HeartCo Data Protection Policy:

In accordance with the EU General Data Protection Regulation (GDPR)

This document was created to meet the requirements indicated by GDPR's introduction in May 2018. Thank-you EU for introducing yet ANOTHER admin job for us. We're not bitter, but we'll be glad to see the back of you after Brexit.

As for the data protection, it will continue to be handled in a confidential and professional manor as best possible for a Sole Trader with websites. This document relates to all sub-sections of HeartCo, up to and including the following titled businesses:

HeartCo Contact information:

Telephone: +44 (0) 1273 04 11 77 | E-mail: info@heartco.co.uk | Web: www.heartco.co.uk

Data protection policy

The goal of the data protection policy is to depict the legal data protection aspects in one summarising document. It can also be used as the basis for statutory data protection inspections, e.g. by the customer within the scope of commissioned processing. This is not only to ensure compliance with the European General Data Protection Regulation (GDPR) but also to provide proof of compliance. But in all honesty, GDPR is the main reason we've written it.

With relation to HeartCo and Media Sussex:

Preamble

Both HeartCo (also referred to as HC in this document) and Media Sussex (also referred to as MS in this document) are primarily media consultancy trades by Stephen Holdstock as a registered Sole Trader. Sub contractors will need to ensure that they have their own GDPR standard policy and agree to HC and MS's policy also. This will be the responsibility of the sub contractor.

Security policy and responsibilities in the company

- Our ongoing corporate objectives are to continue expanding and develop all aspects of HC and MS. At all areas of expansion, Data Protection will be considered and this document amended accordingly.
- The specific terms of HC and MS's data protection policy is outlined in 'Existing technical and organisational measures (TOM)' section.
- The role of data protection manager falls within the job description of the Sole Trader, Stephen Holdstock until further notice. He is contactable through info@heartco.co.uk. If the subject line contains obvious reference to GDPR issues, a response will be issued within 5 working days of the email receipt (except where holidays have been published in Stephen Holdstock's email footer).
- This document will continue to be reviewed as the business changes and expands. If the current goals are sufficient, no changes will be made.
- Data protection and GDPR compliance will be stressed to all subcontractors of HC and MS.

Legal framework in the company

- At this stage of the business life-cycle, no external legal representatives are in place for HC and MS. This will be due for revision once HC expands to Limited Company status.

Documentation

- All inspections have been carried out internally by the Data Protection Manager.
- Where possible, all information will be kept confidentiality, integrity and availability. This will be due for review once HC expands to a Limited Company.
- Once a Limited Company; HC and MS aim to introduce a document that outlines a rating systems of the data it handles, similar to "The BSI Standard 100-2 categories from the German Federal Office for Information Security [*Bundesamt für Sicherheit in der Informationstechnik – BSI*] are helpful, e.g.: 'normal', 'high' and 'very high'."

Existing technical and organisational measures (TOM)

Below reads appropriate technical and organisational measures that must be implemented and substantiated, taking into account, inter alia, the purpose of the processing, the state of the technology and the implementation costs for HC and MS.

1. Online Data Protection
   - 1.1. Ensure that the customer (or user) has direct digital access to their information, where possible. If it is not possible, they will be able to access it through a representative of HC or MS within 5 working days of receipt of request.
   - 1.2. Ensure that the customer (or user) can request an update or removal of data where possible via email (see contact details, page 1).
   - 1.3. Ensure that the data is used only where it is directly required, with the exception of backup purposes.
   - 1.4. Data Backups will be taken daily where HC/MS are in control. Backups for external sources will be maintained by the company handling the data. HC and MS will ensure that they comply with acceptable Backup policies.
   - 1.5. Live data and Backups of customer (or user) data will be kept secure at all times. All computers containing the information will be password protected, along with all online accounts connected to the customer (or user) data.
   - 1.6. Online data usage will be limited to the following:
     - 1.6.1. Xero Accounting Software (xero.com).
     - 1.6.2. Shore Accounting (shoreaccounting.co.uk).
     - 1.6.3. HC or MS Portfolio, with permission (heartco.co.uk, mediasussex.co.uk). Where without permission, only artwork will be displayed unless expressly requested against by the customer (or user).
     - 1.6.4. Apple iCloud based contacts applications for HC, MS or Stephen Holdstock's use only. Customer (or user) data will not be shared from here with anyone else.
     - 1.6.5. Limited and anonymous information captured via Google Analytics for websites.
     - 1.6.6. All emails will be stored on servers and not downloaded to devices permanently. This is currently a dedicated CloudFlare hosting service which is maintained and protected by the hosting client defined and chosen by HC. HC retains the right to keep this information private for security reasons.
       - 1.6.6.1. Although it is not the responsibility of HC and MS, as a sign of goodwill, we will always ensure that the websites' and emails' are securely backed up once every 24 hours.

