DATA PROCESSING AGREEMENT

1 BACKGROUND

1.1 This data processing agreement ("**Data Processing Agreement**") is an integral part of the controller's ("**Controller**") and the processor's ("**Processor**") agreement regarding the provision of the Solution from the latter. This Data Processing Agreement governs the parties' rights and obligations and shall ensure that personal data are not used improperly or disclosed without prior authorisation or otherwise in contravention to the applicable data protection legislation, hereunder Regulation (EU) 2016/679 (GDPR), as well as the at all times applicable data protection legislation.

1.2 By entering into this Data Processing Agreement, the Controller authorises the Processor to process personal data on its behalf in accordance with the protocol in Appendix 1.

2 THE CONTROLLER'S OBLIGATIONS

2.1 The Controller shall comply with the obligations that are stipulated in the GDPR and other applicable data protection legislation, as well as this Data Processing Agreement.

2.2 The Controller shall be responsible, among other, for ensuring that the processing of personal data, which the Processor is instructed to perform, has a legal basis.

2.3 It is the Controller who determines the purpose of the processing of personal data and the means to be used during such processing, cf. the GDPR article 4 no. 7 and the data protection legislation.

3 THE PROCESSOR'S OBLIGATIONS

3.1 The Processor shall comply with the obligations that are stipulated in the GDPR and other applicable data protection legislation, as well as this Data Processing Agreement.

3.2 The Processor shall follow the documented routines and instructions for the processing that the Controller at all times has decided upon and not process personal data provided under the Data Processing Agreement in any other way or for any purpose other than what is necessary to fulfil the Processor's contractual obligations as stipulated in this Data Processing Agreement or in the documented routines or instructions of the Controller, unless processing is required by data protection legislation, in which case the Processor shall, to the extent permitted by applicable laws, inform the Controller of that legal requirement before the relevant processing of that personal data.

3.3 The personal data shall be used only by the Processor in connection with the purpose and nature of the processing as described in Appendix 1.

3.4 The Processor is obliged to notify the Controller without undue delay if the Processor considers that the Controller's instructions are in violation of the data protection legislation.

3.5 The Processor shall keep a record of the processing activities that it performs on behalf of the Controller, which shall contain at least the information required under the GDPR Article 30.

3.6 The Controller has, unless otherwise agreed or stipulated by law, the right to access and review the personal data being processed by the Processor.

3.7 If an approved code of conduct exists according to Article 40 of the GDPR or other approved certification scheme according to Article 42 of the GDPR, which the Processor has undertaken to comply with or be certified under, the Processor is required to comply with such code of conduct or certification requirements in the processing of personal data on behalf of the Controller.

3.8 The Processor is subject to a duty of confidentiality regarding the personal data that the Processor has access to under this Data Processing Agreement. The Processor shall only grant access to the personal data to persons under the Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. The Processor shall at the request of the Controller demonstrate that the concerned persons under the Processor's authority are subject to the abovementioned confidentiality.

3.9 The Processor shall not disclose personal data or information that it processes on behalf of the controller to third parties or data subjects without explicit instruction or permission from the Controller, unless otherwise provided by law. Third-party inquiries to the Processor must be forwarded to the Controller as soon as possible.

4 DATA SUBJECTS

4.1 The Processor shall assist the Controller in safeguarding the rights of the data subjects in accordance with the GDPR Chapter III. This applies to, but is not limited to, providing information on how the personal data is processed, handling inquiries concerning access to personal data and fulfilling the data subjects' rights to demand correction or deletion of the personal data.

4.2 Requests from data subjects or other third parties to the Processor regarding the personal data processed on behalf of the Controller shall be communicated to the Controller as soon as possible. The Processor shall not respond to such requests unless instructed to do so by the Controller.

5 SUB-PROCESSORS

5.1 The Processor is entitled to use sub-processors to process personal data on behalf of the Controller.

5.2 The Processor shall ensure that all sub-processors are informed of and bound by similar requirements for information security, confidentiality, use and other requirements set forth in this Data Processing Agreement and applicable privacy laws.

5.3 If the Processor wishes to engage a new sub-processor, the Processor must notify the Controller of this at least one month before the sub-processor begins processing the personal data. The Controller may deny the use of such sub-processor only if the Controller has well-grounded doubts about the ability of the sub-processor to comply with the applicable data protection legislation. If the Controller has not opposed the intended sub-processor within 14 days of the Processor's notice, the sub-processor shall be deemed approved by the Controller. If the Controller opposes the use of the sub-processor, the Parties shall negotiate in good faith on how to resolve this issue. If the negotiations do not resolve the issue, the Processor may cease the processing and terminate the Agreement with reasonable notice.

