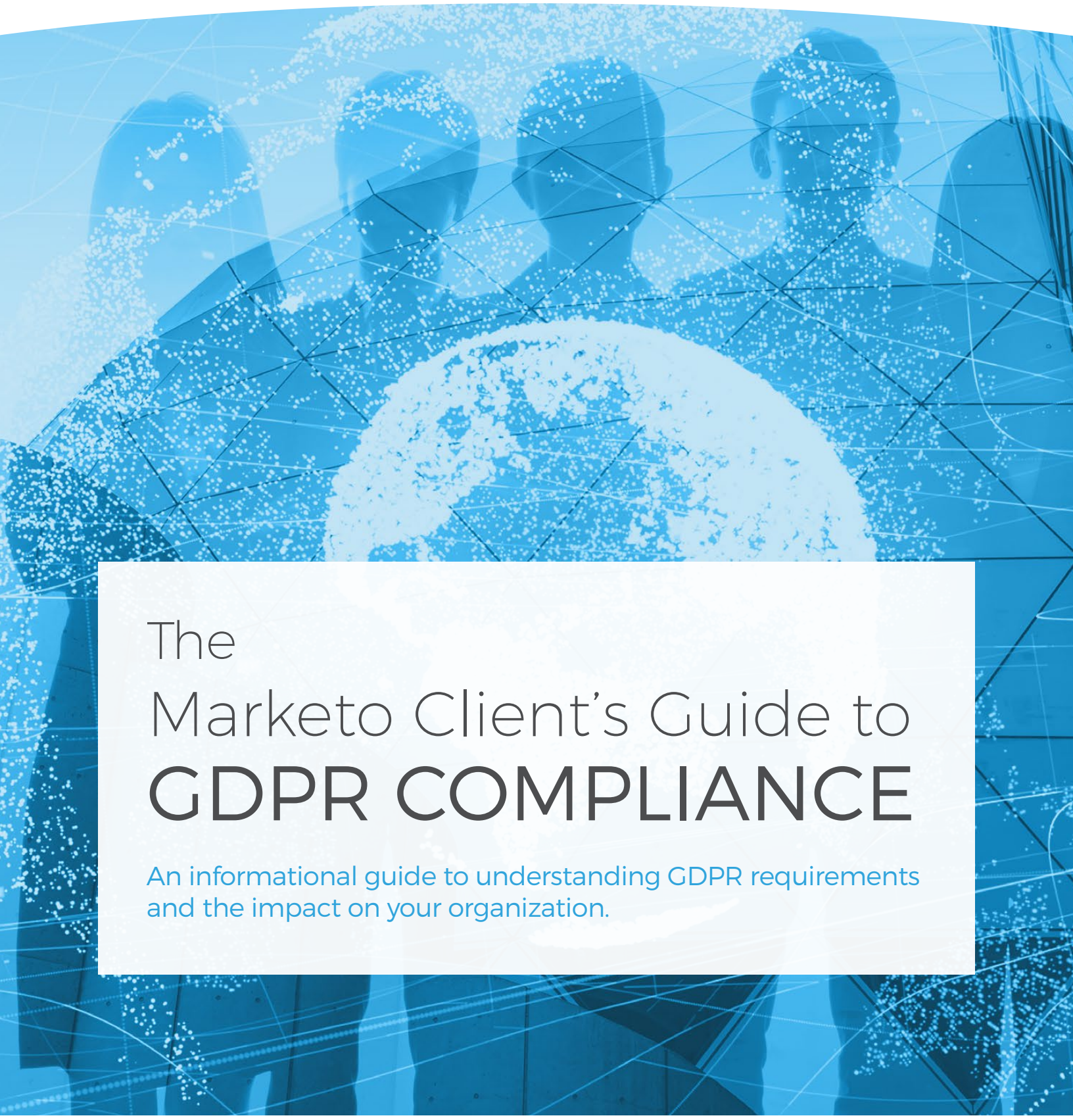
PERKUTO



The Marketo Client's Guide to GDPR COMPLIANCE

An informational guide to understanding GDPR requirements and the impact on your organization.

