T.a.v. ██████████████
Senior adviseur Veiligheid
Stadsplateau 1, 14e etage Zuid
Gemeente Utrecht

Groningen, 13 december 2018

Betreft: SafeCity Utrecht: Offerte dienstverlening 2019

Beste ████

Op basis van het succes van het project in 2018 heb je ons gevraagd een offerte voor onze dienstverlening in 2019. Hierbij zoals beloofd de aangepaste offerte voor de periode tot 31 december 2019 met name gefocust op de mensenhandel module.

Hieronder het overzicht van wat wij aanbieden:

1) **Het Voyager Intelligence Platform**

   Dit betreft het softwareplatform van Web-IQ waarmee wij voor jullie continu data verzamelen uit verschillende online bronnen, waar de extracties, analyses en netwerkanalyses plaatsvinden en waarop jullie team kan inloggen om de data te bevragen, exploreren, prioriteren, trends bekijken en te visualiseren. Dit alles inclusief case management, bookmarks en notificaties.

   Web-IQ biedt jullie de mogelijkheid deze Voyager suite in onze eigen secure cloud te laten draaien. Wij nemen de infrastructuur voor onze rekening, inclusief het technische operationele beheer zodat alles soepel verloopt. Jullie krijgen toegang tot deze online dienst voor een maximum van 10 gebruikers, die eenvoudig met een webbrowser via een beveiligde verbinding inloggen.

   Je kunt daarmee over alle componenten van Voyager beschikken, inclusief alle huidige en toekomstige analyse-plugins en je lift mee op de innovaties die we de komende maanden en jaren op het platform doorvoeren. De capaciteit van deze setup is voldoende om het project zoals we besproken hebben te kunnen ondersteunen. Aanvullende capaciteit (mochten jullie in de toekomst echt aanzienlijk meer data willen verzamelen) is tegen meerprijs te regelen.

2) **Datasets**

   Gedurende 2017 is duidelijk geworden welke websites er ten behoeve van de dienstverlening noodzakelijk zijn om beschikbaar te hebben via Voyager. We zijn gestart met 5 websites en hebben dit uitgebreid naar 27. Wij zorgen ervoor dat gedurende het gehele jaar deze sites (mits nog aanwezig en relevant) continu worden gecrawld en geanalyseerd.

3) Support

Het Internet en het mensenhandel fenomeen dat zich daar ook afspeelt, is onderhevig aan veranderingen. Er komen bijvoorbeeld sites bij en vallen sites af. Ook worden risico-analyses steeds beter als we hier gezamenlijk aandacht aan besteden. Daarnaast zal de manier waarop de Gemeente werkt en waarop jullie prioriteiten stellen ongetwijfeld wijzigen.

Om ervoor te zorgen dat het systeem aansluit bij jullie eisen en wensen komen we in 2019 twee keer bij jullie langs. Voor tussentijdse vragen en verzoeken is directe support via e-mail of telefoon inbegrepen.

Hiermee hebben jullie t.b.v. de openbare orde twee modules tot jullie beschikking:

1) Een operationele module t.b.v. Mensenhandel (betaald)
2) Darknet en Darknet Markets datasets die ook ten behoeve van ondermijningsonderzoeken kunnen worden ingezet. Daarnaast is het voor jullie eigen kennisverwerving op het gebied van de ontwikkelingen die op deze donkere omgeving van het internet plaatsvinden goed om op een veilige manier toegang te hebben tot deze data.

Voor het bieden van bovenstaande dienstverlening rekenen wij € ███████ exclusief btw.

Het privacy statement en de algemene voorwaarden van Web-IQ (bijgevoegd) zijn op deze offerte van toepassing;

Met vriendelijke groet,

████████████████ , Web-IQ

VOYAGER T&C

1.1 Intended Use and Limitations

a. Customer intends to use Voyager as a Service to support Customers insights and processes.

b. Customer will only use these Services in a legal way.

c. Customer will use the API Service to perform ad-hoc (not bulk) searches in the datasets.

d. Supplier will provide service documentation to the Customer.

