



GrowthZone Privacy and Data Security

UPDATED APRIL 2018

MICRONET, INC., DBA GROWTHZONE AND CHAMBERMASTER



Table of Contents

[GDPR Overview and FAQs](#)

[Privacy Policy](#)

[Example Materials/Processes to Aid You in GDPR Compliance](#)

[GDPR Request for Personal Data Report](#)

[GDPR Request for Personal Data Deletion](#)





GDPR Overview and FAQs

1. What is GDPR?

The General Data Protection Regulation (GDPR) is a European Union law enacted in 2016 which will take effect with enforcement beginning on May 25th, 2018. This law was enacted with the goal of providing better data and privacy protection and security for European Union (EU) member states' citizens. Additional details can be found on the [GDPR website](#).

2. Is CM/MZ/GZ GDPR Compliant?

Getting ready for the upcoming GDPR changes in May of 2018 is a major initiative at GrowthZone with changes and improvements already underway; GrowthZone software (including ChamberMaster, MemberZone, and GrowthZone) will be fully compliant by the May 25, 2018 deadline.

3. Does my Chamber/Association need to worry about this? Who does this effect?

This law effects organizations doing business with customers residing in EU countries who are citizens of these countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom

4. Are ChamberMaster/GrowthZone CMS and Mobile App products compliant?

SmartCMS and GrowthZoneCMS do not collect member or visitor data. On pages where member or visitor data appears to be collected by these systems, it is in fact due to an integration of the ChamberMaster/GrowthZone software, and thus these systems do not fall under the GDPR requirements. Our staff and member apps, as extensions of the back office and MIC/Info Hubs, fall under this definition as well.

5. How to handle requests for a complete report of all personal data

This type of request should be in written form and include the signature of the requestor. Before contacting us, you may wish to provide the information directly from ChamberMaster or GrowthZone by running a report and sharing the results. If this is not sufficient for the requester, please fill out the [Request for Personal Data Report form](#), have it signed by an authorized chamber/association employee and email it to us along with a copy of the original request. Emails should be addressed to support@chambermaster.com or GZsupport@growthzoneapp.com with a subject line of "GDPR Personal Data Report Request."

GDPR allows a 30-day window for processing though it won't take nearly that long to process your request. Upon completion, we will reply with an attached report that you can share with the contact that will list all the personal information we have saved regarding that contact along with documentation on the physical location of that data.

Important: This only applies to information saved within the ChamberMaster/GrowthZone system itself and does not apply to other systems you may use either as part of an integration or within your office. It is your responsibility to request info from each of these systems as well.





6. How to handle a request for deletion

Again this request should be a written request from the individual. Please fill out the [Request for Deletion Form](#), get it signed by the authorized executive at your chamber/association, and attach it and the original contact request to an email. The email should be sent to support@chambermaster.com or GZsupport@growthzoneapp.com with a subject line of "GDPR Deletion Request."

GDPR allows a 30-day window for processing. Upon completion we will reply with an attached certificate of deletion signifying that all the contact's data has been purged from our system.

Important: This only applies to information saved within the ChamberMaster/GrowthZone system itself and does not apply to other systems you may use either as part of an integration or within your office. It is your responsibility to request info from each of these systems as well.

7. If GZ/CM is compliant, does that mean we at the chamber/association are compliant?

Not necessarily. Customers that use third party systems for websites or integrations with ChamberMaster and GrowthZone software need to be aware GrowthZone is not responsible for the compliance of these systems; GrowthZone is responsible for GDPR compliance of its products only. Chambers and associations are accountable to ensure overall GDPR compliance for the mix of systems they are using to collect and process member and visitor data.

A common example would be if you use integrations with Google Analytics, Constant Contact or other systems where data from ChamberMaster or GrowthZone is pushed into these other systems. You are required to let the member know this so that they can request deletion from these systems as well. Your payment processors would need to be included as well since financial data is handled directly by these processors without touching GrowthZone's servers. Don't forget that if you have locally stored records on your members or records stored using a cloud service, you need to share this info as well.



