

**Beleid verwerking persoonsgegevens
Taalcentrum-VU**

versie 1.0
14 mei 2018

Inhoud

1. Vooraf.....	3
Begrippenlijst.....	3
De hoofdregel: zo min mogelijk, zo transparant mogelijk	4
Wat is de AVG? & Waarom dit document?	5
Welke gegevens verwerken wij en met welk doel?	5
2. Algemene uitgangspunten	6
Register van verwerkingen	6
Bewaartermijn.....	6
Dataminimalisatie.....	6
Vertrouwelijkheid.....	6
Rechtmatigheid en grondslag.....	6
Delen met derden	6
Rollen.....	7
3. Rechten van betrokkenen	8
Inzage	8
Correctie of verwijderen	8
Dataportabiliteit	8
4. Technische en organisatorische veiligheidsmaatregelen.....	9
Privacy by design	9
Privacy by default	9
5. Draaiboek datalekken.....	10
6. Tot slot.....	12

Dit document is opgesteld door de werkgroep AVG:

Paul Rueckert | 020-5983819

Laila de Miranda | 020-5989459

Mathilde van Arkel | 020-5982817

1. Vooraf

Begrippenlijst

De definities (vrij naar www.autoriteitpersoonsgegevens.nl) voor zover niet al expliciet toegelicht in de lopende tekst:

Begrip	Definitie
Persoonsgegeven	Elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat het gegeven ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.
Betrokkene	De betrokkene is degene van wie een organisatie persoonsgegevens verwerkt. Dit is dus degene op wie de persoonsgegevens betrekking hebben.
Verwerker	Degene (persoon of organisatie) die persoonsgegevens in opdracht van het Taalcentrum verwerkt
Verantwoordelijke	Degene (persoon of organisatie) die het doel van en de middelen voor het gebruik van persoonsgegevens bepaalt.
Verwerking	Een verwerking omvat alles wat je met een persoonsgegeven doet: opslaan, verzamelen, analyseren, doorgeven, verwijderen etc.
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming

De hoofdregel: zo min mogelijk, zo transparant mogelijk

De voornaamste gedragsregel is dat we alleen persoonsgegevens bijhouden en verwerken als dat strikt noodzakelijk is, of als er een zakelijk doel mee gediend wordt (marketingcommunicatie met name). En dat we ons bewust zijn van de gevoeligheid van de gegevens die we opvragen, opslaan en verwerken. Dat betekent:

1. We voldoen aan de bepalingen van de Algemene Verordening Gegevensbescherming (AVG) en overige wetgeving op het gebied van privacy.
2. We gaan zorgvuldig om met de persoonlijke gegevens die je aan ons toevertrouwd. We slaan je gegevens veilig en afgeschermd op (secure clouds) en we zien erop toe dat onze medewerkers en andere betrokkenen veilig met onze clouds omgaan.
3. We verkopen jouw gegevens nooit aan andere partijen.
4. Als wij jouw gegevens moeten delen met anderen, dan zorgen we ervoor dat zij daar net zo zorgvuldig mee omgaan als wij. (We sluiten overeenkomsten met externe partijen.)
5. We zorgen dat jouw en onze persoonlijke gegevens niet in handen van onbevoegden komen.
6. We verzamelen alleen gegevens die we nodig hebben; overige gegevens slaan wij niet op.
7. We bewaren je gegevens niet langer dan nodig is om onze producten en diensten goed te kunnen leveren.
8. We verplaatsen (verzenden) zo min mogelijk persoonsgegevens.
9. We zijn zo transparant mogelijk: je kunt je persoonsgegevens altijd inzien en laten aanpassen of verwijderen. Aan een verzoek daartoe geven wij gehoor, binnen de kaders van de geldende wettelijke bepalingen.
10. We zijn open en communiceren helder over ons privacybeleid.
11. We proberen voortdurend alle medewerkers van het Taalcentrum-VU ervan te doordringen dat zij zorgvuldig, bewust en veilig moeten omgaan met persoonsgegevens.

