



TRUST REPORT: WEBSITE EN E-MAIL

Wat ziet een nieuwe klant van vdhBoekhouding?

Uw website en uw maildomein, bekeken zoals een bezoeker en een mailserver ze zien

vdhBoekhouding BV, Heverlee
Meting van 16 oktober 2026

VOORBEELDRAPPORT - vdhBoekhouding BV is een fictief bedrijf

2 van 9 punten in orde. Twee punten hebben voorrang: analysecookies vóór toestemming en lettertypes bij Google. Daarnaast vraagt uw domein ontvangers niet om valse mail in uw naam te weigeren. Samen 6 tot 10 uur werk voor uw partners.

Inhoud

In het kort	3
1. Hoe wij keken	4
2. Wat een bezoeker ziet	4
2.1 Analysecookies vóór toestemming	4
2.2 Lettertipes rechtstreeks bij Google	5
2.3 Privacyverklaring	5
2.4 Software op de server	6
2.5 Beveiligde verbinding	6
2.6 Meldpunt voor fouten	6
3. Wat een mailserver ziet	7
3.1 Valse mail in uw naam wordt niet geweigerd	7
3.2 Elektronische facturen (Peppol)	8
4. Wat u nu doet	9
5. Wat VDHome voor u kan doen	9
Bijlage A. Hoe wij het bewezen	10
Bijlage B. Bronnen	10
Bijlage C. Mails voor uw partners	11

Zo leest u dit rapport

Wie	Lees
U, als zaakvoerder	"In het kort" (één blad) en hoofdstuk 4: wat er moet gebeuren, door wie en wanneer.
Uw webbouwer en host	Hoofdstuk 2: per punt wat wij zagen, wat te doen en hoe ze zien dat het klaar is. Of stuur de mails uit bijlage C.
Uw IT-partner	Hoofdstuk 3 en het DMARC-stappenplan in 3.1.
Wie het bewijs wil zien	Bijlage A: wat wij bewaarden en hoe u het zelf nakijkt.

Dit is een voorbeeldrapport. vdhBoekhouding BV en alle kantoorgegevens zijn verzonnen. Wij bouwden een kleine website na met de problemen die wij het vaakst zien en lieten ons gereedschap erop lopen zoals bij een klant. De websitebevindingen en het bewijs zijn echte metingen op die nagebouwde site; de cookies werden er nagebootst met de naamgeving van Google Analytics 4. De maildomeingegevens in hoofdstuk 3 zijn voorbeeldwaarden, omdat een fictief domein niet in de publieke DNS staat.

In het kort

Een nieuwe klant leert uw kantoor op twee manieren kennen: hij opent uw website, en hij krijgt een mail van u. Wij keken naar allebei, precies zoals hij dat doet, zonder iets aan te klikken of te testen. Op beide plaatsen is uw kantoor zichtbaar en bereikbaar, maar het laat ook meer zien dan nodig, en het laat toe dat anderen in uw naam mailen.

Score: 2 van 9 punten in orde. 7 te verbeteren, waarvan 2 met voorrang.

Alles in dit rapport is publiek. Wij gebruikten alleen wat elke bezoeker van uw website ziet en wat in de publieke registers staat (DNS, de Peppol-lijst). Bij elk punt staat onder *Waar wij dit zagen* een link: klik erop en u ziet hetzelfde als wij.

Wat	Wat wij zagen	Voorrang
Cookies vóór toestemming	Twee analysecookies, nog voor de bezoeker koos (2.1)	Hoog
Inhoud van Google	Lettertypes rechtstreeks bij Google; Google ziet het IP-adres van elke bezoeker (2.2)	Hoog
Software op de server	De server meldt PHP 8.1, door het PHP-project niet meer ondersteund; laten bevestigen (2.4)	Middel
Privacyverklaring	Aanwezig, maar zegt niets over de website of cookies; van 2021 (2.3)	Middel
Valse mail in uw naam	Uw domein vraagt ontvangers niet om valse mail te weigeren (3.1)	Middel
Beveiligde verbinding	https werkt; de browser wordt niet gevraagd het altijd te gebruiken (2.5)	Laag
Meldpunt voor fouten	Geen security.txt (2.6)	Laag
Mail: afzenders en handtekening	SPF en DKIM in orde (3, voorbeeldwaarden)	In orde
Elektronische facturen	Staat in de publieke Peppol-lijst als ontvanger (3.2, voorbeeldwaarden)	In orde

Doe dit eerst.

