



STATEMENT OF GDPR PREPAREDNESS

Introduction

At iContact we are very aware of the importance of managing the personal data that we hold, whether that be from a customer, an influencer, an employee or anyone else we interact with through the products and services we provide. We take our privacy and data protection obligations very seriously, and a key part of that right now is ensuring that we align all our data practices with the new requirements of General Data Protection Regulation (GDPR) by May 2018. We are fully committed to doing so and working hard to make this happen. We're also very conscious that things don't stop in May 2018. This is an ongoing process and we will be looking to ensure that privacy concerns continue to be built into our products and services, and in our practices and procedures. This note responds to a number of the most frequently asked questions that we have been receiving from our customers about what iContact is doing with respect to GDPR and in particular questions related to data that is provided to us by our customers. This document addresses the following areas:

- **GDPR Awareness at iContact**
- **Data Inventory - what data do we hold?**
- **How We Handle Customer Data**
- **The Rights of Individuals**
- **Data Retention**
- **Notices and Consent**
- **iContact Suppliers**
- **Breach Notification**
- **Protection of IT Assets**

We are conscious that this may not answer all of your questions, but we hope this helps to answer many of them, and of course we are happy to respond to any particular concerns you may have. Rest assured that iContact is committed to a program of full GDPR compliance and has a long-term commitment to privacy.

GDPR Awareness at iContact

GDPR represents a significant change in the European data protection regime but, as the UK regulator (the ICO) has said, in many respects it is an evolution not a revolution. iContact has been subject to and respectful of its data protection obligations under existing law, and will continue to be so leading up to and beyond May 2018. The protection of our customer and employee data has always been a priority for our leadership.

We established a GDPR transformation program in 2017 with, at its heart, a cross disciplinary team including representatives from product design, sales, marketing, research, IT, HR and legal all overseen by management. This team includes a designated data protection officer who will liaise closely with our internal and external advisers.

Each of our businesses has had internal data protection and privacy awareness programs for many years, and a number of our employees have undergone specific GDPR training. We are introducing a range of GDPR awareness sessions as we move towards May 2018 and beyond.

As part of our GDPR transformation program, we have been undertaking a thorough audit of all the personal data we hold throughout the organization and have been conducting a 'gap analysis' of GDPR requirements against an assurance framework and mapping this against all activities in the group. We are investing in the creation of robust and sustainable processes to support a strong, long-term GDPR compliance framework.

iContact is based in the US but does have customers worldwide. Where we are engaged in cross border data transfers from customers located in the European Economic Area (EEA), we will ensure that we continue to follow appropriate practices and follow one or more of the approved means of protecting personal data that leaves the EEA.

This is not something that we can do on our own. The products and services that we provide typically mean that we will be a data processor for data provided to us by our customers which our customers then use through our products and services. As a general rule we do not act as a joint data controller in respect of information provided by our customers. Our customers have their own compliance obligations, and where we can we will work with them to help them comply.

Data Inventory

The main category of personal data that we process as a data processor is data belonging to our customer.

We are enhancing our data protection impact assessment processes and supporting governance frameworks to ensure that privacy issues are considered appropriately in all new product developments that may impact privacy rights.

What iContact Does With Customer Data

The personal data that we process which is provided by our customers falls into two broad categories: first, personal data of our customers (i.e. the representatives that we interact with in order to provide our products and services); and, second, personal data of recipients that our customers provide to us.

Personal information about our customers is usually limited to the contact and other details we need in order to fulfill our obligations to you. Personal information on our customers recipients may be much broader, depending on what our customers provide to us. Typically it will include name and email addresses. With our customers' subscriber lists, we will act as a data processor, and we only process the information in accordance with our customers' instructions.

We do not typically store or process any special categories of personal data (for example, data regarding mental or physical health, sexual orientation, criminal convictions, and religious or political beliefs).

As part of our GDPR transformation program we will be bringing our contractual arrangements with our customers up to date to ensure compliance with new GDPR obligations governing the relationship between data controllers and data processors. We anticipate rolling out our program of updating our contractual relationships before May 25, 2018. This will be to ensure that the contractual provisions required by GDPR are in place so that we and our customers are compliant with the new rules.

