aan	Tweede Kamer der Staten-Generaal Vaste commissie voor Digitale Zaken
ons kenmerk	SPF20241201
datum	1 december 2024
onderwerp	Paper Privacy First inzake rondetafelgesprek Verzamelwet gegevensbescherming 4 december 2024

Geachte Kamerleden,

Op 4 december as. vindt het rondetafelgesprek inzake het wetsvoorstel Verzamelwet gegevensbescherming (36264), hierna: 'het Wetsvoorstel', plaats.

Stichting Privacy First constateert dat tijdens dit gesprek ook platform wordt geboden aan vertegenwoordigers van het bedrijfsleven, zoals de vereniging van datahandelaren (de *Vereniging voor Zakelijke B2B Informatie* VVZBI, https://vvzbi.nl/) en de *Open State Foundation*.

Privacy First wil graag van de gelegenheid gebruikmaken om u te attenderen op een aantal onderwerpen op het gebied van de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG), die aandacht van uw commissie en van de wetgever verdienen.

Wij verzoeken u deze paper toe te voegen aan de openbare stukken inzake het rondetafelgesprek.

1. Onderwerpen

In deze paper zullen we deels teruggrijpen op wetgevingswensen die Privacy First eerder heeft geuit tijdens onder meer wetgevingsconsultaties.

De thema's die we aan de orde willen stellen zijn de volgende:

1. **Regulering van de datahandel**, waarop wij in 2023 al aandrongen in onze bijdrage aan de consultatie over de toekomst van het Bureau Kredietregistratie (BKR).
2. **Verscherping van het toezicht** op de datahandel en op grootschalige verwerking van financiële persoonsgegevens door Nederlandse overheidsinstellingen. De problematiek van grootschalige verwerking van financiële persoonsgegevens door AFM en DNB

Stichting Privacy First
Nieuwe Herengracht 49
1011 RN Amsterdam
https://privacyfirst.nl
info@privacyfirst.nl
+31 20 810 0279
KVK 34298157
ANBI erkend

stelden wij aan de orde in onze deelname aan de consultatie over verdere uitbreiding van dataverwerking door deze financiële toezichthouders.

3. Verbetering van de rechtsbescherming van burgers inzake de wijze waarop wordt omgegaan met financiële persoonsgegevens in het kader van het financiële toezicht en in het kader van de witwasbestrijding (thans de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), vanaf 10 juli 2027 de Europese antiwitwasverordening). Dit heeft betrekking op artikel X van het Wetsvoorstel (wijziging van artikel 3:17 van de Wet op het financieel toezicht).
4. Verbetering van de gang van zaken bij verificatie van de identiteit van natuurlijke personen, inclusief het gebruik van biometrie, onder meer bij financiële instellingen, zoals door ons aan de orde gesteld in ons verzoek aan het ministerie van Financiën en DNB.
5. Aanscherping van de regels inzake (semi-)openbare registers, zoals het Handelsregister, UBO-register en het Kadaster, zodat wordt voorkomen dat deze registers een informatiebron voor criminelen en andere kwaadwillenden worden.
6. Aanvulling van de regels inzake oneerlijke handelspraktijken met de mogelijkheid dat een bedrijf zijn concurrent kan aanspreken op niet-naleving van de AVG.

2. Inleidende opmerking

Privacy First wijst erop dat we niet naïef moeten zijn over de risico's verbonden aan digitalisering (wat onverlet laat dat er ook goede kanten zijn).

Waarschuwing DNB

Op die risico's is recent ook weer door diverse deskundigen gewezen, een voorbeeld is het bericht van DNB: Digitale veiligheid topprioriteit in grimmig geopolitiek klimaat, https://www.dnb.nl/algemeen-nieuws/achtergrond-2024/digitale-veiligheid-topprioriteit-in-grimmig-geopolitiek-klimaat/.

Waarschuwing HCSS

Het rapport dat het Den Haag Centrum voor Strategische Studies (HCSS) eind november jl. heeft uitgebracht, aankondiging https://hcss.nl/report/geweld-aan-de-horizon-trends-omtrent-geweld-en-maatschappelijke-stabiliteit/ en rapport (pdf) https://hcss.nl/wp-content/uploads/2024/11/Geweld-aan-de-horizon-2024-HCSS.pdf, maakt melding van de risico's verbonden aan digitalisering. Zie met name paragraaf 3.5 waarin wordt gesteld:

Soms hebben innovaties dermate sterke ‘pathbreaking’ effecten dat de hele wereldorde zich opnieuw moet schikken. Dat is gebeurd met de introductie van het vuurwapen en de atoombom, en is vermoedelijk aan het gebeuren met AI.

De rapporteurs melden dat digitale vormen van exploitatie, afpersing en intimidatie, op basis van gerichte gegevensdiefstal, zullen toenemen en normaliseren om meerdere redenen:

(1) Het aanvalsoppervlak voor kwaadwillenden is dramatisch vergroot, ofwel, het beschikbare materiaal waarmee we gechanteerd kunnen worden neemt toe; (2) Het stelen van informatie kan worden geautomatiseerd met tooling, cybercrime as a service (via het dark web) plus de echtheidsfactor van fraudemethoden kan door AI worden verhoogd; (3) Digitale assets worden steeds waardevoller, met name door de opkomst van digitale currencies en de mogelijkheden om mensen af te persen; (4) Psychologisch wordt de impact van digitale criminaliteit zoals identiteitsfraude, intimidatie of chantage steeds sterker onderschreven; (5) Wettelijke raamwerken zijn aan het veranderen en bevestigen op een juridische manier de fysieke impactdimensie. Samen zorgt dit ervoor dat datadiefstal zwaardere impact sorteert. Iedereen met een digitaal profiel is kwetsbaar voor digitale afpersing. Daarnaast is er het punt van democratisering van de technologie: men hoeft geen expert te zijn om te hacken om iemands gevoelige gegevens te ontvreemden.

Kwantumtechnologie kan voor grote veranderingen zorgen:

Ze hebben een grotere rekenkracht maar zijn een stuk specifieker in hun toepassingen. Een daarvan is decryptie, en de implicaties ervan zijn significant. Q-Day zal het moment zijn waarop kwantumcomputers in staat zijn veel van de huidige cryptografische standaarden te breken. Er liggen scenario s in het verschiet waarin geen garantie meer kan worden gegeven voor de beveiliging van burgerlijke gegevens, overheidsgegevens of staatsgeheimen. Dit geeft ruimte voor afpersing, chantage van belangrijke personen of sabotage van de vitale infrastructuur. De staatkundige orde is onder druk te zetten wanneer er geen tijdige migratie heeft plaatsgevonden naar nieuwere, bestendige versleutelingsmanieren.

De auteurs signaleren in paragraaf 3.6 de risico's verbonden aan het door private partijen ontwikkelen van digitale innovaties, zie pagina's 28 en 29. Op pagina's 35 en 36 wordt gezegd dat de invloed van de online wereld vraagt om een brede visie.

Er zijn maatregelen nodig

Privacy First acht het van belang om tijdig maatregelen te nemen die voorkomen dat mensen risico lopen door het in verkeerde handen komen van persoonsgegevens. Wij zijn het daarom niet eens met het pleidooi van de Open State Foundation, de vereniging van datahandelaren (Vereniging voor Zakelijke B2B Informatie) en VNO-NCW om 'soepeler' om te gaan met privacy en gegevensbescherming.

