Appendix 1

Technical and organizational security measures of DCMN GmbH according to Art. 32 DSGVO

1. Pseudonymization

- Anonymization of IP Address
- Internal procedures are established so that we are able to cease the processing of data (tracking code on client websites) if the client is not able to prove they possess the legal basis for collecting and processing data.

2. Encryption

- Use of the TLS (Transport Layer Security) protocol during collection of data with tracking codes and with the use of the DC Analytics tool
- All data are stored and processed within the EU. We use Amazon Web Services (AWS) as well as LeaseWeb for data processing. AWS processes this data as Processor (Auftragsverarbeiter) in the sense of the DSGVO. They provide a state-of-the-art Infrastructure as a Service (IaaS) platform with up-to-date encryption capabilities.
  At LeaseWeb we host physical servers which are located in the Datacenter in Amsterdam. The communication to these servers is only possible via encrypted transfer (SSH or TLS).

3. Confidentiality

- **Data from client websites and/or mobile apps (tracking data):** Access to this data is limited to a small group of employees who are authorised to manage and maintain the infrastructure. Access is only possible via secure passwords and access keys.
- **User data:** Access is limited to a small group of users (administrators) with the responsibilities a) to manage clients of our products and b) to assure the operational security and functionality of our products. Access is only possible via secure, regularly-rotating passwords and access keys.
- Access to the premises of DCMN is limited through an automated entry control system. Visitors are required to identify themselves at the reception desk and enter their names into a visitors list. The entry for visitors is controlled and monitored via the reception desk.
- Simple exercise of revocation right (Widerrufrecht) of individuals via technical means (opt-out link).

4. Integrity of data

- Only a small number of selected applications within the infrastructure have access to personal data. In addition, we apply the principle of minimal access permissions, i.e., unless an explicit authorization exists, we allow only read-only access to data. This is, among other measures, implemented through a role-based permissions system.
- Only a small number of selected users within DCMN have access to personal data. This is implemented through a permissions system in which users are assigned

detailed roles, that then dictate access privileges.
- All internal systems at AWS are not publicly accessible on the internet. Systems on LeaseWeb which are reachable via the internet require a valid SSH key for access and an additional password for administrative access.

5. Availability

- All of our data is secured through regular backups and secured against natural catastrophes or system failures through the use of Amazon's redundant infrastructure.

6. Capacity of processing systems

- All of our applications run on highly available, redundant infrastructure with built-in failover mechanisms.

7. Procedures to restore availability and access to personal data in the case of a physical or technical failure

- Our backups are regularly archived. In the case of a physical or technical failure, these backups can be used to restore the original state.

8. Procedures to regularly verify, assess and evaluate the effectiveness of technical and organizational measures

- Through internal technical and organizational processes, we regularly verify if our infrastructure, software and organization meet the legal requirements of data protection regulations.
- LeaseWeb's datacenter is ISO 27001(2013), PCI DSS, SOC I, HIPAA and NEN 75 certified.
- We do not categorically share personal data with external service providers. In the case that DCMN engages an external service provider to processes personal data, they will be audited and made to sign an agreement in the sense of Art. 28 DSGVO before a contract is signed.
- DCMN has appointed the following external operational data protection officer, who is available via the following contact information:

Dr. Felix Wittern
Fieldfisher (GERMANY) LLP
Am Sandtorkai 67
20465 Hamburg

privacy@dcmn.com