorbeeld: het vastleggen van gegevens voor directmailing door een fondsenwervende instelling; het vastleggen van gegevens van leden van een vereniging voor informatieverschaffing aan de leden); bezwaren van derden moeten overigens wel onmiddellijk gehonoreerd worden.

2.4. Partijen bij gegevensverwerking

- Verantwoordelijke
  (de organisatie die de gegevens vastlegt en verwerkt of laat verwerken).
- Verwerker
  (de organisatie die in opdracht van en ten behoeve van de verantwoordelijke persoonsgegevens verwerkt).
- Betrokkene
  (de natuurlijke persoon van wie gegevens worden vastgelegd).

2.5. Relatie met het lid van de vereniging en met de donateur

In de relatie met de betrokkenen is het volgende van belang:

- Er is een duidelijke en bevestigende toestemming voor het vastleggen van de gegevens.
  (betrokkene moet weten waarvoor hij toestemming geeft; organisatie moet zo veel mogelijk bevorderen dat privacy statement wordt gelezen, bijv. met een pop-up venster op de website; in dat geval helpt gelaagdheid → eerste halve A4 is samenvatting van het document).
- Lid of donateur kan kennis nemen van privacy statement dat in duidelijke taal is opgesteld.
- Rechten van betrokkenen zijn sterker geworden:
  - Recht op inzage
  (doel waarvoor de gegevens verwerkt worden, categorieën gegevens die vastgelegd worden, aan wie worden de gegevens verstrekt, bewaartermijn, de logica die ten grondslag ligt aan de

automatische verwerking).

- Recht op rectificatie

(aanpassen; organisatie moet terugmelding doen)

- Recht op vergetelheid

(verwijderen gegevens als: a) gegevens niet langer nodig zijn, b) betrokkene bezwaar maakt tegen de vastlegging, c) eerder gegeven toestemming ingetrokken wordt, d) er geen gerechtvaardigde grondslagen voor verwerking zijn)

- Recht op dataportabiliteit

(opvragen gegevens voor eigen gebruik of om door te geven aan een derde).

- Daarnaast hebben betrokkenen recht op:
  - bezwaar maken tegen de verwerking;
  - intrekken van de eerder gegeven toestemming;
  - klacht indienen bij Autoriteit Persoonsgegevens (AP).
- Organisatie moet de betrokkenen de mogelijkheid geven de rechten uit te kunnen oefenen.
  (bijvoorbeeld: online mogelijkheid; let dan wel op identificatie).
- Wet schrijft voor binnen een maand te reageren als een betrokkene een beroep doet op een van zijn rechten.

2.6. Relatie met derden

- Alleen samenwerken met partijen die betrouwbaar zijn. Actief controleren!
- Verwerkersovereenkomst is verplicht.

2.7. Accountability

Elke organisatie die persoonsgegevens verwerkt, moet kunnen verantwoorden welke maatregelen genomen zijn om te voldoen aan de AVG. Deze verantwoording krijgt gestalte door het opstellen van:

- een dataregister.
- een privacy beleidsplan.

Het is een wettelijke verplichting zowel een dataregister als een privacy beleidsplan op te stellen.

Zowel de (verwerkings)verantwoordelijke als de verwerker moeten een dataregister opstellen.

2.8. Dataregister verwerkingsverantwoordelijke

In het dataregister van de verantwoordelijke worden de volgende gegevens opgenomen:

- naam en contactgegevens van de verantwoordelijke, de vertegenwoordiger van de verantwoordelijke en de functionaris voor gegevensbescherming;
- doeleinde en rechtsgrondslag voor gegevensverwerking;
- een beschrijving van de categorieën betrokkenen en categorieën persoonsgegevens;
- de (voorgenomen) categorieën ontvangers;
- een vermelding van een verstrekking van persoonsgegevens aan een derde land of een internationale organisatie[2];
- de (voorgenomen) bewaartermijnen;
- de rechten van de betrokkenen zoals beschreven in onderdeel 2.5;
- bestaan van geautomatiseerde besluitvorming[3];
- een algemene beschrijving van de beveiligingsmaatregelen.

Het dataregister is een intern verantwoordingsdocument. De tekst hiervan is opgenomen in bijlage 1 van dit protocol.

2.9. Dataregister verwerker

Alle verwerkers die door de IZB worden ingeschakeld zijn verplicht een dataregister aan te leggen, waarin de volgende gegevens worden opgenomen:

- de naam en contactgegevens van de verwerker(s) en van de verantwoordelijk(en) en de functionaris voor gegevensbescherming;
- de categorieën verwerkingsactiviteiten;
- een vermelding van een verstrekking van persoonsgegevens aan een derde land of een internationale organisatie[4];
- een algemene beschrijving van de beveiligingsmaatregelen.

2.10. Functionaris voor gegevensbescherming

Het is verplicht een functionaris voor gegevensbescherming (FG) aan te stellen indien:

- de verwerking wordt uitgevoerd door een overheidsinstelling;
- de verwerking vereist dat de betrokkenen op grote schaal regelmatig en stelselmatig worden geobserveerd;
- hoofdzakelijk sprake is van grootschalige verwerking van bijzondere persoonsgegevens (als kernactiviteit) of persoonsgegevens met betrekking tot strafrechtelijke veroordelingen/strafbare feiten.

[2] Bij de IZB is verstrekking aan een derde land of aan internationale organisaties niet aan de orde.
[3] Vermelding in de trant van ‘wij hebben de mogelijkheid geautomatiseerd doelgroepen te selecteren voor campagnes en mailings’.
[4] Bij de IZB is verstrekking aan een derde land of aan internationale organisaties niet aan de orde.

De FG mag een medewerker van de eigen organisatie zijn, mits deze voldoende kennis heeft van de materie.

2.11. Privacy Impact Assessment

Als een nieuwe technologie beschikbaar komt, dient bij gebruikmaking daarvan een privacy impact assessment gedaan te worden, namelijk indien:

- er sprake is van profilering
  (voorbeeld: selectie van gegevens van 65-jarigen m.b.t. een mailing voor nalatenschappen)
- grootschalige verwerking van bijzondere persoonsgegevens of persoonsgegevens met betrekking tot strafrechtelijke veroordelingen/strafbare feiten.
- Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

2.12. Privacy by design en privacy by default

Privacy by design: privacy waarborgen door het treffen van technische en organisatorische maatregelen.
Privacy by default: privacy waarborgen door de verwerking zo minimaal mogelijk te houden.

2.13. Actieve systeembeveiliging

Er moet een passende beveiliging van de gegevens zijn, zodat de veiligheid wordt gewaarborgd en er geen inbreuk wordt gemaakt op de AVG.
Let wel: dit is dwingend recht; daar mag je ook niet bij afspraak met de donateurs van afwijken; het is strafbaar om niet aan deze verplichting te voldoen.

2.14. Meldplicht datalekken

Melding van een datalek moet worden gedaan bij het meldloket datalekken van de Autoriteit Persoonsgegevens. Dit moet gebeuren binnen 72 uur.
De Autoriteit Persoonsgegevens heeft beleidsregels meldplicht datalekken opgesteld. Deze beleidsregels zijn bedoeld om organisaties te helpen bij het bepalen of er sprake is van een datalek dat zij moeten melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.
Deze beleidsregels zijn leidend voor de IZB bij de vraag of er al dan niet gemeld moet worden.
De interne procedure die van toepassing is bij het constateren van een datalek, is opgenomen in bijlage 4 bij dit protocol.