Privacy Policy

Note: Please refer to the Privacy Policy on our websites or software for the latest version of this document.

GrowthZone and ChamberMaster/MemberZone Privacy Policy

Last updated: May 2018

1. Introduction

1.1 This is the privacy policy that applies to our Sites, Software and our Services. GrowthZone has a strong commitment to safeguarding the privacy of our website visitors and customers' personal information. Personal information is information about an identifiable individual. Publicly available information, such as a public directory listing of your name, address, telephone number, or electronic address, is not considered to be personal information.

Micronet Inc. complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. Micronet, Inc. has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit <https://www.privacyshield.gov/>

1.2 This policy applies where we are acting as a data controller with respect to the personal data of [our website visitors and service users]; in other words, where we determine the purposes and means of the processing of that personal data.

1.3 In this policy, "we", "us" and "our" refer to Micronet, Inc., DBA as GrowthZone and ChamberMaster.

2. Credit

2.1 This document was created using a template from SEQ Legal (<https://seqlegal.com>).

3. How we use your personal data

3.1 In this Section 3 we have set out:

- (a) the general categories of personal data that we may process;
- (b) the purposes for which we may process personal data; and
- (c) the legal bases of the processing.

3.2 We may process data about your use of our website and services ("**usage data**"). The usage data may include your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of your service use. The source of the usage data is our analytics tracking system. This usage data may be processed for the purposes of analyzing the use of the website and services. The legal basis for this processing is our legitimate interests, namely monitoring and improving our website and services.

3.3 We may process your account data ("**account data**"). The account data may include your name, organization and email address. The source of the account data is you, your employer, or an organization that is providing a service to you and using our software for the management of that service. The account data may be processed for the purposes of operating our website, providing our services, ensuring the security of our website and services, maintaining back-ups of our databases and communicating with you. The legal basis for this processing is our legitimate interests, namely the proper administration of our website and business or the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract.



3.4 We may process your information included in your personal profile on our website or within our software ("**profile data**"). The profile data may include your name, address, telephone number, email address, profile pictures, professional bio, IP address. The profile data may be processed for the purposes of enabling and monitoring your use of our website and services. The legal basis for this processing is our legitimate interests, namely to provide our products and services, for billing, for identification and authentication, for the general operation and improvement of our service, and to respond to inquiries, and is not used, shared with or sold to other organizations, except: to our service providers, as required to operate the Site and provide the products or services you've requested; to the applicable customer of the account in respect of which contact information is submitted to us; for collection purposes; to law enforcement agencies, in emergencies, for internal security matters, or where required by court order or search warrant; or when we have your permission. We do not contact our customers' contacts except as related to operating the Site (for example: event notifications and reminders, membership renewals, security and other notifications). We may also disclose personal information in connection with the transfer to the acquirer upon the change of control.

3.5 We may process information that you post for publication on our website or through our services ("**publication data**"). The publication data may be processed for the purposes of enabling such publication and administering our website and services. The legal basis for this processing is consent or our legitimate interests, namely the proper administration of our website and business.

3.6 We may process information contained in any inquiry you submit to us regarding goods and/or services ("**inquiry data**"). The inquiry data may be processed for the purposes of offering, marketing and selling relevant goods and/or services to you. The legal basis for this processing is consent. Additionally, we access other lists generated from advertising, email inquiries, trade shows and conferences.

3.7 We may process information relating to transactions, including purchases of goods and services, that you enter into with us and/or through our website or software ("**transaction data**"). The transaction data may include your contact details, your card details and the transaction details. The transaction data may be processed for the purpose of supplying the purchased goods and services and keeping proper records of those transactions. The legal basis for this processing is the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract and our legitimate interests, namely our interest in the proper administration of our website and business. We may also record your computer's IP address with your order to help us identify fraudulent credit card use. We may share this information with the financial institution that issued the credit card with which an order was placed or with law enforcement authorities if we determine, or are notified, that the use of the credit card was fraudulent.

