GDPR
Frequently Asked Questions

What Is GDPR?

The General Data Protection Regulation (GDPR) is new data protection legislation that replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

Why Was GDPR Needed?

GDPR was created to replace the outdated Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across the EU, to protect and empower all EU citizens' data privacy, and to reshape the way organizations across the region approach data privacy.

When Did GDPR Go Into Effect?

GDPR was in effect as of May 25th, 2018 and impacts all marketers doing business in the EU or with EU citizens independent of residency. Non-compliant organizations will face fines of up to 4% of gross global revenues or $20 million Euros, whichever is higher.

How Does This Compare to US Data Privacy Laws?

The United States does not have an overarching federal data privacy law. There are federal laws that provide some minimal data privacy protection for certain industries (HIPAA, FCRA, FTCA, COPPA, etc.) but otherwise data privacy is based on inconsistent state laws. While the new GDPR law requires more of marketers, it also provides the benefit of uniformity of data protection laws and empowers consumers.

What Rights Will Data Subjects Have Under GDPR?

At the heart of the newly defined data subject rights is control. The key areas they will now legally control are:

- **Conditions of Consent**: Under GDPR, a request for consent must be clear and approving consent must be actively given by the individual. There are more stringent parental consent rights for the processing of data for those under 16 years of age.
- **Right to Object**: When a decision is based on an automated processing, such as an inclusion to direct marketing communications, individuals have the right to be excluded and can opt-out at any point.
- **Right to Access**: Individuals have the Right to Access their personal data free of charge and be provided that data within a month of request date. This is limited to personal data they supplied.
- **Right to Rectification**: Individuals have the right to request that inaccuracies in their personal data be corrected.
- **Right to Portability**: Individuals can request a portable copy of their data for their own use, or for transfer to another party. This must be in a usable format.
- **Right to Erasure**: Requires permanently removing all identifiable traces of personal data at the individual's request. Some permanently anonymized data can be kept for historical analytics purposes.

Is GDPR Based on Citizenship or Residency?

GDPR protects both EU Citizens and EU Residents. Previous EU legislation focused just on the residency of the customer but with GDPR, the legislation is now expanded to include residency or EU citizenship. If a marketer has customers who are EU citizens and the marketer controls or processes customer data as part of a sale of goods or services, communication, etc., whether the marketer is physically in Europe or elsewhere, GDPR regulations apply. It is important to note that the legislation is somewhat inconsistent in its terminology on this area leading to some confusion but nearly all industry and legal experts we have spoken to support this interpretation. Coupled with the recent Equifax and Uber data breaches, and the 2017 US Executive Orders reducing data privacy rights, specifically those of non-US citizens, we fully expect the EU to enforce this law in a way that best protects their citizens.

Does This Affect EU Citizens Outside of the EU?

Yes. For a marketer wanting to distinguish between an EU citizen's foreign and domestic behavior, this may be technologically possible for those collecting citizenship or residency data, but the investment and the risk associated with it is hard to justify. Changes to residency, dual nationality, transactions during international travel, etc. all pose challenging data points to collect. It is important to note that the legislation is somewhat inconsistent in its terminology on this area leading to some confusion but all industry and legal experts we have spoken to support this interpretation. Coupled with the major breaches like those at Equifax and Uber, and the 2017 US Executive Orders reducing data privacy rights, specifically those of non-US citizens, we fully expect the EU to enforce this law in a way that best protects their citizens.

Does This Affect Non-EU Citizens Outside of the EU?

No. While the EU considers data privacy to be a basic human right, extra-territoriality aspects of GDPR do not address non-citizens EU outside of the EU. However, distinguishing citizenship and residency, which can change, is a challenging undertaking with no direct economic benefit so we strongly encourage our clients to treat all of their customers as if they were protected under GDPR.

Can I Use IP Address or Other GeoData to Determine if They Are Subject to GDPR?

No, this would not comprehensively identify all data subjects covered by GDPR, only the ones that took a specific action while associated with an EU IP address or some other location based identifier. Amongst other factors, this would not accurately identify those using VPN networks, traveling, changing residency, etc.

How Is Personal Data Different from PII?

Personal Data includes all PII data but goes far beyond that concept. Marketers need to be thinking in terms of Personal Data going forward, not PII. Persona data includes, but is not limited to, identifiers such as a name, email address, phone number, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data also differs because it not only includes directly identifiable things like email address, but also the concept of indirectly identifiable data points. Consider the example of age. By itself age cannot be used to identify an individual out of a large group. However, in combination with gender, zip code, and birth month, etc. someone could reasonably identify an individual. This indirect concept is why the EU has not published a list of personal data points and why they will not do so in the future. There are also categories of special data that are afforded extra protection as they can easily be used to discriminate.

What Does “Special Data Types” Mean?

Special data types are categories of sensitive personal data such as racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status, and sexual orientation. Processing of these types of data is allowed only under specific conditions so as to protect data subjects from potential discrimination.

Does GDPR Require My Organization to Have a Data Retention Policy?

Yes, a data retention policy is required. This should incorporate key GDPR concepts including data minimization defining business rules to execute Erasure, after a period of inactivity without the data subject requesting the Right to Erasure.