Onze hoofdregel wordt uitgewerkt in de volgende bepalingen.

Waarom dit document?

Het Taalcentrum-VU werkt met persoonsgegevens van cursisten, klanten, leveranciers en medewerkers. Deze gegevens verzamelen we om onze producten en diensten goed aan te kunnen bieden. Het Taalcentrum-VU hecht grote waarde aan ieders privacy en streeft ernaar alle persoonsgegevens die voor bedrijfsdoeleinden opgeslagen worden, toegankelijk en transparant te houden.

Sinds mei 2018 geldt in Europa een algemene wet die de bescherming van persoonsgegevens regelt: de Algemene Verordening Gegevensbescherming (AVG) of General Data Protection Regulation (GDPR). In Nederland is de Autoriteit Persoonsgegevens (het AP) verantwoordelijk voor de uitvoering van deze wet.

Dit document gaat over de verwerking van persoonsgegevens van alle betrokkenen binnen het Taalcentrum-VU. Dat behelst dus medewerkers, klanten (inclusief studenten), leveranciers en freelancers en andere geïnteresseerden (zoals mensen op een mailinglijst of sollicitanten).

Het Taalcentrum-VU heeft met dit document de volgende doelstellingen voor ogen:

- persoonlijke gegevens en ieders privacy als blijvend punt in de aandacht houden;
- transparante en toegankelijke kaders scheppen voor de verwerking van persoonsgegevens;
- een duidelijke norm/stappenplan hebben voor (nieuwe) opslag van persoonlijke gegevens;
- voldoen aan de nieuwste Europese wetgeving.

Welke gegevens verwerken wij en met welk doel?

Het Taalcentrum-VU verwerkt persoonsgegevens die we opvragen en/of ontvangen van onze klanten, medewerkers, leveranciers, en bepaalde organisaties. We verzamelen zaken als naam, adres en/of overige contactgegevens zoals e-mailadres of betalingsgegevens. Van medewerkers houden we ook 'arbogegevens' bij, zoals verzuimfrequentie en verzuimduur, salarisgegevens, en ook gegevens over hun burgerlijke staat, voor zover die voor de pensioenverzekeraar van belang zijn.

Het Taalcentrum-VU gebruikt de gegevens bijvoorbeeld voor de volgende doeleinden:

- administratie en archivering van de gegevens van de eigen werknemers;
- registratie en administratieve afhandeling van cursisten die een training volgen;
- het sturen van nieuwsbrieven en e-mails aan geïnteresseerden;
- het reageren op vragen van (potentiële) klanten;
- het voldoen aan wettelijke bepalingen, bijvoorbeeld als het gaat om de Wet Deregulering Beoordeling Arbeidsrelaties (Wet DBA), of verklaringen omtrent gedrag (vog's) van eigen mensen en externen die voor ons werken.

2. Algemene uitgangspunten

Register van verwerkingen

In het Excelbestand *Verwerkingsregister Taalcentrum-VU* geven we een overzicht van de soorten persoonsgegevens die door het Taalcentrum-VU verwerkt worden en met welk doel dit gebeurt.

Bewaartermijn

We bewaren persoonsgegevens niet langer dan nodig is. Voor sommige producten of diensten kan het nodig zijn om gegevens gedurende een langere periode te bewaren. De exacte bewaartermijn is afhankelijk van het doel waarvoor we ze gebruiken. In het *Verwerkingsregister* geven we duidelijk aan hoe lang we de verschillende gegevens bewaren. Als we gegevens niet langer bewaren, dan verwijderen we ze.

Dataminimalisatie

Het Taalcentrum-VU slaat alleen persoonlijke data op die nodig zijn voor een goede dienstverlening of taalproducten. We streven naar dataminimalisatie; waar dat mogelijk is, verwerken we minder of geen persoonsgegevens.

