EMAIL MARKETING COMPLIANCE — European Union (EU)

Laws/Regulations:

- GDPR (General Data Protection Regulation)
- ePrivacy Regulation
- Privacy Shield

Austria	Germany	Netherlands
Belgium	Greece	Poland
Croatia	Hungary	Portugal
Cyprus	Ireland	Romania
Czech Republic	Italy	Slovak Republic
Denmark	Latvia	Spain
Estonia	Lithuania	Sweden
Finland	Luxembourg	
France	Malta	

Consent Requirements: Please review the country-specific data privacy laws and resources provided by the EU member countries and the General Data Protection Regulation (GDPR) before engaging in email marketing. Certain EU member countries might have more restrictive laws than the GDPR, and you must follow the more restrictive requirements. This overview provides information on the GDPR.

This guidance is intended to provide an overview of the subject matter but is not meant to replace legal advice for your own activities, please ensure you are receiving legal guidance before you undertake a marketing campaign in any of these countries.

- **Information You Hold:**
  - You should document what personal data (data that directly or indirectly reveal a person's identity) you are in possession of, where it came from and who you share it with. You may need to organize a full information audit, across the entire organization, or within a particular business area.
  - The GDPR provides rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organization, you will have to tell the other organization about the inaccuracy so it can correct its own records. You wouldn't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this and keep it up to date. Doing this will also help you to comply with the GDPR's

Please review your email program with your legal counsel to ensure that your program is meeting appropriate legal requirements.

accountability principle, which requires organizations to be able to show how they comply with the data protection principles.

- **Type of Consent:**
    - In general, EU member countries require opt-in for data processing.
    - It is important to note that in Germany double opt-in is recommended for permissioning.
    - You need to document how you are seeking, obtaining, and recording consent. Consent has to be a positive indication of agreement to personal data being processed – it cannot be inferred from silence, pre-ticked boxes or inactivity. If you rely on individuals' consent to process their data, make sure it will meet the standards required by the GDPR (i.e., consent, performance of a contract, a legitimate interest, a vital interest, a legal requirement, and a public interest). If not, alter your consent mechanisms or find an alternative to consent. Note that consent has to be verifiable and that individuals generally have stronger rights where you rely on consent to process their data.
    - The GDPR is clear that controllers must be able to demonstrate that consent was given. You should therefore review the systems you have for recording consent to ensure you have an effective audit trail (i.e., IP, date, time, and time zone).

- **Create a Compliant Unsubscribe Process**
    - You need to process the opt-out request in a timely manner, as soon as possible.

- **Individual's Rights**

  You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

  The main rights for individuals under the GDPR:

  - access data,
  - have inaccuracies corrected,
  - have information erased,
  - prevent direct marketing,
  - prevent automated decision-making and profiling, and
  - have the option and ability to data portability.

- **Legal Basis for Processing Personal Data**

Please review your email program with your legal counsel to ensure that your program is meeting appropriate legal requirements.

Look at the various types of data processing you carry out, identify your legal basis (i.e., consent, performance of a contract, a legitimate interest, a vital interest, a legal requirement, and a public interest) for carrying it out and document it. You need to explain your legal basis for processing personal data in your privacy notice and when you answer a subject access request.

- **Communicating Privacy Information:**
    - Under the GDPR, you will need to explain your legal basis for processing the data, your data retention periods and that individuals have a right to contact the Information Commissioner's Office (ICO), or whichever Data Protection Authority (DPA) you fall under, if they believe their data privacy complaint was not resolved directly by your company. Note that the GDPR requires your privacy notice be concise, easy to read and understand.

- **Children's Data**
    - You should have systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.
    - GDPR brings in special protection for children's personal data, particularly in the context of commercial Internet services such as social networking. In short, if your organization collects information about children – age requirements can vary by Country – then you will need a parent or guardian's consent in order to process their personal data lawfully. This could have significant implications if your organization aims services at children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

- **Data Breaches**
    - You should have the right procedures in place to detect, announce, and investigate a personal data breach. This could involve assessing the types of data you hold and documenting which ones would fall within the notification requirement if there was a breach. In some cases, you will have to notify the individuals whose data has been subject to the breach directly, for example where the breach might leave them open to financial loss. Larger organizations will need to develop policies and procedures for managing data breaches – whether at a central or local level. Note that a failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Please review your email program with your legal counsel to ensure that your program is meeting appropriate legal requirements.

- Not all breaches will have to be notified to the Information Commissioner's Office (ICO) – only ones where the individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach.

- **Data Protection by Design and Data Protection Impact Assessments**
  - It has always been good practice to adopt a privacy by design approach and to carry out a privacy impact assessment (PIA) or data protection impact assessment (DPIA) as part of this. A privacy by design and data minimization approach has always been an implicit requirement of the data protection principles. However, the GDPR makes this an express legal requirement.
  - Note that you do not always have to carry out a PIA – a PIA is required in high-risk situations, for example where a new technology is being deployed or where a profiling operation is likely to significantly affect individuals. Note that where a PIA (or DPIA as the GDPR terms it) indicates high risk data processing, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

- **Data Protection Officers**
  - You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organization's structure and governance arrangements.
  - The GDPR requires some organizations to designate a Data Protection Officer (DPO), for example public authorities or ones whose activities involve the regular and systematic monitoring of data subjects on a large scale. The important thing is to make sure that someone in your organization, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support, and authority to do so effectively.

- **<u>International Considerations</u>**
  - If your organization operates internationally, you should determine which data protection supervisory authority you come under.
  - The GDPR contains quite complex arrangements for working out which data protection supervisory authority takes the lead when investigating a complaint with an international aspect, for example where a data processing operation affects people in a number of Member States. Put simply, the lead authority is determined according to where your organization has its main administration or where decisions about data processing are made. In a traditional headquarters (branches model), this is easy to determine. It is more difficult for complex, multi-site companies where decisions about different processing activities are

Please review your email program with your legal counsel to ensure that your program is meeting appropriate legal requirements.

taken in different places. In case of uncertainty over which supervisory authority is the lead for your organization, it would be helpful for you to map out where your organization makes its most significant decisions about data processing. This will help to determine your 'main establishment' and therefore your lead supervisory authority.

Enforcement:

- **EU Data Protection Authorities**
- Under the GDPR, potential fines can result in up to 20 million euros or 4% of the business's gross annual worldwide income.

Additional Resources:

- **ANA: What U.S. Marketers Need to Know about the GDPR**

Last updated: November 2021

Please review your email program with your legal counsel to ensure that your program is meeting appropriate legal requirements.