INTRODUCTION

GDPR...it's becoming a buzz word in marketing these days. And for a good reason. This intricate European legislation is a game changer for marketing operations, has martech teams scurrying to comply with data security requirements, is giving entire organizations good experience in process documentation, plus is keeping legal teams busy advising on the ambiguities of the law.

The impact and ramifications of GDPR are not to be underestimated. GDPR is the most significant change in European privacy laws in two decades; the legislation is vast, and consequences for non-compliance are enormous.

This guide is intended to help your organization understand and prepare for GDPR. It is not meant to replace legal advice, rather, consulting legal counsel for clarification on GDPR's policies and requirements is highly recommended.

WHAT IS GDPR?

GDPR, **General Data Protection Regulation**, is legislation aimed at protecting the privacy of EU residents. The primary objective of the regulation is to give the consumer control over his or her data by providing transparency of information collected and for what purpose as well as the right to consent to the data collection—or not.

The key themes of GDPR are "**CONSENT**" and "**ACCOUNTABILITY**" surrounding behavior monitoring and data collection.

GDPR also regulates the process in which companies may monitor online behavior and collect, store and use personal data, requiring legal documentation for data processing practices, mandates for data protection, and strict reporting requirements should a security breach occur.

The European Parliament, the Council of the European Union, and the European Commission adopted GDPR on April 27, 2016, and the legislation becomes enforceable on May 25, 2018. Non-complying companies will be subject to severe financial penalties.

DOES GDPR APPLY TO YOU?

All companies—big, small, old, new, domestic or international—are subject to GDPR compliance if you are marketing to, doing business with, and processing or storing data of European Union (EU) residents in your database, regardless of your organization's location. GDPR legislation pertains to all personal data collected, appended, processed and stored on EU residents. Additionally, the term "residents" is not limited to Europeans. It also applies to (and protects) citizens of another country who are residing in EU, throughout their stay.

GDPR PRE-PREPARATION ASSESSMENT: Audit your database. Do all records have correct (normalized) country data tied to them? How many EU names are in your database? Are they viable? Knowing this will help assess the potential impact GDPR has on your business.

COUNTRIES IN THE EU INCLUDE:

- Austria
- Belgium
- Bulgaria
- Croatia
- The Republic of Cyprus
- The Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- The Netherlands
- The UK

GDPR SPECIFICS FOR MARKETO CLIENTS

Marketo clients are accustomed to using data to better engage customers, enhance customer experiences and focus marketing efforts. So it's natural that you may be questioning if your marketing automation will be able to coexist with the GDPR's consent-driven legislation. **Yes**. Absolutely. However, organizational changes are necessary to ensure your marketing operations meet the obligations of GDPR compliance.

TYPES OF DATA PROTECTED

One of the first areas to examine is the type of data your company collects. GDPR protects:

- Basic identity: name/address, ID numbers
- Web data: location, IP address, cookie data, RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation
- A personal photo
- Posts on social media
- Banking details

DATA COLLECTION REQUIREMENTS

The manner in which your company collects data is also significant. As mentioned previously, a core theme of GDPR is "**consent**." GDPR mandates obtaining explicit permission from the individual before you may collect and store personal data. Requirements include:

Data retention requires consent and transparency in usage. Putting an end to opt-out models and going beyond an implied opt-in, GDPR requires explicit consent to collect and retain personal data. What this means to you: no more pre-checked permission forms—you must state how you will use the data obtained, and, include a link to your privacy policy indicating how customer information will be handled and stored. Additionally, opt-in consent cannot be "bought" with another transaction, such as downloading a white paper. Rather, opt-in consent to receive ongoing marketing communications must be an independent action.