The Rights of Data Subjects

Existing law had long provided individuals with certain rights related to the processing of their personal data (such as subject access rights and rights to object to direct marketing). GDPR enhances some of those existing rights, and introduces some new ones, and we ensure that we have in place appropriate procedures and technology solutions to enable us to fulfill our obligations and respond appropriately to individual requests, including for example data subject access requests, and requests for erasure or for restricted processing, and, where applicable, requests related to data portability and profiling.

Data Retention and Security

We are taking the opportunity to review our data retention policies to ensure that we do not keep personal data for periods longer than is necessary. Where we process customer data, that obligation rests primarily on the customer and we will comply with our obligations as a data processor in that regard. We ensure that we have appropriate technical and organizational measures in place to protect the personal data we process and have always adopted strict IT security measures to protect personal data.

As part of our GDPR transformation program we are reviewing our encryption, anonymization, and pseudonymizing controls across customer and supplier data to see where there are opportunities to further protect the data we hold.

Notices and Consent

Our GDPR transformation program is a work in progress. We are currently reviewing all of our policies in light of the requirements of GDPR and other relevant legislation, and where necessary, will update relevant processes, policies, and documentation and provide notice of such changes to our customers, suppliers, and employees at the appropriate time.

We are currently completing a review of our lawful basis for processing the various categories of personal data that we deal with. Some of our customers are asking questions about consent, which is understandable given the amount of publicity that there has been about changes to the consent regime under GDPR. It is important to remember that under GDPR (as with the current law) there are a number of different grounds on which it is permissible to process personal data. Consent is one of them, and the one that has caught most attention, but it is not the only one, and may not always be the most appropriate. Another ground for processing personal data is where that processing is necessary for the performance of a contract (e.g. a customer contract) or where the processing is in the legitimate interests of the data controller (provided that there is no unwarranted adverse effect on the rights of the individual). Legitimate interests include legitimate business interests, such as the interests of iContact in providing its products and services to our customers.

iContact Suppliers

Where we engage third party service providers, we do so in accordance with best practice to ensure that those providers are obliged to only process such data in accordance with our instructions, to keep it secure, and not to transfer it outside the EEA other than with our consent or in accordance with the appropriate frameworks.

Under GDPR we are obliged to impose certain additional obligations on our data processors, and we are enhancing our framework of controls around such third parties suppliers and sub-processors. We will be updating our supplier contracts and seeking confirmation of GDPR readiness across all of our suppliers' data processing facilities and security controls surrounding the processing and management of data.

We will expect all our data processors to comply with their contractual obligations and more widely with their own obligations under GDPR.

Communicating Breaches

Data breach notification is one of the key new requirements under GDPR. We are reviewing our controls and processes around data breach detection, investigation and reporting to ensure we can comply with our obligations as data controller and as a data processor, by May 2018. This includes our obligations as a controller to report to the appropriate data protection regulator within 72 hours of discovery, to the data subjects where appropriate, and our obligations as a data processor (e.g. of customer data) to report to the data controller (in this case our customer) without undue delay after becoming aware of a breach.

This review also includes assessing the adequacy of present information security assessment programs.

IT Protection

We have reviewed current IT services and systems and are carrying out remedial actions, where required, to strengthen our IT controls around personal data.

We are also reviewing our encryption, anonymization and pseudonymizing controls across customer and supplier data, and on all of our databases.

Summary

This statement is intended to provide responses to the most common inquiries we have received from our customers. As part of ongoing transformation, iContact will be communicating regularly with its customer base in 2018 about what it is doing on its journey to achieve compliance and how we are protecting customer data, retraining staff and upgrading systems, processes and governance as we move towards compliance with GDPR by May 2018 and onwards, and to ensuring privacy issues continue to sit at the heart of our product and service development plans in the future.

If you have more detailed questions that are not covered by this document, please contact gdpr.help@icontact.com and we will respond to you as soon as possible.