5.4 The Controller shall be entitled to receive a copy of any sub-processing agreement between the

Processor and a sub-processor. The Processor is entitled to redact such parts of relevant contract documents that are irrelevant for the control purposes of this Data Processing Agreement (e.g. financial conditions).

5.5 At the conclusion of this Data Processing Agreement, the Controller has approved the sub-processors listed in Appendix 1 of this Data Processing Agreement.

6 SECURITY

6.1 The Processor is obliged to implement all necessary organisational and technical measures to safeguard the confidentiality, integrity and availability of the personal data and to prevent the personal data from being exposed to unauthorised access, dissemination, alteration, damage, destruction or inaccessibility.

6.2 The Processor shall comply with the requirements for security measures imposed by the at all times applicable data protection legislation, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

6.3 The technical and organisational measures are subject to technical development and the Processor may implement adequate alternative measures in the course of the Data Processing Agreement. Such measures shall comply with the legal provisions set out in Article 32 of the GDPR and must not fall short of the level of security previously held. No special agreement is required if these changes lead to an improvement to the level of data protection that was previously part of this Data Processing Agreement in the context of commissioned processing and if the Controller is informed about these changes.

6.4 The Processor shall assist the Controller so that it can fulfil its own duties in regard to information security, personal data breaches and data protection impact assessments pursuant to the GDPR Articles 32 to 36 and the at all times applicable data protection legislation. At the request of the Controller, the Processor is obliged to assist in assessing the privacy-related consequences prior consultations, as well as in the dialogue with the Norwegian Data Protection Authority, where required to handle the privacy risk as identified through impact assessments.

7 BREACH NOTIFICATION

7.1 The Processor is obliged to notify the Controller without undue delay if the Processor discovers that personal data is or has been exposed to unauthorised access, dissemination, alteration, damage, destruction or inaccessibility or another form of security breach or otherwise used in an unauthorised manner or handled in violation of the data protection legislation and/or the terms of this Data Processing Agreement.

7.2 The breach notification shall document the breach and contain, as a minimum:

a) A description of the nature of the breach, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.

b) The name and contact details of the data protection officer or other contact point with the Processor.

c) A description of the likely or realised consequences of the breach.

d) A description of the measures that has been taken or which is proposed to be taken to address the breach, including where relevant, measures to mitigate its possible adverse effects.

7.3 If the Processor is unable to provide the above-mentioned information at the same time, the information can be provided in phases without further undue delay.

7.4 In the event of a breach, the Processor is obliged to ensure the security of the personal data by implementing appropriate measures and co-operate with the Controller in the investigation and mitigation of each such breach. Such assistance shall be provided to the Controller at no extra cost.

7.5 The Processor agrees and understands that, except when the Processor is required to do so by applicable law, the Controller has the sole right to determine:

a) whether to provide notice of the breach to any data subjects or to the Data Protection Authority, as required by law or regulation or at the Controller's discretion, including the contents and delivery method of the notice; and

b) whether to offer any type of remedy to affected data subjects, including the nature and extent of such remedy.

8 AUDIT

8.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the GDPR Article 28 and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

8.2 The Controller or a third party appointed by the Controller may at any time demand access to and verification of the Processor's processing of personal data, including access to and verification of documentation for fulfilment of the requirements for information security and this Data Processing Agreement as well as assessments of organisation, routines, security measures and use of communications between partners and suppliers, random checks, site controls or other appropriate control measures, as well as a description of how the Processor secures personal data against unauthorised access, dissemination, alteration, damage, destruction or inaccessibility. If the Controller uses a third party to carry out the audit, such third party cannot be a direct competitor to Processor and must be bound by a duty of confidentiality before commencing with the audit.

8.3 The Controller shall insofar as possible, give the Processor notice in reasonable time when requiring access and control, normally at least 30 days. For request for access to documents at least 14 days' notice should be given.

8.4 Audits shall not impair the confidentiality, integrity and access to personal data, nor shall it impair the confidentiality, integrity and access to the Processor's internal reports, prices or other clients' information.