- **Vandaag, 15 minuten (u zelf):** stuur de drie kant-en-klare mails uit bijlage C naar uw webbouwer, uw hostingpartij en uw IT-partner.
- **Deze week (uw partners, samen 3 tot 5 uur):** analysecookies pas na toestemming, lettertypes op de eigen server, en bij de host navragen of uw PHP nog beveiligingsupdates krijgt.
- **Deze maand:** privacyverklaring aanvullen, HSTS en security.txt toevoegen, en de eerste van drie stappen zetten om valse mail in uw naam te laten weigeren (in totaal ongeveer twee maanden).

Nieuwe meting inbegrepen. Na 30 dagen herhalen wij dezelfde meting en sturen u een vergelijking.

Hoe wij voorrang geven. *Hoog:* kan bezoekers of klanten nu raken, of volgt een duidelijke wettelijke regel. *Middel:* een reëel punt, maar nog te bevestigen of met weinig kans op schade. *Laag:* goede praktijk, snel gedaan.

Kleine woordenlijst. *Cookie:* klein bestand dat een website in de browser bewaart. *HSTS:* instructie aan de browser om uw site altijd beveiligd te openen. *SPF, DKIM, DMARC:* drie instellingen in uw domeinnaam die samen bepalen of mail “van uw domein” te vertrouwen is. *security.txt:* klein bestand dat zegt bij wie men een fout kan melden.

1. Hoe wij keken

- **Eén bezoek aan uw homepage** in een nieuwe, lege browser, zonder iets aan te klikken en zonder toestemming te geven; daarna een bezoek aan `http://` om de doorverwijzing te zien en een opvraging van `/.well-known/security.txt`. Op 16 oktober 2026 om 19:01 UTC.
- **De publieke DNS-gegevens van uw maildomein**: dezelfde gegevens die elke mailserver leest die mail van u krijgt.
- **De publieke Peppol-lijst** (`directory.peppol.eu`) voor uw ondernemingsnummer, zonder contact met uw systemen.
- **Niet gedaan**: inloggen, formulieren invullen, andere pagina's afzoeken, kwetsbaarheden testen, of iets proberen dat een gewone bezoeker niet doet.

Dit rapport is een technische vaststelling van wat op dat moment zichtbaar was, geen oordeel over uw wettelijke verplichtingen en geen volledige beveiligingsaudit. Elke stap kunt u zelf nakijken met de uitleg op <https://www.vdhome.be/webcheck>. Het bewijs bewaren wij met hashes en twee onafhankelijke tijdstempels (bijlage A).

2. Wat een bezoeker ziet

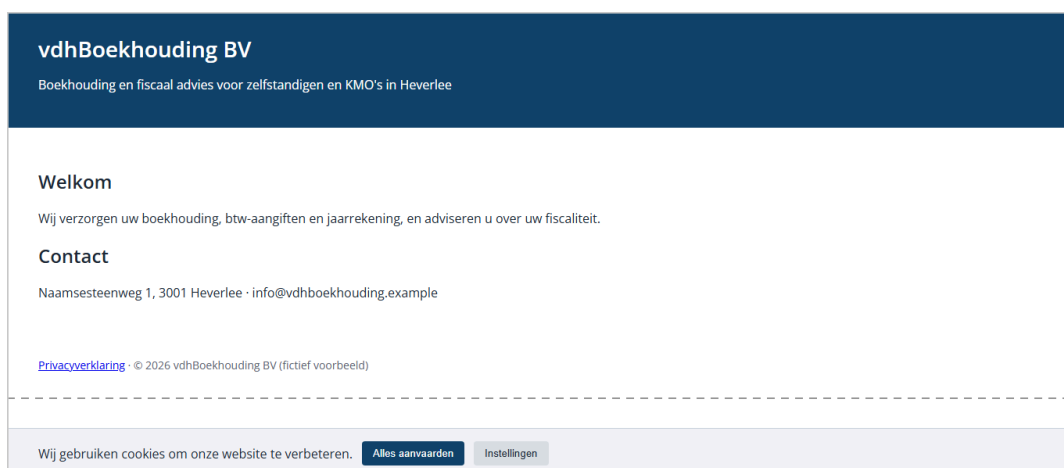
Een nieuwe bezoeker opent uw homepage. Nog voor hij iets aanklikt, gebeurt er al van alles: zijn browser haalt inhoud op, krijgt cookies en leest de antwoorden van uw server. Dat is wat wij in dit hoofdstuk beschrijven, in de volgorde waarin het gebeurt.