Wij denken dat op het gebied van gegevensbescherming de regels en het toezicht moeten worden aangescherpt, om schade voor mensen te voorkomen.

3. Uitwerking onderwerpen

3.1 Persoonsgegevens zijn het nieuwe goud en verdienen gouden bescherming / regulering van datahandel

Privacy First ziet met zorg dat de risico's rondom de datahandel met de dag toenemen. Dat betreft dan niet alleen de handel in persoonsgegevens door advertentiebedrijven die mensen lokken met gratis diensten, zoals Google en Meta/Facebook.

Er is een zeer grootschalige bedrijvigheid in andere vormen van datahandel, zoals kredietregistratiegegevens, organisaties die zwarte lijsten bijhouden (bijvoorbeeld van wanbetalers en andere ongewenste klanten) en levering van bedrijfsgegevens en criminaliteitsbestrijdingsinformatie (onder andere informatie ten behoeve van de 'witwasbestrijding' door Wwft-plichtigen).

Al deze datahandel is volledig ongereguleerd, afgezien van de toepasselijkheid van de AVG. Het zal u bekend zijn dat persoonsgegevens, en al helemaal financiële persoonsgegevens, het nieuwe 'goud' zijn dat grote bedrijven en overheden graag willen delven. Dat nieuwe goud verdient ook een hoogwaardige bescherming. Die bescherming ontbreekt nu.

Gerechtvaardigd belang is geen grondslag voor datahandel

Voor de goede orde wijst Privacy First erop dat datahandelaren zich op gerechtvaardigd belang plegen te beroepen.

Als bijlage bij deze paper gaat een geanonimiseerd voorbeeld van de correspondentie die een zzp'er in 2023 voerde met één van de datahandelaren van de *Vereniging voor Zakelijke B2B Informatie*. Daarin beweert die datahandelaar dat zij geen toestemming nodig heeft om:

[a] gegevens over de zzp'er van onbekende derden te ontvangen;
[b] gegevens over de zzp'er (die niet aan de zzp'er bekend worden gemaakt) te leveren aan
[c] klanten van de datahandelaar, zonder dat de zzp'er weet wie dit zijn.

De datahandelaar meende dat zij zelf de toetsing kon doen die op grond van de grondslag gerechtvaardigd belang nodig is, terwijl het voor de zzp'er niet mogelijk is te verifiëren of de onder [a] genoemde gegevens juist zijn en terecht worden verstrekt, of de onder [b] genoemde gegevens juist zijn en of de onder [c] genoemde klanten wel recht hebben op de bedoelde gegevens.

Verder vindt bij deze datahandelaar - zonder dat sprake is van enig toezicht of enige toetsing - geautomatiseerde besluitvorming plaats, nu er aan de zzp'er een kredietprofiel wordt toegekend.

Risico's

Uw commissie dient zich te realiseren dat datahandelaren uit allerlei bronnen persoonsgegevens oogsten, zonder dat:

- de betrokkenen daarvan op de hoogte zijn,
- betrokkenen toestemming hebben gegeven voor dat oogsten,
- betrokkenen de kwaliteit hebben kunnen verifiëren,
- betrokkenen kunnen nagaan of de datahandelaar de interne processen (bijvoorbeeld cybersecurity, toegang op need-to-know basis) wel op orde heeft.

Die datahandelaren leveren de gegevens aan klanten, terwijl zij niet weten of die klanten wel integer zijn.

Onlangs werd bekend dat de Autoriteit Persoonsgegevens heeft opgetreden tegen datahandelaren Experian, Focum en EDR (zie onder meer https://privacy-web.nl/nieuws/ap-treedt-op-tegen-privacypraktijken-kredietinformatiebureaus-experian-focum-en-edr/). Dat is niet voor niets.

Enkele voorbeelden van de risico's van de datahandel zijn:

- World-Check, leverancier van persoonsgegevens voor de witwasbestrijding, had een groot datalek, lees bijvoorbeeld het artikel van TechCrunch, *Hackers are threatening to leak World-Check, a huge sanctions and financial crimes watchlist*, https://techcrunch.com/2024/04/18/world-check-database-leaked-sanctions-financial-crimes-watchlist/ (april 2024).
- Cracked Labs maakte in februari 2024 bekend dat datahandelaar LiveRamp een bevolkingsregister heeft aangelegd van alle burgers ter wereld, lees de aankondiging https://crackedlabs.org/en/identity-surveillance en het rapport https://crackedlabs.org/dl/CrackedLabs_IdentitySurveillance_LiveRamp.pdf.
- In januari 2024 maakte BNR bekend dat locatiegegevens van Nederlandse mobiele telefoons online te koop zijn, "*Het gaan en staan van veel Nederlanders is hierdoor tegen betaling te volgen. Het aantal slachtoffers loopt mogelijk in de miljoenen. (…) De gigantische berg gegevens omvat ook verplaatsingen van mensen met functies waarin veiligheid een belangrijke rol speelt.*", lees https://www.bnr.nl/nieuws/technologie/10537256/nederlandse-telefoons-online-stiekem-te-volgen-extreem-veiligheidsrisico.
- RTL publiceerde in januari 2024 *Hoe datahandelaren adressen van jou én van bedreigde personen te koop aanbieden*, https://www.rtl.nl/boulevard/crime/artikel/5425259/geheime-adressen-bedreigde-journalisten-politici-en-advocaten-te. Uit het artikel blijkt dat kredietregistratiebureaus zoals Experian en Focum persoonsgegevens die zij van hun klanten (bijvoorbeeld KPN) krijgen doorleveren aan iedereen die er voor wil betalen. KPN kondigde na de RTL-berichtgeving aan hiermee te stoppen.

Regulering nodig

Dit zijn ongewenste praktijken die duidelijk maken dat bedrijven die zich met “het nieuwe goud” bezighouden net zo gereguleerd moeten worden als financiële instellingen, namelijk:

- vergunningplicht, waarbij bij de aanvraag de integriteit van de leidinggevenden en andere personen met zeggenschap (bijvoorbeeld aandeelhouders) wordt getoetst;
- toetsing van de digitale systemen en van de naleving van de AVG en andere relevante regelgeving;
- verplichte compliance audits.