8.5 The Processor is obliged to give the supervisory authorities or representatives acting on behalf of such authorities' access to the Processor's physical

facilities after presentation of appropriate identification and basis for the access.

8.6 If the audits reveal defects, the Processor shall promptly rectify such deficiencies at no cost to the Controller. Any material deficiencies that constitute an obvious threat to information security should be corrected immediately.

9 TRANSFER

9.1 Personal data processed by the Processor on behalf of the Controller may be transferred to, stored and processed in those countries listed in Appendix 1.

9.2 The Processor shall not transfer personal data to or allow persons outside of the countries listed in Appendix 1 to gain access to personal data, without the explicit prior written consent of and appurtenant instructions for transfer by the Controller. Consent and instructions must cover which countries the personal data may be transferred to. Transfer to a third country requires that the requirements contained in the data protection legislation for the information security and protection of the rights of the data subjects are met as well as the use of approved EU transfer mechanisms.

10 TERM

10.1 This Data Processing Agreement shall apply for as long as the Processor processes personal data on behalf of the Controller.

10.2 In the event of a breach of this Data Processing Agreement or the data protection legislation, the Controller may instruct the Processor to discontinue further processing of the personal data with immediate effect.

11 TERMINATION

11.1 Upon termination or expiry of this Data Processing Agreement, the Processor shall cease the processing of all personal data. The provisions relating to confidentiality of documentation and personal data that the Processor may access pursuant to this Data Processing Agreement shall survive this Data Processing Agreement.

11.2 Upon termination or expiry of this Data Processing Agreement, or upon the Controller's written request, the Processor shall either, at the choice of the Controller, return and/or destroy personal data processed (including security copies). If the Controller requires the personal data to be returned to the Controller or transferred to a third party.

11.3 If shared infrastructure is used where direct erasure is not directly possible, the Processor shall ensure that personal data is rendered unavailable until such data is overwritten by the system.

11.4 The Processor may not retain any copies of personal data provided by the Controller under this Data Processing Agreement, in any format, and any physical and logical access to such personal data shall be erased. The Processor shall document in writing, within 21 days after the receipt of the Controller's instruction, that it has returned, deleted and/or destroyed all personal data and all documents and electronically stored data containing such personal data, in accordance with this Data Processing Agreement. The Processor shall warrant to the Controller that neither the Processor nor its sub-processors has retained any copy, print or any other form of personal data in any form, unless data protection legislation prevents deletion or return. In such cases, the Processor shall guarantee that it will no longer process the personal data.

12 AMENDMENTS

12.1 Changes to this Data Processing Agreement shall be agreed in writing by and between the Parties. The Controller is entitled to change the content of this Data Processing Agreement where necessary to comply with changes in the data protection legislation.

APPENDIX 1 – PROTOCOL

1 NOTICES

All notices under this Data Processing Agreement shall be sent in writing to the representatives listed in the Order Form.

2 THE PURPOSE AND NATURE OF PROCESSING

The purpose is to provide personalised movies and appurtenant media services to the data subjects chosen by the Controller.

3 THE NATURE OF PROCESSING

The Processor will use personal data to create personal engagement for an individual. Personal data belonging to the Controller's end customers / members / employees is collected from the Controller's systems and is transmitted via Application Programming Interface (API), or as encrypted data file to the Processor and thereafter to a data subject ("**Recipient**").

If the Controller wishes to utilise the "**Referral solution**" functionality of the Processor, the Recipients are able to generate subsequent movies for a third-party individual ("**Friend**"). The Friend may in turn generate subsequent movies for other Friends. While personal data from original Recipients will be collected from the Controller, data from Friends will be collected from a prior Recipient or Friend. The Processor will not process personal data about the Friend to a greater extent than when processing personal data belonging to the Controller's end customers / members / employees or other Recipients.

Behaviour statistics are registered in connection with the distribution of the film to the Recipient so that the Controller can assess the success rate. The Processor will register a variety of statistics such as visits, IP-addresses, seek time, clicks, and general statistics about the user and their behaviour while engaging with SEEN's platform.

4 CATEGORIES OF DATA SUBJECTS

The data subjects which the personal data shared by the Controller concerns.

5 CATEGORIES OF PERSONAL DATA

The personal data shared by the Controller.

