Gearbubble GDPR Whitepaper
May 20, 2018

Disclaimer

Please note that this document is provided for informational purposes only. Its contents may be subject to change over time. The information in this whitepaper does not modify existing contractual arrangements and may not be construed as legal advice.

Introduction

Gearbubble is working to make sure that it will comply with the European Union's General Data Protection Regulation (GDPR) when it takes effect on May 25, 2018, and to make sure that its sellers will also be in a position to comply in relation to their use of Gearbubble. This whitepaper presents Gearbubble's approach to GDPR preparation and compliance.

Terms

Buyer: Person visiting Gearbubble for purchasing product.
Controller: Party that determines how and for what purposes personal data is processed.
Data subject: Person about whom personal data relates.
DPIA: Data Protection Impact Assessment.
EEA: European Economic Area. EEA countries currently include Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.
GDPR: General Data Protection Regulation.
Seller(Pro sellers): Party using Gearbubble to host their store.
NDA: Non-disclosure Agreement
Provider: Person who provides the product.
Personal data: Any information relating to an identified or identifiable person.
PIPEDA: Personal Information Protection and Electronic Documents Act.
Processor: Party that processes personal data on behalf of the controller.

Global GDPR application

Who does the GDPR apply to?

Gearbubble
The GDPR applies to any company that handles the personal data of residents in the European Economic Area (EEA). Because Gearbubble itself serve and works with sellers who serve buyers in the EEA, the GDPR applies to these elements of its business. However, because Gearbubble believes strongly in data protection and privacy, it will give all of its sellers the ability to offer their buyers the rights afforded by the GDPR to control their personal data. Additionally, Gearbubble will provide tools and processes to fulfill GDPR-related requests from their buyers.

Providers
Separate from the way in which the GDPR applies to Gearbubble, the regulation also applies to Gearbubble's providers who operate in the EEA or offer goods or services to residents of the EEA. While Gearbubble is working to make sure that its own operations will comply with the GDPR, and to provide its sellers with the tools to help to comply with the GDPR, each provider is ultimately responsible for ensuring that their business complies with the laws of the jurisdictions in which they operate. Using Gearbubble does not guarantee that a provider complies with the GDPR.

Buyers
The GDPR also gives certain rights to identified or identifiable persons (referred to as data subjects), including buyers visiting the campaigns or stores belonging to sellers. These include the right to request:

- Deletion (erasure) of their personal data
- Correction (rectification) of their data
- Access to their data
- An export of their data in a common (portable) format

What data does the GDPR apply to?

The GDPR generally applies to the collection and processing of personal data. Under the GDPR, personal data means any information relating to a data subject. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as:

- Name
- Identification number
- Location data
- Online identifier (such as IP address or cookie ID)

Controller vs. processor status

The GDPR separates data protection responsibilities into two categories: controllers and processors.

Controller: The party that determines for what purposes and how personal data is processed.

Processor: The party that processes personal data on behalf of the controller.

Under the GDPR, in most cases the sellers collects information from their buyers as a controller. In case of Gearbubble we acts as processor as well as controller for the buyers personal data. For the Pro sellers we acts as processor whereas Pro sellers act as controllers for the buyers data.

Processor obligations

Gearbubble is a processor for a Pro seller, it processes personal data on documented instructions from Pro sellers. For example, when a Pro seller connects the store, they give Gearbubble the instruction to process the necessary actions with the buyers personal data.

Data protection impact assessments

Gearbubble is formalising the process for conducting data protection impact assessments (DPIAs) any time a change in processing procedure occurs that is likely to

result in a high risk to individuals' privacy rights. Gearbubble will help answer reasonable questions a buyer has about Gearbubble's processing activities.

Appointment of a Data Protection Officer

Processors must appoint a Data Protection Officer if they conduct certain types of personal data processing. Gearbubble's Data Protection Officer can be reached at privacy@gearbubble.com. Sellers and providers should consider whether they also need to appoint a Data Protection Officer.

Controller obligations

Under the GDPR, the controller has the following responsibilities:.

Facilitating requests

Controllers are obligated to help data subjects exercise their rights.

Gearbubble's sellers can do this by forwarding buyer requests to Gearbubble, as detailed in the Data subject rights section of this document.

Posting a privacy notice

When personal data is collected from a data subject, controllers must provide certain minimum information about the intended processing of the personal data, as well as information about how to contact and identify the controller.