2.15. Verantwoordelijkheid organisatie en boetes

De organisatie is te allen tijde verantwoordelijk voor toereikende maatregelen. Ingewikkelde wetgeving of onvoldoende techniek zijn geen geldig excuus. Bij uitbesteding van verwerking blijft de organisatie verantwoordelijk[5].

De boetes, die onder de huidige regeling al hoog zijn, worden vanaf 25 mei 2018 fors verhoogd:

- tot maximaal € 10 miljoen bij niet nakomen van de verplichtingen.
- tot maximaal € 20 miljoen bij overtreden van beginselen/grondslagen.

De huidige drempel om een boete op te leggen (opzet of grove schuld), komt te vervallen. Het is daarom te allen tijde van belang aan te kunnen tonen dat de organisatie het noodzakelijke heeft gedaan om aan de wet te voldoen.

2.16. Meldingsplicht gegevensverwerking

Geautomatiseerde verwerking van persoonsgegevens moeten op grond van de huidige regelgeving worden gemeld bij de Autoriteit Persoonsgegevens. Op deze meldingsplicht zijn uitzonderingen, die zijn vastgelegd in het Vrijstellingsbesluit[6]. Als per categorie aan de gestelde voorwaarden wordt voldaan, geldt geen meldingsplicht als alleen m.b.t. de volgende categorieën gegevens worden verwerkt:

- Leden of begunstigers van verenigingen en stichtingen[7].
- Personeelsadministratie
- Salarisadministratie
- Uitkeringen bij ontslag
- Abonnementen
- Debiteuren en crediteuren

De in het Vrijstellingenbesluit gestelde voorwaarden voor de verschillende categorieën zijn opgenomen in bijlage 6 bij dit protocol.

Omdat de IZB ook bijzondere persoonsgegevens vastlegt, zoals lidmaatschap van een kerkelijke gemeente, is sprake van een meldingsplicht.
In verband met een besluit van de Autoriteit Persoonsgegevens d.d. 6 november 2017 kan melding achterwege blijven; de meldingsplicht vervalt bij inwerkingtreding van de AVG.

[5] Verantwoordelijkheid kan overgaan op de verwerker als de uitbestedende organisatie zich houdt aan de verplichting een verwerkersovereenkomst met toereikende inhoud aan te gaan.
[6] Het Vrijstellingsbesluit Wbp is te raadplegen via de volgende link: http://wetten.overheid.nl/BWBR0012461/2017-05-25
[7] Het Vrijstellingsbesluit Wpb kent meer categorieën; deze zijn echter niet relevant voor de IZB.

3. Vastlegging, bewerken en verwerken van gegevens bij de IZB

3.1 Categorieën betrokkenen (personen van wie de IZB persoonsgegevens vastlegt)

Het betreft de volgende categorieën:

- Leden van de vereniging.
- Overige donateurs.
- Abonnees op door de IZB uitgegeven bladen
- Personen die zich inschrijven voor nieuwsbrieven (algemeen of afdeling)
- Deelnemers cursussen.
- Debiteuren en crediteuren in NAV
- Personeelsleden.
- Bestuursleden.
- Derden aan wie een fiscaal belaste vergoeding wordt betaald.
- Vrijwilligers Dabar.
- Overige vrijwilligers.
- Stagiaires.
- Overige betrokkenen bij de werkvelden van de IZB.

Van enkele categorieën worden, op grond van (arbeids)overeenkomsten en wettelijke verplichtingen, ook BSN-nummers vastgelegd. In die gevallen is daarom sprake van bijzondere persoonsgegevens.

3.2. Categorieën gegevens die vastgelegd worden m.b.t. leden / donateurs / personen die zich aanmelden voor het ontvangen van informatie, deelname aan cursussen of vrijwilligerswerk Dabar

In het CRM-systeem van Microsoft Dynamics worden voor natuurlijke personen uitsluitend de volgende gegevens vastgelegd:

- Naam, adres, woonplaats.
- Telefoonnummer.
- E-mailadres.
- Geboortedatum.
- Bankrekeningnummer.
- Ontvangen giften, contributies en bijdragen.
- Kerkgenootschap.
- Aanduiding kerkelijke gemeente

Overigens worden geen gegevens vastgelegd, tenzij er een gerechtvaardigd belang is.

Uitzondering op deze hoofdregel is de verwerking van gegevens m.b.t. vrijwilligers van Dabar. Voor hen worden aanvullend de volgende gegevens vastgelegd:
[het gaat hierbij o.a. om een referentie van iemand uit de kerkelijke gemeente (voorganger) m.b.t. de geestelijke achtergrond van de vrijwilliger]
Voor vrijwilligers van Dabar worden de volgende documenten gehecht aan de vastlegging in CRM:

- Verklaring omtrent het gedrag.
- Curriculum vitae
- Referentie

3.3. Verwerkingsgronden m.b.t. de bovengenoemde categorieën

De IZB verwerkt gegevens uitsluitend:

- Op verzoek van en met expliciete toestemming van betrokkene.
  De toestemming wordt verkregen door hetzij digitaal een vinkje te plaatsen voor toestemming hetzij bij formulieren de toestemming expliciet te vermelden.
- Bij een gerechtvaardigd belang van de IZB
  M.b.t. leden: het gerechtvaardigde belang voor de IZB is de mogelijkheid van het verzenden van contributienota's en herinneringen en het informeren van de leden.
  M.b.t. donateurs: het gerechtvaardigde belang voor de IZB is de mogelijkheid om door middel van direct mailing te informeren en fondsen te werven.

3.4. Omgaan met rechten van betrokkenen

De IZB respecteert de rechten van betrokkenen zoals vastgelegd in hoofdstuk 2.5, te weten:

- Recht op inzage
  Op verzoek wordt aan de betrokkene inzage verstrekt in de van hem/haar vastgelegde gegevens. Een beschrijving van de vastlegging en het doel van de vastlegging is opgenomen wordt opgenomen in het privacy statement, dat op de website wordt gepubliceerd.
- Recht op rectificatie
  Wijzigingen die worden doorgegeven worden binnen een maand verwerkt. Er wordt standaard een terugkoppeling gegeven.
- Recht op vergetelheid
  Wanneer een betrokkene aangeeft niet langer in het bestand van de IZB opgenomen te

willen zijn, zullen de gegevens worden verwijderd, tenzij de verwijdering in strijd is met de wettelijke boekhoudplicht en bewaarplicht.

- Recht op dataportabiliteit[8]

3.5. Bewaartermijn

Persoonsgegevens worden niet langer bewaard dan strikt noodzakelijk. Uitgangspunten zijn:

- Gegevens van leden worden bewaard zolang er geen opzegging van het lidmaatschap heeft plaats gevonden.
- Gegevens van inschrijvingen op digitale nieuwsbrieven en van andere betrokkenen worden bewaard zolang er geen opzegging heeft plaatsgevonden.
- Dabar vrijwilligers verstrekken (t.o.v. de andere categorieën betrokkenen) aanvullende gegevens. Deze aanvullende gegevens worden bewaard t/m het eind van het kalenderjaar na het laatste jaar waarin zij vrijwilligerswerk hebben gedaan. Daarna worden deze verwijderd.[9]
- Gegevens van betrokkenen die langer dan 7 jaar geen gift hebben gegeven of anderszins van hun betrokkenheid blijk hebben gegeven, worden in het volgende kalenderjaar verwijderd.