3.8 We may process information that you provide to us for the purpose of subscribing to email notifications and/or newsletters ("**notification data**"). The notification data may be processed for the purposes of sending you the relevant notifications and/or newsletters. The legal basis for this processing is the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract.

3.9 We may process information contained in or relating to any communication that you send to us ("**correspondence data**"). The correspondence data may include the communication content and metadata associated with the communication. Our website will generate the metadata associated with communications made using the website contact forms. The correspondence data may be processed for the purposes of communicating with you and record-keeping. The legal basis for this processing is our legitimate interests, namely the proper administration of our website and business and communications with users.

3.10 We may process any of your personal data identified in this policy where necessary for [the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. The legal basis for this processing is our legitimate interests, namely the protection and assertion of our legal rights, your legal rights and the legal rights of others.

3.11 We may process any of your personal data identified in this policy where necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, or obtaining professional advice. The legal basis for this processing is our legitimate interests, namely the proper protection of our business against risks.

3.12 In addition to the specific purposes for which we may process your personal data set out in this Section 3, we may also process any of your personal data where such processing is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

4. Providing your personal data to others





4.1 We may disclose your personal data to our insurers and/or professional advisers insofar as reasonably necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, obtaining professional advice, or the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. By accepting this privacy policy, you give consent for your data to be shared with these parties.

4.2 Financial transactions relating to our website and services may be handled by our payment services providers. We will share transaction data with our payment services providers only to the extent necessary for the purposes of processing your payments, refunding such payments and dealing with complaints and queries relating to such payments and refunds. You can find information about the payment services providers' privacy policies and practices at <https://stripe.com/guides/general-data-protection-regulation>. By accepting this privacy policy, you give consent for the transaction data described above to be shared.

4.3 In addition to the specific disclosures of personal data set out in this Section 4, we may disclose your personal data where such disclosure is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person. We may also disclose your personal data where such disclosure is necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

4.4 We do not disclose your data to other third-party sources beyond what is outlined in section 4 without your expressed consent. In the context of an onward transfer of data under the aforementioned criteria, we acknowledge responsibility for the processing of personal information we receive under the Privacy Shield and subsequently transfer to a third party acting as an agent, including proper usage and protection under the principles of the Privacy Shield except in cases where Micronet has proven to not be responsible for processing inconsistent with Privacy Shield Principles and therefore is held harmless.

4.5 If you object to or have questions regarding the conditions laid out in section 4 dealing with the sharing of your data with 3rd parties, you may contact us in writing at gzsupport@growthzone.com or support@chambermaster.com or at the address in section 13 to exercise your rights as described in section 8.

5. International transfers of your personal data

5.1 We have offices and facilities in the United States.

5.2 The hosting facilities for our website and software are located in the United States. The European Commission has made an "adequacy decision" with respect to the data protection laws of this country herein called the Privacy Shield Framework.

5.3 You acknowledge that personal data that you submit for publication through our website or services may be available, via the internet, around the world. We cannot prevent the use (or misuse) of such personal data by others.

6. Retaining and deleting personal data

6.1 This Section 6 sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of personal data.

6.2 Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

7. Amendments

7.1 We may update this policy from time to time by publishing a new version on our website.

7.2 You should check this page occasionally to ensure you are happy with any changes to this policy.

7.3 We may notify you of changes to this policy by email or through messaging on our website.

8. Your rights





8.1 In this Section 8, we have summarised the rights that you have under data protection law. Some of the rights are complex, and not all of the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

8.2 Your principal rights under data protection law are:

- (a) the right to access;
- (b) the right to rectification;
- (c) the right to erasure;
- (d) the right to restrict processing;
- (e) the right to object to processing;
- (f) the right to data portability;
- (g) the right to complain to a supervisory authority; and
- (h) the right to withdraw consent.