Privacy First heeft afgelopen zomer deelgenomen aan de wetgevingsconsultatie over de toekomst van het Bureau Kredietregistratie (BKR) en heeft toen al op regulering aangedrongen, lees onze aankondiging: https://privacyfirst.nl/artikelen/kredietregistratie-in-nederland-bkr-in-huidige-vorm-moet-verdwijnen/ en het consultatiedocument: https://www.internetconsultatie.nl/kredietregistratie/reactie/b34311f1-f92d-4367-8110-3f69b33a5e9a. Wij schreven toen onder andere (pagina 15):

Naast het centrale kredietregistratiebureau zijn diverse andere partijen in de Nederlandse markt bezig met het registreren van kredietwaardigheidsgegevens van Nederlandse burgers en organisaties, zoals deurwaarderskantoren, incassobureaus en handelsinformatiebureaus. Voor zover Privacy First bekend leven deze ondernemingen de AVG niet of beperkt na. Wij zijn van mening dat het nodig is dat er aanvullende regulering plaats vindt van kredietregistratie door anderen dan het centrale kredietregistratiebureau. (…)

Voorbeeld: handelsinformatiebureau Graydon schrijft in haar privacyverklaring [21] dat zij persoonsgegevens van derden ontvangt, "klanten van Graydon en anderen die een zakelijke of financiële relatie met Graydon hebben die relevant is voor het doel van het verzamelen en verwerken van de gegevens; Betaalgedrag van uw onderneming aan de hand van betaalervaringen van andere organisaties met uw onderneming." (punt 3) en dat zij die persoonsgegevens verstrekt aan klanten en meent dit te mogen doen met gerechtvaardigd belang als verwerkingsgrondslag (punt 4 en punt 6). Graydon vraagt geen toestemming voor het ontvangen van financiële persoonsgegevens van derden en evenmin voor het verstrekken van die gegevens aan haar klanten. Graydon meent haar gerechtvaardigd belang te kunnen onderbouwen met het volgende argument:

Uw privacyverwachtingen: Omdat u een onderneming heeft, neemt u deel aan het economisch verkeer. Daarom worden gegevens over uw onderneming opgenomen in registers die, omwille van de zekerheid en de betrouwbaarheid, voor iedereen toegankelijk zijn. Ondernemers kunnen daarom ook over het algemeen verwachten dat deze openbare gegevens worden verwerkt door bijvoorbeeld bedrijfsinformatiespecialisten zoals Graydon,

die op deze manier een bijdrage leveren aan de zekerheid in het economische verkeer en aan een gezonde economie.

Privacy First stelt zich op het standpunt dat de opvatting van Graydon (en andere handelsinformatiebureaus) in strijd is met de AVG, nu de betrokkene (natuurlijke persoon) weliswaar ondernemer is, maar ook hij het recht heeft te weten welke gegevens over hem worden rondgestrooid. Hier is 'gerechtvaardigd belang' geen grondslag voor de gegevensverwerking. Voorts leeft voor zover ons bekend Graydon niet de verplichting na om de betrokkene te informeren over de ontvangst van gegevens van derden en het verschaffen van gegevens aan derden. Daarmee worden de gegevensbeschermingsrechten van burgers ondergraven.
[21] https://graydon.nl/nl/avg

Aanbeveling Privacy First

Het is gewenst dat er met spoed wordt gewerkt aan regulering van de datahandel. Privacy First dringt er bij uw commissie op aan dat dit met spoed wordt opgepakt.

3.2 Verscherping van het toezicht op de naleving van de gegevensbeschermingsregels

Ter bescherming van burgers is het essentieel dat er krachtig toezicht is op grootschalige verwerking van persoonsgegevens door bedrijven zoals de hiervoor genoemde datahandelaren. Daarbij moeten Nederlandse overheidsinstellingen niet worden vergeten.

Zo verwerken De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM) op zeer grote schaal persoonsgegevens van Nederlandse burgers en zijn er plannen om financiële instellingen te verplichten nog meer persoonsgegevens te laten leveren. Privacy First heeft deelgenomen aan de internetconsultatie daarover, lees onze aankondiging https://privacyfirst.nl/artikelen/geen-carte-blanche-voor-dnb-en-afm-om-massaal-persoonsgegevens-binnen-te-harken/ en het consultatiedocument https://www.internetconsultatie.nl/rapportagehypotheekmarkt/reactie/248331/bestand (één reactie inzake zowel DNB als AFM).

Voorbeelden:

- De AFM ontvangt van financiële instellingen alle persoonsgegevens van beleggers. Wat daar precies mee gedaan wordt is onbekend. De website van de AFM zegt er niets over.
- Accountantskantoren leveren complete gegevenssets aan de AFM, vol met persoonsgegevens, lees https://www.accountant.nl/discussie/columns/2022/4/afm-wordt-meest-data-driven-accountantskantoor-van-nederland/.
- DNB krijgt grote gegevenssets van financiële instellingen, zo valt af te leiden uit de mededeling van bestuurder Steven Maijoor op LinkedIn, https://www.linkedin.com/posts/stevenmaijoor_how-can-supervisors-use-the-huge-potential-activity-6930955246798020608-UB6J, waarin hij trots vertelt: "*At DNB we applied an outlier detection tool in Know Your Customer examinations. We used it to detect anomalous transactions in a dataset that contains millions of customers and bank accounts and billions of transactions.*" Op de site van DNB is over deze verwerking - waarin zeer veel persoonsgegevens zullen zitten - niets te vinden.
- DNB is druk met AI, zo blijkt onder meer uit de berichtgeving over de ChatDNB tool, https://www.centralbanking.com/awards/7960892/initiative-of-the-year-the-netherlands-banks-chatdnb, het artikel vermeldt onder andere: "*DNB is currently looking into developing more use cases for ChatDNB. The first step is to train the tool not only on publicly available information, but also confidential information. In December, the team gained approval from management to explore use cases using confidential data, where the most potential for the tool can be achieved internally*".

DNB en AFM zijn niet transparant over de verwerking van persoonsgegevens, terwijl zij zeer veel persoonsgegevens verwerken en daarbij ook kunstmatige intelligentie (AI) inzetten, wat hen ongeschikt maakt als AI-toezichthouder. Privacy First is het eens met Simon Lelieveldt, die in het artikel 'Toezicht AI moet onafhankelijk zijn' in het NRC,

https://www.nrc.nl/nieuws/2024/09/09/toezicht-ai-moet-onafhankelijk-zijn-a4865011, dat standpunt innam.

Aanbevelingen Privacy First

- Privacy First is van mening dat de verscherping van het toezicht ook betrekking dient te hebben op DNB en AFM en verzoekt uw commissie hierop aan te dringen en te laten nagaan voor welke andere overheidsorganisaties dit dient te gelden.
- Zorg ervoor dat DNB en AFM niet worden aangewezen als AI-toezichthouder op grond van de AI-verordening.
- Bij die verscherping hoort ook dat de AP een veel hoger budget krijgt. Privacy First verzoekt uw commissie hierop aan te dringen.

3.3 Rechtsbescherming klanten van financiële instellingen en witwasbestrijdingsplichtigen

Artikel X van het Wetsvoorstel (wijziging van artikel 3:17 van de Wet op het financieel toezicht) maakt het mogelijk dat banken en betaalinstellingen betalingen blokkeren of opschorten. De gevolgen van de wijziging zijn groot, want de tekst luidt:

Aan artikel 3:17 van de Wet op het financieel toezicht worden twee leden toegevoegd, luidende:

9. Ter uitvoering van het bepaalde in het eerste lid beschikt een bank of betaalinstelling als bedoeld in dat lid over procedures en maatregelen met betrekking tot het monitoren en analyseren van betalingstransacties van cliënten. Een bank of betaalinstelling kan in dat kader geautomatiseerd besluiten om betalingstransacties die zijn gekoppeld aan een financieel product te blokkeren of op te schorten, indien:

a. het blokkeren of opschorten plaatsvindt op basis van afwijkende individuele transactiepatronen ten opzichte van het gebruik van het individuele financieel product van cliënten;
b. de bank of betaalinstelling de betalingstransacties na het blokkeren of opschorten onverwijld door menselijke tussenkomst onderzoekt; en
c. cliënten hun standpunt omtrent het blokkeren of opschorten van de betalingstransactie kenbaar kunnen maken.