Vertrouwelijkheid

Het Taalcentrum gaat zorgvuldig en vertrouwelijk om met persoonsgegevens. Zowel alle medewerkers, als ook de freelancekrachten hebben bijvoorbeeld een geheimhoudingsplicht. Daarbij is onze werkwijze zowel in praktische als ook in technische zin zo ingericht dat het risico op verlies van data zo klein mogelijk is.

Rechtmatigheid en grondslag

Volgens de wet mogen alleen persoonsgegevens verzameld worden als daar een goede reden voor is (rechtmatige grondslag). Zo'n grondslag kan zijn:

- Toestemming van de betrokkene
- Uitvoering overeenkomst
- Wettelijke verplichting
- Vitaal belang
- Algemeen belang
- Gerechtvaardigd belang

Voor het Taalcentrum-VU zijn de eerste drie punten relevant. Als een cursist zich inschrijft voor een training, vragen we expliciet en op een duidelijke manier toestemming om de persoonsgegevens te gebruiken gedurende de termijn van de training. Ook wijzen wij op de bewaartermijn en de mogelijkheid om de persoonsgegevens te laten verwijderen.

Delen met derden

Wij werken samen met externe partners zoals trainers, vertalers of IT-leveranciers. Wanneer we persoonsgegevens delen met deze externe partijen maken we vooraf duidelijke afspraken over het gebruik van de persoonsgegevens. Uiteraard voldoen deze afspraken aan de wet.

We hebben Verwerkersovereenkomsten opgesteld met de volgende partijen:

- Parentix B.V. (cloudservice hosted desktop)
- Qube B.V. (leverancier Synergy Enterprise en Globe)
- UP-Learning B.V. (e-learning host)
- ETS Global (ITP TOEFL toets)
- Grant Thornton Accountants en Adviseurs B.V. (salaris- en verlofadministratie medewerkers Taalcentrum)
- ttif en arbo (Arbodienst medewerkers Taalcentrum)
- Delta Lloyd Verzekeringen NV (pensioenverzekering)
- XTRF (vertaalsoftware)
- Memo-Q (vertaalsoftware)
- Sterc Internet & Marketing (beheerder van onze belangrijkste website)
- Qlic Internetbureau (beheerder van twee van onze websites)

Het Taalcentrum zal nooit persoonsgegevens verkopen of doorgeven aan personen of organisaties die niets met onze producten of diensten te maken hebben.

Rollen

Soms zijn wij verantwoordelijke, soms verwerker. Die verschillende rollen bepalen welke verantwoordelijkheid en verplichting op ons rust en welke niet.

3. Rechten van betrokkenen

Het Taalcentrum-VU wil met zorg de gegevens van medewerkers, klanten, leveranciers en andere betrokkenen verwerken. Iedere betrokkene heeft daarbij het recht om zijn of haar gegevens in te zien, te wijzigen, te verwijderen of over te (laten) dragen.

We streven ernaar je verzoek binnen vier weken te behandelen. Vanzelfsprekend draagt het Taalcentrum zorg voor een secure vaststelling van de identiteit van de verzoeker. Een verzoek kan worden ingediend via info@taalcentrum-vu.nl. Wij sturen dan een aanvraagformulier toe.

Inzage

Iedere betrokkene heeft recht op inzage in zijn of haar eigen persoonsgegevens die het Taalcentrum-VU (in digitale vorm) beheert.

Correctie of verwijderen

Iedere betrokkene heeft het recht om zijn of haar persoonsgegevens voor zover bekend bij het Taalcentrum-VU (naar waarheid) te veranderen of aan te vullen. Verder bestaat onder de nieuwe wet 'het recht om vergeten te worden'. Deze laatste wijze van het volledig verwijderen van gegevens kan, afhankelijk van het moment van het verzoek, gevolgen hebben voor de samenwerking of de dienstverlening. Ook kan er sprake zijn van een wettelijke bewaartermijn waardoor verwijderen van de gegevens niet mogelijk is.