Privacy policies must be clear. If your current privacy policy is complicated legalese, you'll need to rewrite it. GDPR mandates that privacy policies are easy to access and easy to understand. Additionally, the ability to withdraw consent must be as simple as giving it.

Data cannot be stored forever. Under GDPR, you can retain customer data only "as long as it is necessary," and you must inform the customer how long his or her data will be kept on file. If it's not possible to state a specific length of time, then the criteria that determine how long you will keep his or her information must be given instead. Recommended: consult with your legal team to define what "as long as necessary" means for your organization.

Consumers have control over data portability. GDPR gives an individual the right to obtain his or her data to share with another data controller. What does this mean? Essentially, it means that as a

business that collects consumer data, you are in the role of a "data controller" and must provide individuals with their data—in a commonly used, machine-readable format for ease of transfer—so that they may share it with any other business or data controller of their choice.

Data must be erased upon request. More complicated than it sounds, GDPR includes a "right to be forgotten" clause, which allows the customer to request removal of all personal data from your database. The challenge of this requirement is if your data lives in silos, you must ensure complete erasure occurs in all locations where data might be stored. There are a few exceptions to this clause, including legal requirements to retain data such as HIPAA health records, criminal history or certain types of scientific, historical or statistical research.

GDPR CAUTION AREAS

Reverse IP tracking and use of cookies to identify users requires consent. Implied consent or "by using this site, you accept cookies" messages do not count as consent. You must give users the ability to specify their preferences and give permission to collect ID and behavioral data.

Data enhancements must be declared. Under GDPR, transparency in the use of MAP (marketing automation platform) is required and pre-GDPR data collected must be audited. If you are further enhancing your data from a third-party source, you may need to state the origin and the purpose. Keep in mind, anyone processing your prospects' data must be GDPR compliant too.

Lead scoring is considered user profiling, which requires consent. Using lead scoring or propensity-to-purchase calculations to schedule follow-up sales calls? You guessed it...under GDPR, you must have

permission to use the consumer's data in this capacity. Your privacy policy is an ideal place to state this information, with all forms linking to your privacy policy.

Parental consent required for children. Mainly aimed at social media and websites providing online services, GDPR offers special protection for children. According to GDPR, a child may give his or her consent at the age of 16 although this may be lowered to age 13 in the UK. To process personal data on younger children, you must have consent from a person holding "parental responsibility."

OPERATIONAL IMPACT

The other core theme of GDPR is **"accountability**." Our focus now shifts from how you are collecting data to the process in which you are handling and storing it. To meet the obligations of GDPR, you must be able to prove your company's practices are compliant with GDPR requirements. Specifically:

Document your data protection plan. This written document states your internal procedures for protecting data and should be reviewed periodically to ensure ongoing compliance with GDPR requirements.

Maintain records of processing activities. If your company has 250 employees or more and you are controlling or processing data OR your business is smaller but is processing data on a regular basis or processing sensitive data, you are required to keep data processing records. This documentation must be available to GDPR's supervisory authorities/national regulators upon request.

Document your team structure. Who can design data collection forms? Who has access to your database? While not a specific GDPR requirement, documenting roles and permissions can be helpful, especially in the unfortunate event of a data breach.

GDPR and marketing automation can coexist. However, changes to both front and back-end operations are necessary.

Hire a Data Protection Officer (DPO). GDPR stipulates the addition of the DPO role but leaves the decision of hiring a dedicated DPO, a shared/outsourced DPO or appointing a member of your existing team up to the company. The DPO is responsible for advising and informing your organization of their obligations to GDPR as well as providing ongoing compliance monitoring. The DPO also acts as the company liaison with GDPR supervisory authorities. The DPO can be an internal employee or an external shared resource.