10. Bij algemene maatregel van bestuur worden nadere regels gesteld over passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van cliënten in geval van het blokkeren of opschorten van betalingstransacties, bedoeld in het negende lid, die in ieder geval betrekking hebben op:

a. gegevensanalyse
b. beveiliging en integriteit.

Vanuit de financiële sector heeft Privacy First vernomen dat het blokkeren en opschorten van betalingstransacties reeds gebeurt. Dat is dan kennelijk zonder wettelijke grondslag…

Wij kennen een geval waarin een grootbank ingekomen betalingen langdurig (maanden) vasthield, zonder het betrokkene te melden. Die betrokkene kwam daar pas achter na aanmaning van degenen die hadden betaald (in de veronderstelling dat van wanbetaling sprake was). De betrokkene heeft een zaak bij het Kifid aanhangig gemaakt en de zaak is met bemiddeling van Kifid geschikt, zodat de feiten niet in een door Kifid gepubliceerde uitspraak bekend zijn geworden. Op welke schaal dit soort praktijken voorkomen, is onbekend.

Onverkwikkelijk is dat banken soms plotseling betalingen blokkeren en de rekeninghouder daarmee in problemen brengen. Een voorbeeld daarvan is te vinden in de uitspraak van de rechtbank Den Haag tegen bunq, https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2024:14477. De rechter oordeelde dat de bank geen verantwoording hoeft af te leggen van het risicoprofiel dat aan de rekeninghouder was toegekend en ook niet hoefde toe te lichten waarom de rekeningen zo plotseling waren geblokkeerd.

Dit heeft de ongewenste consequentie dat banken en andere financiële instellingen niet op de vingers kunnen worden getikt als onzorgvuldig wordt omgegaan met hun overheidstaken op grond van de Wwft. Daarbij is eveneens problematisch dat het overstappen naar een andere bank vaak niet eenvoudig is, zodat klanten gedwongen zijn om onjuist handelen van de bank te accepteren.

Privacy First is van mening dat de rechtsbescherming van klanten in zaken op het gebied van de Wwft en het financiële recht volstrekt onvoldoende is. Consumenten kunnen soms bij het Kifid terecht, die door de financiële sector wordt gefinancierd en niet echt onafhankelijk is. De manier waarop bij het Kifid wordt geprocedeerd is niet burgervriendelijk. Probleem is dat zzp'ers en het mkb niet bij het Kifid terecht kunnen.

Vanwege de overheidstaken die financiële instellingen en andere witwasbestrijdingsplichtigen op grond van de Wwft hebben en hun ingrijpende bevoegdheden en grote marktmacht, is het gewenst dat de rechtsbescherming aanzienlijk wordt verbeterd.

Aanbevelingen Privacy First

- Wij achten het ongewenst (anders dan wat in het Wetsvoorstel staat) dat bij algemene maatregel van bestuur nadere regels worden gesteld over passende maatregelen ter bescherming van klanten. Dergelijke nadere regels horen in de wet thuis. Bovendien gaan die maatregelen volgens het Wetsvoorstel alleen over gegevensanalyse, beveiliging en integriteit en niet over adequate communicatie met de klant en volwassen rechtsbescherming. Een wettelijke regeling is hier gewenst.

Voorts is het volgende nodig:

- Een onafhankelijke ombudsman voor de financiële sector en de witwasbestrijding ('financiële ombudsman'), waar consumenten en het midden- en kleinbedrijf terecht kunnen voor alle geschillen met financiële instellingen en met andere ondernemingen die overheidstaken op grond van de witwasbestrijding hebben, zoals accountants en notarissen. Deze ombudsman kan signalen van burgers ontvangen en behandelen en adviezen uitbrengen, op een vergelijkbare manier als de Nationale Ombudsman. De

financiële ombudsman dient ook toegang te krijgen tot de geheime informatie die de klant van bunq in de hiervoor genoemde uitspraak van rechtbank Den Haag niet kreeg.
- Een **gespecialiseerde procedure bij de onafhankelijke rechter**, waar consumenten en het midden- en kleinbedrijf hun problemen met financiële instellingen en witwasbestrijdingsplichtige ondernemingen kunnen voorleggen.

Wij verzoeken u het er toe te leiden dat zo spoedig mogelijk de rechtsbescherming van klanten van financiële instellingen en witwasbestrijdingsplichtigen ingrijpend wordt verbeterd.

4. Verificatie van de identiteit

In september jl. deed Privacy First aan het ministerie van Financiën en DNB een verzoek tot aanpassing van identificatiepraktijken van financiële instellingen, lees onze aankondiging https://privacyfirst.nl/artikelen/privacy-first-verzoekt-aanpassing-identificatiepraktijken-van-financiele-instellingen/ en het juridisch uitvoerig gemotiveerde verzoek, https://privacyfirst.nl/wp-content/uploads/Wwft_identificatie_verzoek_PrivacyFirst_sept2024.pdf. Dit verzoek is ook ter informatie aan uw commissie gestuurd.

Wij hopen in januari as. te kunnen overleggen met het ministerie en DNB.

Wetenschap

Promovendus Danny Mekić heeft in vakblad Privacy & Informatie van februari 2024 het artikel '*Het opslaan van kopieën van legitimatiebewijzen, foto s en video s van cliënten: de grenzen van de Wwft-reconstructieplicht in het licht van fundamentele rechten*' gepubliceerd. In dat artikel besteedde hij aandacht aan de risico's bij verificatie van de identiteit. Hij heeft tevens een radio-interview aan De Nieuws BV gegeven, https://www.nporadio1.nl/fragmenten/de-nieuws-bv/9d689f29-ba3f-4723-8d60-2c2b3990127e/2024-11-04-identificatie-bij-banken-gebeurt-te-vaak-onveilig.

Zie over dit onderwerp ook het proefschrift van N.S. van der Meulen, *Fertile grounds: The facilitation of financial identity theft in the United States and the Netherlands* (2010), https://research.tilburguniversity.edu/files/8718805/Van_der_Meulen_Fertile_10_12_2010.pdf . Daarin wordt gewezen op toenemende risico's op financiële identiteitsfraude. De door haar beschreven problematiek is onverminderd actueel.

Biometrie

Bij verificatie van de identiteit wordt in toenemende mate gebruik gemaakt van biometrie, terwijl dat riskant is aangezien biometrische gegevens overal geoogst kunnen worden en in verkeerde handen kunnen raken.

Zo wordt biometrie gebruikt om betalingen te authenticeren, lees daarover het artikel van een AlgorithmWatch auteur, https://berlinergazette.de/countering-creeping-algorithmic-automation-pushing-back-against-performing-happiness-to-purchase/. Daarin wordt beschreven dat bedrijven systemen introduceren om delen van het menselijk lichaam te scannen om te gebruiken als unieke identificatiemiddelen voor betalingsverificatie. Als voorbeelden worden de irisscanner van MasterCard en de handpalmafdruklezer van Amazon genoemd en wordt gemeld dat grote betaaldienstverleners zoals Visa en Stripe bezig zijn met biometrische identificatie bij betalingen. Volgens het artikel maken Mastercard en Alipay gebruik van gebarengebaseerde authenticatie, het gebruik van de

glimlach om een betaling te authenticeren ("*using one s smile to trigger a payment authentication*").