8.3 You have the right to confirmation as to whether or not we process your personal data and, where we do, access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the personal data. Providing the rights and freedoms of others are not affected, we will supply to you a copy of your personal data. The first copy will be provided free of charge, but additional copies may be subject to a reasonable fee.

8.4 You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed.

8.5 In some circumstances you have the right to the erasure of your personal data without undue delay. Those circumstances include: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; you withdraw consent to consent-based processing; you object to the processing under certain rules of applicable data protection law; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise or defence of legal claims.

8.6 In some circumstances you have the right to restrict the processing of your personal data. Those circumstances are: you contest the accuracy of the personal data; processing is unlawful but you oppose erasure; we no longer need the personal data for the purposes of our processing, but you require personal data for the establishment, exercise or defence of legal claims; and you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data. However, we will only otherwise process it: with your consent; for the establishment, exercise or defence of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest.

8.7 You have the right to object to our processing of your personal data on grounds relating to your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party. If you make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

8.8 You have the right to object to our processing of your personal data for direct marketing purposes (including profiling for direct marketing purposes). If you make such an objection, we will cease to process your personal data for this purpose.





8.9 To the extent that the legal basis for our processing of your personal data is:

- (a) consent; or
- (b) that the processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract,

and such processing is carried out by automated means, you have the right to receive your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.

8.10 If you consider that our processing of your personal information infringes data protection laws and requests to GrowthZone have not led to resolution, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. This, in some cases and under certain conditions, may include the possibility of invoking binding arbitration. A Dispute Resolution Provider is available at <https://www.jamsadr.com/eu-us-privacy-shield>. You may do so in the EU member state of your habitual residence, your place of work or the place of the alleged infringement.

8.11 To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

8.12 You may exercise any of your rights in relation to your personal data by written notice to us. This can easily be done via sending an email to gzsupport@growthzone.com for GrowthZone customers or support@chambermaster.com for Chambermaster customers. You may also provide notice via the mailing address in section 13.

9. About cookies

9.1 A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.

9.2 Cookies may be either "persistent" cookies or "session" cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.

9.3 Cookies do not typically contain any information that personally identifies a user, but personal information that we store about you may be linked to the information stored in and obtained from cookies.

10. Cookies that we use

10.1 We use cookies for the following purposes:

- (a) authentication - we use cookies to identify you when you visit our website and as you navigate our website;
- (b) status - we use cookies to help us to determine if you are logged into our website;
- (c) analysis - we use cookies to help us to analyze the use and performance of our website and services.

11. Cookies used by our service providers

11.1 Our service providers use cookies and those cookies may be stored on your computer when you visit our website.

11.2 We use Google Analytics to analyse the use of our website. Google Analytics gathers information about website use by means of cookies. The information gathered relating to our website is used to create reports about the use of our website. Google's privacy policy is available at: <https://www.google.com/policies/privacy/>.

12. Managing cookies





12.1 Most browsers allow you to refuse to accept cookies and to delete cookies. The methods for doing so vary from browser to browser, and from version to version.

12.2 Blocking all cookies will have a negative impact upon the usability of many websites.

12.3 If you block cookies, you will not be able to use all the features on our website.

13. Our details

13.1 This website is owned and operated by Micronet, Inc., DBA GrowthZone and/or ChamberMaster.

13.2 Our principal place of business is at 24400 Smiley Road, Suite 4, Nisswa, MN 56468, USA.

13.3 You can contact us:

(a) by mail, to the postal address given above;

(b) using our website contact form;

(c) by the contact number published on our website from time to time; or

(d) by email, using the email address published on our website from time to time.

13.4 Micronet, Inc. is subject to the investigatory & enforcement powers of the Federal Trade Commission (FTC)

14. Data protection officer

14.1 Our data protection officer's contact details are: Scott Juranek via the contact means given above.



Internal Company Practices to Protect Data

GrowthZone needs to gather and use certain information about individuals to fulfill the needs of our customers. These can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

Everyone who works for or with GrowthZone has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed to meet the company's data protection standards.

