DATA PROCESSING AGREEMENT
LUCRASOFT DIGITAL B.V.

Comprised of:

Part 1. Data Pro Statement

Part 2. Standard Clauses for Data Processing

Version: 5-2018

Dutch and English version

The Data Pro Code was originally drafted in Dutch. The English version is for convenience only. In case of conflict between the Dutch and the English version, the Dutch version prevails.

PART 1: DATA PRO STATEMENT

Along with the Standard Clauses for Data Processing, this Data Pro Statement constitutes the data processing agreement for the product or service provided by the company that has drawn up this Data Pro Statement.

GENERAL INFORMATION

1. **This Data Pro Statement was drawn up by**

   Lucrasoft Digital B.V.
   Located: De Zelling 8, 3342GS Hendrik Ido Ambacht
   Trademarks/brands: Dutch Grit, Picario, Movin

   If you have any queries about this Data Pro Statement or data protection in general, please contact:

   Steven Somer
   steven@dutchgrit.nl
   +31 78 6811 501

2. **This Data Pro Statement will enter into force on *May 25 2018***

   We regularly revise the security measures outlined in this Data Pro Statement to ensure that we are always fully prepared and up to date with regard to data protection. If this document is updated, we will notify you of the revised versions through our regular channels.

3. **This Data Pro Statement applies to the following products and services provided by the data processor**

   a) Web hosting of live and test environments
   b) Emma mailing campaigns
   c) Picario XPO
   d) Movin SDK

4. **A. A description of the web hosting of live and test environments**

   Lucrasoft Digital develops and hosts web solutions for SMEs and small corporate businesses. Examples include webshops, websites, mobile apps, web applications and data integrations.
   The hosting consists of the hosting of the web solution on our web servers and data storage on our SQL and RavenDB database servers.
   During the development phase, we host a copy of the product databases on our internal SQL and RavenDB test servers for test purposes.

B. A description of the Emma mailing campaigns

Emma is a mailing application that allows clients to design mail campaigns and send them to contact persons who subscribed to the mailing.

C. A description of Picario XPO

Picario offers visualisation software that integrates a photo and design in order to visualise them together. Our XPO engine enables users to display lifelike visualisations of colour and/or design on a photographed or modelled object.

D. Movin SDK

Movin offers development tools for developers of mobile applications via our software development kit ("SDK"). Our SDK enables developers to use our positioning and map technology and to collect location data.

5. Intended use

A. Web hosting and Web development are designed and equipped for processing the following types of data:

The hosted data is dependent on the solution that is realised. Normally, this concerns account data and web orders from the webshop. We do not receive and host payment details and/or credit card details. The visitor always exchanges these directly with the specific payment provider. If the web application sends out e-mails, it is done via the Postmark data processor.

In the case of this service, the processing of special personal data is not taken into account. We will advise whether or not the web application qualifies for this. The decision is at the client's own discretion.
Special personal data is data in relation to an individual's race, ethnic origin, political beliefs, religious or philosophical convictions, membership of a trade union, genetic details, biometric details, details about an individual's health, details with regard to sexual behaviour or sexual preferences or criminally relevant details. The processing of special data is subject to stricter standards under a different processor's agreement.

B. Emma mailing campaigns are is designed and equipped for processing the following types of data:

As a standard, we register name, e-mail address, IP address and geographical location such as town/city/province/country.

At the client's request, additional filter fields can be added The client will use these fields for mailings with a specific target group. Examples include fields of interest, position, address details, labels.

When we send out mailings, we track statistics in order to measure the success of a mailing. They are:

a) Opened by means of date, time and number of times opened.

b) Click on link yes/no and date/time.

c) IP address of the mail client and from that, the geographical location such as town/city/province/country.

d) Type of mail client.

e) Type of device and OS version.

C. Picario XPO is designed and equipped for processing the following types of data:

In order to prepare the visualisation, it must be possible to use the name and address details in order to specify an object/location.

In the case of this product/service, the processing of special personal data or data in relation to criminal convictions and offences was not taken into account. The client can process this data with the aforesaid product or service at its own discretion.

D. Movin SDK is designed and equipped for processing the following types of data:

For the collection of location details, the Movin SDK generates a unique device-specific ID for every end user device. This unique ID is always generated randomly and it is reset every time the app is installed or reinstalled. Furthermore, limited information about the device is collected such as the manufacturer, the model and information about the operating system.

In the case of this product/service, the processing of special personal data or data in relation to criminal convictions and offences was not taken into account. The client can process this data with the aforesaid product or service at its own discretion.