2. Offline Data Protection, *Local (offline) data usage will consist of the following (but may include individual cases of alternative use):*
   - 2.1. Label Printing for postage
     - 2.1.1. All received or discarded postage labels will be shredded on site.
   - 2.2. Email software

2.2.1. This may vary depending on the machine the information is being managed.

2.3. Design software

2.3.1. For the production of documents, designs and media-related items in line with the customer/user project needs.

2.4. iCloud Directory for files and project items

2.4.1. An Apple managed secure basis for backups.

2.5. Word processing software

2.6. Local Backup (automatic)

2.6.1. Through the use of Apple OSX Time Machine

2.6.2. Using Apple Time Capsule on a LAN (Local Area Network)

2.6.2.1. Located in an alternative room to the computer where information is used.

Guidelines for the rights of data subjects

A customer or user may request an outline of the data stored, may request changes or removal (unless the information is directly being used to meet other requirements that they have set out).

This may be done by emailing info@heartco.co.uk, where a response will be issued within 5 working days of email receipt (unless Stephen Holdstock is on holiday – in which case, 5 working days upon return to work). If the information is not available within that period, an estimation of delivery will be emailed to the customer/user within 5 working days of email receipt.

Access control will be delivered where possible so the customer can access their information directly. This may not always be possible. *Due for review once HC becomes a Limited Company.*

Information Classification

All information used for accounting and invoice purposes will be handled with care and entered in applications as outlined in TOM 1.6.

All information used for website management and optimisation will be anonymous except for items outline in Google's Analytics Data Protection Policy.

All website sales will also be logged securely on the websites where purchases have been placed.

Protection against Malware, Viruses and Hacking

All care is taken to ensure data is kept safe. Only Apple Macs are used to process data, which are not prone to viruses or malware. All updates are performed on machines within 2 weeks of release (unless technically

not possible). All emails are stored on the servers only, not downloaded to machines (expect while processing). All machines are password protected and can be wiped remotely if stolen (providing they are connected to the Internet).

Data Protection for websites hosted by clients

HC and MS offer a service where hosting is provided for the emails and websites of its clients. In these cases, the responsibility of GDPR compliance lies entirely with the client of HC/MS and not with HC/MS. Existing customers were reminded through email on the 15th and 16th January 2018 to give them notice and time to act before GDPR comes into effect in May 2018. New customers are notified when they are given the terms and conditions of HC/MS's services.

Any HC or MS clients' non-compliance for GDPR is not the responsibility of HC/MS to fix.

With relation to Build Me Mini (Minifigure Me):

Preamble

Build Me Mini (also known as Minifigure Me, further referred to as BMM) is a media media consultancy online store that enables users to submit basic information about an individual and BMM will product a miniature of that individual using LEGO™ parts.

BMM trades as a registered Sole Trader, Stephen Holdstock. Sub contractors will need to ensure that they have their own GDPR standard policy and agree to BMM's policy also. This will be the responsibility of the sub contractor.