General Staff Guidelines

- All staff must accept and comply with a company Code of Conduct which includes a specific clause regarding the Protection and Proper Use of Company Assets, of which the data that customers have entrusted to the Company are clearly included.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below, along with the terms of the company's Privacy Policy.
- Internally, strong passwords must be used for all equipment and password-protected programs and services and they should never be shared.
- Personal data should not be disclosed to unauthorized people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their manager if they are unsure about any aspect of data protection.

Data Storage, Access and Management

1. Website databases, servers and equipment are contained in locked equipment racks. The equipment racks are housed in keycard accessible SAS compliant cages. The cages are located in keycard/bio-scan accessible data centers, all serviced by a SAS-compliant collocation provider. Additional data center security measures include: surveillance cameras, badge IDs and limited facilities access granted to SAS-compliant collocation provider technicians. Network and server firewalls are configured to protect all website servers. Intrusion detection systems alert for potential malicious network activity. Website servers and equipment require administrator authentication to gain console access at all times. Limited remote management is allowed through strict firewall IP access lists and allowed to only a limited number of trusted employees. All data is stored in the United States.
2. Password data is hashed.
3. Data is protected in transit by SSL.





4. To provide trouble-shooting to customers, GrowthZone employees will, as necessary assume an administrative role that allows staff to masquerade as a user in the customers' instance of GrowthZone. At no time does GrowthZone staff have access to a user's password.
5. The GrowthZone software includes audit logs to note any customer or staff updates or changes to data. This audit log includes the ability to determine the source of changes or additions.
6. GrowthZone utilizes a full source control management system for all software code commits.





Product Features for Data Protection

Expressed Consent for New Members

It will soon be easier to gain expressed consent for data processing and storage when contacts sign up for a membership. You will still need to gain expressed consent from current members during a one-time process. However, after that you can simply enable this required step as part of your standard membership application and immediately capture your new members' consent.

Unsubscribe & Communications Flexibility

You will have greater flexibility to easily add standardized disclaimer/privacy text to the bottom of all emails including single emails allowing to actively communicate your GDPR compliance to contacts and allow them to manage more of the usage of their data for communication purposes.

Security Improvements

In relation to the security by design and security transparency tenets of GDPR, we're introducing a host of optional security features that can be enabled a la carte to enhance the security and restriction regarding the authentication of your members, ensuring an added level of security for their data. Options are configurable allowing you to tailor your requirements to your needs.

Privacy Shield

In regards to GDPR's requirements about data sequestration in the EU or an outside nation that has been officially recognized by the EU as in compliance with GDPR, GrowthZone/Chambermaster will be certified via the PrivacyShield framework. This means that your customer's data will be housed outside of the EU but still in compliance with GDPR.





Example Materials/Processes to Aid You in GDPR Compliance

Members Asking Questions? We've Got Answers!

General Information Request

You have members or contacts questioning how you are using their data in relation to GDPR; what now?

You should expect to field most general information questions regarding your organization's compliance with GDPR as a processor of personal data. For questions that relate specifically to ChamberMaster or GrowthZone, please reach out. We're here to help. Most questions have been addressed in this packet, but we can help you answer other questions or help you find the spot in the software where you find the information you're looking for. In many cases, individuals are either simply curious about what you're collecting/how you're using their data OR they want reassurance your business practices, including the software you're using, are keeping their data safe.

Request for Personal Data Report

You just got a request for a Personal Data Report. What do you do next?

This request should be in written form and include the signature of the requestor. Before contacting us, you may wish to provide the information directly from ChamberMaster or GrowthZone by running a report and sharing the results. If this is not sufficient for the requestor, please fill out the [Request for Personal Data Report](#) form, have it signed by an authorized chamber/association employee and email it to us along with the copy of the original request. Emails should be addressed to support@chambermaster.com or GZsupport@growthzoneapp.com with a subject line of "GDPR Personal Data Report Request."

