Zo bescherm je je privacy op internet

computertotaal.nl

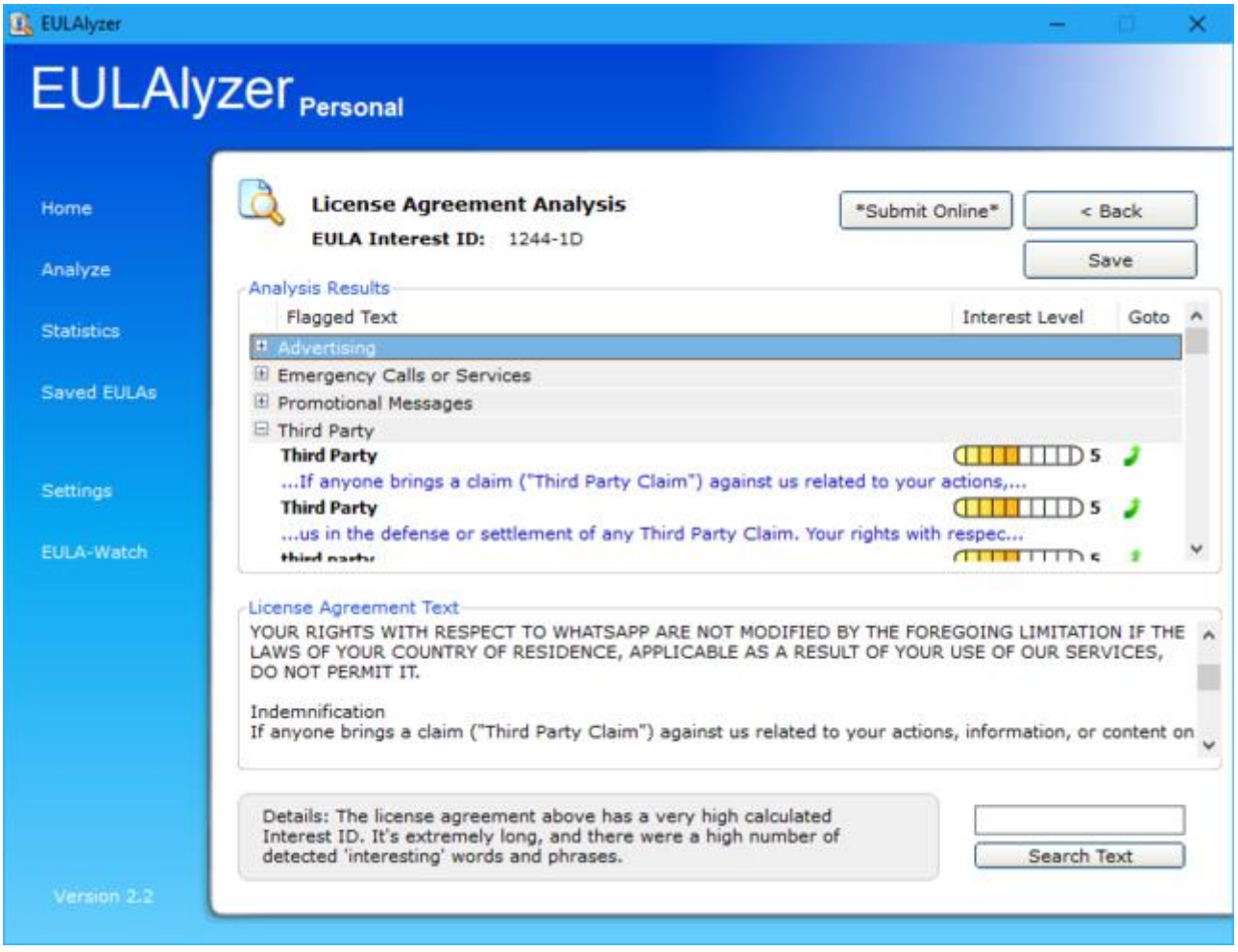
Zodra je het internet opgaat laat je sporen na en die kunnen natuurlijk privacygevoelig zijn. Met de juiste instellingen en tools kun je deze informatiestroom beter controleren en op die manier beter met je persoonsgegevens omgaan.

Tip 01: EULA

Voor je een contract afsluit neem je waarschijnlijk grondig de overeenkomst door, inclusief de 'kleine lettertjes'. Veel gebruikers beseffen echter onvoldoende dat ze ook een contract afsluiten zodra ze software installeren of wanneer ze een webservice gebruiken, zoals sociale media. Zowat elke service of software gaat namelijk vergezeld van een eindgebruikersovereenkomst

oftewel EULA (end user's license agreement), een 'privacy policy' en/of 'Terms of service'.