2.1 Analysecookies vóór toestemming

Hoog Wie: webbouwer | Tijd: 1 tot 2 uur

Wat wij zagen. Terwijl de cookiebanner nog onbeantwoord op het scherm stond, zette een script in de pagina zelf twee cookies:

Cookie	Naam wijst op	Bewaard tot	Doel
<code>_ga</code>	Google Analytics 4	20 november 2027	herkent dezelfde bezoeker bij een volgend bezoek
<code>_ga_VDH4DEMO7</code>	Google Analytics 4	20 november 2027	houdt de sessie bij voor het meetaccount



Figuur 1: Uw homepage zoals de bezoeker ze zag (ingekort; de stippellijn markeert het weggelaten lege deel): de cookiebanner staat nog open, de twee analysecookies zijn al gezet.

Waarom het telt. Volgens art. 10/2 van de wet van 30 juli 2018 en de cookierichtlijnen van de Gegevensbeschermingsautoriteit vraagt het plaatsen van analysecookies voorafgaande toestemming van de bezoeker; cookies die strikt noodzakelijk zijn om de gevraagde dienst te

leveren, vallen daarbuiten. Een banner die er staat terwijl de cookies al gezet zijn, laat de keuze van de bezoeker niet echt werken. Bij een boekhoudkantoor letten bezoekers extra op vertrouwen.

Wat te doen.

1. **Zoek waar de analysecode zit.** Meestal in het thema (Weergave > Thema-editor, `header.php`), in een plugin als "Insert Headers and Footers" of "WPCode", in Google Site Kit, of in Google Tag Manager. Een code die rechtstreeks in het thema staat, kan de cookieplugin niet tegenhouden.
2. **Laat de code pas laden na "Aanvaarden".** Plaats ze in de categorie "statistieken" van de cookieplugin, of gebruik Google Consent Mode v2 in de *basic*-modus: dan laden de Google-tags helemaal niet vóór toestemming. De *advanced*-modus stuurt vóór toestemming al cookieeloze meldingen naar Google; kies die niet zonder juridisch na te gaan of dat voor u aanvaardbaar is.
3. **Geef een even zichtbare knop "Alles weigeren"** naast "Alles aanvaarden", op de eerste laag van de banner.

WAAR WIJ DIT ZAGEN Uw homepage in een privévenster, developer tools (F12), tabblad Application > Cookies. vdhome.be/webcheck [art. 10/2 wet 30 juli 2018](#) [cookiechecklist van de GBA](#)

Zo ziet u dat het klaar is. Open de site in een privévenster en klik niets aan: bij de developer tools (F12) > Application > Cookies staat geen `_ga` meer.

2.2 Lettertypes rechtstreeks bij Google

Hoog Wie: webbouwer | Tijd: minder dan 1 uur

Wat wij zagen. Bij elk bezoek haalt de browser de lettertypes op bij `fonts.googleapis.com` en `fonts.gstatic.com`, binnen drie seconden na het openen en vóór elke keuze in de banner.

Waarom het telt. Daarbij ontvangt Google het IP-adres van de bezoeker. Een IP-adres kan een persoonsgegeven zijn (art. 4.1 AVG; Hof van Justitie, Breyer, C-582/14). U moet die verwerking dan kunnen rechtvaardigen en in uw privacyverklaring vermelden; voor een lettertype is dat moeilijk te onderbouwen, omdat hetzelfde lettertype van uw eigen server kan komen.

Wat te doen. Zet de lettertypes op uw eigen server, bijvoorbeeld met een plugin die Google Fonts lokaal bewaart (zoals "OMGF"), of door de bestanden zelf in het thema te laden, en verwijder de verwijzing naar `fonts.googleapis.com`. Het uitzicht van de site verandert niet.

WAAR WIJ DIT ZAGEN Uw homepage, developer tools (F12), tabblad Network, filter `fonts.g`. vdhome.be/webcheck [art. 13 AVG](#) [Breyer \(C-582/14\)](#)

Zo ziet u dat het klaar is. Developer tools (F12) > Network, pagina herladen, filter `fonts.g`: de lijst is leeg.