GDPR allows a 30-day window for processing, though it won't take nearly that long to process your request. Upon completion, we will reply with an attached report that you can share with the contact that will list all the personal information we have saved regarding that contact along with documentation on the physical location of that data.

Important: This only applies to information saved within the ChamberMaster/GrowthZone system itself and does not apply to other systems you may use either as part of an integration or within your office. It is your responsibility to request info from each of these systems as well.

Request for Deletion

You have received a request from a contact to be deleted from your systems. Now what?

Again, this request should be a written request from the individual. Please fill out the [Request for Deletion](#) form (link to doc), get it signed by the authorized executive at your chamber/association, and attach it and the original contact request to an email. The email should be sent to support@chambermaster.com or GZsupport@growthzoneapp.com with a subject line of "GDPR Deletion Request."



GDPR allows a 30-day window for processing. Upon completion we will reply with a certificate of deletion signifying that all of the contact's data has been purged from our system.

Important: This only applies to information saved within the ChamberMaster/GrowthZone system itself and does not apply to other systems you may use either as part of an integration or within your office. It is your responsibility to request info from each of these systems as well.

GDPR Consent for Existing Members

Overview

In an effort to make it easier for chambers and associations to comply with the EU's General Data Protection Regulation (GDPR), we at GrowthZone are providing some training and sample/example language that can be used with both ChamberMaster & GrowthZone products. This language can be added to the terms & conditions area in the Membership Application for new members. For guidance in making this addition, review the instructions in our online support wiki: [GrowthZone Instructions](#) or ChamberMaster/MemberZone Instructions (feature coming in May).

But what about existing members?

Adding language as part of an expressed consent process attached to your membership application will allow you to gain consent for new members, but what about your existing members? You also need to inform your existing members about your GDPR compliance and gain their consent to continue processing their data. While the process you use for this may be different, the information you are sharing with existing members is the same as with new members.

1. The steps the chamber has taken to comply with the GDPR
2. How the member's data will be stored and used
3. How the member's privacy is secured
4. How the member can request a report of all personal data kept by the chamber
5. How the member can request complete deletion of their personal data

Process

It is up to the individual chamber/association to determine the best process for notifying existing members of GDPR. We advise you to work with your policy team to determine the best way to accomplish this one-time process. Options could include using an online consent form or including requirement to accept new terms of service as part of your GDPR compliance processes.

If you're creating a form or text for your members to review, we've included this example/sample text as a starting point. This is the same text that we've offered as a starting point for setting up new terms/conditions and/or membership application. This text is a starting point and should not be used as is.

1. Steps to comply

The General Data Protection Regulation (GDPR) is a European Union regulation enacted in 2016 which takes effect on May 25th, 2018. This law was enacted with the goal of providing better data and privacy protection and security for European Union (EU) member states' citizens. Currently, UK citizens are covered under the



GDPR until a time at which the United Kingdom is no longer a member state and thus subject to the laws and regulations.

As a result, <Chamber/Association Name>, has taken steps as a controller of data to comply with the regulation and its intent in order to safeguard your personal data ensuring its privacy and security, transparency and complying with your rights as a citizen of an EU member state to maintain ownership of your data at all times.

Understanding your rights regarding your personal data is an important first step . At a high level, your data rights under the GDPR are:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

These rights along with details and further explanation can be view on the [GDPR site](#).

<Chamber/Association Name> uses the <ChamberMaster/GrowthZone> product to manage your data as it relates to the business relationship between the chamber and you. <Chamber/Association Name> has worked with GrowthZone to ensure your data is secure, private and will not be shared with other entities without your expressed consent.

2. Data Storage & Use

The GDPR requires that your data be stored in the EU or in a country that has an official agreement with the EU regarding the GDPR. GrowthZone, a United States company, stores all of <Chamber/Association Name>'s data on its servers in the United States. GDPR allows this under the Privacy Shield framework by which US business entities can certify their compliance with GDPR.