Prepare a security breach action plan. With the rise of security breaches and cybersecurity attacks, it's no surprise GDPR addresses this area as well. Should your company experience a security breach, under GDPR, you are required to report it to the supervisory authority within 72 hours of your data controller becoming aware of the incident. Additionally, if the breach is of a "serious nature," meaning it impacts the rights and freedoms of individuals in your database, you are also required to inform the public without delay. Just like a disaster management plan, prepare a security breach action plan to proactively test your systems, evaluate potential vulnerabilities, and document breach reporting procedures.

RAMIFICATIONS OF NON-COMPLIANCE

GDPR is not only a big issue for businesses; it could prove to be a big business. (For EU, that is.) Should your company be found out of compliance, you could be facing a fine of 20 million Euro or 4% of total global revenues, whichever is greater.

Due to the massive requirements, 52% of companies expect fines in the first year of enforcement. Additionally, first-year revenue from penalties are predicted to reach 6 billion dollars.[1]

To put the fines in perspective:
The 2017 Equifax data breach, the most massive and most catastrophic security breach of the year, involved enormous amounts of personal data stolen, compounded by delays in reporting the events and allegations of executive misconduct before and after the hacks— allareas GDPR also seeks to protect and regulate. Hypothetically applying GDPR principles and penalties to this incident, if Equifax has an annual (estimated) revenue of $3.1 billion, by our math, Equifax would be facing a fine of $124 million. Talk about a pricey penalty!

GDPR IS NOT TO BE TAKEN LIGHTLY.
Penalties for non-compliance can be a maximum of 20 million Euro or 4% of global revenues, whichever is higher.

While GDPR's financial penalties can be staggering and enough to put

some companies out of business, there are other ramifications not to be overlooked, such as the loss of consumer trust and damage to brand reputation. Studies have surfaced alarming statistics:

57% of Europeans do not trust brands to use their data resposibly [2] and 89% of Americans avoid companies who do not protect their privacy.[3]

GDPR addresses a growing need to protect consumer privacy and regulate cybersecurity measures amidst an increasingly data-driven world. It's legislation we need to take seriously and could be just the beginning of more regulations tto come.

YOUR OPTIONS

May 25, 2018, is looming; you are at the proverbial fork in the road with regards to compliance. Assuming you have EU records in your database, you have two options:

1. Remove all EU records from your systems, discontinuing sales and marketing communications to European residents

OR

2. Move forward with GDPR compliance efforts. Time is of the essence and expert guidance is highly recommended. To assist with your preparations, we've included a GDPR compliance checklist in the next section.

GDPR COMPLIANCE PREPARATION CHECKLIST

This checklist is designed to help your organization meet the obligations of GDPR compliance; it is not intended to replace legal counsel. Depending on your company's level of operations, you may need additional preparation. For expert guidance, Perkuto's team of Marketo Certified Solutions Architects is available to evaluate your systems, implement GDPR modifications, and provide training for your organization.

PHASE 1: GDPR Readiness Assessment

AUDIT YOUR DATABASE: ARE EU RECORDS PRESENT?	COMPLETED
Examine current opt-in sources to determine compliance (or determine if an opt-in campaign before the GDPR deadline is necessary)	☐
Evaluate information stored in the lead/contact objects vs. the account object and amount of information populated	☐
Determine the degree of missing country information and if it's normalized	☐
Create marketable records segmentation and inactive smart lists to assess data quality	☐
Determine the age of records; flag those outside of your defined period for record retention (no more than 3 years from last lead engagement)	☐
Segment the database based on current compliance status of records	☐
Determine if your database contains records of youth under the age of 16 and age 13 in the UK	☐

AUDIT YOUR DATA COLLECTION ENTRY POINTS/FORMS	COMPLETED
Assess current subscription center to ensure all necessary data points are collected for proper record keeping	☐
Review all data collection entry points and forms to ensure they align with GDPR	☐
Review current privacy policies, data collection and usage policy, data breach notification policy, and related documentation for gaps	☐
Review cookie tracking. Is it being used? Is it compliant?	☐