[8] Dataportabiliteit zal bij de IZB naar verwachting niet van toepassing zijn.
[9] Als een vrijwilliger drie jaar aaneengesloten Dabarwerk doet, dan worden de gegevens niet steeds verwijderd en opnieuw opgevraagd.

4. Risico's

Bij de IZB zijn de volgende risico's te onderscheiden:

4.1. Onvrijwillige datalekken, bijvoorbeeld het hacken van gegevens door derden, waarbij niet uitgesloten kan worden dat toegang is verkregen tot gevoelige personeelsgegevens.

4.2. Onvrijwillige datalekken, omdat het verzenden van bestanden met persoonsgegevens (bijvoorbeeld aan drukkerijen) onderschept wordt door kwaadwillige derden.

4.3. Onvrijwillige datalekken, omdat computers of dragers van gegevens bestanden kwijtraken of worden gestolen.

4.4. Onvrijwillige datalekken, omdat bewerkers van de gegevens deze per ongeluk of moedwillig misbruiken.

4.5. Onbewuste datalekken, bijvoorbeeld het per ongeluk verzenden van gegevensbestanden naar een onjuist e-mailadres.

4.6. Onbewuste datalekken, bij het gebruik maken van eigen laptops, computers en internetverbindingen van medewerkers (die wellicht minder goed beveiligd zijn dan het netwerk van de IZB).

4.7. Bewuste datalekken door medewerkers.

5. Technische maatregelen

De IZB realiseert zich dat, hoe adequaat de beveiliging is, er nooit een 100% garantie kan zijn dat een inbreuk op het systeem uitgesloten is. M.b.t. de mogelijke technische maatregelen laat de IZB zich adviseren door de ICT adviseur. Hieronder worden maatregelen onderverdeeld in maatregelen die al genomen zijn, maatregelen die uiterlijk op 1 oktober 2017 geïmplementeerd moeten zijn en maatregelen die op langere termijn overwogen worden.

Maatregelen die reeds geïmplementeerd zijn

5.1 Toegang tot het systeem

De toegang tot de server van de IZB is uitsluitend mogelijk via RDS of een beveiligde VPN-verbinding, waarbij de gegevens versleuteld over het internet worden getransporteerd.

Tevens wordt gebruik gemaakt van een naar het oordeel van de ICT-leverancier toereikende firewall.

5.2 Fysieke beveiliging van het kantoorpand

Er wordt gebruik gemaakt van alarmering, met doormelding naar een alarmcentrale.

5.3 Wachtwoordbeleid

Het wachtwoordbeleid is als volgt:

- Toegang tot het systeem door medewerkers is uitsluitend mogelijk met een password.
- Het password dient uit ten minste 10 karakters te bestaan en heeft één of meer karakters uit ten minste 3 van de 4 volgende groepen: hoofdletters, kleine letters, cijfers van 0 t/m 9 en speciale leestekens.
- Een maal per jaar wordt elk password gewijzigd. Als wijziging niet plaats vindt wordt de toegang geblokkeerd.
- Administrator password wordt ten minste twee maal per jaar aangepast; ook dit password voldoet aan de hiervoor genoemde kenmerken.

5.4 Back-up en recovery

Dagelijks wordt een dubbele back-up gemaakt:

- Naar een lokale NAS, waar de gegevens versleuteld worden opgeslagen (Acronis)
- Een externe online back-up (IASO).

Twee maal per jaar wordt de back-up getest, om zekerheid te verkrijgen dat deze bruikbaar is.

5.5. WIFI

Voor toegang tot WIFI is een sleutel nodig. Dataverkeer wordt versleuteld getransporteerd. Er is een afzonderlijk gastennetwerk, dat geen toegang heeft tot de servers.

5.6 Patchmanagement

IZB maakt gebruik van monitoring door de ICT-adviseur. Daarbij is gekozen voor patchmanagement, dat wil zeggen dat de belangrijkste veiligheidsupdates van leveranciers als Microsoft, Java, Adobe etc. automatisch op een afgesproken tijdstip op servers en pc's wordt geïnstalleerd.

5.7 Mail archivering

IZB past een vorm van e-mailarchivering toe, waarbij alle inkomende en uitgaande e-mails gearchiveerd worden.

Maatregelen die uiterlijk op 1 oktober 2017 geïmplementeerd moeten zijn

5.8. Multi-factor authenticatie

Inloggen op het systeem vindt plaats met een extra beveiliging naast inlognaam en password, namelijk met een bevestiging via een smartphone-app.

5.9 Periodieke penetratietest (ethical hacking)

Na de implementatie van de overige maatregelen in deze categorie en het live gaan van de website zal een penetratietest uitgevoerd worden. Deze zal één maal per jaar in het najaar herhaald worden. Daarbij zal aan steeds verschillende aspecten bijzondere aandacht gegeven worden.

Maatregelen die op langere termijn overwogen worden

5.10 Mobile device management

Als zakelijke e-mail op een mobiele telefoon ontvangen wordt, zijn vrijwel zeker persoonsgegevens (zoals op een individu terug te voeren e-mailadressen) op de mobiele telefoon aanwezig. De mogelijkheid van mobile device management zal worden onderzocht. In juni 2018 zal een besluit genomen worden of deze beschermingsmaatregel geïmplementeerd wordt.

5.11 Microsoft EMS

EMS is een totaalconcept van Microsoft m.b.t. beveiliging van data. Deze dienst is vooral interessant als veel gebruik gemaakt wordt van cloud toepassingen. Beleid is dat per 1 januari 2020 ‘in de cloud’ gewerkt zal worden. De server wordt dan buiten gebruik gesteld, alles wordt in de cloud gearchiveerd, de nieuwe versie van CRM wordt geïmplementeerd en er zal gebruik gemaakt worden van EMS.

5.12 Patch- en updatebeleid hardware

In juni 2018 zal een besluit genomen worden of deze beschermingsmaatregel geïmplementeerd wordt.

6. Organisatorische maatregelen

Maatregelen die reeds geïmplementeerd zijn dan wel uiterlijk op 1 oktober 2017 geïmplementeerd dienen te zijn

6.1 Bewustwording medewerkers m.b.t. datalekken en de risico's daarvan

- Bewustwording m.b.t. datalekken en de risico's daarvan is onderdeel van het inwerkprogramma van iedere nieuwe medewerker.
- Ten minste 1 x per jaar wordt het onderwerp databeveiliging in een bijeenkomst van medewerkers besproken.

Doel hiervan is het vergroten van de bewustwording bij de medewerkers m.b.t. de keuzes en risico's bij de vastlegging en verwerking van persoonsgegevens. Veel datalekken zijn immers het gevolg van menselijke fouten.