Security policy and responsibilities in the company

- Our ongoing corporate objectives are to continue expanding and develop all aspects of BMM. At all areas of expansion, Data Protection will be considered and this document amended accordingly.
- The specific terms of BMM's data protection policy is outlined in 'Existing technical and organisational measures (TOM)' section.
- The role of data protection manager falls within the job description of the Sole Trader, Stephen Holdstock until further notice. He is contactable through info@heartco.co.uk. If the subject line contains obvious reference to GDPR issues, a response will be issued within 5 working days of the email receipt (except where Stephen Holdstock is on holiday).
- This document will continue to be reviewed as the business changes and expands. If the current goals are sufficient, no changes will be made.

- Data protection and GDPR compliance will be stressed to all subcontractors of BMM.

Legal framework in the company

- At this stage of the business life-cycle, no external legal representatives are in place for BMM. This will be due for revision once HC (HeartCo) expands to Limited Company status.

Documentation

- All inspections have been carried out internally by the Data Protection Manager.
- Where possible, all information will be kept with confidentiality, integrity and availability. This will be due for review once HC expands to a Limited Company.
- Once a Limited Company; HC and MS aim to introduce a document that outlines a rating systems of the data it handles, similar to "The BSI Standard 100-2 categories from the German Federal Office for Information Security [*Bundesamt für Sicherheit in der Informationstechnik – BSI*] are helpful, e.g.: 'normal', 'high' and 'very high'."

Existing technical and organisational measures (TOM)

Below reads appropriate technical and organisational measures that must be implemented and substantiated, taking into account, inter alia, the purpose of the processing, the state of the technology and the implementation costs for BMM.

3. Online Data Protection

3.1. Ensure that the customer (or user) has direct digital access to their information, where possible. If it is not possible, they will be able to access it through a representative of HC or BMM within 5 working days of receipt of request.

3.2. Ensure that the customer (or user) can request an update or removal of data where possible via email (see contact details, page 1).

3.3. Ensure that the data is used only where it is directly required, with the exception of backup purposes.

3.4. Data Backups will be taken daily where BMM are in control. Backups for external sources will be maintained by the company handling the data. BMM will ensure that they comply with acceptable Backup policies.

3.5. Live data and Backups of customer (or user) data will be kept secure at all times. All computers containing the information will be password protected, along with all online accounts connected to the customer (or user) data.

3.6. Online data usage will be limited to the following:

3.6.1. Xero Accounting Software (xero.com).

3.6.2. Shore Accounting (shoreaccounting.co.uk).

3.6.3. BMM, HC or MS Portfolio, with permission (buildmemini.co.uk, heartco.co.uk, mediasussex.co.uk). Where without permission, only artwork will be displayed unless expressly requested against by the customer (or user).

3.6.4. Limited and anonymous information captured via Google Analytics for websites.

3.6.5. Full details of a purchase will be logged and stored permanently in PayPal through their online payments system.

3.6.6. All emails will be stored on servers and not downloaded to devices permanently. This is currently a dedicated CloudFlare hosting service which is maintained and protected by the hosting client defined and chosen by HC. HC retains the right to keep this information private for security reasons.

3.6.7. All data collected from the customer for personalised items will be stored in the following locations:

3.6.7.1. The website (buildmemini.co.uk)

3.6.7.2. PayPal, for Payment reference (paypal.com)

3.6.7.3. Accounting Software (Xero.com); which may be accessed only by the following users: Stephen Holdstock (Manager); Shore Accounting (Stephen Holdstock's accountancy firm); Sheila White (bookkeeper).

4. Offline Data Protection, *Local (offline) data usage will consist of the following (but may include individual cases of alternative use):*

4.1. Label Printing for postage

4.1.1. All received or discarded postage labels will be shredded on site.

4.2. Email software

4.2.1. This may vary depending on the machine the information is being managed.

4.3. Design software

4.3.1. For the production of documents, designs and media-related items in line with the customer/user project needs.

4.4. iCloud Directory for files and project items

4.4.1. An Apple managed secure basis for backups.

4.5. Word processing software (where needed)

4.6. Local Backup (automatic)

4.6.1. Through the use of Apple OSX Time Machine

4.6.2. Using Apple Time Capsule on a LAN (Local Area Network)

4.6.2.1. Located in an alternative room to the computer where information is used.

Guidelines for the rights of data subjects

A customer or user may request an outline of the data stored, may request changes or removal (unless the information is directly being used to meet other requirements that they have set out).