1.2 Performance. Support and Updates

a. Supplier will inform Customer on forehand (at least 24 hours) when it plans to perform scheduled maintenance to the Service.

b. Supplier offers technical support via email (support@web-iq.eu) or phone (+31502111622) during Dutch office hours (9:00-17:00 CET). Supplier will respond to support requests within 1 working day.

c. Bugs and operational interruptions in the Services that affect the Intended Use, as described above, will be solved by the Supplier within 7 working days after notification by the Customer.

d. The Supplier will update agreed datasets on a daily basis. The content of these datasets is determined by the Supplier.

1.3 Ownership & Intellectual Property

a. Web-IQ is the sole owner of Voyager and the API Service. Intellectual property of Voyager and the API Service is and will remain with Web-IQ at all times. Web-IQ grants to Customer a non-exclusive, non-transferable license to use the Services.

b. The Customer may use the Services only for its own use. Customer may not transfer or sublicense direct access to the Services to any third party by sharing credentials.

1.4 Miscellaneous

a. Customer represents and warrants that, except with prior permission in writing from Web-IQ, Web-IQ and its personnel will be not be exposed as the developer and supplier of Voyager nor the API Service to any third party. Customer will indemnify and hold Web-IQ harmless from any and all costs, expenses, claims, charges, damages and fees that may arise from a breach of this article.

b. Customer represents and warrants to Web-IQ that the use of Voyager and the API Service by Customer shall not infringe on any local, national or international law and/or other privacy right of any third party or person (data protection laws). Web-IQ will not be in any way liable for any issue occurring in this matter. The total liability in these occurring cases shall rest with Customer. Customer will indemnify and hold Web-IQ harmless from any and all costs, expenses, claims, charges, damages and fees that may arise from a breach of this article.

c. Before, during and after Voyager and the API Service is used by Customer, any result used will be Customer's sole responsibility. Web-IQ will not in any way be responsible nor liable for any consequences of Customer using Voyager or the API Service.

Web-IQ Privacy Statement

Web-IQ (Web-IQ B.V) takes data privacy seriously. This document sets out who we are, what we do and when and how we use your personal information.

In addition to this privacy statement, we make formal agreements with our customers and partners about the exchange of information. If this information includes personal data, we make sure that a proper Data Protection Agreement is in place.

We have appointed a data protection officer who is responsible for overseeing questions in relation to this privacy statement. If you have any questions about this privacy statement, including any requests to exercise your legal rights, please contact our data protection officer (Ronald Hoek) by email at dpo@web-iq.org.

This privacy statement was last updated on **28th August 2018**.

1.1   What we do

Web-IQ offers services that enable our customers to search public data from the internet and use this for their own objectives. We work primarily for customers who are active in the field of security, justice, risk assessment and fraud prevention and who use our services to make the world a better and safer place.

To make this possible, Web-IQ collects public data on behalf of its customers. This may include your personal data.

Web-IQ collects public data from various online sources, such as social media, news sites, market places, blogs, forums and the dark web. Web-IQ does not collect any protected information and guarantees to keep the collection process limited to data that contributes to the information needs of our customers. We collect data on behalf of our customers. This means that in terms of the GDPR, Web-IQ acts as the data processor.

In addition, Web-IQ enables customers to install and operate Web-IQ software themselves on their own servers. As part of this, customers may capture public data from the internet or dark web onto their own

systems, potentially including your personal data. We help our customers to comply to the privacy and data protection regulations for their situation by providing software that allows them to control and limit what data is being collected, how long the data is stored and who and how the data can be accessed.

In our agreements with our customers we state that our customers may only use our services, data and products in a lawful manner that respects all applicable privacy aspects. Web-IQ will not do business with organizations that are related to countries, individuals or groups on the European Union Sanctions List.

We also use personal information from our customers, business contacts, web site visitors and people who signed up for our newsletters.

1.2 How we use your data

1.2.1 When you partner with us or purchase our services or products

If you become our customer or partner, we may collect personal information about you or your employees, like names, email addresses, telephone numbers. We use this information only to contact you and fulfill our contractual obligations.

We will not share this information with other customers nor third-parties without your consent and we will make sure that this information is protected properly.