6.2 Werken met een betrouwbare ICT-partner

De IZB werkt met een betrouwbare ICT-partner, in ons geval met Continue IT. Deze partner heeft de betrouwbaarheid in de afgelopen jaren bewezen en heeft er in 2017 ook blijk van gegeven serieus met het onderwerp databeveiliging aan de slag te zijn (o.a. met een protocol databeveiliging).
De relatie met de ICT partner wordt jaarlijks in het 4^{e} kwartaal geëvalueerd.

6.3 Jaarlijkse evaluatie technische en organisatorische maatregelen

De technische ontwikkelingen staan niet stil. Jaarlijks in het 2^{e} kwartaal evalueren operationeel directeur, hoofd financiën en bedrijfsvoering en de ICT-adviseur de getroffen technische maatregelen (zijn ze toereikend, gezien de stand van de techniek en gezien de wettelijke verplichtingen). Tevens evalueren operationeel directeur en hoofd financiën en bedrijfsvoering de getroffen organisatorische maatregelen.
Op basis van deze evaluaties worden eventueel noodzakelijke aanvullende maatregelen getroffen.

6.4 Arbeidsovereenkomsten

In elke arbeidsovereenkomst wordt een passage opgenomen m.b.t. databeveiliging met de volgende tekst 'De medewerker is zich bewust van de risico's die bestaan bij het gebruik en de verwerking van persoonsgegevens en zal te allen tijde de procedures in het 'Protocol IZB en databeveiliging' (waaronder maar niet daartoe beperkt het verbod op het onrechtmatig aan derden ter beschikking stellen van deze data) en de aanwijzingen van de

systeembeheerder over de bescherming van gegevens opvolgen, zowel bij gebruik van de computers op het kantoor van de werkgever, van een laptop van de werkgever als bij het gebruik van een privé computer of laptop'.

Voorts wordt in elke arbeidsovereenkomst een passage opgenomen m.b.t. geheimhouding en het vertrouwelijk omgaan met gegevens van de organisatie en de relaties van de organisatie.

Overtreden van het verbod op lekken van data kan disciplinaire maatregelen tot gevolg hebben, waaronder ontslag op staande voet.

6.5 Verwerkersovereenkomsten

Met alle leveranciers, die gebruik maken van of inzicht (kunnen) hebben in persoonsgegevens wordt een verwerkersovereenkomst aangegaan, waarin de gewenste interne waarborgen bij de verwerker worden vastgelegd. In bijlage 4 is een overzicht opgenomen van de eisen, die de IZB aan de verwerkersovereenkomst stelt. Op grond van deze eisen heeft de IZB een standaard verwerkersovereenkomst opgesteld, die door de verwerkers getekend dient te worden.
Van bestaande leveranciers die weigeren een verwerkersovereenkomst te sluiten, wordt afscheid genomen.
De IZB werkt alleen met betrouwbare partijen. Bij het aangaan van nieuwe relaties met verwerkers van persoonsgegevens wordt actief gecontroleerd welke waarborgen er zijn dat deze relaties zorgvuldig en op een veilige wijze met de persoonsgegevens omgaat. Nieuwe relaties worden uitsluitend aangegaan als er sprake is van een verwerkersovereenkomst. Zonder vooraf getekende verwerkersovereenkomst mogen geen opdrachten worden uitgezet c.q. gegevensbestanden worden verzonden.

De partijen waarmee een verwerkersovereenkomst[10] aangegaan wordt zijn:

- Drukkerijen die bladen of communicatie-uitingen drukken en verzenden naar door de IZB aangeleverde adressen.
- ICT adviseur
- Microloon

[10] In formele zin zijn ook bankrelaties, de Belastingdienst en het Pensioenfonds PFZW aan te merken als bewerkers van persoonsgegevens. Na ingewonnen advies gaat de IZB er van uit dat het niet noodzakelijk is voor deze partijen een verwerkersovereenkomst aan te gaan.
De externe accountant wordt evenmin aangemerkt als verwerker, maar dient een verklaring af te geven dat de technische en organisatorische maatregelen, die getroffen zijn, toereikend zijn voor de bescherming van de persoonsgegevens.

- Oudshoorn Consultants (salarisverwerkingsbureau)
- I-funds (adviseur voor CRM)
- 2 Control (adviseur voor NAV)
- Website facilitator (indien deze aanmelding van personen faciliteert)
- Lokale Dabarcommissies[11]

In nieuw te sluiten 'hoofd'overeenkomsten met verwerkers worden de volgende bepalingen opgenomen:

1. Naast deze overeenkomst is een verwerkersovereenkomst gesloten tussen partijen. Bij strijdigheid tussen de bepalingen van de overeenkomst en van de verwerkersovereenkomst prevaleren de bepalingen uit de verwerkersovereenkomst.
2. Indien opdrachtnemer zich niet houdt aan de bepalingen uit de verwerkersovereenkomst, heeft opdrachtgever het recht met onmiddellijke ingang, dat wil zeggen zonder inachtneming van enige opzegtermijn te beëindigen. In verband met beëindiging van enige overeenkomst als bedoeld in de vorige volzin, heeft opdrachtgever jegens opdrachtnemer nimmer recht op schadevergoeding en/of compensatie.

6.6. Werkproces vastlegging persoonsgegevens

Persoonsgegevens van de hierna genoemde categorieën relaties worden *uitsluitend* in CRM vastgelegd.

- Leden van de vereniging.
- Overige donateurs.
- Abonnees op door de IZB uitgegeven bladen
- Personen die zich inschrijven voor nieuwsbrieven (algemeen of afdeling)
- Deelnemers cursussen.
- Vrijwilligers Dabar.
- Overige betrokkenen bij werkvelden van de IZB.

Er worden geen andere registraties bijgehouden, zoals in Excel.

6.7 Functionaris gegevensbescherming

Het hoofd financiën en bedrijfsvoering wordt met ingang van 1 september 2017 aangesteld als functionaris gegevensbescherming.

[11] Voor lokale Dabarcommissies worden bepalingen naar analogie van de verwerkersovereenkomst standaard in de overeenkomst met de commissie opgenomen.

6.8 Wijzigingen werkprocessen

Bij wijzigingen van werkprocessen m.b.t. persoonsgegevens wordt getoetst of het nieuwe werkproces past binnen de wet en het privacy beleid van de organisatie[12]. De inhoud van de toets en de besluitvorming worden vastgelegd ten behoeve van eventuele latere verantwoording van de gemaakt keuze.
De functionaris voor gegevensbescherming is verantwoordelijk voor de registratie van de besluitvorming.

6.9 Geen ter beschikking stelling aan derden

Verwerkte gegevens worden uitsluitend gebruikt voor het doel waarvoor ze gebruikt worden. Gebruik vindt plaats door de IZB en door de contractueel ingeschakelde bewerker. Gegevens worden nimmer aan overige derden ter beschikking gesteld, niet tegen betaling en evenmin om niet.

6.10 Vastleggingen in de personeels- en salarisadministratie

Ten behoeve van de opgave van verstrekte vergoedingen aan de Belastingdienst worden bijzondere personeelsgegevens vastgelegd, waaronder het BSN-nummer. Vastlegging van de (bijzondere) personeelsgegevens in de personeels- en salarisadministratie vindt plaats in verband met de daartoe door de Belastingdienst opgelegde verplichting. Na het verstrijken van de wettelijke bewaartermijn van 7 jaar na het einde van het dienstverband worden deze gegevens in het daarop volgende kalenderjaar vernietigd.