For buyers on Gearbubble we have provided certain information about the intended processing of the personal data on the purchase page where buyer fill up the personal information.

Sellers are responsible for providing this information to their buyers. Gearbubble provides this information in the Gearbubble Privacy Policy, and encourages sellers to provide this information in their own privacy policies.

Complying with marketing regulations

Controllers are responsible for making sure that they comply with marketing and cookie regulations in the jurisdictions in which they operate.

Controllers with EU buyers should make sure that they obtain appropriate consent for the use of cookies—the ePrivacy Directive generally requires some form of consent in order to use tracking technologies. All controllers should similarly make sure that their email marketing practices comply with applicable e-marketing or anti-spam requirements.

Gearbubble for EU buyers makes sure to obtain appropriate consent for the use of their email for marketing practices to comply with applicable e-marketing or anti-spam requirements.

Obtaining consent to process children’s data

When offering goods or services online directly to children under 16 years of age, the controller is responsible for obtaining verifiable consent from the child's parents for processing their data.

Gearbubble for EU buyers makes sure to obtain appropriate consent that the buyer must be over of 16 years of age.

Legal basis for processing

Personal data cannot be processed except under a recognized legal basis (unless an exemption applies). The GDPR sets out a list of possible legal bases under which personal data may be processed.
These reasons include:

- Consent

- Contractual obligations
- Legal obligations
- The public's interests
- Legitimate interests of the controller or third party, balanced against the rights of the data subject.

Consent of the data subject means the data subject has agreed to the processing of their personal data with a clear affirmative action.
This agreement must be:

- Freely given
- Specific
- Informed
- Unambiguous

Sellers, as controllers of their buyers' personal data, are responsible for ensuring they have a proper legal basis for doing so, including keeping evidence of consent when processing is based on consent. As its sellers' processor, Gearbubble is not responsible for the sellers' legal bases but only processes buyers' personal data on behalf of and on the instructions of the sellers.

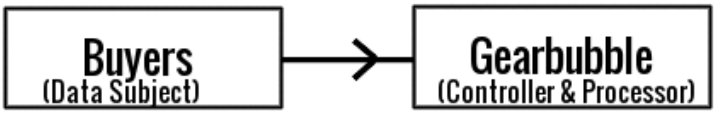
Upon request, Gearbubble will provide sellers with any reasonable information they require to obtain consent.

Data transfers

Personal data of residents of the EEA can only be transferred to recipients outside the EEA if the recipient has adequate protections in place.
These protections may include:

- Adherence to domestic laws that have been deemed adequate by the European Commission
- Negotiated agreements (such as the EU-U.S. Privacy Shield)
- Contractual protections
- Approved sets of internal policies (Binding Corporate Rules)
- Approved codes of conduct or certifications

Gearbubble has protections for personal data in every step of its data flow, as described below. The following diagram illustrates Gearbubble's data transfer structure:



Gearbubble uses a combination of data centers and cloud service providers to store this personal data in the United States.

Disclosures to third parties

Gearbubble will never independently sell personal data for commercial purposes. However, Gearbubble does disclose personal data to third parties or allow third parties to access personal data to help provide services—for example, to:

- Store platform data.
- Sharing personal data with providers used to ship the product.
- Respond to and manage support inquiries.

Additionally, Gearbubble may provide personal data, where permitted, to prevent, investigate, or respond to:

- Potential fraud
- Illegal conduct
- Physical threats
- Violations of any agreements with Gearbubble

Gearbubble is not responsible for the data practices of these third-party service providers.

Use of personal data

Gearbubble itself uses the personal data of the buyers for:

- Transactional emails with updates about buyers orders.
- Broadcast emails with promotions of other Gearbubble products.

Data subject rights

The GDPR provides data subjects (in this case, buyers) with certain rights over their personal data. Generally, data subject requests must be addressed within one month, unless they are exceptionally complex or numerous. The following rights are granted to data subjects:

Erasure
Data subjects have the right to request that their personal data be erased in certain circumstances. If Gearbubble or a seller receives a request from a buyer to delete their personal data, before forwarding the request to Gearbubble, the seller should:

- Verify that the requester is the same as the data subject (that is, the requester is not asking to erase someone else's personal data)
- Confirm there is no legal reason to preserve this data

If both conditions are satisfied, the merchant should forward the request to Gearbubble, either through Gearbubble's support system, or by emailing privacy@gearbubble.com.

