Legitimate Interest Assessment (GDPR)

This LIA was conducted by Mononox with regards to the web application firewall (WAF) we deploy on our own and our client's websites in order to maintain their security. In the process of scanning website traffic, malicious IP addresses will be shared with the WAF vendor: Defiant Inc. (USA) – Privacy Policy (Privacy Shield: **Pending**, compliant via SCC's)

Part 1: Purpose test

Assessing whether there is a legitimate interest behind the processing.

1. Why do you want to process the data?
2. What benefit do you expect to get from the processing?
3. Do any third parties benefit from the processing?
4. Are there any wider public benefits to the processing?
5. How important are the benefits that you have identified?
6. What would the impact be if you couldn't go ahead with the processing?
7. Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)?
8. Are you complying with other relevant laws?
9. Are you complying with industry guidelines or codes of practice?
10. Are there any other ethical issues with the processing?

Answers:

1. Strictly for security reasons.
2. Blocking malicious visitors/bots and hackers.
3. Yes, the firewall vendor will be glad to know about malicious IP addresses.
4. Yes, since the website its kept clean, browsing is safer for all users.
5. Absolutely inevitable.
6. We would have to rely on a significantly less secure solution.
7. EU-GDPR
8. Data protection laws of: Germany
9. At all times, we deploy the firewall in the most secure way (as an auto-prepend script, so it gets loaded before anything else)
10. No

Part 2: Necessity test

Assess whether the processing is necessary for the purpose that’s been identified.

1. Will this processing actually help you achieve your purpose?
2. Is the processing proportionate to that purpose?
3. Can you achieve the same purpose without the processing?
4. Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Answers:

1. Yes
2. Yes
3. No
4. No

Part 3: Balancing test

Consider the impact on individuals’ interests and rights and freedoms and assess whether this overrides any legitimate interests.

Nature of the personal data

1. Is it special category data or criminal offence data?
2. Is it data which people are likely to consider particularly ‘private’?
3. Are you processing children’s data or data relating to other vulnerable people?
4. Is the data about people in their personal or professional capacity?

Answers:

1. No
2. No
3. Yes, in theory (a firewall scans all traffic) but it’s not at all targeted at them
4. Theoretically, both

Reasonable expectations

1. Do you have an existing relationship with the individual?
2. What’s the nature of the relationship and how have you used data in the past?
3. Did you collect the data directly from the individual? What did you tell them at the time?
4. If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?
5. How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
6. Is your intended purpose and method widely understood?
7. Are you intending to do anything new or innovative?
8. Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation?
9. Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

Answers:

1. No
2. Visitors, customers and their employees. We've only ever shared bad IP's.
3. No, it's a passive system but it's outlined in the Privacy Policy.
4. No
5. N/A
6. Yes
7. No
8. N/A
9. People who attempt to hack a website would perhaps know that there's a firewall in place that may record and share their malicious activity.

Likely impact

1. What are the possible impacts of the processing on people?
2. Will individuals lose any control over the use of their personal data?
3. What is the likelihood and severity of any potential impact?
4. Are some people likely to object to the processing or find it intrusive?
5. Would you be happy to explain the processing to individuals?
6. Can you adopt any safeguards to minimise the impact?

Answers:

1. People may become personally identifiable by means of their IP address.
2. Hackers, Spambots, etc. but we allow to have falsely blocked IP's cleared.
3. Very low for regular visitors, rather high for attackers.
4. We think not, as security is in the interest of everyone and we're not using a cloud/proxy solution but a locally installed one that only shares positive matches.
5. Absolutely, it's outlined in our privacy policy (https://mononox.com/privacy/)
6. Yes, we're using the most secure way to implement the firewall.

Can you offer individuals an opt-out?	Yes / [✓ No]

Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

Can you rely on legitimate interests for this processing?	[✓ Yes] / No
We're going to stay alert on changes to policies and practices of our subprocessor and will frequently revisit the means and justification of this processing.	
LIA completed by	Sven Tolle (Mononox)
Date	May 20 2018