6.11 Vastleggingen ten behoeve van Belastingdienst

Ten behoeve van de opgave van verstrekte vergoedingen aan de Belastingdienst worden bijzondere personeelsgegevens vastgelegd, met name het BSN-nummer. In het declaratieformulier voor dergelijke vergoedingen wordt ter informatie van de betrokkene de volgende voetnoot opgenomen: ‘Vastlegging van de (bijzondere) personeelsgegevens in dit document vindt plaats in verband met de daartoe door de Belastingdienst opgelegde verplichting. Na het verstrijken van de wettelijke bewaartermijn van 7 jaar worden deze gegevens vernietigd.’

6.12 Gebruik van laptops of eigen computers thuis

Eigen of zakelijke laptops of eigen computers thuis mogen alleen gebruikt worden als het volgende in acht genomen wordt:

[12] Voorbeeld: een nieuwe vorm van profilering (specifieke selectie van gegevens) wordt toegepast.

- Medewerkers gaan, ook tijdens dienstreizen of woon-werkverkeer, zorgvuldig om met computers en gegevensbestanden die persoonsgegevens bevatten.
- Er wordt alleen via RDS of VPN verbinding gemaakt met het systeem van de IZB.
- Persoons- en andere gegevens mogen niet lokaal opgeslagen worden; data van de organisatie worden uitsluitend op de server opgeslagen.
  Let wel: ook via Outlook binnengehaalde zakelijke e-mail kan persoonsgegevens bevatten
- Computers en dragers van gegevensbestanden worden beveiligd met een password.
- Passwords inzake toegang tot het systeem van de IZB mogen niet op computers of gegevensdragers worden opgeslagen.

6.13 E-mailverkeer via mobiele telefoon

Na toestemming van de functionaris voor gegevensbescherming is het toegestaan zakelijke e-mails op de mobiele telefoon te ontvangen. Deze mogelijkheid wordt geboden onder de strikte voorwaarde dat de mobiele telefoon met een password beveiligd is.

6.14 Disclaimer in uitgaande e-mails

Er wordt een standaard disclaimer in *alle* uitgaande e-mails opgenomen met de volgende tekst:
'De informatie verzonden met dit e-mailbericht is uitsluitend bestemd voor de geadresseerde[n] en kan persoonlijke of vertrouwelijke informatie bevatten, beschermd door wettelijke regels m.b.t. databescherming. Gebruik van deze informatie door anderen dan de geadresseerde[n] en gebruik door hen die niet gerechtigd zijn van deze informatie kennis te nemen, is verboden. Indien u niet de geadresseerde bent of niet gerechtigd bent tot kennisneming, is openbaarmaking, vermenigvuldiging, verspreiding en/of verstrekking van deze informatie aan derden niet toegestaan en wordt u verzocht dit bericht terug te sturen en het origineel te vernietigen'.

6.15 Beveiliging van te verzenden gegevensbestanden met een password

Verzenden van gegevensbestanden per mail, via Wetransfer en andere manieren van digitale overdracht (bijvoorbeeld aan een drukkerij) vindt alleen plaats met beveiliging van het bestand met een password.
Passwords worden niet gelijktijdig respectievelijk via een ander kanaal met de bewerker van de gegevens gecommuniceerd.

6.16 Toestemming vragen voor vastlegging van persoonsgegevens

In CRM wordt een invulveld ‘toestemming gegeven’ opgenomen, waar ja of nee vermeld kan worden. Bij vermelding ‘ja’ wordt de vorm van toestemming vermeld, zoals: op eigen verzoek, via webformulier.
In beginsel worden persoonsgegevens alleen opgenomen na ontvangen toestemming van de betrokkene.
Voor bestaande relaties per 1 oktober 2017 (die al regelmatig met post etc. benaderd zijn en van wie daarom verondersteld wordt dat zij impliciet toestemming gegeven hebben) wordt standaard ‘ja’ vastgelegd met de reden ‘bestaande relatie per 01-10-2017’.

In enkele gevallen worden namen op initiatief van de IZB toegevoegd, bijvoorbeeld van predikanten uit het achterland. Er moet dan een verwerkingsgrond zijn, zoals het belang van realiseren van de doelstelling en het belang van fondsenwerving. De functionaris voor gegevensbescherming houdt een overzicht van verwerkingsgronden bij. Bij twijfel is overleg met deze functionaris verplicht.

6.17 Vernietigen fysieke documenten

Documenten waarop personeelsgegevens zijn vastgelegd (zoals dagafschriften bank, geprinte e-mails met aanmeldingsgegevens, machtigingskaarten) worden digitaal bewaard. De originele documenten worden niet bij het oud papier gedaan, maar vernietigd in de papiervernietiger of verzameld om periodiek aan een vernietigingsbedrijf aangeboden te worden.

Maatregelen die op langere termijn overwogen worden

6.18 Update rechtenstructuur mappen op server, NAV en CRM

In de loop van 2018 zal een update van de rechtenstructuur voor de mappen op de server, voor het boekhoudprogramma NAV en voor de database met persoonsgegevens CRM plaats vinden.

Bijlage 1 Dataregister IZB

Naam en contactgegevens van de verantwoordelijke + vertegenwoordiger van de verantwoordelijke

IZB, vereniging voor zending in Nederland
t.a.v. de heer G.J. de Groot, operationeel directeur
Breestraat 59-61
3811 BH Amersfoort
T: 033 46 11 949
E: directie@izb.nl

Naam en contactgegevens van de functionaris voor gegevensbescherming

IZB, vereniging voor zending in Nederland
t.a.v. de heer P.J. Oudshoorn, hoofd administratie en bedrijfsvoering
Breestraat 59-61
3811 BH Amersfoort
T: 033 46 11 949
E: p.oudshoorn@izb.nl

Categorieën betrokkenen

- Leden van de vereniging.
- Overige donateurs.
- Abonnees op door de IZB uitgegeven bladen
- Personen die zich inschrijven voor nieuwsbrieven (algemeen of afdeling)
- Deelnemers cursussen.
- Debiteuren en crediteuren in NAV
- Personeelsleden.
- Bestuursleden.
- Derden aan wie een fiscaal belaste vergoeding wordt betaald.
- Vrijwilligers Dabar.
- Overige vrijwilligers.
- Stagiaires.

Doeleinde en rechtsgrondslag voor gegevensverwerking

Leden van de vereniging

Doeleinden: creëren ledenbestand; informatieverstrekking aan leden; inning contributies.

Rechtsgrondslag: aanmelding als lid (expliciete toestemming).

Overige donateurs

Doeleinden: creëren ledenbestand; informatieverstrekking aan leden; inning contributies.

Rechtsgrondslag: aanmelding als lid (expliciete toestemming).

Abonnees op door de IZB uitgegeven bladen

Doeleinden: creëren bestand van abonnees; facturering en inning abonnementsgelden.

Rechtsgrondslag: aanmelding als abonnee (expliciete toestemming).