Biometrie is onveilig, omdat het makkelijk geoogst kan worden, het niet vervangen kan worden en omdat betrokkene kan worden gedwongen tot gebruik bij authenticatie.

Steeds vaker verificatie nodig

Privacy First signaleert dat er in toenemende mate om verificatie van de identiteit wordt gevraagd, niet alleen als dat verplicht is op grond van de Wwft, en dat die verificatie regelmatig op een onveilige manier gebeurt.

Aanbevelingen Privacy First

- Wij verzoeken u aandacht te besteden aan dit onderwerp en te volgen of er verbetering optreedt bij de verificatie van de identiteit door financiële instellingen.
- Privacy First denkt dat het een goed moment is om de regels in de UAVG inzake de biometrie-uitzondering bij verificatie van de identiteit te beperken tot die situaties waarin dit daadwerkelijk noodzakelijk is en er voldoende waarborgen zijn dat het integer wordt ingezet en misbruik wordt voorkomen.

5. (Semi-)openbare registers

Privacy First is al geruime tijd bezorgd over de misbruikmogelijkheden die openbare registers zoals het Handelsregister, UBO-register en Kadaster bieden.

Zoals u bekend zal zijn heeft Privacy First geprocedeerd tegen de openbaarheid van het UBO-register. In september jl. schreef Privacy First een brief aan de Tweede Kamer naar aanleiding van het voorstel voor een wijzigingswet, waarin zij de Kamer verzocht niet akkoord te gaan met een openbaar UBO-register, zie het artikel https://privacyfirst.nl/artikelen/privacy-first-verzoekt-tweede-kamer-niet-akkoord-te-gaan-met-openbaar-ubo-register/ en onze brief https://privacyfirst.nl/wp-content/uploads/UBO_PrivacyFirst_TK_20september2024.pdf.

Een aantal opmerkingen over het UBO-register gelden ook voor andere openbare registers. Zo is het onverstandig om toegang te verschaffen aan ongereguleerde organisaties en personen, zoals journalisten en non-profit organisaties voor persoonsgericht onderzoek of data-analyse. Zoals ook in de hiervoor genoemde brief aan de Tweede Kamer inzake het UBO-register is toegelicht, is het ongewenst dat niet op integriteit en kwaliteit getoetste personen en organisaties toegang tot persoonsgegevens uit openbare registers krijgen voor persoonsgericht onderzoek of data-analyse.

Ook de toegang van datahandelaren tot persoonsgegevens dient beperkt te zijn, zolang er geen vergunningen- en toezichtregime is zoals wij hiervoor hebben bepleit.

Aanbeveling Privacy First

- Privacy First dringt er op aan dat de gegevensbescherming van de Nederlandse openbare registers wordt verbeterd.

6. Aanvulling van de regels inzake oneerlijke handelspraktijken

Het Europese Hof van Justitie heeft recent beslist dat de Duitse wettelijke regel is toegestaan die het mogelijk maakt dat een onderneming die de AVG aan zijn laars lapt door concurrenten kan worden aangepakt.

Dit is uitgemaakt in de uitspraak van 4 oktober 2024 inzake de Lindenapotheke, kenmerk ECLI:EU:C:2024:846, zie het Nederlandstalige persbericht, https://curia.europa.eu/jcms/jcms/p1_4584870/en/, en de uitspraak https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:62023CJ0021.

Wij zagen dat de Autoriteit Persoonsgegevens eveneens voorstelt om deze mogelijkheid in de Nederlandse wet op te nemen.

Aanbeveling Privacy First

- Wij dringen aan op spoedige aanvulling van de regels inzake oneerlijke handelspraktijken met de mogelijkheid dat een bedrijf zijn concurrent kan aanspreken op niet-naleving van de AVG.

Dit kan voorkomen dat niet-naleving van de AVG onrechtmatig voordeel oplevert.

7. Bijlage - Voorbeeld datahandel

Onderstaand het geanonimiseerde voorbeeld van correspondentie met een datahandelaar.

Bericht aan de datahandelaar

De zzp'er ontving bericht van de datahandelaar dat deze de zzp'er heeft geregistreerd. De zzp'er schreef de volgende e-mail:

Geachte dames en heren,

Onlangs ontving ik van u de melding dat u meent dat u mijn persoonsgegevens, die u uit het handelsregister heeft verkregen, kunt verwerken en dat u meent deze te mogen verrijken met informatie uit mij onbekende bronnen:

Hoe komt [datahandelaar] aan informatie over uw onderneming?
[datahandelaar] haalt haar informatie uit een aantal openbare bronnen, bijvoorbeeld het Handelsregister, openbare registers (zoals het insolventie- of curatele- en bewindregister) en (gerechtelijke) uitspraken zoals gepubliceerd op rechtspraak.nl, websites zoals overheid.nl en in de Staatscourant. [datahandelaar] verkrijgt tevens informatie uit niet-openbare bronnen, van uzelf, bijvoorbeeld als het gaat om de door betrokken onderneming verstrekte gegevens (vb uw jaarcijfers) of klanten van [datahandelaar] en anderen die een zakelijke of financiële relatie met [datahandelaar] hebben (betaalervaringen) of van andere (commerciële) partijen waarmee [datahandelaar] zaken doet.

en dat u de gegevens mag leveren aan mij onbekende derden:

[datahandelaar] levert de door haar verzamelde bedrijfsinformatie, waaronder (zakelijke) persoonsgegevens aan haar klanten. Dat zijn ondernemingen en overheden in Nederland. Verder deelt [datahandelaar] informatie met de aan haar gelieerde entiteit in België, en andere partijen waarmee [datahandelaar] samenwerkt, zoals buitenlandse bedrijfsinformatiebureaus. Zo kan het bijvoorbeeld voorkomen dat een buitenlands bedrijfsinformatiebureau voor een buitenlandse klant bij [datahandelaar] bedrijfsinformatie opvraagt over een in Nederland ingeschreven onderneming.

Hierbij bericht ik u dat ik niet akkoord ga met de verrijking van de door u van mij verkregen persoonsgegevens met onbekende bronnen. Als deze mij onbekende bronnen (onderstreept in het eerste citaat) gegevens over mij aan u zouden leveren, handelen zij in strijd met de AVG. Ook u handelt in strijd met de AVG door dergelijke gegevens te ontvangen. Als derden mijn persoonsgegevens aan u wensen te verstrekken, hebben zij mijn toestemming nodig en wens ik hen te screenen alvorens toestemming te geven.

Voorts ga ik niet akkoord met het leveren van mijn gegevens, voor zover meer dan wat in het handelsregister is geregistreerd, aan onbekende derden. De AVG schrijft voor dat betrokkenen (zoals ikzelf) het recht hebben zelf te bepalen aan wie hun gegevens worden geleverd. Ik wens zelf de ontvangers van mijn persoonsgegevens op relevantie, integriteit e.d. te screenen.

Ten onrechte doet u beroep op gerechtvaardigd belang in de zin van de AVG en meent u dat u de belangenafweging zelf kunt maken. Zoals u weet is er inmiddels voldoende Europese rechtspraak waaruit volgt dat aan die belangenafweging strenge eisen worden gesteld en dat het uitzonderlijk is dat die afweging in het voordeel van een bedrijf uitvalt.