Special personal data is data in relation to an individual’s race, ethnic origin, political beliefs, religious or philosophical convictions, membership of a trade union, genetic details, biometric details, details about an individual's health, details with regard to sexual behaviour or sexual preferences or criminally relevant details. The processing of special data is subject to stricter standards under a different processor’s agreement.

6. **When the data processor designed the product or service, it applied the privacy-by-design approach in the following manner:**

A./ B.

a) The forms in our applications only contain fields that were built in at the client's request. We check if the fields are necessary for the intended purpose and we aim to eliminate surplus fields.

b) Our web solutions only contain hashed passwords, not passwords in a readable or decodable format.

c) We do not receive payment or credit card details. The visitor exchanges these details directly with the payment provider selected by the client.

d) User tracking is implemented at the client's request only and it is activated only when the visitor has given his explicit consent.

e) The user is registered for a newsletter only when he has actively ticked the opt-in box.

f) All our web solutions come with an SSL certificate as a standard.

g) We do not use the collected data and the visitor tracking and we will only view the data at the client's request, for instance, when this is necessary in order to resolve a support query or a breakdown.

h) At the client's request, customer records can be removed from the databases.

C. a) we do not collect information that can be used to identify individuals. Furthermore, Picario does not retain any data that contains personal details.

D. a) We collect indoor location data via the Movin SDK. However, we do not collect information that can be used to identify individuals. Furthermore, Movin only retains anonymised positions for statistical use.

7. **The Data Processor uses the Data Pro Standard clauses for processing, which can be found elsewhere in this document.**

8. **The data processor will process the personal data provided by its clients:**

A. Web hosting and Web development data storage: within the EU/EEA.

Sending e-mails for web hosting: outside the EU/EEA in the US.

To send e-mails, Lucrasoft Digital uses the following method to guarantee an appropriate level of protection:

a) For the US, the processor has indicated that it offers an appropriate level of protection;

The supplying processor (Postmark) is affiliated with the EU-US Privacy Shield: https://postmarkapp.com/eu-privacy

B. Emma mailing campaigns data storage: outside the EU/EEA in the US.
For Emma mailing campaigns, Lucrasoft Digital uses the following method to guarantee an appropriate level of protection:

a) For the US, the processor has indicated that it offers an appropriate level of protection;
b) The supplying processor (Active Campaign) is affiliated with the EU-US Privacy Shield: https://www.activecampaign.com/privacy-policy/

C. Picario XPO processes the personal data within the EU/EEA.

D. Movin SDK processes the personal data within the EU/EEA.

9. The data processor uses the following sub-processors:

	Sub-procesor	**Within the EU/EEA**	**Privacy statement**
A. / B.	Google Analytics	data storage in the US, EU-US Privacy Shield-compliant	https://policies.google.com/privacy
A. / B.	Postmark	data storage in the US, EU-US Privacy Shield-compliant	https://postmarkapp.com/eu-privacy
A. / B.	Active Campaign	data storage in the US, EU-US Privacy Shield-compliant	https://www.activecampaign.com/privacy-policy/
C.	Leaseweb	Outside the EU	https://www.leaseweb.com/nl/legal/privacy-statement
C.	Lucrasoft ICT Group	Within the EU	https://www.lucrasoftitbeheer.nl/nl/privacy-statement/
D.	Microsoft Azure	Within the EU	https://privacy.microsoft.com/nl-nl/privacystatement
D.	Lucrasoft ICT Group	Within the EU	https://www.lucrasoftitbeheer.nl/nl/privacy-statement/

At the client's request, other sub-processors can also join. In that case, the client concludes an agreement directly with the processor. The processor's agreement directly concluded between the client and the processor subsequently forms a part of this agreement. In that case, Lucrasoft Digital will only realise the technical integration. Examples of such processors are payment providers, social media integrations, Hotjar, Piwik and other SAAS solutions.

10. **Lucrasoft Digital supports the client with requests from data subjects as follows:**
    Requests to inspect, correct or remove data should be sent to support@dutchgrit.nl. After receiving the request, we will process and confirm/deliver within five (5) working days.

11. **Termination of the agreement:**
    After the termination of the agreement with a client, Lucrasoft Digital will remove the application-specific databases, including personal details.
    At the client's request, Lucrasoft Digital removes the database with all personal data it has processed for the client via a single download.
    The retention and/or destruction of this data is subsequently the client's responsibility. Backup retention means that the data is, indeed, removed after three (3) months. As this concerns an automated process, manual or earlier removal is not possible.