Personen die zich inschrijven voor nieuwsbrieven (algemeen of afdeling)

Doeleinden: creëren van bestand van ontvangers van nieuwsbrieven

Rechtsgrondslag: eigen aanmelding (expliciete toestemming).

Deelnemers cursussen.

Doeleinden: registratie van cursisten; facturering deelnemersbijdragen

Rechtsgrondslag: eigen aanmelding (expliciete toestemming).

Debiteuren en crediteuren in NAV

Doeleinden: financiële afwikkeling vorderingen en schulden, voortvloeiend uit de bedrijfsvoering.

Rechtsgrondslag: overeenkomsten met afnemers en leveranciers.

Personeelsleden.

Doeleinden: personeelsadministratie, salarisadministratie, aangifteplicht Belastingdienst en PFZW

Rechtsgrondslag: arbeidsovereenkomst; fiscale wet- en regelgeving,

Bestuursleden.

Doeleinden: registratie van bestuursleden

Rechtsgrondslag: benoemd door leden en aanvaarding van de benoeming (expliciete toestemming)

Derden aan wie een fiscaal belaste vergoeding wordt betaald.

Doeleinden: financiële administratie; jaarlijkse opgave aan Belastingdienst

Rechtsgrondslag: fiscale wet- en regelgeving

Vrijwilligers Dabar.

Doeleinden: registreren van vrijwilligers die bij de activiteiten van Dabar betrokken zijn

Rechtsgrondslag: eigen aanmelding (met expliciete toestemming op aanmeldingsformulier)

Overige vrijwilligers.

Doeleinden: registreren van vrijwilligers die bij de activiteiten van de IZB betrokken zijn

Rechtsgrondslag: vrijwilligersovereenkomst (met expliciete toestemming)

Andere betrokkenen bij werkvelden van de IZB.

Doeleinden: communicatie met betrokkenen bij de verschillende werkvelden en bestaande projecten.
Rechtsgrondslag: gerechtvaardigd belang in het kader van de uitvoering van de doelstelling.
Stagiaires.
Doeleinden: registreren van personeelsgegevens van stagiaires; salarisadministratie (indien van toepassing)
Rechtsgrondslag: aanvullende stageovereenkomst (met expliciete toestemming)

Voorgenomen categorieën ontvangers (bewerkers) van persoonsgegevens

- Alle gegevens: kantoormedewerkers van de IZB en ICT-adviseurs (Continue IT; Ifunds; 2-Control)
- M.b.t. leden, overige donateurs, abonnees op bladen: drukkerijen en verzendhuizen
- Ontvangen donaties: bankrelatie.
- Gegevens vrijwilligers Dabar: lokale Dabarcommissies.
- Personeelsgegevens: Microloon, externe salarisadministrateur, Belastingdienst en PFZW
- Betalingen aan derden: Belastingdienst.

Verstrekking van persoonsgegevens aan een derde land of een internationale organisatie
Verstrekking van persoonsgegevens aan een derde land of aan een internationale organisatie is bij de IZB niet van toepassing.

(Voorgenomen) bewaartermijnen
In beginsel hanteert de IZB een bewaartermijn van 7 jaar. In de meeste gevallen worden financiële gegevens vastgelegd. De organisatie dient rekening te houden met de wettelijke bewaartermijn van 7 jaar. D.w.z. na afloop van het desbetreffende kalenderjaar worden gegevens nog 7 volle kalenderjaren bewaard.
Bij opzegging van het lidmaatschap, bij een verzoek om uit het bestand te worden verwijderd en bij overlijden wordt de relatie gedeactiveerd (status ‘inactief’ met als reden van de status resp. ‘inactief’ en ‘overleden’). Tot en met medio 2017 werden de gegevens niet gewist, mede om te voorkomen dat de relatie opnieuw aangemaakt zou worden.
In verband met de wettelijke bewaarplicht en het recht op vergetelheid (die deels strijdig met elkaar zijn) wordt het volgende afgesproken: naam, woonplaats en ontvangsten blijven gedurende de bewaartermijn bestaan; gegevens als adres, postcode, telefoonnummer, e-mailadres en bankrekeningnummer worden gewist.

Rechten van de betrokkenen

De IZB respecteert de (wettelijke) rechten van betrokkenen, te weten:

- Recht op inzage
  Op verzoek wordt schriftelijk (al dan niet per e-mail) inzage verstrekt aan betrokkenen in de persoonsgegevens, die m.b.t. hen zijn vastgelegd.
- Recht op rectificatie
  Als een verzoek om rectificatie wordt gedaan, wordt dit gehonoreerd, waarbij de betrokkenen een terugkoppeling ontvangen.
- Recht op vergetelheid
  Bezwaar maken tegen verwerking
  Intrekken eerder gegeven toestemming
  Gegevens worden verwijderd als a) de gegevens niet langer nodig zijn, b) betrokkene bezwaar maakt tegen de vastlegging, c) eerder gegeven toestemming ingetrokken wordt, d) er geen gerechtvaardigde grondslagen voor verwerking zijn). Hierbij wordt rekening gehouden met de wettelijke bewaartermijnen (zie hiervoor).
- Recht op dataportabiliteit
  Als de vraag zich voordoet zullen de gewenste gegevens op een toegankelijke manier ter beschikking gesteld worden.
- Recht om een klacht in te dienen bij Autoriteit Persoonsgegevens
  In de privacy statement zal deze mogelijk onder de aandacht van de betrokkenen worden gebracht.

Geautomatiseerde besluitvorming

Het CRM-systeem biedt de mogelijkheid geautomatiseerd doelgroepen te selecteren voor campagnes en mailings. Bij het selecteren van geadresseerden van campagnes en mailings maakt de IZB gebruik van deze mogelijkheid.

Algemene beschrijving van de beveiligingsmaatregelen

De beveiligingsmaatregelen betreffen zowel technische als organisatorische maatregelen. Deze zijn opgesomd in het Protocol Databeveiliging. Jaarlijks wordt, mede op basis van de stand van de techniek, geëvalueerd of de beveiligingsmaatregelen toereikend zijn.

Bijlage 2 Privacy statement IZB

Privacy statement IZB

IZB - vereniging voor zending in Nederland verwerkt persoonsgegevens en andere data in overeenstemming met de geldende wetgeving. Wij vinden uw privacy erg belangrijk en gaan zorgvuldig met uw persoonsgegevens om. Uw persoonsgegevens worden uitsluitend door of namens ons gebruikt en worden niet aan derden ter beschikking gesteld. Hieronder staat precies wat u van ons kunt verwachten en aan welke regels we ons houden.

Toepasselijkheid

Dit privacy statement is van toepassing op de verwerking van:

- de door leden, donateurs, relaties en vrijwilligers verstrekte persoonlijke informatie en
- data verkregen naar aanleiding van uw bezoek aan en gebruik van onze website.

Verwerking van uw gegevens

IZB houdt een leden- en donateursadministratie bij, waarin ook persoonsgegevens van andere relaties worden vastgelegd. Relaties zijn personen die een cursus bij IZB hebben gedaan, zich hebben opgegeven voor een nieuwsbrief of (als vrijwilliger) bij een van onze programma's betrokken is, maar geen lid of donateur zijn.