Als [datahandelaar] zonder toestemming van natuurlijke personen aan wie ondernemingen toebehoren (zzp'ers, personenvennootschappen) hun persoonsgegevens verwerkt, is dat in strijd met de AVG.

Ik adviseer u de verwerking van persoonsgegevens van zzp'ers en van natuurlijke personen die vennoot van personenvennootschappen zijn per ommegaande te staken, aangezien die verwerking niet op gerechtvaardigd belang kan worden gebaseerd.

Graag verzoek ik u mij per ommegaande aan mij te bevestigen dat u zich aan de AVG zult houden en dat u van mij geen andere persoonsgegevens zult verwerken en aan derden zult verschaffen, anders dan bij het handelsregister openbaar beschikbaar.

Graag verzoek ik u de goede ontvangst van deze e-mail te bevestigen.

Reactie datahandelaar

Na enige correspondentie komt de datahandelaar met de volgende reactie inzake de toepassing van de grondslag 'gerechtvaardigd belang':

Hartelijk dank voor uw reactie. Zoals u in onze eerdere mail kunt lezen doet [datahandelaar] voor wat betreft het verwerken van persoonsgegevens beroep op haar gerechtvaardigde organisatiebelang. Dit is gebaseerd op art. 6 lid 1 sub f AVG. Uw toestemming danwel een contract is hiervoor dan niet nodig. Wel is het nodig dat [datahandelaar], zoals de AVG dat verlangt, van tevoren een belangenafweging gemaakt. Deze treft u als bijlage aan.

Wij vatten uw oorspronkelijke verwijderingsverzoek daarom op als een bezwaar tegen de gegevensverwerking. Als uw bezwaar inderdaad aan de juiste voorwaarden voldoet, dan is [datahandelaar] verplicht om de gegevensverwerking te stoppen en uw gegevens te verwijderen.

Het bezwaarrecht van de AVG is echter niet absoluut. Om uw bezwaar te kunnen honoreren, moet [datahandelaar] haar gerechtvaardigde belangen om de gegevens wél te verwerken opnieuw afwegen tegen uw beschermingswaardige belangen om de gegevens níet te verwerken.

In uw reactie vooronderstelt u dat we onze zakelijke klanten niet screenen. Deze aanname is onjuist, wij screenen weldegelijk onze klanten om uit te sluiten dat wij met criminelen zaken doen.

Wij zijn graag bereid om onze eerder gemaakte belangenafweging voor uw specifieke situatie nogmaals te bekijken. Zou u ons daarom uw belangen kunnen toelichten zodat wij onze afweging opnieuw kunnen beoordelen?

NB: Er is nooit een verwijderingsverzoek gedaan, zie het bericht aan de datahandelaar.

Bij deze e-mail was een bijlage gevoegd, waarin wordt verhuld dat de datahandelaar van onbekende derden persoonsgegevens ontvangt en onbekende persoonsgegevens levert aan niet gescreende klanten:

Het gerechtvaardigd belang van het [datahandelaar] Bedrijfsinformatie product

i. Het gerechtvaardigde belang van [datahandelaar] Bedrijfsinformatie product;

[datahandelaar] is actief binnen het domein van de zakelijke bedrijfsinformatie. Eenmanszaken spelen een belangrijke rol in de Europese economie. Zoals elke andere onderneming, hebben ook zij klanten en leveranciers. Daarom behoren ook eenmanszaken tot de B2B relaties. Met bedrijfsinformatie biedt [datahandelaar] een hulpmiddel dat een essentieel onderdeel vormt binnen B2B relaties. bedrijfsinformatie helpt de verschillende stakeholders –onder meer bedrijven, privépersonen en overheidsinstantieszowel bij het correct inschatten van mogelijk belastende risico s als bij het creëren van nieuwe mogelijkheden die verdere ontwikkeling en groei mogelijk maken. Met deze bedrijfsinformatie ondersteunt [datahandelaar] op een actieve manier de ontwikkeling van een gezonde economie waarbij vertrouwen en transparantie centraal staan.

Belangrijke stakeholders die gebruik maken van bedrijfsinformatie zijn:

- *Bedrijven, zowel MKB (NL) als grotere ondernemingen die zich richten op een B2B markt*
- *Banken, verzekeringsmaatschappijen, …*
- *Lokale-, regionale- en Rijksoverheden*
- *Belangenorganisaties*
- *Accountants*

• Deurwaarders, advocaten, notarissen, juristen
• Academici

Het verzamelen van bedrijfsinformatie bestaat al lang. Het helpt bedrijven om te beslissen met wie ze zaken willen doen. Het belang van [datahandelaar] is dan ook om een kwalitatief hoogwaardig product samen te stellen waarmee haar klanten optimaal deel kunnen nemen aan het economisch verkeer. De doelstelling van [datahandelaar] is om organisaties te helpen om betere keuzes te maken op basis van accurate en volledige informatie. Dit is alleen mogelijk door het verwerken van de relevante gegevens uit de originele bronnen van het Handelsregister. In het geval van eenmanszaken kan het hier ook persoonsgegevens betreffen.

De toegevoegde waarde die [datahandelaar] aan allerlei stakeholders biedt behelst vele aspecten:

• Bedrijfsinformatie wordt intensief gebruikt voor onder meer concurrentie analyse, strategische planning, fraude en compliance doeleinden en vele andere strategische functies. bedrijfsinformatie stelt bedrijven in staat op efficiënte wijze de kredietwaardigheid, de risico s (waaronder de kans op faling, het risico op vertraagde betaling,…)te beoordelen en te beheersen. Inderdaad vormen vertraagde betalingen, wanbetalingen en faillissementen binnen de klantenportefeuille een belangrijke bedreiging voor de continuïteit van een onderneming.

• Bedrijfsinformatie en de daar bijhorende scoring wordt ook actief gebruikt door banken ter acceptatie van een kredietopname en door oa leasingmaatschappijen voor het afsluiten van een leasecontract.

• Bedrijfsinformatie stelt bedrijven en overheden in staat hun supply-chain veilig te stellen: om zo de continuïteit van het productieproces en de daadwerkelijke uitvoering van (openbare) werken te garanderen.

• Bedrijven die gebruik maken van inzichten uit bedrijfsinformatie exploreren zo op gerichte wijze nieuwe marktsegmenten en genereren zo extra, gezonde en dus rendabele handel. Dit is een onontbeerlijke functie die de groei van bedrijven, en dus de economie, stimuleert.

• Banken en verzekeringsmaatschappijen maken gebruik van de [datahandelaar]-bedrijfsinformatie als belangrijk hulpmiddel om kredietmogelijkheden en risico s correcter in te schatten. Omgekeerd: daar waar bedrijfsgegevens ter beschikking zijn vinden de bedrijven dankzij deze transparantie sneller nieuwe banken- en zakenpartners, en, indien het aantal kredietincidenten beperkt is, betalen ze – in navolging van de Basel normen1 - ook minder rente bij het opnemen van bancaire kredieten.

• Overheden maken op vele terreinen gebruik van inzichten verworven uit bedrijfsinformatie:

o om de continuïteit van het uitvoeren van openbare werken veilig te stellen.

o binnen het kader van preventief bedrijfsbeleid, stimuleren van bedrijven in ontwikkeling en ondersteunen van bedrijven in moeilijkheden. We verwijzen hier onder meer naar de benadering door de Europese commissie in het Early restructuring and second chance for entrepreneurs beleid voorgesteld om met nieuwe regelgeving overheden en bedrijven te stimuleren proactief early warning tools aan te wenden.

o als documentatiebron met betrekking tot diverse aspecten van beleidsondersteuning- en ontwikkeling.