SECURITY POLICY

10. **The data processor has implemented the following security measures to protect its product or service:**

    a) The data centres (Databarn Rivium & Databarn Amsterdam), where Lucrasoft ICT Group has servers, are equipped with camera surveillance and visitor registration systems and are ISO:27001:2013-certified.
    b) The (database) servers can be accessed only via Lucrasoft's trusted network locations.
    c) Procedures are in place, which means only authorised personnel have access to the personal data. A non-disclosure agreement ensures this still applies when a member of staff leaves the company.
    d) Our web servers and database servers are firewall-protected in accordance with the least privileged principle. Applications have their own database for every application. Every application has access to its own database only.
    e) All data within Lucrasoft's services will be stored as securely as possible. Encryption will be used when possible.
    f) All data will be transmitted with the highest possible form of encryption that is supported.
    g) Our web servers are patched in accordance with the latest Window updates every month.
    h) All mobile carriers (such as laptops, USB sticks and portable HDs) of Lucrasoft Systems B.V. are encrypted.

DATA LEAK PROTOCOL

11. In the unfortunate event that something does go wrong, the data processor will follow the following data breach protocol to ensure that clients are notified of incidents:

The Data Protection Officer (or DPO) will be notified of the possible data breach. A relevant internal data breach procedure is in place. He will set up a team in order to analyse the cause, the impact and the affected customers. Depending on the outcome of this analysis, customers will be notified by means of an e-mail that is sent to the technical contact person within 24 hours.

Lucrasoft Digital B.V. will provide highly detailed information about:

a. The nature of the breach, including a description of the incident, the nature of the personal data or categories of affected data subjects, an estimate of the number of affected data subjects and databases that may be affected, as well as an indication of when the incident occurred;
b. Any measures already taken by Lucrasoft Digital in order to stop the breach;
c. Any measures to be taken by the controller or the affected data subjects (what can the affected data subjects themselves do, such as “keep an eye on your e-mails, change your passwords”);
d. Any measures to be taken by Lucrasoft Digital in order to prevent a future breach.

Clients are notified within 24 hours, if possible. Lucrasoft Digital B.V. does not own the data and cannot notify AP or data subjects. The data processor will support the client or the controller during the notification process, if so required.

PART 2: STANDARD CLAUSES FOR DATA PROCESSING

Version: January 2018

Along with the Data Pro Statement, these standard clauses constitute the data processing agreement. They also constitute an annex to the Agreement and to the appendices to this Agreement, e.g. any general terms and conditions which may apply.

ARTICLE 1. DEFINITIONS

The following terms have the following meanings ascribed to them in the present Standard Clauses for Data Processing , in the Data Pro Statement and in the Agreement:

1.1 **Dutch Data Protection Authority (AP):** the regulatory agency outlined in Section 4.21 of the GDPR.

1.2 **GDPR:** the General Data Protection Regulation.

1.3 **Data Processor**: the party which, in its capacity as an ICT supplier, processes Personal Data on behalf of its Client as part of the performance of the Agreement.

1.4 **Data Pro Statement**: a statement issued by the Data Processor in which it provides information on the intended use of its product or service, any security measures which have been implemented, sub-processors, data breach, certification and dealing with the rights of Data Subjects, among other things.

1.5 **Data Subject**: a natural person who can be identified, directly or indirectly.

1.6 **Client:** the party on whose behalf the Data Processor processes Personal Data. The Client may be either the controller (the party who determines the purpose and means of the processing) or another data processor.

1.7 **Agreement**: the agreement concluded between the Client and the Data Processor, on whose basis the ICT supplier provides services and/or products to the Client, the data processing agreement being part of this agreement.

1.8 **Personal Data** any and all information regarding a natural person who has been or can be identified, as outlined in Article 4.1 of the GDPR, processed by the Data Processor to meet its requirements under the Agreement.

1.9 **Data Processing Agreement**: the present Standard Clauses for Data Processing , which, along with the Data Processor's Data Pro Statement (or similar such information), constitute the data processing agreement within the meaning of Article 28.3 of the GDPR.

ARTICLE 2. GENERAL PROVISIONS

2.1 The present Standard Clauses for Data Processing apply to all Personal Data processing operations carried out by the Data Processor in providing its products and services, as well as to all Agreements and offers. The applicability of the Client's data processing agreements is expressly rejected.

2.2 The Data Pro Statement, and particularly the security measures outlined in it, may be adapted from time to time to changing circumstances by the Data Processor. The Data Processor will notify the Client in the event of significant revisions. If the Client cannot reasonably agree to the revisions, the Client will be entitled to terminate the data processing agreement in writing, stating its reasons for doing so, within thirty days of having been served notice of the revisions.