2.3 Privacyverklaring

Middel Wie: u, met ons tekstvoorstel | Tijd: 1 uur

Wat wij zagen. Onderaan elke pagina staat een link "Privacyverklaring" (goed). De tekst gaat over de verwerking van klantgegevens, maar zegt niets over de website: niet welke cookies er zijn, niet dat Google Analytics en Google Fonts gebruikt worden, niet hoe lang gegevens bewaard worden. Laatst bijgewerkt op 12 maart 2021.

Waarom het telt. Art. 13 AVG verplicht de verwerkingsverantwoordelijke om bezoekers te informeren over onder meer de doeleinden, de ontvangers, de bewaartermijn en hun rechten.

Wat te doen. Een paragraaf over de website toevoegen: welke cookies (naam, doel, bewaartermijn, van wie), welke ontvangers, en hoe de bezoeker zijn keuze later wijzigt. Datum aanpassen. Doe dit na 2.1 en 2.2, want die veranderen wat er te vertellen is.

WAAR WIJ DIT ZAGEN

De link onderaan uw homepage naar uw privacyverklaring.

vdhome.be/webcheck[art. 13 AVG](#)

2.4 Software op de server

Middel Wie: hostingpartij, webbouwer | Tijd: 1 tot 3 uur

Wat wij zagen. Het antwoord op de homepage bevat X-Powered-By: PHP/8.1.29, en de broncode van de homepage vermeldt WordPress 6.6.2 (meta-tag "generator").

Waarom het telt. Het PHP-project ondersteunt versie 8.1 sinds 31 december 2025 niet meer. Sommige hostingpartijen blijven fouten in hun eigen pakketten herstellen onder hetzelfde versienummer; of dat hier zo is, kunnen wij van buitenaf niet zien. Bevestigt de host dat er geen updates meer komen, dan wordt dit punt Hoog. Of WordPress 6.6.2 achterloopt, ziet u in uw beheerpaneel onder Dashboard > Updates.

Wat te doen.

1. Vraag uw hostingpartij of uw PHP nog beveiligingsupdates krijgt, en zo niet, om over te schakelen naar een ondersteunde versie: 8.4 (beveiliging tot 31 december 2028) of nieuwer. Maak eerst een back-up en test daarna het contactformulier en het inloggen.
2. Werk WordPress, het thema en de plugins bij en zet automatische kleine updates aan.
3. Laat de versievermeldingen weg: `expose_php = off` in `php.ini`, en de generator-tag via het thema of een beveiligingsplugin.

WAAR WIJ DIT ZAGENDe headers die uw homepage meestuurt (F12, tabblad Network, eerste regel, Headers). php.net

Zo ziet u dat het klaar is. `curl -sI https://uwdomein.be` toont geen X-Powered-By meer.

2.5 Beveiligde verbinding

Laag Wie: hostingpartij | Tijd: 15 minuten

Wat wij zagen. De site werkt via https (TLS 1.3), en wie `http://vdhboekhouding.example` intypt, komt automatisch op `https://` terecht (goed). In de headers die uw site meestuurt, ontbreekt Strict-Transport-Security (HSTS).

Waarom het telt. HSTS zegt de browser dat hij uw site voortaan altijd via https opent, ook als iemand een oude http://-link volgt. Het werkt vanaf het eerste https-bezoek.

Wat te doen. Laat deze header toevoegen; begin eventueel met een kortere `max-age` en verhoog na enkele weken.

- Apache (.htaccess): `Header always set Strict-Transport-Security "max-age=31536000"`
- NginX: `add_header Strict-Transport-Security "max-age=31536000" always;`
- Veel hostingpanelen hebben er een schakelaar voor ("HSTS" of "Forceer HTTPS").

Voeg `includeSubDomains` of `preload` alleen toe als alle subdomeinen via https werken; `preload` is bijna onomkeerbaar.

WAAR WIJ DIT ZAGEN

De headers die uw homepage meestuurt.

vdhome.be/webcheck[RFC 6797](#)

Zo ziet u dat het klaar is. `curl -sI https://uwdomein.be | grep -i strict` geeft een regel terug.

2.6 Meldpunt voor fouten

Laag Wie: webbouwer | Tijd: 10 minuten

Wat wij zagen. `https://vdhboekhouding.example/.well-known/security.txt` geeft "niet gevonden" (404).