After a request is received, Gearbubble will ensure that the relevant personal data is erased. If erasing it is impossible, Gearbubble will let the merchant know to what degree it is impossible, and why.

In addition to contacting Gearbubble, the merchant should also work with any relevant third parties to make sure that they delete or anonymise the personal data.

Timing
Personal data cannot be erased from Gearbubble while it is:

- Associated with a pending order
- Associated with an order made fewer than 180 days before the request (the usual window in which a buyer can make a chargeback).

If the buyer's personal data cannot be erased for this reason, the merchant should re-submit the deletion request after the appropriate time has passed.

Scope

When processing a request for erasure, Gearbubble will anonymise the personal data of the buyer, but keep non-personal data such as revenue information and order details. Order details that are retained include the gateway used to process payment, time of sale, amount paid, currency, subtotal, shipping cost, taxes added, shipping method, item quantity, item name, SKU, and payment method.

If no data erasure requests are received, Gearbubble will keep data for the lifetime of a store.

Access
Controllers must, upon request, explain to data subjects how their personal data is processed and provide access to this personal data. If sellers cannot export data sufficient to fulfill the request from their admin, they can forward the request to Gearbubble. Similar to a request for erasure, if a buyer requests access to their personal data, the seller should first validate the identity of the requester.

The sellers can then reach out to Gearbubble, either through Gearbubble's support system, or by emailing privacy@gearbubble.com.

When Gearbubble receives the request, it will:

- Confirm whether personal data about a buyer is being processed by Gearbubble.
- Confirm what categories of data are being processed by Gearbubble.
- Provide the buyer with the relevant information from Gearbubble systems.

Data portability
Controllers who process data using automation must, in limited circumstances, provide data subjects with their personal data upon request. This data must be provided in a commonly used and machine-readable format.

If a seller contacts Gearbubble to request copies of processed data, Gearbubble will make the data available in a common format.

Rectification
Data subjects have the right to correct incomplete or inaccurate personal data held or processed by a controller. Gearbubble will make the change for customer records on request.

Automated decision-making

Data subjects have the right to object to processing based solely on automated decision-making (which includes profiling), when that decision making has a legal effect on the data subject or otherwise significantly affects them. An example of a legal effect is a decision that impacts an individual's legal or civil rights, or their rights under a contract. Examples of significant effects include decisions that have a financial impact on individuals, or impact their employment.

Gearbubble does not currently engage in fully automated decision-making that has a legal or otherwise significant effect using buyer data.

Services that include elements of automated decision-making are highlighted below:

- Gearbubble has procedure for blacklisting the credit cards involved in fraudulent transactions.
- Gearbubble is implementing automated decision-making process for capturing the payment by analysing the data provided by the buyers for avoiding the fraudulent transactions.

Data protection and security

Under the GDPR, controllers and processors are required to implement appropriate technical and organisational measures.

Gearbubble has implemented many of the controls and processes identified in the GDPR, including:

- Anonymising and encrypting personal data
- Ensuring confidentiality, integrity, availability, and resilience of processing systems
- Restricting who may access personal data
- Ensuring availability and access to personal data in the event of a physical or technical incident
- Performing regular testing, assessments and evaluation of technical and organisational security measures

Organisational measures

Gearbubble has a robust, cross-functional data protection program that is integrated with its information security program and includes several teams across the organisation. In particular, the data protection program includes a designated Data Protection Officer, who reports to senior management, as well as individuals from:

- Internal Security
- Legal
- Legal Operations
- Production Security
- Processing Integrity

Technological measures

Monitoring and logging
Controllers—and where applicable, their representative—must maintain records of the personal data processing activities for which they are responsible.

Gearbubble maintains system and application logs relating to events and access to certain systems used for the processing of personal data. These logs are stored on log servers for approximately a month.

Security controls

Gearbubble encrypts data sent to and from sellers and buyers using the HTTPS protocol. Gearbubble also encrypt the personal data of data subjects.

Contractual agreements and data processing addenda

Gearbubble's Terms of Service, Data Processing Addendum, Privacy Policy, and Acceptable Use Policy can be found online at https://www.gearbubble.com/terms