Zo'n overeenkomst is echter vaak ellenlang, complex en niet zelden Engelstalig en dus voelt u er ongetwijfeld weinig voor die allemaal door te nemen. U kunt zich echter laten bijstaan door de gratis Windows-tool EULAlyzer: die speurt specifiek naar clausules waarin uw privacy mogelijk in het gedrang komt. Het volstaat de – Engelstalige - tekst van zo'n EULA in het programmavenster te plakken en de tool wijst u automatisch op belangwekkende en mogelijk 'verdachte' onderdelen. Aan jou om te beslissen of je daar mee kunt leven voor je je akkoord verklaart met de overeenkomst.



Tip 01 EULAlyzer speurt overeenkomsten af naar passages die mogelijk van invloed zijn op uw privacy.

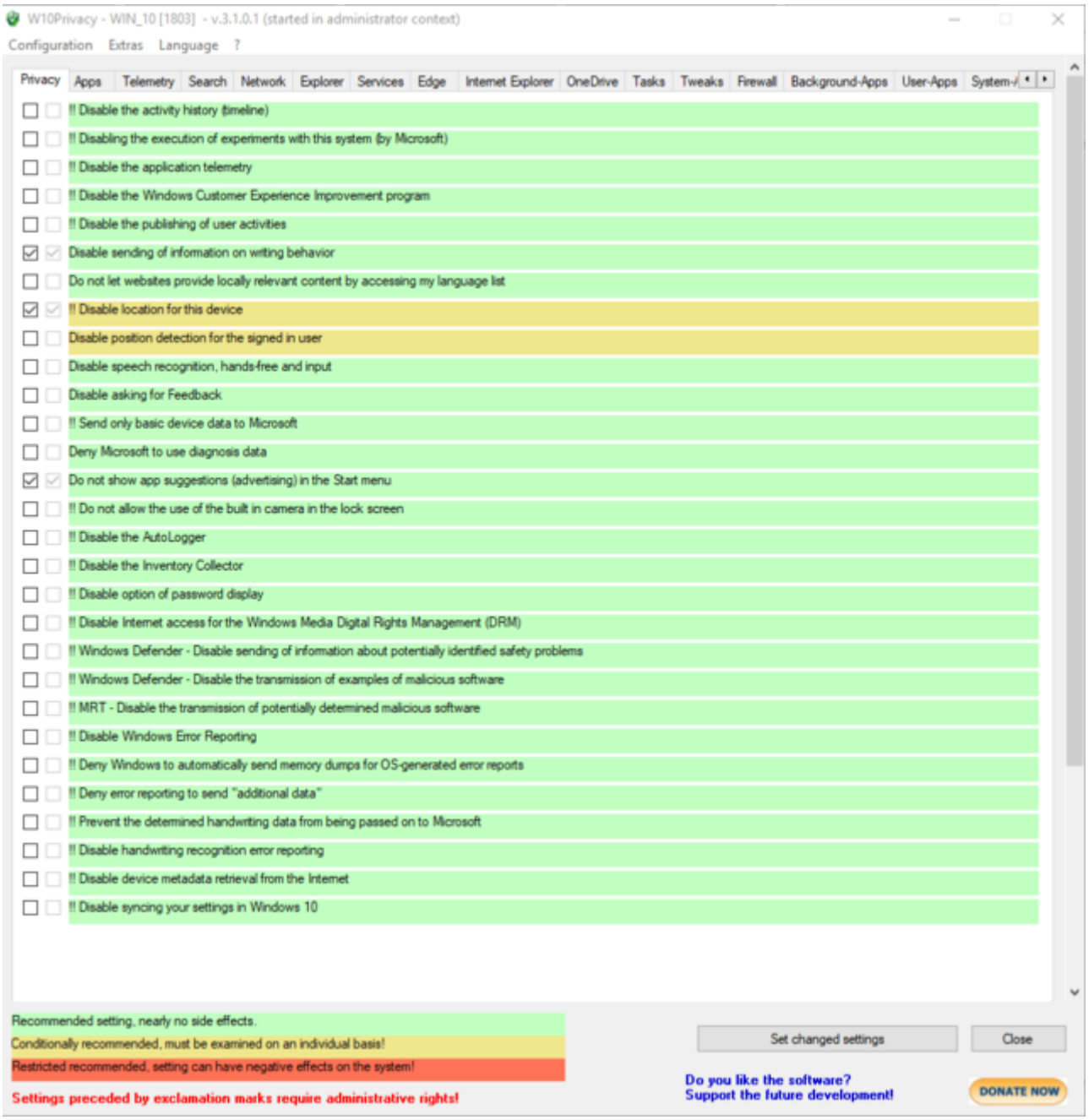
GDPR

Wie het over privacy heeft, kan nog moeilijk om het begrip GDPR heen. Dat staat voor General Data Protection Regulation en heet in het Nederlands Algemene Verordening Gegevensbescherming (AVG). Deze Europese regelgeving werd al meer dan twee jaar geleden in het leven geroepen, maar is pas sedert 25 mei 2018 officieel van kracht. Het algemene principe is dat bedrijven alleen gegevens mogen inwinnen die ze echt nodig hebben en ze moeten daarover naar de gebruiker toe ook in zeer duidelijke termen communiceren. Zo moet elk bedrijf of organisatie expliciet melden waarvoor ze – na je expliciete goedkeuring - je gegevens nodig hebben en hoe ze die opslaan. Deze informatie mag niet langer dan nodig worden bewaard en mag niet zomaar aan derden worden doorgespeeld. Elke gebruiker heeft bovendien het recht om die data op elk moment te kunnen raadplegen en om die weer te laten weghalen.