EVALUATE SYSTEM INFRASTRUCTURE	COMPLETED
Analyze third party tools or services for GDPR processor compliance and changes needed due to GDPR workflows	☐
Review how data management programs and sales workflows for downstream effects from GDPR	☐
Review Marketo security settings, roles, and permissions	☐
Review data consent center to track data opt-in information, if any	☐
Review campaigns to manage GDPR rights, if any	☐
Review data breach notification processes	☐

PHASE 2: Implementing Compliance Measures

FRONT END/CUSTOMER-FACING ADJUSTMENTS	COMPLETED
GDPR compliant subscription management in place: includes data forms, landing pages, email opt-out language, subscription management pages, privacy policy	☐
Enable withdrawal of data consent option	☐
If processing data on children, age verification systems ("age-gating") and parental consent collection forms are in place	☐
Opt-in mechanism to be cookied on the website in place	☐

BACK-END/OPERATIONAL ADJUSTMENTS	COMPLETED
Database has been appropriately segmented, outdated data removed, country normalized, data backfilled as needed, data points migrated from person to account records as needed	☐
Subscription center has been updated to comply with GDPR and captures appropriate information for complete record keeping	☐
Opt-in/whitelist campaign completed (before GDPR going into effect)	☐
Underage (children) data without parental consent has been removed	☐
Compliant data consent center created to track data opt-in information	☐
Right for removal/erasure programs enabled and working	☐
Right to transport data program enabled and working	☐
User notification alerts enabled and working: right to be informed	☐
User notification alerts enabled and working: data breach notifications	☐

PHASE 3: Compliance Documentation and Systems Test Run

INTERNAL STRUCTURE AND DOCUMENTATION	COMPLETED
Update your privacy policy	☐
Update your website Terms & Conditions	☐
Create (or update) your data processing record-keeping plan	☐
Create (or update) your security breach action plan/incident response plan	☐
Create (or update) your Data Protection Impact Assessment process	☐
Document your team structure, including who has access to your database and at what level, who designs your data collection forms, etc.	☐
Hire or assign a DPO	☐
Identify regularly used contractors and implement data privacy and security documentation into contracts. Document proof of data processor compliance.	☐

TEST YOUR SYSTEMS	COMPLETED
Test all new programs: subscription center, cookie functionality, data consent center and campaigns to manage GDPR rights	☐
Practice a data breach scenario and your team's ability to isolate and report the incident within 72 hours	☐

Meeting the obligations of GDPR compliance is a complex process. Further, the penalties for non-compliance are significant. Hiring a team of experts to assist with your GDPR preparations is smart business and a sound return on your investment. Or as the British would say, be careful not to be "penny wise, pound (Euro) foolish."

SUMMARY

GDPR is coming, whether we're ready or not. New, permission-based requirements for data collection and strict, transparency-focused data processing and handling stipulations are intended to protect the privacy of EU residents. For organizations that are marketing to Europeans, GDPR brings operational challenges to meet the May 2018 compliance deadline. Penalties for violators are severe—GDPR is not to be taken lightly. However, once all systems and updated processes are in place, we may begin to appreciate the intentions of GDPR and become better marketers as a result.

ABOUT PERKUTO

Perkuto helps marketing leaders who feel frustrated with not having a bigger impact on revenue. As a Marketo Platinum Partner, our team of experienced consultants create impactful strategies, optimize marketing operations, simplify MarTech and execute on day-to-day campaigns. We assist marketing leaders in exceeding their goals and rising to the top.

Visit perkuto.com to learn more.

1. Oliver Wyman, a Marsch & McLennan Company, Research Data, June 2017
2. The Chartered Institute of Marketing, September 2016
3. TRUSTe/National Cyber Security Alliance, US Consumer Privacy Index 2016

PERKUTO

Headquarters

5455, Avenue de Gaspé, Suite 330
Montreal, Quebec, Canada, H2T 3B3

1-844-PERKUTO

success@perkuto.com • perkuto.com