Dataportabiliteit

Iedere betrokkene heeft het recht om zijn of haar persoonsgegevens door te geven, over te brengen of over te laten brengen naar een andere organisatie of instelling.

4. Technische en organisatorische veiligheidsmaatregelen

Privacy by design

Privacy by design houdt in dat er zowel technische als organisatorische maatregelen worden genomen om persoonsgegevens van meet af aan zorgvuldig te behandelen. Dit principe ziet er in de dagelijkse praktijk als volgt uit:

- Wij werken volledig vanuit 'de cloud' van onze IT-leverancier. Alle gegevens van zowel medewerkers als klanten en leveranciers staan in deze beveiligde omgeving opgeslagen. In de Verwerkersovereenkomst met onze IT-leverancier hebben we duidelijke afspraken gemaakt over de beveiliging van onze data.
- Voor de online leeromgeving werken we samen met een externe partij. Ook hier staan de gemaakte afspraken in een Verwerkersovereenkomst. Verder gelden als standaard werkwijze rondom onze online leeromgeving:
 - Om in te kunnen loggen in onze online leeromgeving krijgt de cursist inloggegevens, die gekoppeld zijn aan een naam en e-mailadres.
 - Deze gegevens zijn gedurende een periode van ongeveer drie weken voor tot drie weken na afloop van de training bruikbaar in onze online leeromgeving.
 - Na die periode worden de gegevens volledig gewist. Ze blijven nog wel gedurende zeven jaar als niet direct toegankelijke back-up beschikbaar bij UP-Learning.
- Minimaal een keer per jaar nemen we onze opgeslagen bestanden onder de loep en verwijderen we zo veel mogelijk verouderde data.

Privacy by default

Privacy by default houdt in dat er bij het verkrijgen van persoonsgegevens als standaard niet meer gegevens opgeslagen worden dan voor de dienstverlening noodzakelijk is. Dit principe komt in de volgende werkwijze naar voren:

- Als cursisten zich inschrijven voor een training kunnen ze zelf (al dan niet) de keuze maken om zich aan te melden voor de nieuwsbrief, zijnde ons online magazine CNTXT (opt-in).
- Afmelden voor een mailing is duidelijk en eenvoudig. Dit kan via een 'unsubscribe' link onderaan elk bericht (opt-out).
- We maken geen gebruik van Big-dataonderzoek (verschillende soorten gegevens verzamelen en aan elkaar koppelen, al dan niet voor een nieuw doel).

5. Draaiboek datalekken

Het Draaiboek datalekken treedt in werking op het moment dat het vermoeden bestaat dat er persoonsgegevens in handen zijn gevallen van derden die geen toegang tot deze persoonsgegevens zouden mogen hebben. Verlies van persoonsgegevens zonder dat er een (duidelijk aanwijsbare) ontvanger is, is ook een datalek.

1. Degene die een ernstige datalek vermoedt, meldt dit zo spoedig mogelijk, **maar uiterlijk 12 uur na de eerste constatering** bij de werkgroep AVG en directe leidinggevende/de directie.
2. Bij afwezigheid/onbereikbaarheid van de leden van de werkgroep AVG wordt de melding gedaan aan de direct leidinggevende.

Van een datalek is sprake op het moment dat persoonsgegevens terecht zijn gekomen bij derden die geen toegang tot deze gegevens mogen hebben. Onder persoonsgegevens verstaan we niet alleen namen, adressen en geboortedata, maar ook andere gegevens die via nadere stappen in verband kunnen worden gebracht met een bepaald persoon.

Bij twijfel nemen we het zekere voor het onzekere en melden het vermoedelijke datalek of we doen een voorlopige melding van het datalek.

3. Na kennisname van een mogelijk datalek brengen de werkgroep AVG en de directie de relevante afdelingen c.q. personen op de hoogte.
4. We bekijken aan de hand van de Richtsnoeren van de AP of er sprake is van een datalek dat gemeld moet worden aan de AP en aan de betrokkenen.