GDPR biedt meer bescherming voor uw privacy, maar ontslaat je niet van je eigen verantwoordelijkheid.

Tip 02: Windows 10

Het doorsturen van mogelijk privacygevoelige gegevens begint al zodra Windows 10 is geladen en je met het internet bent verbonden: er zitten namelijk heel wat functies ingebouwd in Windows en bijhorende apps als Edge die allerlei gegevens aan Microsoft doorspelen. Via **Instellingen / Privacy** kun je weliswaar heel wat van die functies bijstellen, maar met een gratis tool als W10Privacy kan dat nog grondiger. Start het portable programma op als administrator en laat een herstelpunt creëren. Op tabbladen als **Privacy**, **Apps**, **Telemetry**, **Search**, **Services**, **Edge**, enz. vind je dan allerlei privacy-gerelateerde onderdelen terug. Je hoeft slechts een vinkje te plaatsen om de bijhorende optie te activeren, waarna je bevestigt met **Set changed settings**. In principe kun je de groen gekleurde opties probleemloos activeren, maar bij de gele en vooral rode onderdelen kun je het best eerst nagaan wat de mogelijke implicaties zijn. Desnoods zoek je naar meer informatie op het internet.



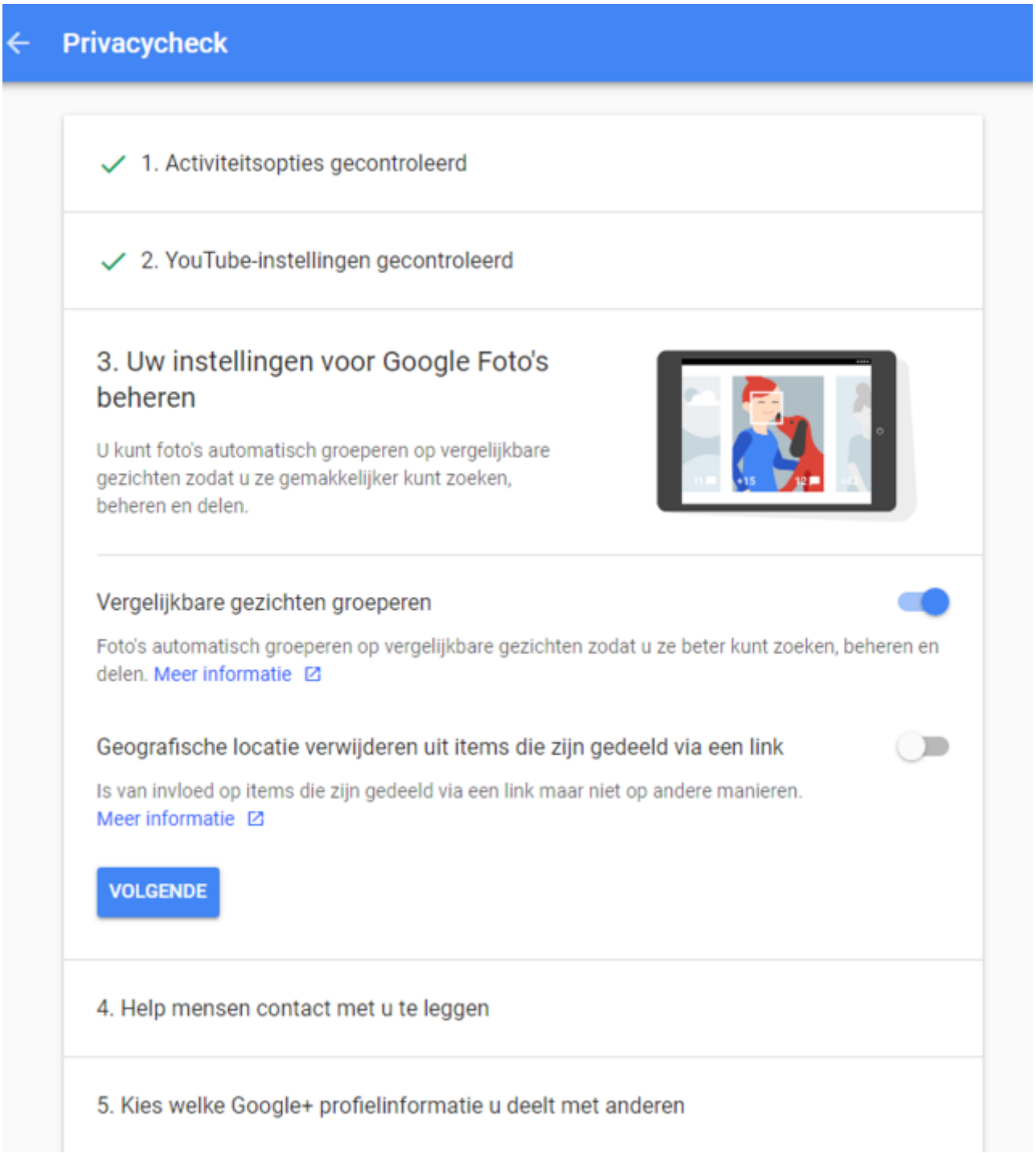
Tip 02 Windows bevat meer privacygerelateerde instellingen dan Microsoft je laat vermoeden.