Waarom het telt. Wie een fout op uw site vindt, weet nu niet bij wie hij die kan melden. security.txt is daar een veelgebruikte afspraak voor (RFC 9116).

Wat te doen. Plaats op /.well-known/security.txt een tekstbestand zoals dit, en vernieuw Expires elk jaar:

```
Contact: mailto:info@vdhboekhouding.example
Expires: 2027-07-31T00:00:00Z
Preferred-Languages: nl, en
Canonical: https://vdhboekhouding.example/.well-known/security.txt
```

WAAR WIJ DIT ZAGEN

Het adres /.well-known/security.txt op uw site.

vdhome.be/webcheck**RFC 9116**

Zo ziet u dat het klaar is. De URL toont de tekst.

3. Wat een mailserver ziet

Wanneer u een mail verstuurt, kijkt de server van de ontvanger in uw domeinnaam of die mail echt van u kan komen. Wie uw naam wil misbruiken, rekent erop dat die controle ontbreekt of niet streng is.

De waarden in dit hoofdstuk zijn **voorbeeldwaarden**: het fictieve domein staat niet in de publieke DNS (onze opzoeking gaf “bestaat niet”). In een echt rapport staat hier de letterlijke uitvoer, met het tijdstip.

Instelling	Gevonden waarde	Beoordeling
SPF	v=spf1 include:spf.protection.outlook.com -all	In orde: alleen Microsoft 365 mag voor u versturen
DKIM (selector1)	sleutel aanwezig, 2048 bit	In orde
DMARC	v=DMARC1; p=none; rua=mailto:dmarc@vdhboekhouding.example	Alleen meekijken

3.1 Valse mail in uw naam wordt niet geweigerd

Middel | Wie: IT-partner | Tijd: 3 x 30 minuten, over twee maanden

Wat dit betekent. SPF en DKIM controleren elk een deel van een mail. DMARC bepaalt wat er gebeurt als die controle faalt, en vraagt dat het domein in de zichtbare “Van”-regel overeenkomt met het gecontroleerde domein. Nu staat DMARC op p=none: “toch afleveren”. Een mail die van info@vdhboekhouding.example lijkt te komen maar van iemand anders is, kan dus nog aankomen, omdat uw domein de ontvanger niet vraagt om ze te weigeren. Grote providers zoals Gmail en Microsoft 365 zetten zulke mail meestal bij spam, maar kleinere providers en bedrijfservers leveren ze soms gewoon af.

Waarom het telt. De bekendste vorm van misbruik is een valse factuur of een valse melding “ons rekeningnummer is gewijzigd”, in naam van een kantoor dat klanten vertrouwen. Zo’n mail kan klanten naar een verkeerd rekeningnummer sturen. Met DMARC op p=reject vraagt u elke ontvanger om zulke mail te weigeren.

Wat te doen: in drie stappen naar p=reject, met zo weinig mogelijk risico op verloren mail.

Stap	Instelling	Wanneer
1	Behoud <code>p=none</code> en lees de rapporten (<code>rua</code>). Staan alle diensten erin die in uw naam mailen (boekhoudpakket, nieuwsbrief, scanner, websiteformulier), slagen ze, en komt hun domein overeen?	weken 1-4
2	<code>v=DMARC1; p=quarantine; rua=mailto:dmarc@vdhboekhouding.example</code>	week 5, als alle echte afzenders slagen
3	<code>v=DMARC1; p=reject; sp=reject; rua=mailto:dmarc@vdhboekhouding.example</code>	week 9, na een maand zonder fouten

- De rapporten zijn XML-bestanden; een gratis lezer zoals die van Postmark of dmarcian zet ze om in een overzicht.
- Die termijnen volgen de DMARC-norm (RFC 9989, mei 2026): een maand meekijken, een maand quarantaine. Posten medewerkers op mailinglijsten, blijf dan op `p=quarantine`; sommige lijsten breken de controle.
- Stap 2 geldt meteen voor alle mail; `sp=reject` sluit ook subdomeinen af die niet voor mail gebruikt worden.
- Verlaag de TTL van het DMARC-record naar 300 seconden, minstens een dag vóór u het wijzigt, zodat een rollback meestal binnen enkele minuten doorwerkt.