IZB is een vereniging voor zending in Nederland en roept haar relaties via acties en campagnes op om een bijdrage te leveren aan de doelstelling van onze vereniging. Het werk van IZB wordt voornamelijk gefinancierd door giften van leden en donateurs. Wij verzamelen persoonsgegevens (naam, adres, woonplaats, telefoonnummer, e-mailadres, geboortedatum en kerkelijke achtergrond) om u gericht te kunnen informeren over ons werk en om u te vragen om financiële ondersteuning daarvan. Het verzamelen van persoonsgegevens gebeurt via de website wanneer u zich aanmeldt voor een van onze nieuwsbrieven, bladen, cursussen of acties en wanneer u zich aanmeldt als lid, donateur of als vrijwilliger. Ook vindt persoonlijke werving plaats via een aanmeldformulier of een telefoongesprek. IZB maakt van tijd tot tijd gebruik van diensten van derden om het relatiebestand aan te vullen en te actualiseren. In alle gevallen vragen wij u om daar expliciet toestemming voor te verlenen.

Financiële data en persoonsgegevens worden verzameld om uitvoering te geven aan de overeenkomst (donatie, lidmaatschap). Deze gegevens worden niet aan derden verstrekt voor commerciële doeleinden.

IZB heeft een CBF-erkenning voor goede doelen en de ANBI-status.

Gegevens inzien, wijzigen of verwijderen
U kunt op elk moment inzage vragen in de gegevens die wij over u hebben vastgelegd of deze laten wijzigen of verwijderen. U kunt uw wijzigingen telefonisch doorgeven aan de administratie van IZB: 033 - 461 1949 (tijdens kantooruren) of per e-mail: info@izb.nl.

Hier kunt u ook terecht als u niet langer op de hoogte gehouden wilt worden van onze activiteiten. IZB is verplicht om een bewijs van identiteit te vragen voordat wij u informatie mogen verstrekken over uw persoonlijke gegevens in onze administratie. U kunt ook een verzoek indienen per brief, voorzien van uw naam, adres, telefoonnummer en een kopie van een geldig legitimatiebewijs, gericht aan de administratie van IZB, Breestraat 59-61, 3811 BH Amersfoort.

E-mail
Wanneer u als abonnee van één van onze nieuwsbrieven of bladen, als lid, donateur of informatieaanvrager uw e-mailadres aan IZB hebt verstrekt, wordt u per e-mail geïnformeerd, om u op de hoogte te brengen van ons werk en behaalde resultaten en voor incidentele verzoeken om een financiële bijdrage.
IZB maakt bij het verzenden van e-mailnieuwsbrieven gebruik van een systeem waarbij inzicht wordt verkregen over de wijze waarop deze e-mails worden geopend. Ook kan bekeken worden of je de links in onze e-mail aanklikt. Op deze wijze kan IZB haar informatie aan jou verder optimaliseren en beter afstemmen op jouw interesses. Ons registratiesysteem maakt het ook mogelijk om selecties aan te maken, waardoor wij meer gericht specifieke doelgroepen kunnen benaderen.

Afmelden e-mail nieuwsbrieven of actienetwerken
Wilt u minder of geen berichten van ons ontvangen? Dan kunt u zich op elk moment afmelden bij de administratie van IZB, telefonisch: 033 - 461 1949 (tijdens kantooruren) of per e-mail: info@izb.nl.

Contact met leden, donateurs en relaties
IZB informeert haar leden en donateurs over haar werk via bladen, per e-mail, post, telefoon en/of sociale media. Regelmatig wordt daarbij een verzoek gedaan het werk van de IZB te steunen door een financiële bijdrage en gebed.

Bezoek aan onze website
IZB gebruikt op haar website geen cookies. Uw gegevens worden niet met derden uitgewisseld.

Beveiliging

IZB heeft technische en organisatorische maatregelen genomen om persoonlijke gegevens te beschermen tegen verlies of elke vorm van onwettige verwerking. Op deze manier zorgen we ervoor dat persoonsgegevens alleen toegankelijk zijn voor medewerkers die daar vanuit hun functie toe bevoegd zijn en dat we de persoonsgegevens alleen gebruiken voor de doeleinden waarvoor ze zijn verkregen en daarmee verenigbare doeleinden.

Vragen over privacybeleid

IZB houdt het recht het privacybeleid te wijzigen. Als u vragen hebt over dit beleid, neem dan contact op met onze functionaris voor gegevensbescherming. Zijn gegevens vindt u aan het eind van dit document.

Contactgegevens

Onze contactgegevens voor vragen / opmerkingen / klachten m.b.t. de verwerking van persoonsgegevens zijn:

IZB, vereniging voor zending in Nederland
t.a.v. de heer P.J Oudshoorn, functionaris voor gegevensbescherming
Breestraat 59-61
3811 BH Amersfoort
T: 033 46 11 949
E: p.oudshoorn@izb.nl

Privacy beleid IZB - vereniging voor zending in Nederland. Versie: 6 juli 2017.

Bijlage 3 Privacy beleidsplan (versie 6 juli 2017)

Dataregister

De IZB heeft een dataregister, dat voldoet aan de wettelijke vereisten. In het register zijn derhalve de volgende gegevens opgenomen:

- de naam en contactgegevens van de verantwoordelijke;
- de doeleinden voor gegevensverwerking;
- een beschrijving van de categorieën betrokkenen en categorieën persoonsgegevens;
- de (voorgenomen) categorieën ontvangers;
- een vermelding van een verstrekking van persoonsgegevens aan een derde land of een internationale organisatie;
- de (voorgenomen) bewaartermijnen;
- een algemene beschrijving van de beveiligingsmaatregelen.

Het dataregister wordt aangepast, zodra actuele ontwikkelingen daartoe aanleiding geven.

Agendering in DTO (directieteamoverleg) en bestuur

Het onderwerp 'Persoonsgegevens en databeveiliging' wordt zowel in het DTO als in het bestuur ten minste één maal per jaar geagendeerd.

Datalekprocedure

De IZB heeft een datalekprocedure. Deze 'Interne procedure bij het constateren van een datalek' is mede gebaseerd op de beleidsregels van de Autoriteit Persoonsgegevens en is dwingend van toepassing zodra een datalek geconstateerd/gemeld wordt.

Rechten van betrokkenen

De IZB respecteert de rechten van de betrokkenen, zoals deze in de wet zijn neergelegd, te weten:

- het recht op inzage
  (betrokkene heeft recht om te weten welke categorieën persoonsgegevens worden verwerkt, wat het doel van deze verwerking is, welke bewaartermijnen gelden, de logica die ten grondslag ligt aan de automatische gegevensverwerking; de IZB heeft dit vastgelegd in het dataregister / privacy statement)
- het recht op rectificatie
  (betrokkene heeft het recht op rectificatie van onjuiste vastleggingen en ontvangt een terugmelding dat de rectificatie heeft plaats gevonden)

- het recht op vergetelheid
  (niet-actieve relaties worden na 7 jaar verwijderd; op verzoek worden relaties gedeactiveerd, waarbij beperkte gegevens achterblijven om te voorkomen dat een relatie opnieuw wordt geactiveerd en waarbij financiële gegevens niet verwijderd worden gedurende de wettelijke bewaartermijn)
- het recht op dataportabiliteit
  (dat is het recht van een betrokkene om de m.b.t. hem of haar vastgelegde gegevens te ontvangen voor persoonlijk (her)gebruik of om door te geven aan een derde)

Bijlage 4 Interne procedure bij het constateren van een datalek

Als een datalek geconstateerd wordt, worden de volgende maatregelen genomen:

1 De medewerker die een datalek constateert meldt dit onverwijld bij de functionaris voor gegevensbescherming.

2 Het IT-bedrijf wordt (afhankelijk van de aard van het datalek) ingeschakeld om de mogelijke consequenties van de datalek in beeld te brengen.