1.2.2 When you use our Voyager Cloud services

Customers that sign up for our Voyager Cloud services (such as DarkCloud or SafeCity) need to provide a valid email address to create an account. We will use this email address only to send you monitoring alerts and other automated system notifications (opt in) and system maintenance updates. Your email address will never be disclosed to third-parties, nor will it be used for promotional or commercial purposes by Web-IQ without your prior consent.

Web-IQ does not actively collect nor monitor your navigational actions (like queries and clicking on items of interest). However, this information, including personal information like your IP address can appear in the log files of our underlying services. Log files are kept for a limited period (7 days) and only for support and maintenance purposes.

If you need more information about how we protect your case data in our Voyager Cloud services, the user agreement and the terms and conditions that apply, please contact us at info@web-iq.com.

1.2.3   When our software captures your online information

In a similar way to how search engines work, Web-IQ searches and stores public data from the internet and the dark web on behalf of its customers. As part of this, we may capture your personal information which is publicly available.

We only collect public data. This is data that is actively shared online at places such as social media, news sites, darknet market places, blogs and forums and can be found with a standard internet search engine or by visiting the relevant site on the internet or dark web.

We have designed our services with privacy in mind:

- We do not collect data that is protected or shared in private.
- We aim not to collect nor store data when there is no specific reason to do so. We only search and collect data that is required to answer the questions from our customers.
- We do not store data longer than needed. Some use cases, such as discovering trends over time and reconstructing events from the past, require us to store the collected public data for a longer period. Other use cases, like most of our risk and fraud detection services keep the collected data in memory for only a few seconds but never store any data on disk or in a database at all. We will delete data when the contract with our customer ends.
- We aim to anonymize the data as much as possible, although this might not always be possible given the use cases of our customers.
- We will always be open about our intended use of the data and we will inform our customers about how we have collected the data, so our customers can make sure that the way they use the data on their side is lawful and respects privacy.
- We will make sure that all data that is collected is linked to the original source, so the information can always be placed in its original context.
- When requested by an individual we will disclose all public information held on that individual.

1.2.4   **When you visit our web site**

Our public web site (www.web-iq.com) does not use cookies, nor does it use third-party services to track you.

However, your IP address is logged temporary in the access log of our web server for debugging purposes. These log files are deleted after 10 days.

1.2.5   **When you subscribe to one of our newsletters**

When you subscribe to one of our newsletters, such as the Darknet Update, we keep your email address and name, so we can send you the information you signed up for. We will not use this email address to spam you with other information or for any other purpose.

We use a newsletter service that allows us to keep track of how many subscribers open and interact with our newsletter emails. We use this information solely to learn how we can improve the content of our newsletter.

Each newsletter contains a link that allows you to unsubscribe. We permanently remove the personal data from inactive subscribers on a monthly basis.

1.3   **Your rights**

You have the right to object to us handling your personal information (as described in the "How do we use your data" section above). If you ask us to stop handling your personal information in this way, we will stop unless we can show you that we have compelling grounds as to why our use of your personal information should continue. For other questions regarding your rights under the data protection laws, please contact us at dpo@web-iq.org

1.4   **Data Security**

To protect your personal information, we have implemented several measures:

- The Web-IQ software is hosted on secure servers in The Netherlands.
- To operate our services, we work together with known partners within the European Economic Area that have the appropriate certifications and clearances for providing services to government organizations and law enforcement agencies.

- Within our organization, data is only made available on a need-to-know basis. All employees of Web-IQ can present a certificate of conduct and additional screening is required for some functions.
- Information security is on top of our agenda. We have appointed an Information Security Officer and are taking major steps to become ISO 27001 certified next year.
- Periodically, independent parties perform penetration tests and scan for potential vulnerabilities in our systems.
- We apply best-practices and guidelines ensuring privacy and information security in our organization, such as separation of environments, encryption of documents and communication, access control, incident report procedures, monitoring and audits.

1.5   Changes to this privacy statement

We may update this privacy statement from time to time. The latest version of this privacy statement can be found on our web site: https://web-iq.com/privacy-statement/

If you have any questions about this privacy statement, please contact us.

Data Protection Officer

█████████

dpo@web-iq.org

Web-IQ B.V.

Helperpark 284

9723 ZA Groningen

The Netherlands

31 (0)50 21 11 622

info@web-iq.com