Your rights under GDPR allow you to request from <Chamber/Association Name> a full data report, which includes a full record of the data being stored about you, how that data is being used/processed, who that data is being shared with, and the physical location of the data.

In compliance with GDPR, you may make this request in writing at any time to <Chamber/Association Name> and we will provide a written report within the allowed 30-day response period.

If, at any time, you wish to have your data deleted completely from all systems and servers, you may submit a written request to us and we will initiate a full deletion process that will purge all your personal data from our systems within 30 days. Upon completion, we will send you a certification of deletion confirming this process. It is important to understand that once this process has been initiated, it cannot be halted and there is no way to recover data should you change your mind.





We do not share/sell your data to other companies and only use your personal data for purposes relating to the established business relationship between <Chamber/Association Name> and you.

3. Data Security & Integrity

As a processor of your data, it is our duty to ensure your personal data remains safe and secure at all times. We have introduced enhanced security methods to keep your data safe. Accounts and passwords feature enhanced security requirements and financial transactions are processed using industry best practices relating to encryption and data integrity. You have the right to request in writing more information about data security and system integrity.

By clicking accept and proceed, I consent to my data being stored and processed by <ChamberName/AssociationName> and understand my rights under GDPR.

Other Important Items

GrowthZone is a processor of your member's data but it is unlikely the only processor. The terms and conditions language you draft for your members should include language from all processors. Even though you may not think you are sharing your members' data with other systems because you're not selling it, you may still have compliance issues.

A common example would be if you use integrations with Google Analytics, Constant Contact or other systems where data from ChamberMaster or GrowthZone is pushed into these other systems. You are required to let the member know this so that they can request deletion from these systems as well. Your payment processors would need to be included as well since financial data is handled directly by these processors without touching GrowthZone's servers. Don't forget that if you have locally stored records on your members or records stored using a cloud service, you need to share this info as well.

This language has been drafted with the intent of presenting it to new and existing members for collecting, storing and processing their information. Be advised that this regulation also applies to your contacts that may be non-members. Therefore, if you are collecting and storing contact information on non-members, we advise you to work with your legal team to devise to what degree and at what point you need to gain consent.





GDPR Request for Personal Data Report from GrowthZone, ChamberMaster or MemberZone Systems

This form is to be used when requesting that GrowthZone provide all contact data in compliance with the EU's General Data Privacy Regulation. Chambers/Associations who have received a request for a full contact data report must complete this form, have it signed by an authorized chamber/association employee, and return it along with a copy of the original contact request to support@chambermaster.com or support@growthzone.com. Please allow 10 business days for processing.

Association Information

Chamber/Association Name	City, Country
Chamber/Association Employee making request	Today's Date

Contact Information

Contact First Name	Contact Last Name	Contact ID#
Contact Email	Contact City, Country (physical address)	
Special instructions		

Authorized Signature

Date

OFFICE USE

Rec'd _____ Processed by _____ Completed _____





GDPR Request for Deletion from GrowthZone, ChamberMaster or MemberZone Systems

This form is to be used when requesting that GrowthZone permanently delete contact data in compliance with the EU's General Data Privacy Regulation. Chambers/Associations who have received a request for deletion must complete this form, have it signed by an authorized chamber/association executive, and return it along with a copy of the original contact request to support@chambermaster.com or support@growthzone.com. Please allow 10 business days for processing.

Association Information

Chamber/Association Name	City, Country
Chamber/Association Employee making request	Today's Date

Contact Information

Contact First Name	Contact Last Name	Contact ID#
Contact Email	Contact City, Country (physical address)	
Special instructions		

By signing, I am authorized to make this request and understand that all personal data relating to this contact will be completely and permanently deleted from the GrowthZone/ChamberMaster system. This process is not reversible and this data is not recoverable.

Authorized Signature

Date

OFFICE USE

Rec'd _____ Processed by _____ Completed _____