WAAR WIJ DIT ZAGEN De publieke DNS, zoals elke mailserver ze leest: in een echt rapport een link naar het DMARC- en SPF-record van uw domein (bijvoorbeeld via dns.google), en de leesbare test van internet.nl. internet.nl vdhome.be/webcheck [RFC 9989](https://rfc9989.org)

Zo ziet u dat het klaar is. `nslookup -type=TXT _dmarc.uwdomein.be` toont `p=reject`.

3.2 Elektronische facturen (Peppol)

Sinds 1 januari 2026 moeten Belgische btw-plichtige ondernemingen onderling gestructureerde e-facturen versturen en kunnen ontvangen, in principe via Peppol. Of uw onderneming als ontvanger bekend is, staat meestal in de publieke Peppol-lijst (directory.peppol.eu); vermelding daar is niet verplicht, dus een ontbrekende vermelding is een vraag voor uw boekhoudpakket, geen bewijs. Wij kijken in die lijst, zonder contact met uw systemen.

Wat wij nakeken	Gevonden	Beoordeling
Ondernemingsnummer (0208)	0208:0000000097	In orde
Btw-nummer (9925)	9925:be0000000097	In orde
Facturen en creditnota's ontvangen (Peppol BIS 3.0)	ja, beide	In orde
Geregistreerd sinds	2025-11-04	

Voorbeeldwaarden: het fictieve kantoor staat niet in de echte lijst. Staat uw onderneming er niet in, vraag dan aan uw boekhoudpakket of Peppol-aanbieder of u geregistreerd bent; een registratie is meestal binnen een dag geregeld, ook via een gratis toegangspunt.

Zo kijkt u het zelf na. Zoek uw ondernemingsnummer op directory.peppol.eu.

4. Wat u nu doet

Alles op één blad, in de volgorde waarin wij het zouden aanpakken. De mails in bijlage C zeggen elke partner precies wat er van hem verwacht wordt.

	Actie	Wie	Tijd	Voorrang	Wanneer
1	Analysecookies pas na toestemming; knop "Alles weigeren"	webbouwer	1-2 u	Hoog	deze week
2	Lettertipes op de eigen server	webbouwer	< 1 u	Hoog	deze week
3	DMARC in drie stappen naar p=reject	IT-partner	3 x 30 min	Middel	start deze maand
4	PHP-updates laten bevestigen of PHP 8.4	hosting	1-3 u	Middel	deze week
5	WordPress, thema en plugins bijwerken	webbouwer	1 u	Middel	deze week
6	Privacyverklaring aanvullen	u, met ons tekstvoorstel	1 u	Middel	na 1 en 2
7	HSTS-header	hosting	15 min	Laag	deze maand
8	security.txt	webbouwer	10 min	Laag	deze maand

Samen: ongeveer 6 tot 10 uur werk bij uw partners, plus 15 minuten voor u, aan hun gebruikelijke uurtarief.

Nieuwe meting na 30 dagen. Wij herhalen hetzelfde bezoek en dezelfde DNS-opzoeking en sturen een vergelijking: per punt "opgelost", "deels" of "nog open", met nieuw bewijs.

5. Wat VDHome voor u kan doen

Alles in dit rapport kunt u zelf of via uw webbouwer en IT-partner laten doen; niets vereist ons. Wilt u het uit handen geven of laten nakijken, dan kan dat aan een vaste prijs:

Dienst	Wat u krijgt
DMARC naar p=reject	de rapporten gelezen, de exacte instellingen per stap, en de eindcontrole
Cookiefix nakijken	zodra uw webbouwer het plan uit 2.1 en 2.2 uitvoerde, meten wij opnieuw en bevestigen wij schriftelijk wat wij dan zien
Tekst privacyverklaring	een paragraaf over uw website, klaar om te plaatsen
Doorlopend toezicht	elke maand dezelfde meting en een melding als er iets terugkomt

Dit rapport kost EUR 250, bij bestelling tot 31 december 2026 EUR 150 (excl. btw). Bestelt u binnen drie maanden na levering een bundel of CyberFundamentals Basic, dan trekken wij het volledige bedrag van dit rapport daarvan af (eenmaal per klant). Vraag gerust een offerte via info@vdhome.be.

Bijlage A. Hoe wij het bewezen

Wat wij beschrijven, moet later nog aantoonbaar zijn, ook als uw website intussen veranderd is. Daarom bewaren wij van elke meting een bewijsmap met hashes en onafhankelijke tijdstempels.