6 SUB-PROCESSORS

The Controller has approved of the following sub-processors:

Name:	LINK Mobility AS
Location:	Norway and Sweden
Purpose:	SMS distribution (if applicable). Link Mobility will receive access to phone numbers and the content of the SMS and the landing page.
Policies	https://linkmobility.no/wp-content/uploads/sites/3/2020/11/DPA-LINK-as-Processor-V1.34_29November2020_fixed.pdf

Name:	Amazon Web Services EMEA SARL (AWS Europe)
Location:	Luxembourg, Germany and Sweden
Purpose:	The Processor may use Amazon to host and distribute movies to Recipients. Amazon is an integral part of the Processor's solution and will not store such e-mail addresses after distribution. Database backups are also stored here.
Policies:	https://aws.amazon.com/compliance/gdpr-center/
Name:	Hetzner Online GmbH
Location:	Germany
Purpose:	Our solution is deployed on bare-metal machines in Germany with provider Hetzner.
Policies	https://www.hetzner.com/news/vertrag-zur-auftragsverarbeitung-gemaess-art-28-ds-gvo-steht-ab-sofort-online-zur-verfuegung-eintrag/
Name:	Google Ireland Limited
Location:	EU/EEA
Purpose:	The Processor may use Google to host and distribute movies to Recipients and store database backups. Google is an integral part of the Processor's solution. Our solution and database are also stored here.
Policies:	https://cloud.google.com/terms/data-processing-terms
Name:	LeaseWeb Netherlands B.V
Location:	Netherlands
Purpose:	Backups of solution and databases
Policies:	https://www.leaseweb.com/legal/personal-data-protection-acts

APPENDIX 2 – SEEN'S SECURITY BASELINE

1 INTRODUCTION

1.1 The Data Processor strives for a high level of security in all of its operations and the Data Processor's reputation as a secure and reliable actor is of utmost importance to the Data Processor.

1.2 This Appendix lays out the self-imposed security baseline of the Data Processor, the purpose of which is to reassure the Controller that the Processor places the highest emphasis on safeguarding the personal data which the Data Processor has been entrusted to process.

1.3 The Data Processor shall maintain sufficient administrative, physical, organisational and technical safeguards designed for protection of the security, including protection against unauthorised or unlawful processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorised disclosure of, or access to, personal data.

1.4 Measures for ensuring information security have been specified and implemented by the Data Processor and the Data Processor has appointed a person who is responsible for the implementation. The Data Processor's security policy and its implementation have been reviewed at the appropriate management level.

1.5 The Data Processor shall have a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2 PREMISES

2.1 The Data Processor's premises must be physically protected against unauthorised entry. This includes network devices, connections and routing points. Detected attacks must generate alarm with an appropriate response.

2.2 The Data Processor will at all times have in place technical and organisational measures to control access to premises, particularly to check authorisation to ensure that only employees with work-related purposes have access to personal data (Principle of least privilege). This includes, but is not limited to:

a) Access control system (ID reader, magnetic card, chip card).
b) (Issue of) keys.
c) Door locking (electric door openers etc.).
d) Security staff, janitors
e) Surveillance facilities (Alarm system, video/CCTV monitor)
f) Logging of access to data centres
g) Regular review of permanent access permits.

2.3 Periodic review of access has been implemented for physical (workplace) access.

2.4 The Processor shall have a clean screen policy.

3 SYSTEM ACCCES

3.1 The Data Processor's access rights management procedures must be defined, and access rights given based on roles and responsibilities.

3.2 The Data Processor must have documented system access policy and process for the applications in the scope of the Solution or used in connection with the provision of the Solution. In general, all access rights must be based on roles and responsibilities based on the principle of "least privileged" access right.

3.3 Roles must be separated so that access rights do not create such work combinations, that could present higher than normal risks of misconducts, abuse or heighten the risks arising from negligence or mistakes. Access rights must be removed immediately when the related need for them no longer exists.

3.4 Access rights must be personal, and they cannot be given to others. A responsible person must be nominated for all technical user access codes, who shall responsible for all actions made with the access code.

3.5 Periodic review of access has been implemented for logical (network) access.

4 SECURITY

4.1 The Data Processor's Solution servers are running the latest version of Debian with security updates applied automatically on a daily basis.

4.2 The Data Processor shall ensure that IT equipment used for access to the Controller's systems by the Data Processor is protected by a firewall, running on supported versions of software, regularly updated with security patches and have antivirus solutions with updated antivirus definitions.