• Bedrijfsinformatie wordt actief gebruikt binnen de opdracht van de Kamers voor Handelsonderzoek (onderdeel van de handelsrechtbank) in het streven van de wetgever om enerzijds het aantal faillissementen terug te dringen en anderzijds concurrentieverstorende of oneerlijke (malafide) elementen uit het maatschappelijk verkeer te weren2 .

De voornoemde stakeholders hebben er dus alle belang bij de goede werking van bedrijfsinformatiekantoren te ondersteunen, door informatie die openbaar dient te zijn ook maximaal voor de bedrijfsinformatiekantoren ter beschikking te stellen. Een gebrek aan essentiële data die bedrijfsinformatie voeden zet een rem op de ontwikkeling van de economie en stuit het (her)opleven ervan. Het brengt de economie bovendien schade toe door gezonde ondernemingen bloot te stellen aan de nadelige gevolgen van zaken doen met insolvente of zelfs malafide bedrijven.

Het zijn onder andere de bovenstaande aspecten waar [datahandelaar] een belangrijke rol speelt. Data is overal aanwezig, maar is al te vaak onvolledig en sterk vervuild. Bovendien is het samenbrengen van de vele gegevens bijzonder arbeidsintensief en tijdrovend. Bedrijven en andere stakeholders snakken naar snelle, efficiënte en waardevolle informatie, die leidt tot duidelijke inzichten. [datahandelaar] verzamelt de gegevens door haar bestaande relaties met officiële bronnen, evenals eigen onderzoek en past hier markt gedreven analyses en statistische technieken op toe. Deze informatie en de daaraan gekoppelde inzichten is wat bedrijfsinformatiekantore leveren, en waarvoor wij de hoogst mogelijke kwaliteit nastreven.

Bij het vergaren, verwerken, systematiseren, analyseren en interpreteren van bedrijfsgegevens hanteert [datahandelaar] een strikte deontologie, waarbij het streven naar het opleveren van kwalitatief hoogwaardige, juiste, actuele en volledige gegevens centraal staat. Bovendien wordt elke actie secuur getoetst aan de verschillende regelgevingen met betrekking tot het verzamelen en verwerken van data.

ii. De mate waarin de verwerking noodzakelijk is voor de behartiging van dit gerechtvaardigde belang;

De noodzakelijkheid van deze verwerking kan gemeten worden aan de hand van proportionaliteit en subsidiariteit.

Het Handelsregister is de enige (accurate) bron voor het verkrijgen van informatie over Nederlandse ondernemingen (inclusief eenmanszaken). Er is dus geen andere bron om de databank van [datahandelaar] accuraat en volledig te houden.

Indien [datahandelaar] deze openbare informatie niet verkrijgt, kan zij dus niet de volledige Nederlandse markt in kaart brengen voor haar klanten noch bedrijven helpen (financieel) inzicht te geven in hun bestaande klantenportefeuille om zo risico s tot handelen met partners in (financiële) moeilijkheden te beperken. [datahandelaar] kan zonder deze informatie niet helpen bij de ontwikkeling in een gezonde economie. Daarnaast hebben ondernemingen, overheden en organisaties die zaken doen belang bij een database die volledig, up to date en accuraat is. Op die wijze wordt een maatschappelijk verantwoorde dienstverlening op financieel gebied bevorderd, waarbij zowel voor ondernemingen die zaken doen als bij kredietgevers als voor kredietnemers de risico's bij het zakendoen en het verstrekken van kredieten beperkt. Dit systeem kan alleen functioneren indien alle gegevens in de database én alle onregelmatigheden bij de ondernemingen in de database daadwerkelijk worden gemeld.

Proportionaliteit
Proportionaliteit houdt in dat het doel van de verwerking van de persoonsgegevens (in dit geval de zakelijke contactgegevens) in verhouding moet staan tot de inbreuk op de privacy van de betrokkenen (in dit geval eenmanszaken en bestuurders). De inbreuk op de privacy van de betrokkenen is beperkt, omdat de gegevens worden verkregen van een bron die al wettelijke openbaar is. [datahandelaar] filtert de bron voor relevante informatie voor de klanten. Op basis van de oorspronkelijke data uit het handelsregister kunnen selecties worden gemaakt die relevant zijn. De data is beperkt tot de eerder genoemde set. Vooropgesteld dient te worden dat [datahandelaar] bedrijfsinformatiespecialist is, en uit is op het zo accuraat mogelijk weerspiegelen van ondernemingen. Voor zover [datahandelaar] daarbij persoonsgegevens in de zin van de AVG verwerkt is dit niet het doel maar een bijkomend effect. De gegevens die direct of indirect op een natuurlijke persoon betrekking hebben zullen echter altijd slechts zien op diens zakelijke hoedanigheid binnen de onderneming. Voor zover dus sprake is van de verwerking van persoonsgegevens, betreft dat altijd persoonsgegevens die betrekking hebben op de zakelijke hoedanigheid van een natuurlijk persoon, en niet diens privéleven en persoonlijke levenssfeer. [datahandelaar] beperkt de gegevens dus tot het strikt noodzakelijke ter behartiging van de economische (dus zakelijke) belangen die zij dient.

Dit brengt verder met zich mee dat [datahandelaar] dus ook geen bijzondere of gevoelige persoonsgegevens verwerkt. Zo worden bijvoorbeeld geen gegevens verwerkt over, gezondheid, religie, etniciteit of ras, politieke voorkeur of seksuele geaardheid. Ook verwerkt [datahandelaar] geen gegevens van kinderen of andere kwetsbare groepen. In tegendeel, ieder van de personen van wie gegevens worden verwerkt heeft een bestuurlijk mandaat en functioneert als contactpersoon voor de onderneming.

Subsidiariteit
Subsidiariteit houdt in dat het beoogde doel dat voor de verwerking is vastgesteld, niet op een minder ingrijpende manier en/of met minder ingrijpende middelen kan worden bereikt.

Het doel kan niet op een minder ingrijpende manier worden bereikt. Het handelsregister van de KvK is juist bedoeld als bron voor rechtszekerheid in het economisch verkeer en voor de verstrekking van gegevens van algemene feitelijke aard omtrent de samenstelling van ondernemingen en rechtspersonen ter bevordering van de economische belangen van handel, industrie, ambacht en dienstverlening. Bij een andere manier van verzamelen van informatie zou het risico bestaan van minder accurate informatie en zouden mogelijk onbedoeld meer gegevens worden verwerkt dan noodzakelijk.

Met haar dienstverlening beoogt [datahandelaar] een hoge mate van accuraatheid en transparantie te bieden aan haar klanten, zodat die klanten bedrijfsinzichten kunnen gebruiken om weloverwogen beslissingen te nemen. Daarbij onderscheidt [datahandelaar] de volgende drie factoren:

i. Datakwaliteit – kloppen de gegevens die [datahandelaar] gebruikt;
ii.Dataopbouw – uit welke elementen bestaan de gegevens; en
iii. Historiek – welke mutaties ondergaan de gegevens in de loop der tijd.