This may be done by emailing info@heartco.co.uk, where a response will be issued within 5 working days of email receipt (unless Stephen Holdstock is on holiday – in which case, 5 working days upon return to

work). If the information is not available within that period, an estimation of delivery will be emailed to the customer/user within 5 working days of email receipt.

Access control will be delivered where possible so the customer can access their information directly. This may not always be possible. *Due for review once HC becomes a Limited Company.*

A further set of terms and conditions for using the BMM website are available at the following link: https://www.minifigureme.co.uk/terms-and-legal/

Information Classification

All information used for accounting and invoice purposes will be handled with care and entered in applications as outlined in TOM 1.6.

All information used for website management and optimisation will be anonymous except for items outline in Google's Analytics Data Protection Policy.

All website sales will also be logged securely on the websites where purchases have been placed.

Protection against Malware, Viruses and Hacking

All care is taken to ensure data is kept safe. Only Apple Macs are used to process data, which are not prone to viruses or malware. All updates are performed on machines within 2 weeks of release (unless technically not possible).

All emails are stored on the servers only, not downloaded to machines (expect while processing).

All machines are password protected and can be wiped remotely if stolen (providing they are connected to the Internet).

The BMM website has various security features built into it's Content Management System. This are available upon request, but HC reserve the right to retain this information privately for security reasons.

Protection against Malware, Viruses and Hacking

All care is taken to ensure data is kept safe. Only Apple Macs are used to process data, which are not prone to viruses or malware. All updates are performed on machines within 2 weeks of release (unless technically not possible). All emails are stored on the servers only, not downloaded to machines (expect while processing). All machines are password protected and can be wiped remotely if stolen (providing they are connected to the Internet).

The BMM website actively works to ensure it complies with the SSL certificate that precedes its URL.

With relation to OliveJoy Photography:

Preamble

OliveJoy Photography (also referred to as OJP in this document) is primarily a photography consultancy business which trades under the Sole Trader name of Becky Holdstock. Sub contractors will need to ensure that they have their own GDPR standard policy and agree to HC and OJP's policy also. This will be the responsibility of the sub contractor.

Security policy and responsibilities in the company

- Our ongoing corporate objectives are to continue expanding and develop all aspects of OJP. At all areas of expansion, Data Protection will be considered and this document amended accordingly.
- The specific terms of HC and MS's data protection policy is outlined in 'Existing technical and organisational measures (TOM)' section.
- The role of data protection manager falls within the job description of the Sole Trader, Stephen Holdstock until further notice. He is contactable through info@heartco.co.uk. If the subject line contains obvious reference to GDPR issues, a response will be issued within 5 working days of the email receipt (except where holidays have been published in Stephen Holdstock's HC email footer).
- This document will continue to be reviewed as the business changes and expands. If the current goals are sufficient, no changes will be made.
- Data protection and GDPR compliance will be stressed to all subcontractors of HC and MS.

Legal framework in the company

- At this stage of the business life-cycle, no external legal representatives are in place for OJP. This will be due for revision once HC expands to Limited Company status.

Documentation

- All inspections have been carried out internally by the Data Protection Manager.
- Where possible, all information will be kept confidentiality, integrity and availability. This will be due for review once HC expands to a Limited Company.

Existing technical and organisational measures (TOM)

Below reads appropriate technical and organisational measures that must be implemented and substantiated, taking into account, inter alia, the purpose of the processing, the state of the technology and the implementation costs for OJP.

5. Online Data Protection

5.1. Informational data in this section (5 & 6) is specifically referring to the data captured by OJP, not the artwork or photography that is captured of the subject via OJP, which is subject to a separate section below (7).

5.2. Ensure that the customer (or user) has direct digital access to their information, where possible. If it is not possible, they will be able to access it through a representative of HC or OJP within 5 working days of receipt of request.