Het (heimelijk) verzamelen van privacygevoelige data begint al bij het opstarten van Windows

Tip 03: Sociale media

Facebook (waartoe ook WhatsApp behoort) en Google behoren ongetwijfeld tot de meest notoire sprokkelaars van gebruikersgegevens. Zoals bij veel andere webservices kun je gelukkig ook hier een en ander bijstellen. Google biedt hiervoor een privacytool aan, die je hier vindt. Je hoeft hier weinig meer te doen dan ongewenste functies of opties uit te schakelen bij diverse Google-services, waaronder Web- en app-activiteit, Locatiegeschiedenis, Spraak- en audioactiviteit, YouTube zoek- en kijkgeschiedenis, Google Foto's, Google+, enzovoort.

Ook Facebook bevatte een privacytool, die je vanaf de website kon bereiken met de optie **Privacycontrole**. Die blijkt echter verdwenen, maar je kunt wel nog allerlei privacy-opties aanpassen via **Instellingen / Privacy**. Controleer hier echter ook andere rubrieken als **Locatie**, **Gezichtsherkenning**, **Advertenties** en **Apps en websites**. De Facebook-app biedt echter een handig privacy-overzicht. Tik het hamburgerknopje aan en kies **Instellingen en privacy / Privacysnelkoppelingen**. Je krijgt dan een overzicht van wat je zoal kunt doen om je account en je privacy te beschermen.



Tip 03 Google voorziet in een handige privacytool.

Tip 04: Browserdata

Je browser is wellicht de tool waarmee je het vaakst op het internet gaat en dus wil je vast wel weten welke informatie die zoal naar de exploitanten van de bezochte sites stuurt. Een handige site om dat uit te vissen is

www.browserspy.dk: in het linkerpaneel tref je namelijk heel wat tests aan. Zo kom je te weten of de geolocatie-functie van je browser is geactiveerd en hoe nauwkeurig die werkt, welke cookies worden aanvaard, welke UserAgent-string je browser doorstuurt, enz. Ook www.ip-check.info levert interessante feedback op – wel eerst even op **Start test** klikken. Overigens is deze site wel bedoeld om je anonimisering via JonDonym aan te bevelen (zie tip 07). Opvallend is Panopticlick, die tracht je browser op basis van allerlei unieke eigenschappen te identificeren, het zogenoemde browser fingerprinting. Je hoeft hiervoor slechts op de knop **Test me** te drukken en na afloop **Show full results for fingerprinting** aan te klikken. Ook https://absolutedouble.co.uk bezorgt je een 'fingerprint' van je browser (klik ook hier op **Start test**).