Stappenplan Richtsnoeren AP:

- Is er sprake van een inbreuk op de beveiligingsmaatregelen (een datalek)?
- Zo ja, zijn de verwerkte persoonsgegevens daardoor blootgesteld aan verlies of onrechtmatige verwerking?
- Zo ja, heeft deze blootstelling geleid tot ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens?
Ja: het datalek moet gemeld worden aan de AP.
- Zal de inbreuk waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van betrokkenen?
Ja: het datalek moet ook gemeld worden aan de betrokkenen.

5. Bij een meldingsplichtig datalek zorgen we voor melding **binnen 72 uur na constatering**, ongeacht avonden, weekend of feestdag.
6. Melding vindt plaats via het meldformulier voor datalekken op de site van de AP (www.autoriteitpersoonsgegevens.nl).
7. Na de melding aan de AP en eventueel aan de betrokkenen of medewerkers beoordelen we of er externe partijen betrokken zijn bij het datalek.

Aandachtspunten:

- a. Heeft het datalek plaatsgevonden bij een van de medewerkers?

In dit geval besteden we aandacht aan het datalek in een individueel gesprek. De directe leidinggevende en de directie bepalen of het datalek een reden is voor ontslag op staande voet of een beëindiging van het dienstverband op korte termijn. Ook kunnen minder vergaande maatregelen genomen worden, zoals een schorsing of formele waarschuwing.

Is het datalek het gevolg van onachtzaamheid, dan wordt de medewerker gewaarschuwd.

Het datalek wordt besproken in een groepsgesprek, zodat de organisatie ervan kan leren.

- b. Heeft het datalek plaatsgevonden bij een externe partij?

Zijn er met deze externe partij afspraken over een melding en zo ja, heeft deze partij het datalek binnen de afgesproken tijd gemeld?

Is met deze externe partij een verwerkingsovereenkomst gesloten of geldt een geheimhoudingsbeding?

Stel deze externe partij alvast aansprakelijk voor huidige en toekomstige schade.

Is er reden voor een (externe) audit bij deze externe partij?

8. De melding van een datalek dat ook gemeld moet worden aan de betrokkenen, wordt zo spoedig mogelijk gedaan.

De melding aan de betrokkenen bevat in ieder geval:

- de aard van de inbreuk (meestal een algemene omschrijving);
- de instanties waar betrokkenen meer informatie over de inbreuk kunnen krijgen;
- de maatregelen die we de betrokkenen aanbevelen om de negatieve gevolgen van de inbreuk te beperken.

9. Na de vereiste melding(en), nemen wij het datalek op in het Register Datalekken Taalcentrum-VU.

Hierbij worden in ieder geval de feiten en gegevens omtrent de aard van de inbreuk vermeld. Indien het datalek ook gemeld is aan betrokkenen, wordt in het register ook de tekst van de kennisgeving aan de betrokkenen opgenomen en alle relevante zaken omtrent het datalek.

10. Uiterlijk een maand na de melding(en) vindt een evaluatie plaats.

In deze evaluatie wordt nagegaan hoe een vergelijkbaar lek in de toekomst kan worden voorkomen. Naar aanleiding van de uitkomsten worden eventueel maatregelen genomen om de persoonsgegevens beter te beveiligen en het risico op verdere inbreuken en lekken zoveel mogelijk te beperken.

6. Tot slot

Dit document is opgesteld door de werkgroep AVG van het Taalcentrum-VU en goedgekeurd door Rob Doeve (directeur) op 14 mei 2018.

Wij doen onze uiterste best om dit beleid naar behoren uit te voeren. Heb je vragen of klachten over ons privacybeleid? Neem dan contact op met een van de leden van de werkgroep AVG van het Taalcentrum-VU:

Paul Rueckert | 020-5983819

Laila de Miranda | 020-5989459

Mathilde van Arkel | 020-5982817

Daarnaast kun je voor (algemene) vragen of klachten terecht bij de Autoriteit Persoonsgegevens:
www.autoriteitpersoonsgegevens.nl.