2.3 The Data Processor will process the Personal Data on behalf and on behalf of the Client, in accordance with the written instructions provided by the Client and accepted by the Data Processor.

2.4 The Client or its customer will serve as the controller within the meaning of the GDPR, will have control over the processing of the Personal Data and will determine the purpose and means of processing the Personal Data.

2.5 The Data Processor will serve as the processor within the meaning of the GDPR and will therefore not have control over the purpose and means of processing the Personal Data, and will not make any decisions on the use of the Personal Data and other such matters.

2.6 The Data Processor will give effect to the GDPR as laid down in the present Standard Clauses for Data Processing, the Data Pro Statement and the Agreement. It is up to the Client to judge, on the basis of this information, whether the Data Processor is providing sufficient guarantees with regard to the implementation of appropriate technical and organisational measures so as to ensure that the processing operations meet the requirements of the GDPR and that Data Subjects' rights are sufficiently protected.

2.7 The Client will guarantee to the Data Processor that it acts in accordance with the GDPR, that it provides a high level of protection for its systems and infrastructure at all time, that the nature, use and/or processing of the Personal Data are not unlawful and that they do not violate any third party's rights.

2.8 Administrative fines imposed on the Client by the Dutch Data Protection Authority will not be able to be recouped from the Data Processor, except in the event of wilful misconduct or gross negligence on the part of the Data Processor's management team.

ARTICLE 3. SECURITY

3.1 The Data Processor will implement the technical and organisational security measures outlined in its Data Pro Statement. In implementing the technical and organisational security measures, the Data Processor will take into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing operations and the intended use of its products and services, the risks inherent in processing the data and risks of various degrees of likelihood and severity to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of the Data Processor's products and services.

3.2 Unless explicitly stated otherwise in the Data Pro Statement, the product or service provided by the Data Processor will not be equipped to process special categories of personal data or data relating to criminal convictions and offences.

3.3 The Data Processor seeks to ensure that the security measures it will implement are appropriate for the manner in which the Data Processor intends to use the product or service.

3.4 In the Client's opinion, said security measures provide a level of security that is tailored to the risks inherent in the processing of the Personal Data used or provided by the Client, taking into account the factors referred to in Article 3.1.

3.5 The Data Processor will be entitled to adjust the security measures it has implemented if it feels that such is necessary for a continued provision of an appropriate level of security. The Data Processor will record any significant adjustments it chooses to make, e.g. in a revised Data Pro Statement, and will notify the Client of said adjustments where relevant.

3.6 The Client may request the Data Processor to implement further security measures. The Data Processor will not be obliged to honour such requests to adjust its security measures. If the Data Processor makes any adjustments to its security measures at the Client's request, the Data Processor will be allowed to invoice the Client for the costs associated with said adjustments. The Data Processor will not be required to actually implement these security measures until both Parties have agreed in writing and signed off on the security measures requested by the Client.

ARTICLE 4. DATA BREACHES

4.1 The Data Processor does not guarantee that its security measures will be effective under all conditions. If the Data Processor discovers a data breach within the meaning of Article 4.12 of the GDPR, it will notify the Client without undue delay. The "Data Breach Protocol" section of the Data Pro Statement outlines the way in which the Data Processor will notify the Client of data breaches.

4.2 It is up to the Controller (the Client or its customer) to assess whether the data breach of which the Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (the Client or its customer) will at all times remain responsible for reporting data breaches which must be reported to the Dutch Data Protection Authority and/or Data Subjects pursuant to Articles 33 and 34 of the GDPR. The Data Processor is not obliged to report data breaches to the Dutch Data Protection Authority and/or to the Data Subject.

4.3 Where necessary, the Data Processor will provide more information on the data breach and will help the Client meet its breach notification requirements within the meaning of Articles 33 and 34 of the GDPR by providing all the necessary information.

4.4 If the Data Processor incurs any reasonable costs in doing so, it will be allowed to invoice the Client for these, at the rates applicable at the time.

ARTICLE 5. CONFIDENTIALITY

5.1 The Data Processor will ensure that the persons processing Personal Data under its responsibility are subject to a duty of confidentiality.

5.2 The Data Processor will be entitled to furnish third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or legal order to do so issued by a government agency.

5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by the Data Processor to the Client, and any and all information provided by the Data Processor to the Client which gives effect to the technical and organisational security measures included in the Data Pro Statement are confidential and will be treated as such by the Client and will only be disclosed to authorised employees of the Client. The Client will ensure that its employees comply with the requirements outlined in this article.