4.3 The Data Processor's utilises iptables for the software-based firewall, with automatic banning of IP addresses that try to brute-force attack its services.

4.4 The Data Processor shall perform periodic scans using its antivirus programs, which must be capable of detecting, removing and protecting against all known types of malicious software.

4.5 Access to the servers is allowed via SSH with public-key authentication on a non-standard port. The Data Processor's staff have access to the servers, though only one employee has root access.

4.6 The Data Processor shall have in place sufficient security measures when using equipment outside the Data Processor's workplace, as well as an assessment of risk factors during such use.

5 ENCRYPTION

5.1 The Data Processor only adopt connections that support secure protocols such as HTTPS, SSH v2 etc.

5.2 The Data Processor's Solution (the PVM Manager) runs inside of a Debian Linux container (LXD), which itself is stored on an AES-256 encrypted RAID-1 volume.

5.3 For the database, the Data Processor utilises PostgreSQL, with passwords stored using the PBKDF2 algorithm with a SHA256 hash. The database files are also AES-256 encrypted.

5.4 Backups are encrypted on-server using a strong passphrase and uploaded to an encrypted Amazon S3 bucket. Backups are rotated daily and expire after a few weeks.

6 PASSWORDS

6.1 The Data Processor shall have a password policy which mandates special characters, minimum length and regular change of password.

6.2 The Data Processor shall ensure that it does not use group, shared or generic IDs, passwords, or other authentication methods.

7 DEVELOPMENT

7.1 Development of the Data Processor's Solution is mostly handled by the Data Processor in-house. No development is done via any external third parties. Because of this, only the Data Processor has access to the source code and its repository, which is also hosted in-house.

7.2 The PVM Manager, Django and its dependencies are updated regularly to make sure that any CVEs or potential vulnerabilities are patched.

8 LOGGING

8.1 The Data Processor shall ensure that all systems used

by the Data Processor to process the Controller's data produce sufficient and accurate audit logs.

9 BACKUPS

9.1 The Data Processor shall establish backup and recovery procedures that cover both application and software backups as well as backups of all data processed relating to the Solution.

9.2 Backup and recovery procedures shall be reviewed and tested.

10 DATA MINIMISATION

10.1 To aid the Controller in fulfilling the principle of data minimisation, the Data Processor's Solution is structured in such a way that only requires data strictly necessary for necessary to the campaign of the Controller, e.g. first name only, email addresses and/or phone numbers if the Data Processor is delivering via email and/or SMS. Data is handled internally using Data Processor-generated IDs so that personal data is not used unless necessary.

10.2 When the campaign has finished and unless otherwise agreed, the Data Processor exports and transfers the campaign's statistics to the Controller and deletes all of the received data from the Data Processor's system. While this data will still exist in the encrypted backups, it will expire after a number of weeks, as the backups are rotated.

11 TRAINING

11.1 The Data Processor shall ensure that all employees are aware of routines on security and confidentiality

11.2 The Data Processor shall ensure that all employees have unambiguous regulations in employment contracts on confidentiality, security and compliance with internal routines

11.3 The Data Processor has in place internal routines and courses on requirements of processing of personal data to create awareness

11.4 The Data Processor shall ensure that there is a proper human resources process, including hiring and screening processes, a transfer process and a contract termination process preventing unqualified and unauthorised personnel to participate in the provision of the processing of personal data.

12 SECURITY TESTING

12.1 The Data Processor is responsible for conducting security testing and fixing any security defects in the Solution and/or in any applications, functionalities or processes relating thereto.

13 VULNERABILITY TRACKING

13.1 The Data Processor shall track and keep itself informed on vulnerabilities related to the Solution as well as to monitor the security and lifecycle management of the Solution.

14 RISK ASSESSMENTS

14.1 The Data Processor shall perform a risk assessment for all new applications and/or functionalities or critical application changes in the Solution.

14.2 Depending on the type of the application and/or the new functionality to be implemented, the Data Processor shall evaluate potential threats and risk of misuse of the Solution and/or new functionality.

15 INCIDENT RESPONSE

15.1 The Data Processor will report all major operational or security incidents affecting the processing of personal data on behalf of the Controller ("**Incidents**"). Such Incidents are singular events or a series of linked events which have or may have a material adverse effect on the integrity, availability, confidentiality, of the personal data.

16 DATA DISPOSAL

16.1 Personal data on paper must be destroyed in a shredder or a locked confidential waste container.