DATAGRAIL®

CHEAT SHEET

Data Privacy and GDPR Synopsis, and Business Practices for Compliance

Does GDPR Apply to you?

GDPR applies to any entity that is established in the EU, processes data on persons of the EU of which you provide goods and services to, or monitors behavior of EU residents.

Classes of Entities: Processors and Controllers

The two classes defined by the law are controllers and processors:

Controllers determine the purposes and means of processing data, while a processor simply works with the data on behalf of the controller. Controllers primarily interface with data subjects and must be able to respond quickly to requests, by providing access or deletion with regard to personal data within 30 days.

Processors must then be capable of assisting the controller in deleting, manipulating, or sharing data of the subject. Identifying whether your business is a controller or processor, or both, is essential to coming in compliance with GDPR.

Action Items

- ✓ Automatically opt users out of mailing lists and subscriptions and allow them to unsubscribe
- ✓ Communicate with customers if you process their data
- ✓ Do not share or sell personal data without explicit consent from the data subject
- ✓ Prepare for and address subject access and deletion requests

Consent

Users from the EU must not be opted-in into marketing by default

Consent for processing cannot be required of a consumer to use a service. Marketing may be considered a legitimate interest in certain cases if a balancing test and analysis is performed.

Consent is required to be:

- Opt-out by default
- Explicit for uses of personal data
- Informative of all processors
- Concise and transparent

Privacy by Design

From Article 25: **“Data protection by design and by default”**

Controllers must minimize:

- Data collection: specific purpose required with legitimate interest or consent
- Accessibility and transfers of collected data
- Retention of collected data

Rights of Data Subjects

Data Subjects, or any users with personal data, have the right to:

- Delete their data
- Request all their personal data through a Subject Access Request (SAR)
- Withdraw consent at any time
- Correct their personal data

This document was created for informative purposes only. To understand how GDPR or any other law applies to your business, seek qualified legal counsel.