ARTICLE 6. TERM AND TERMINATION

6.1 This data processing agreement constitutes part of the Agreement, and any new or subsequent agreement arising from it and will enter into force at the time of the conclusion of the Agreement and will remain effective until terminated.

6.2 This data processing agreement will end by operation of law when the Agreement or any new or subsequent agreement between the parties is terminated.

6.3 If the data processing agreement is terminated, the Data Processor will delete all Personal Data it currently stores and which it has obtained from the Client within the timeframe laid down in the Data Pro Statement, in such a way that the Personal Data will no longer be able to be used and will have been *rendered inaccessible*. Alternatively, if such has been agreed, the Data Processor will return the Personal Data to the Client in a machine-readable format.

6.4 If the Data Processor incurs any costs associated with the provisions of Article 6.3, it will be entitled to invoice the Client for said costs. Further arrangements relating to this subject can be laid down in the Data Pro Statement.

6.5 The provisions of Article 6.3 do not apply if the Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such cases, the Data Processor will only continue to process the Personal Data insofar as such is necessary by virtue of its statutory obligations. Furthermore, the provisions of Article 6.3 will not apply if the Data Processor is the Controller of the Personal Data within the meaning of the GDPR.

ARTICLE 7. THE RIGHTS OF DATA SUBJECTS, DATA PROTECTION IMPACT ASSESSMENTS (DPIA) AND AUDITING RIGHTS

7.1 Where possible, the Data Processor will cooperate with reasonable requests made by the Client relating to Data Subjects claiming alleged rights from the Client. If the Data

Processor is directly approached by a Data Subject, it will refer the Data Subject to the Client where possible.

7.2 If the Client is required to carry out a Data Protection Impact Assessment or a subsequent consultation within the meaning of Articles 35 and 36 of the GDPR, the Data Processor will cooperate with such, following a reasonable request to do so.

7.3 The Data Processor will be able to demonstrate its compliance with its requirements under the data processing agreement by means of a valid Data Processing Certificate or an equivalent certificate or audit report (third-party memorandum) issued by an independent expert.

7.4 In addition, at the Client's request, the Data Processor will provide all other information that is reasonably required to demonstrate compliance with the arrangements made in this data processing agreement. If, in spite of the foregoing, the Client has grounds to believe that the Personal Data are not processed in accordance with the data processing agreement, the Client will be entitled to have an audit performed (at its own expense) not more than once every year by an independent, fully certified, external expert who has demonstrable experience with the type of data processing operations carried out under the Agreement. The audit will be limited to verifying that the Data Processor is complying with the arrangements made regarding the processing of the Personal Data as laid down in the present data processing agreement. The expert will be subject to a duty of confidentiality with regard to his/her findings and will only notify the Client of matters which cause the Data Processor to fail to comply with its obligations under the data processing agreement. The expert will furnish the Data Processor with a copy of his/her report. The Data Processor will be entitled to reject an audit or instruction issued by the expert if it feels that the audit or instruction is inconsistent with the GDPR or any other law, or that it constitutes an unacceptable breach of the security measures it has implemented.

7.5 The parties will consult each other on the findings of the report at their earliest convenience. The parties will implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. The Data Processor will implement the proposed measures for improvement insofar as it feels these are appropriate, taking into account the processing risks associated with its product or service, the state of the art, the costs of implementation, the market in which it operates, and the intended use of the product or service.

7.6 The Data Processor will be entitled to invoice the Client for any costs it incurs in implementing the measures referred to in this article.

ARTICLE 8. SUB-PROCESSORS

8.1. The Data Processor has outlined in the Data Pro Statement whether the Data Processor uses any third parties (sub-processors) to help it process the Personal Data, and if so, which third parties.

8.2. The Client authorises the Data Processor to hire other sub-processors to meet its obligations under the Agreement.

8.3. The Data Processor will notify the Client if there is a change with regard to the third parties hired by the Data Processor, e.g. through a revised Data Pro Statement. The Client will be entitled to object to the aforementioned change implemented by the Data Processor. The Data Processor will ensure that any third parties it hires will commit to ensuring the same level of Personal Data protection as the security level the Data Processor is bound to provide to the Client pursuant to the Data Pro Statement.

ARTICLE 9. OTHER PROVISIONS

These Standard Clauses for Data Processing, along with the Data Pro Statement, constitute an integral part of the Agreement. Therefore, any and all rights and requirements arising from the Agreement, including any general terms and conditions and/or limitations of liability which may apply, will also apply to the data processing agreement.