Elk van deze drie factoren is van cruciaal belang om tot een volwaardig informatieproduct te komen.

In het kader van de subsidiariteitsafweging kan de vraag gesteld worden of factor iii. ook daadwerkelijk noodzakelijk is. Dit is het geval. Om een eerlijk en accuraat beeld te geven van een onderneming, is niet alleen logisch maar strikt noodzakelijk dat daar historische gegevens bij worden betrokken. Door de doorlopende monitoring door [datahandelaar] wordt voorkomen dat haar klanten een momentopname of snapshot krijgen van hun (potentiële) zakenpartner, die geen volwaardig beeld geeft. Zit die bijvoorbeeld in een stijgende lijn, of een dalende? Door doorlopend te monitoren, kan [datahandelaar] een organisatie op waarde analyseren, en daarnaast benchmarken tegen haar branchegenoten en andere vergelijkbare organisaties.

iii. De mate waarin de belangen of de grondrechten en de fundamentele vrijheden van de betrokkenen worden geschaad als gevolg van de verwerking;

Aangezien de persoonsgegevens die verwerkt worden een beperkte set zijn en deze gegevens raadpleegbaar zijn via een openbare bron, is de inbreuk op de persoonlijke levenssfeer van betrokkenen gering. De gegevens zijn openbare gegevens van ondernemingen en bestuurders die daar werkzaam zijn. Het gebruik is puur zakelijk en in een B2B context.

De score die [datahandelaar] toekent aan elke onderneming, is ook van belang voor de onderneming zelf, dit kan gezien worden als een early warning tool, om zo eigen financiële moeilijkheden te detecteren. De onderneming in kwestie heeft op deze manier ook het belang om opgenomen te worden in de [datahandelaar] database ter verwerking van het opstellen van een score.

Verder heeft een onderneming er belang bij opgenomen te zijn in de [datahandelaar] database. Klanten van [datahandelaar] (waaronder banken en verzekeraars) vertrouwen op de informatie van [datahandelaar]. Wanneer een onderneming niet opgenomen staat in de databank en bijgevolg niet uitgeleverd wordt aan klanten van [datahandelaar], kan dit nadelige gevolgen hebben voor de beslissing van een klant om zaken te doen met die onderneming. Het heeft voor een onderneming voordelen om in de database van [datahandelaar] voor te komen. De [datahandelaar] database omvat het complete Nederlandse, Belgische en UK bedrijfsleven met uitzondering van ondernemingen of organisaties die om speciale redenen uit de database zijn gehaald. Hierbij kun je denken aan een blijf van mijn lijf huis . Deze organisatie is er juist voor bedoeld om niet gevonden te worden.

iv. De maatregelen die [datahandelaar] heeft genomen om de schade aan de belangen of de grondrechten en de fundamentele vrijheden van de betrokkenen zo veel als mogelijk te beperken;

Op de website van [datahandelaar] is een aparte AVG pagina ingericht om betrokkenen te informeren. Deze pagina bestaat uit onder andere uit de privacyverklaring, een FAQ, een informatiefilm Privacy & Persoonsgegevens: Hoe werkt dit in de praktijk?", de digitale versie van een kennisgevingsbrief, contactgegevens van [datahandelaar] en de contactgegevens van de DPO om de betrokken op een toegankelijke manier te kunnen informeren.

[datahandelaar] heeft een service team waar betrokkenen terecht kunnen voor vragen en de rechten onder de AVG. Met de komst van de AVG is er een vernieuwde procedure ingericht om zo goed mogelijk inrichting te geven aan de rechten van betrokkenen. Daarnaast is het serviceteam getraind om de betrokkenen zo goed mogelijk te woord te kunnen staan.

Door middel van de continue aanlevering van de officiële gegevens van de KvK zorgt [datahandelaar] ervoor dat gegevens in de database accuraat en up to date gehouden worden. Dit gaat ook de vervuiling en de veroudering van de gegevens van de database tegen.

[datahandelaar] heeft met externe partijen contractuele afspraken gemaakt om de rechten en plichten onder de AVG te waarborgen.

In haar algemene voorwaarden geeft [datahandelaar] onder andere meer informatie over zorgvuldige gegevensverwerking en rechtmatig gebruik van de persoonsgegevens verstrekt aan de klant.

[datahandelaar] heeft een informatiebeveiligingsbeleid om de beveiliging van de data te waarborgen. Zo doet zij het oa het volgende: versleutelen van laptops en verbindingen, werkt ze met het UAM is Key-proces en zijn haar servers fysiek enkel door een beperkt aantal (IT) medewerkers te benaderen. Daarnaast kunnen klanten alleen de informatie uit de database verkrijgen door middel van een beveiligde inlog.

Bovendien heeft [datahandelaar] het ISO27000 certificaat.

v. De weging tussen onderdeel i/ii enerzijds en iii/iv anderzijds

De inbreuk op de persoonlijke levenssfeer van betrokkenen is zoals eerder opgemerkt gering en het risico op nadelige gevolgen van de verwerkingen door [datahandelaar] daarmee ook. De verwerkte set gegevens is beperkt en betreft alleen informatie die al via openbare bronnen beschikbaar is. Bovendien hebben betrokkenen zelf een belang bij de vermelding in de database, omdat zij zo ook gevonden kunnen worden door mogelijke zakelijke partners in het kader van B2B activiteiten. Voor zover de beperkte risico s voor betrokkenen aanwezig zijn, zijn deze op basis van de maatregelen zoals beschreven in onderdeel iv geminimaliseerd.

Het belang van een kwalitatief hoogwaardig product op basis waarvan de klanten van [datahandelaar] de juiste keuzes kunnen maken is gerechtvaardigd. De juistheid en volledigheid van de gegevens helpt bedrijven, maar ook de betrokkenen zelf in het optimaal deel kunnen nemen aan het Nederlandse zakelijke verkeer. Dat is ook het doel van het Handelsregister. Het Handelsregister is de enige (accurate) bron voor het verkrijgen van informatie over Nederlandse ondernemingen (inclusief eenmanszaken). Er is dus geen andere bron om de databank van [datahandelaar] accuraat en volledig te houden. Het belang van een kwalitatief product met diensten die het vergaren van extra informatie uit (delen) van de dataset mogelijk maken is daarmee groot. Dit belang van [datahandelaar] als onderneming die ten doel heeft bedrijven en andere organisaties te helpen door het bieden van hoogwaardige producten prevaleert daarom boven de

belangen van de betrokkenen. Doch wordt elke individuele situatie van een betrokkene bekeken en afgewogen.

1 www.bis.org
2 https://www.1819.brussels/nl/content/kamers-voor-handelsonderzoek

Ten onrechte veronderstelt de datahandelaar een afweging inzake de zzp'er te kunnen maken, nu sprake is van verwerking van persoonsgegevens inzake de zzp'er uit bronnen die de zzp'er niet kent (en die dus fouten kunnen bevatten). Deze onbekende gegevens worden door de datahandelaar aan onbekende klanten geleverd.

Tot slot

Voor nadere informatie of vragen met betrekking tot bovenstaande is Privacy First te allen tijde bereikbaar op telefoonnummer 020-8100279 of per email: info@privacyfirst.nl.

Hoogachtend,

Vincent Böhre
directeur Stichting Privacy First