Onderdeel	Inhoud
Bewijsmap	15 bestanden: netwerkverkeer, screenshot, paginabron, local storage, cookies met het script of de header die ze zette, alle headers, IP-adres en TLS-gegevens van de server, DNS-antwoorden, browser en versies, en een kopie van ons meetscript
Hashes	SHA-256 van elk bestand, in <code>MANIFEST.sha256</code> (zelf: <code>eb35b825b166e309...0e2760fb28d91fbe61f3c</code>)
Tijdstempels	twee onafhankelijke diensten (RFC 3161): freetsa.org om 19:01:10 UTC en DigiCert om 19:01:11 UTC, beide geverifieerd; freetsa.org is geen gekwalificeerde dienst in de zin van eIDAS, daarom het tweede
Meetpunt en klok	gemeten vanuit België; klokafwijking 0,1 seconde tegenover <code>time.cloudflare.com</code> . Voor dit voorbeeld, gemaakt vanaf een privéverbinding, laten wij het IP-adres van het meetpunt weg; bij een klantrapport meten wij vanaf een server van VDHome
Privacy	alleen gegevens van onze eigen meetbrowser, geen gegevens van echte bezoekers; cookiewaarden enkel als hash; u krijgt de geredigeerde kopie van het netwerkverkeer
Bewaring	12 maanden, alleen gedeeld met u; <code>CUSTODY.log</code> houdt bij wie wat deed

Zelf nakijken of opnieuw meten.

```
sha256sum -c MANIFEST.sha256
openssl ts -verify -in tsa/freetsa.tsr -queryfile tsa/freetsa.tsq \
  -CAfile tsa/freetsa-ca.crt -untrusted tsa/freetsa-chain.crt
python capture.py https://uwdomein.be/ nieuwe-map
```

Bijlage B. Bronnen

- [Wet van 30 juli 2018](#) betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, art. 10/2 (toestemming voor cookies; ingevoegd bij de wet van 21 december 2021).
- Gegevensbeschermingsautoriteit, cookiechecklist: <https://www.gegevensbeschermingsautoriteit.be/publications/cookie-checklist.pdf>
- [AVG](#), art. 4.1 en 13; Hof van Justitie, 19 oktober 2016, [Breyer, C-582/14](#).
- PHP, ondersteunde versies: <https://www.php.net/supported-versions.php>
- [RFC 6797](#) (HSTS), [RFC 9116](#) (security.txt), [RFC 9989](#) (DMARC), [RFC 3161](#) (tijdstempels).

Bijlage C. Mails voor uw partners

Kopieer en verstuur; pas de naam en het domein aan.

Aan uw webbouwer. Onderwerp: website - cookies, lettertypes en updates

Dag [naam],

Een controle van onze website toonde enkele punten die ik graag laat aanpassen:

1. De Google Analytics-cookies (`_ga`, `_ga_`...) worden gezet vóór de bezoeker toestemming geeft. Kun je de analysecode pas laten laden na "Aanvaarden" (cookieplugin, of Consent Mode v2 in basic-modus), en een knop "Alles weigeren" toevoegen? Kijk ook of de code niet rechtstreeks in het thema of in Site Kit of GTM staat.
2. De lettertypes komen van `fonts.googleapis.com`. Kun je ze op onze eigen server zetten?
3. Kun je WordPress, het thema en de plugins bijwerken, de generator-tag weglaten en een `security.txt` plaatsen?

Laat je weten wanneer het klaar is? Dank je!

Aan uw hostingpartij. Onderwerp: PHP-versie en beveiligingsheaders

Goeiedag,

Onze website meldt PHP 8.1.29. Krijgt die nog beveiligingsupdates van jullie? Zo niet: kunnen we overschakelen naar PHP 8.4? Kunnen jullie ook de header `Strict-Transport-Security: max-age=31536000` toevoegen en `expose_php` uitzetten?

Met vriendelijke groeten

Aan uw IT-partner. Onderwerp: DMARC naar p=reject

Dag [naam],

Ons DMARC-record staat op `p=none`. Ik wil in drie stappen naar `p=reject`: eerst de rapporten nakijken of al onze afzenders slagen, dan `p=quarantine`, en na een maand zonder fouten `p=reject` met `sp=reject`. Kun je de TTL van het record eerst naar 300 seconden zetten en de rapporten met mij overlopen?

Dank je!