If I Don't Have Personal Data in My CRM Platforms Will That Reduce the Risk of Violating GDPR?

No, in fact it may increase your risk of violating GDPR and other laws like CAN-SPAM and CASL. GDPR is designed to help marketers understand their responsibilities, not keep them from functioning. For example, maintaining personal data in a safe environment is necessary to safeguard against accidental deployments to opt-outs. Creating a scenario where information is not used to create meaningful, relevant communications that effectively "listen" to what the data subject wants and acts accordingly is contrary to the intent of GDPR and the upcoming ePrivacy Directive

Can I Still Have Pre-checked Opt-in Consent for My Marketing Programs?

No. This is specifically called out in GDPR as no longer permissible.

How Will Agreements Need to Change Before May 25th, 2018?

The United States does not have an overarching federal data privacy law. There are federal laws that provide some minimal data privacy protection for certain industries (HIPAA, FCRA, FTCA, COPPA, etc.) but otherwise data privacy is based on inconsistent state laws. While the new GDPR law requires more of marketers, it also provides the benefit of uniformity of data protection laws and empowers consumers.

Do I Need to Review All My Technology Platforms and Evaluate Them for Unnecessary Exposure of Personal Data?

We strongly recommend this. Unnecessary exposure of personal data creates unnecessary risk and is clearly defined within GDPR's concept of Privacy by Design.

Do I Need to Review Who Has Access to What Data?

We strongly recommend this. Unnecessary access creates unnecessary risk.

How Are Controller and Processor Roles Different?

In most cases the brand or marketing organization is the Controller as it is the organization the data subjects are interacting with, buying from, etc. The definition of a Controller under GDPR is "The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". The definition of a Processor under GDPR is "The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

What Data Can Data Subjects Access Based on Their Rights of Access, Rectification, & Portability?

This topic was specifically addressed by the EU following the release of the GDPR regulation and it was clarified that the personal data that must be provided to meet the requirements of Access, Rectification, and Portability are limited to the data provided by the data subject.

What Does Erasure Mean in the Context of GDPR?

Erasure means the permanent deletion of Personal Data that can be used to identify the individual data subject. However, it does not require the deletion of all data associated with the individual as long as it can be permanently anonymized and is kept for historical research purposes only.

What Does Profiling Mean Under GDPR?

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

What Does Processing Mean Under GDPR?

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Do I Need to Hire or Appoint a DPO?

If you are processing large volume of data then you need to appoint a Data Protection Officer (DPO). For those not processing large volumes of data other requirements may still require you to appoint a DPO. However, we consider all of our marketers using our email and database platforms to be Controllers of large volumes of data.

Can a Controller Delegate Their Obligations to a Processor?

No. This is specifically forbidden within the legislation.

What Happens if We Do Not Have Everything in Place by May 25th, 2018?

While there is some industry discussion of showing meaningful progress towards compliance being acceptable, there is nothing in GDPR saying this will protect a Controller from prosecution so we strongly recommend being fully compliant by May 25th, 2018. The legislation calls for fines of up to 4% of gross global revenues or $20 million Euros, whichever is higher. In some cases, Processors may decline to provide continuing services to Controllers that are in violation of GDPR.

When Did GDPR Go Into Effect?

GDPR went into effect on May 25th, 2018 and impacts all marketers doing business in the EU or with EU citizens independent of residency. Non-compliant organizations will face fines of up to 4% of gross global revenues or $20 million Euros, whichever is higher.

What Is Your Advice for Marketers on Addressing GDPR?

Marketers should evaluate all their programs, policies, vendor contracts, and data management practices. Any necessary changes should be made prior to May 2018. Here are a few items that all marketers should address at a minimum:

- Any terms, conditions, and data usage language that are part of your subscription process should be made clear. To do so, audit all sign-in programs, preferences centers, and unsubscribe processes.
- Do not use pre-checked boxes (Affirmative Consent) and enable easily opt-out (Right to Object), data access (Right to Access), and correction of any inaccuracies in their personal data (Right to Rectification).
- Update consent language terms to ensure the use of profiling activities for marketing purposes is clear. Implement processes that provide the ability to halt automated profiling of personal data. Review and update T&Cs, and privacy notices to make sure they are transparent, concise, written in plain language and easily accessible.
- Regarding the individual's Right to Portability, Erasure, Access, Objection, and Rectification consider creating a request tracking mechanism with defined relevant data fields, request rejection rules, and transfer or erasure security rules in order to efficiently fulfill requests.
- Update all contractual agreements between Controllers, Processors, and Sub-Processors, with clearly defined processing instructions in all cases where personal data is involved. This should also include direction on data retention.
- Evaluate, document, and keep records of all processing activities along with consent and objections. This applies to marketers (controllers) and vendors (processors).
- Consider large scale data cleansing prior to May 2018 to comply with retention for old and unused data.
- Review and update your protocols for data breach management, notifications, and escalation. Accounting for the 72 hour timeframe to notify controlling authorities.
- Hire or appoint a DPO who has access to senior management to manage process change, compliance, and education. Provide DPO's information to all processors.
- Privacy Impact Assessments are mandatory when there is automated processing of personal data. If this applies to you, establish processes to conduct them.
- Implement Privacy by Design in development of products, systems, and processes.