3 Operationeel directeur, functionaris voor gegevensbescherming en een medewerker van het IT-bedrijf stellen gezamenlijk vast of sprake is van een datalek dat gemeld moet worden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen. Leidend hierbij zijn de beleidsregels die door de Autoriteit Persoonsgegevens zijn opgesteld.

4 Met betrekking tot de melding aan betrokkenen worden tevens de volgende afwegingen gemaakt:
- was het gelekt bestand adequaat versleuteld?
- was er sprake van bijzondere/gevoelige persoonsgegevens?
- zijn er deugdelijke back-ups, die in staat stellen gelekte gegevens terug te plaatsen.

5 Melding vindt onverwijld plaats (zo mogelijk binnen 72 uur).

6 Er wordt een besluit genomen over te nemen maatregelen, die herhaling van het datalek zoveel mogelijk voorkomen c.q. de gevolgen van het datalek zoveel mogelijk beperken:
- maatregelen die direct genomen moeten worden;
- structurele maatregelen, zowel op het gebied van technische beveiliging als organisatorisch.

7 Implementatie van de genomen besluiten op korte termijn.

8 Onder verantwoordelijkheid van de functionaris voor gegevensbescherming wordt een register bijgehouden waarin de geconstateerde datalekken worden opgenomen, inclusief de afwegingen waarom er wel of niet gemeld wordt.

Bijlage 5 Eisen die de IZB stelt aan een verwerkersovereenkomst

De verwerkersovereenkomst, die aangegaan wordt met dienstverleners, mag een model zijn dat door een beroeps- of belangenorganisatie van de desbetreffende sector is vastgesteld. Daarbij geldt echter als eis dat de voorschriften van de AVG daarin geheel zijn verwerrkt, dat wil zeggen dat ten minste het volgende is opgenomen:

- Nadere omschrijving van onderwerp en duur van de verwerking.
- Aard en doeleinden van de verwerking.
- Soort persoonsgegevens en categorieën van betrokkenen.
- De bewerker houdt een dataregister bij conform de wettelijke bepalingen.
- De toegestane bewaartermijn die de bewerker hanteert.

Bijlage 6 Voor de IZB relevante voorwaarden, deel uit makend van het Vrijstellingenbesluit

Voor **leden of begunstigers van verenigingen** of stichtingen gelden de volgende voorwaarden:

- De verwerking geschiedt slechts voor:
  - de activiteiten die gelet op de doelstelling van de vereniging, stichting of publiekrechtelijke beroepsorganisatie gebruikelijk zijn of die door de ledenvergadering zijn goedgekeurd;
  - het verzenden van informatie aan de betrokkenen;
  - het bekend maken van informatie over betrokkenen en activiteiten van de vereniging, stichting of publiekrechtelijke beroepsorganisatie na instemming van de ledenvergadering, voorzover aanwezig, op de eigen website;
  - het berekenen, vastleggen en innen van contributies en giften, waaronder begrepen het in handen van derden stellen van vorderingen, alsmede andere activiteiten van intern beheer;
  - het behandelen van geschillen en het doen uitoefenen van accountantscontrole.
- Geen andere persoonsgegevens worden verwerkt dan:
  - naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, alsmede bank- en girorekeningnummer van de betrokkene;
  - een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
  - gegevens als bedoeld onder a, van de ouders, voogden of verzorgers van minderjarige leden of begunstigers;
  - gegevens betreffende het lidmaatschap of de begunstiging, waaronder begrepen de aard daarvan, alsmede de functie binnen en de deelname aan de activiteiten van de vereniging, de stichting of publiekrechtelijke beroepsorganisatie;
  - foto’s en videobeelden met of zonder geluid van activiteiten van de vereniging, stichting of publiekrechtelijke beroepsorganisatie;
  - gegevens met het oog op het berekenen, vastleggen en innen van contributies en giften.
- De persoonsgegevens worden slechts verstrekt aan:
  - de leden of begunstigers;
  - de ouders, voogden of verzorgers van minderjarige leden of begunstigers;
  - degenen, waaronder begrepen derden, die belast zijn met of leiding geven aan de in het tweede lid bedoelde activiteiten of die daarbij noodzakelijk zijn betrokken;

- etc.

- Gegevens op de website van de vereniging, stichting of publiekrechtelijke beroepsorganisatie worden slechts verstrekt aan:
  - de leden of begunstigers;
  - de ouders, voogden of verzorgers van minderjarige leden of begunstigers;
  - degenen, waaronder begrepen derden, die belast zijn met of leiding geven aan de in het tweede lid bedoelde activiteiten of die daarbij noodzakelijkerwijs zijn betrokken, voor zover zij daartoe door het bestuur zijn geautoriseerd.
- De verantwoordelijke draagt zorg voor een adequate toegangsbeveiliging van de website, alsmede voor een afdoende bescherming van persoonsgegevens voor verdere verwerking door zoekmachines.
- De persoonsgegevens worden verwijderd uiterlijk twee jaren nadat het lidmaatschap is beëindigd of de betrokkene te kennen heeft gegeven dat hij niet langer als begunstiger wil worden beschouwd, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht. De gegevens op de website worden onverwijld verwijderd wanneer de betrokkene of diens wettelijk vertegenwoordiger daarom verzoekt.

Voor **abonnementen** gelden de volgende voorwaarden:

- De verwerking geschiedt slechts voor:
  - het verzenden of bezorgen van de publicaties waarop het abonnement betrekking heeft en van andere informatie ten behoeve van de abonnees;
  - het berekenen, vastleggen en innen van abonnementsgelden, waaronder begrepen het in handen van derden stellen van vorderingen, alsmede andere activiteiten van intern beheer;
  - het behandelen van geschillen en het doen uitoefenen van accountantscontrole.
- Geen andere persoonsgegevens worden verwerkt dan:
  - naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, alsmede bank- en girorekeningnummer van de betrokkene;
  - een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
  - gegevens betreffende opleiding, functie of beroep, lidmaatschappen en interessegebieden, die met het oog op de aard van de publicatie redelijkerwijs van belang zijn;
  - gegevens betreffende het abonnement, waaronder begrepen de aard van het abonnement;
  - gegevens met het oog op het berekenen, vastleggen en innen van de abonnementsgelden;

- een aanduiding betreffende de reden van beëindiging van het abonnement.

- De persoonsgegevens worden slechts verstrekt aan:
  - degenen, waaronder begrepen derden, die belast zijn met of leiding geven aan de in het tweede lid bedoelde activiteiten of die daarbij noodzakelijk zijn betrokken;
  - etc.
- De persoonsgegevens worden verwijderd uiterlijk twee jaren na de beëindiging van het abonnement, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht.