DiVetro
analyse • sourcing • management

www.divetro.nl

PRIVACYBELEID

Auteur:
Werkgroep Privacybeleid

Opdrachtgever:
Functionaris Gegevensbescherming (FG)

Versie 1.0
Status: Goedgekeurd
Vertrouwelijkheid: Openbaar

DiVetro
analyse • sourcing • management

www.divetro.nl

Versiebeheer

VERSIE	DATUM	STATUS	AUTEUR
0.1	*10-04-2018*	*concept*	*Werkgroep AVG*
0.2	*13-04-2018*	*concept*	*Werkgroep AVG*
0.6	*13-04-2018*	*concept*	*Werkgroep AVG*
0.9	*19-4-2018*	*concept*	*Werkgroep AVG*
1.0	*24-05-2018*	*definitief*	*Job van Weeren*

Geraadpleegde bronnen

AUTORITEIT	BRON
Autoriteit Persoonsgegevens	https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wet-bescherming-persoonsgegevens https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/europese-privacywetgeving
Centrum informatiebeveiliging en privacybescherming	https://www.cip-overheid.nl/

DiVetro
analyse • sourcing • management

www.divetro.nl

INLEIDING

Toelichting Privacybeleid

Dit document beschrijft het Privacybeleid van DiVetro. Het beantwoordt aan de eisen van de huidige wetgeving. Het geeft aan waarom het Privacybeleid voor DiVetro noodzakelijk is, wat de uitgangspunten zijn en op welke manier het in de organisatie en beleidscyclus verankerd is.

Het is een normatief en richtinggevend plan, dat voorschrijft hoe binnen DiVetro met persoonsgegevens wordt omgegaan en welke ontwikkeling wij willen doormaken. Het document beschrijft ook de maatregelen die worden getroffen om het Privacybeleid te vertalen in levende praktijk.

Het Privacybeleid heeft betrekking op het beschermen van Persoonsgegevens van alle Betrokkenen binnen DiVetro waaronder in ieder geval alle medewerkers, klanten, gasten, bezoekers en externe relaties evenals op andere Betrokkenen waarvan DiVetro Persoonsgegevens verwerkt.

De Algemene Verordening Gegevensbescherming (AVG)

Op 25 mei 2016 is de (Europese) Algemene Verordening Gegevensbescherming (hierna: AVG) in werking getreden. Deze nieuwe wetgeving moet zorgen voor harmonisatie van de huidige privacyregelgeving in Europa en een verbetering van de privacy(bescherming) van burgers.

De oude privacyregelgeving (uit 1995) werd vastgesteld toen internet nog in de kinderschoenen stond. Bij de nieuwe regelgeving gaat het daarom vooral om het beschermen van persoonsgegevens in de digitale wereld. De Europese Unie wil met deze AVG het vertrouwen bij burgers en consumenten in de verwerking van persoonsgegevens door overheid en bedrijven vergroten.

Waarom dit Privacybeleid belangrijk is voor alle klanten en medewerkers?

Opslag en verwerking van Persoonsgegevens is noodzakelijk bij vrijwel alle bedrijfsvoeringsprocessen. De opslag en verwerking van deze gegevens dient met de grootst mogelijke zorgvuldigheid te gebeuren omdat misbruik van Persoonsgegevens grote schade kan berokkenen aan klanten, medewerkers en andere Betrokkenen.

DiVetro hecht veel waarde aan het beschermen van de Persoonsgegevens die aan haar worden verstrekt en aan de wijze waarop deze Persoonsgegevens worden verwerkt binnen DiVetro.

Ver- of ontvlechting informatiebeveiliging en privacy (IBP)

Er bestaat een belangrijke relatie tussen de beschermingsmaatregelen ter bescherming van privacy en informatiebeveiliging. Desalniettemin zien we ook een groot aantal verschillen, zoals bij het beleggen van verantwoordelijkheden en bij de inrichting van processen. Bij DiVetro is bewust gekozen voor een apart Informatiebeveiligingsbeleid en een apart Privacybeleid. Daarmee is exact duidelijk waar beide onderwerpen van elkaar verschillen. Bij het uitwerken van het beleid naar de organisatie is juist gekeken naar wat beide onderwerpen gemeenschappelijk hebben om de organisatie zo efficiënt mogelijk in te richten.

Doelstelling privacybeleid

Het privacybeleid heeft als primair doel de privacy van klanten, medewerkers en derden te waarborgen. Het is de leidraad voor alle activiteiten die verband houden met privacy.

BELEIDSUITGANGSPUNTEN EN PRIVACYPRINCIPES

Beleidsuitgangspunten privacy

Het beleid kent de volgende uitgangspunten:

- DiVetro is een betrouwbare en eerlijke (integere) organisatie die vanuit zichzelf gemotiveerd is om te handelen conform geldende wet- en regelgeving en zichzelf opgelegde normen.
- Integer en compliant handelen is een mentaliteit, geen set afdwingbare regels. Veilig en betrouwbaar omgaan met informatie in het dagelijkse werk is ieders professionele verantwoordelijkheid en zit bij ons “tussen de oren”.
- Het privacybeleid is in lijn met en ondersteunt de strategie van DiVetro.
- Het privacybeleid geldt voor alle interne en externe medewerkers en verwerkers van DiVetro.
- Bescherming van persoonsgegevens wordt pragmatisch toegepast waarbij wordt gestreefd naar een goede balans tussen maatregelen en businessbehoeften.
- Privacy is een onderdeel van de integrale managementverantwoordelijkheid.
- Het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging en privacy te toetsen aan een vastgestelde best practice of norm en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen.
- Informatiebeveiliging en privacy zijn een continu proces. Informatiebeveiligings- en Privacybeleid wordt op procesniveau geïmplementeerd en uitgevoerd.
- DiVetro is eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert DiVetro informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers, gasten en klanten zijn goed geïnformeerd over de regelgeving voor het (her)gebruik van deze informatie.

Privacyprincipes

Om aan bovenstaande beleidsuitgangspunten te voldoen gelden de volgende privacyprincipes:

Doelbinding

Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de Verwerking geformuleerd.

Zo weinig mogelijk gegevens

Bij een Verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de Persoonsgegevens die strikt noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn.

Redelijke verhouding

Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde.

Kwaliteit van persoonsgegevens

Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.

Altijd versleutelen

Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen.

Niet doorgeven aan derden

Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

Geen koopwaar

Divetro verkoopt geen persoonsgegevens.

Zo kort mogelijk bewaren

Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de Verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigingstermijnen in acht genomen.

Recht op correctie

Iedere Betrokkene heeft recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van de in de afzonderlijke Verwerkingen hem betreffende Persoonsgegevens, en heeft het recht van verzet.

Recht op transparantie

De instelling kan aan Betrokkenen op transparante wijze verantwoording afleggen over welke gegevens er allemaal verzameld worden en over de verwerkingen daarvan en de daarbij gehanteerde principes.

DiVetro
analyse • sourcing • management

www.divetro.nl

Respecteer rechten	DiVetro respecteert en faciliteert waar mogelijk de rechten van klanten, medewerkers en andere betrokkenen bij het beschermen van hun persoonsgegevens die door of namens DiVetro worden verwerkt.
Recht op rectificatie	Iedere Betrokkene heeft het recht om onjuiste persoonsgegevens te (laten) rectificeren.
Recht op inzage	DiVetro kan Betrokkenen uitsluitsel geven of en zo ja welke data verzameld worden, over de verwerkingen daarvan en de daarbij gehanteerde principes
Geen geautomatiseerde besluitvorming	DiVetro neemt geen beslissingen over individueen op basis van geautomatiseerde procedés

VERWERKINGEN

Verwerkingen door DiVetro

De verwerkingen die DiVetro doet liggen vast in het verwerkingenregister.

Aan wie worden gegevens verstrekt?

De persoonsgegevens worden uitsluitend verstrekt:

- aan de betrokkenen als het om hun eigen persoonsgegevens gaat;
- aan derden
    - voor zover vermeld in de meldingen in het privacystatement
    - voor zover hiervoor een ondubbelzinnige wettelijke basis bestaat
- gegevens aan de Belastingdienst;
    - na voorafgaande expliciete en vrijwillige toestemming van de betrokkene;
    - op gerechtelijk verzoek of bevel;
    - na zorgvuldige afweging van de FG in het geval van ernstige inbreuk op de privacy van een derde persoon, dan wel in het kader van waarheidsvinding.
- voor historisch, statistisch of wetenschappelijk onderzoek
    - met expliciete, schriftelijke toestemming van de betrokkenen;
    - of op basis van een melding van de verwerking bij de FG.

Hoe gaan wij om met verwerkers?

- DiVetro streeft naar verwerkersovereenkomsten met alle bewerkers.
- Met alle nieuwe bewerkers (of bij vernieuwing van bestaande contracten) wordt standaard een verwerkersovereenkomst afgesloten.
- DiVetro verzekert zich regelmatig, lopende de contracttermijnen, van de door de verwerker toegepaste (en aan de stand van de techniek aangepaste) beveiligingsmaatregelen, behoudt zich het recht voor hiertoe ter plekke bij de verwerkers controles uit te voeren en geeft daar ook daadwerkelijk invulling aan.

ORGANISATIE VAN HET PRIVACYBELEID

Inbedding in de organisatie

Als 'verantwoordelijke' in de zin van de AVG zijn de partners verantwoordelijk voor de bescherming van de persoonsgegevens van de betrokkenen die bij, door of namens DiVetro worden verwerkt. De partners zijn verantwoordelijk voor het Privacybeleid en stellen dit vast en houden toezicht op de risico's. Het niet naleven van de privacywetgeving kan op korte termijn leiden tot reputatieschade en op middellange termijn tot aanzienlijke boetes. Daarmee wordt een onvoldoende bescherming van de persoonsgegevens een risico van materieel belang.

DiVetro heeft (op vrijwillige basis) een Functionaris voor de Gegevensbescherming (FG) aangesteld. De aanstelling is in de partnermeeting bevestigd en aangemeld bij de Autoriteit Persoonsgegevens (AP).

Een belangrijke taak van de FG is intern toezicht houden op het naleven van de privacywet. Om dit te kunnen doen, zal de FG:

- informatie verzamelen over gegevensverwerkingen binnen de organisatie;
- deze verwerkingen analyseren en beoordelen of ze aan de wet voldoen;
- informatie, adviezen en aanbevelingen geven aan de organisatie.

Voor de organisatie van de informatiebeveiliging verwijzen wij naar het informatiebeveiligingsbeleid.

Planning en controlecyclus

Privacyprocessen volgen het principe van Plan, Do, Check, Act: de kwaliteitscyclus van Deming:

- **Plan**: wat doen we. De maatregelen om de privacy te borgen zijn vastgelegd in een (meerjaren)plan.
- **Do**: wat doen we hiervoor? De maatregelen worden bij voorkeur projectmatig gerealiseerd.
- **Check**: wat doen we hiervoor? De effectiviteit van de (genomen) maatregelen wordt periodiek geëvalueerd.
- **Act**: wat doen we hiervoor? Als blijkt dat een maatregel niet voldoende (meer) functioneert worden nieuwe maatregelen gedefinieerd.

BIJLAGE A: MAATREGELEN

Om de privacy te beschermen treffen en onderhouden wij een samenhangend pakket aan maatregelen om de kwaliteit van de informatievoorziening te waarborgen. Om het totaalpakket aan maatregelen te beheersen zijn individuele maatregelen gebundeld tot een zogenaamd pakket aan basismaatregelen of “baselines”. Dit betekent dat er, in navolging van de verschillende securitybaselines, een aparte privacy baseline dient te worden opgesteld.

Maatregelen om te voldoen aan de AVG

De DiVetro privacy baseline

Een security of privacy baseline is een nadere en vooral concrete uitwerking van een aantal beschermingseisen. Een geïmplementeerde security/privacy Baseline geldt daarmee als een beschermingsmaatregel voor een specifiek deel van de informatievoorziening. De DiVetro privacy baseline bestaat uit:

- Een aantal technische maatregelen rondom de werkplek van elke medewerker (of partner). Deze technische maatregelen zijn verder uitgewerkt in het informatiebeveiligingsbeleid (denk aan het opheffen van een apparaat vergrendeling met biometrische persoonskenmerken, gegevensversleuteling van data, two-factor- authentificatie, anti-malwarebescherming, etc.)
- Tijdens de introductie van nieuwe medewerkers wordt apart aandacht geschonken aan het onderwerp privacy en informatiebeveiliging. Voor alle medewerkers zijn de belangrijkste privacythema’s terug te vinden in de ‘wegwijzer’ van DiVetro;
- Op de DiVetro website is een privacystatement gepubliceerd;
- Op de DiVetro website is een Cookiebeleid gepubliceerd;
- Er is beleid opgesteld m.b.t. bewaartermijnen;
- Er is een datalekprocedure opgesteld;
- Er is een FG aangesteld en aangemeld bij de autoriteit persoonsgegevens;
- Er is een verwerkingsregister opgesteld en het secretariaat is als beheerder daarvan aangewezen;
- Er is een template opgesteld voor een verwerkingsovereenkomst;
- Er is een afspraak gemaakt om binnen DiVetro continu te werken aan het verhogen van het privacy- (en security)bewustzijn van alle medewerkers. (awareness-sessies, blogs, etc.).

DiVetro privacy verbeterplan

Naast de DiVetro privacy baseline is er een apart privacy verbeterplan. In dit plan worden alle actuele verbetermaatregelen benoemd en geprioriteerd. Ook maatregelen als gevolg van actuele risico’s of privacy impactanalyses. Het verbeterplan onderkent een drietal maatregel categorieën gericht op:

1. Afscherming,
2. Corrigeerbaarheid
3. en Transparantie.

BIJLAGE B BEGRIPPEN

Persoonsgegevens

Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke levende persoon. Persoonsgegevens kunnen direct of indirect identificeerbaar zijn.

- **Direct identificeerbaar**: Gegevens die naar hun aard rechtstreeks betrekking hebben op een persoon, zoals iemands naam.
- **Indirect identificeerbaar**: Gegevens die naar hun aard geen betrekking hebben op een persoon worden als persoonsgegeven aangemerkt als deze mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld. Voorbeelden hiervan zijn het type huis of auto van een betrokkene, omdat dit iets zegt over het inkomen en vermogen van de betrokkene. Ook gegevens die in combinatie met andere gegevens tot identificeerbaarheid kunnen leiden worden aangemerkt als persoonsgegeven.

Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn naar hun aard of hun gedrag vertrouwelijker dan 'gewone' persoonsgegevens en verwerking ervan geschiedt op andere gronden dan 'gewone' persoonsgegevens. Dit zijn gegevens over:

- Godsdienst of levensovertuiging;
- Ras;
- Politieke gezindheid;
- Gezondheid;
- Seksuele leven;
- Lidmaatschap van een vakvereniging;
- Strafrechtelijke persoonsgegevens;
- Persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod;
- Een wettelijk voorgeschreven identificatienummer (zoals een BSN-nummer of een kentekennummer).

De verwerking van persoonsgegevens

Verwerking: het begrip 'verwerking' is heel breed en omvat alle handelingen van het creëren, opslaan, gebruiken, delen en archiveren tot de vernietiging van persoonsgegevens. Het is voor iedereen binnen DiVetro belangrijk om zich goed te realiseren dat doorgifte van persoonsgegevens naar personen en organisaties in landen binnen de EU (en dus binnen Nederland, ook tussen personen of afdelingen binnen de eigen organisatie) ook onder het algemene begrip 'verwerking' valt. Op elke doorgifte van persoonsgegevens binnen de EU zijn dus alle wettelijke eisen die voorverwerking gelden van toepassing.

De oorspronkelijke verantwoordelijke – dat is hij die het doel en de middelen voor de verwerking vaststelt – blijft dus ook na de doorgifte verantwoordelijk voor een rechtmatige omgang met persoonsgegevens en is dus ook (juridisch) aansprakelijk als er een onrechtmatigheid in de omgang met persoonsgegevens optreedt. De ontvangende partij is de bewerker van de persoonsgegevens. Tussen de verstrekker en ontvanger dient dus te allen tijden verplicht een bewerkersovereenkomst opgesteld te zijn.

Voor doorgifte van persoonsgegevens naar personen en organisaties in landen buiten de EU gelden andere/aanvullende gronden en eisen. Hoewel niet limitatief, vallen de volgende handelingen in ieder geval onder verwerking van persoonsgegevens: verzamelen;

- vastleggen,
- bewaren;
- ordenen; wijzigen;
- opvragen;
- raadplegen;
- gebruiken;
- samenbrengen;
- met elkaar in verband brengen (koppelen);
- afschermen;
- uitwissen;
- vernietigen;
- profilen;
- doorgifte (elke vorm van ter beschikkingstelling, zoals doorzending en verspreiding).

Kortom: alles wat je doet met persoonsgegevens, valt onder het begrip verwerken.