5.3. Ensure that the customer (or user) can request an update or removal of data where possible via email (see contact details, page 1).

5.4. Ensure that the data is used only where it is directly required, with the exception of backup purposes.

5.5. Data Backups will be taken daily where OJP are in control. Backups for external sources will be maintained by the company handling the data. HC will ensure that they comply with acceptable Backup policies.

5.6. Live data and Backups of customer (or user) data will be kept secure at all times. All computers containing the information will be password protected, along with all online accounts connected to the customer (or user) data.

5.7. Online data usage will be limited to the following:

5.7.1. Xero Accounting Software (xero.com).

5.7.2. Shore Accounting (shoreaccounting.co.uk).

5.7.3. OJP Portfolio, with permission (olivejoyphotography.co.uk, olivejoy.smugmug.co.uk). Where without permission, only artwork will be displayed unless expressly requested against by the customer (or user).

5.7.4. Apple iCloud based contacts applications for OJP or Becky Holdstock's use only. Customer (or user) data will not be shared from here with anyone else.

5.7.5. Limited and anonymous information captured via Google Analytics for websites.

5.7.6. All emails will be stored on servers and not downloaded to devices permanently. This is currently a dedicated CloudFlare hosting service which is maintained and protected by the hosting client defined and chosen by HC. HC retains the right to keep this information private for security reasons.

6. Offline Data Protection, *Local (offline) data usage will consist of the following (but may include individual cases of alternative use):*

6.1. Label Printing for postage

6.1.1. All received or discarded postage labels will be shredded on site.

6.2. Email software

6.2.1. This may vary depending on the machine the information is being managed.

6.3. Design software

6.3.1. For the production of documents, designs and media-related items in line with the customer/user project needs.

6.4. iCloud Directory for files and project items

6.4.1. An Apple managed secure basis for backups.

6.5. Word processing software

6.6. Local Backup (automatic)

6.6.1. Through the use of Apple OSX Time Machine

6.6.2. Using Apple Time Capsule on a LAN (Local Area Network)

6.6.2.1. Located in an alternative room to the computer where information is used.

7. Artwork and Photography Data

7.1. Photographs taken by OJP are subject to be kept as portfolio work for OJP as per the terms and conditions provided in the terms and conditions provided to the customer upon booking.

7.1.1. Where a customer requests the work be kept private, either an anonymous identity will be provided for the customer or the photos will not be published publically (whichever is agreed between OJP and the client).

7.1.2. Clients may request that photos be kept private at a later date, but OJP photography cannot ensure that photos that have already been shared will cease where it is outside of OJP's control. A copy will still be kept in private for OJP reference.

7.2. All photos that are taken will be provided via the third party software: Smugmug, which will keep a record of the photos for future downloads and ensure its secure and regular backup.

Guidelines for the rights of data subjects

A customer or user may request an outline of the data stored, may request changes or removal (unless the information is directly being used to meet other requirements that they have set out).

This may be done by emailing info@heartco.co.uk, where a response will be issued within 5 working days of email receipt (unless Stephen Holdstock is on holiday – in which case, 5 working days upon return to work). If the information is not available within that period, an estimation of delivery will be emailed to the customer/user within 5 working days of email receipt.

Access control will be delivered where possible so the customer can access their information directly. This may not always be possible. *Due for review once HC becomes a Limited Company.*

Information Classification

All information used for accounting and invoice purposes will be handled with care and entered in applications as outlined in TOM 1.6.

All information used for website management and optimisation will be anonymous except for items outline in Google's Analytics Data Protection Policy.

Protection against Malware, Viruses and Hacking

All care is taken to ensure data is kept safe. Only Apple Macs are used to process data, which are not prone to viruses or malware. All updates are performed on machines within 2 weeks of release (unless technically not possible).

All emails are stored on the servers only, not downloaded to machines (expect while processing).

All machines are password protected and can be wiped remotely if stolen (providing they are connected to the Internet).