

What is **GDPR** and how can it impact you?

GDPR is the European General Data Protection Regulation which becomes enforceable on May 25, 2018.

In general, the Regulation provides for the protection of personal data, for individuals in one of 32 European countries.

Where is your potential exposure in the United States?

- Do you have **Prospects or Customers** that reside in one of the EU 32?
- Do you have **Website Visitors** that are entering from one of the EU 32?
- Do you have **Email Recipients** that are opening from one of the EU 32?
- Do you **Process or Handle Data** on individuals that are from one of the EU 32?

If you don't follow the GDPR rules, the penalties and fines are severe (up to 4% of gross revenue), and they are enforceable internationally.

As a valued data processor, **Direct Services Inc.** is well-informed on the GDPR Regulation and is prepared to work closely with your Management Team, IT Team, and Data Privacy Officer (DPO) to support your compliance.

Attached is our "GDPR Compact Guide" which we compiled from our review of the Regulation's 119 pages, 99 Articles and 173 Citations, to help facilitate our discussions with your team.

If you have any comments or questions, please do not hesitate to contact our offices.

Respectfully,

Brent J. Dreyer
VP of Emerging Technologies
bdreyer@directservices.com

DIRECTSERVICES

14505 COMMERCE WAY SUITE 550 MIAMI LAKES, FL 33016-1530

PHONE (954) 433 9810 FAX (954) 433 8950

DIRECTSERVICES.COM

GDPR COMPACT GUIDE

Copyright 2017 Direct Services Inc.
www.DirectServices.com
Brent J Dreyer

COMING MAY 25, 2018

WHAT IS GDPR ?

General Data Protection Regulations (GDPR) is a law that was adopted by the European Parliament in April 2016 and will become enforceable on May 25, 2018. The regulation applies to the collection, processing and movement of personal data for individuals residing in 32 European States. (28 EU States + 4 other European States)

WHAT IS YOUR EXPOSURE ?

- How many individuals (prospects and customers) are in your database, with data collected from the 32 States?
- What data do you collect or process that is identifiable to a person?

WHAT ARE YOUR OPTIONS ?

- If no exposure, implement ongoing process to monitor for future exposure.
- Stop collecting personal data on EU residents and destroy existing data.
- Identify all personal data being processed, modify notifications, processes, business practices, vendor contracts, security procedures and communications to accommodate GDPR requirements.

YOU WILL NEED TO DISCLOSE

1. Who is managing their data (contacts)
2. What you intend to do with their data
3. How you will protect their data
4. Why you need their data
5. How long will you store their data
6. What are their rights to their data
7. Who else will get their data

LAWFUL PROCESSING (PICK 1)

1. Explicit Consent for each purpose of use
2. Performance of a Contract
3. Legal Obligation
4. Vital Interest of Individual(s)
5. Public Interest - Official Authority
6. Legitimate Interests

INDIVIDUAL RIGHTS

- Rights of **Access** to their data
- Rights of **Rectification**, corrections
- Rights of **Erasure**, To Be Forgotten
- Rights of **Restriction** on processing
- Right to **Object** to processing
- Rights of **Portability**, I want my data
- Rights over algorithmic **Automated Decisions**, including **Profiling**

OVERSIGHT

- European Data Protection Board
- Supervisory Authority (Local and in EU)
- Representatives in EU
- Controllers
- Processors
- DPO - Data Protection Officer (corporate)
- Data Protection Impact Assessment (corporate)
- Certifications
- Codes of Conduct
- Binding Corporate Rules
- Model Clauses
- EU-US Privacy Shield

PERSONAL DATA

EXAMPLES

- Name
- ID Number(s)
- Home Address
- Phone Number
- Payment Information
- Website Login
- Username
- Password
- Email Address
- Website Session ID
- Geo Location
- Device and App. IDs
- IP Address
- Cookies
- RFI Tags

ONLINE IDENTIFIERS

WHO IS LIABLE ?

- Companies
- Employees
- Controllers
- Processors
- Representatives

THE EUROPEAN STATES

- Austria
- Belgium
- Bulgaria
- Croatia
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Rep. of Cyprus
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- United Kingdom

SENSITIVE PERSONAL DATA

Need **CONSENT** or other reason in Article 9 to process Sensitive Data, like these;

- Behavioral Characteristics (Profiling)
- Biometric Data
- Cultural Background
- Dactyloscopic Data (Fingerprints)
- Health Data
- Economic Data
- Facial Images
- Genetic Data
- Mental Data
- Philosophical Beliefs
- Physical Data
- Physiological Data
- Political Opinions
- Genetic Data
- Racial or Ethnic Origin
- Religious Beliefs
- Sex Life/Sexual Orientation
- Social Identity
- Trade Union Membership

RIGHTS, REMEDIES, PENALTIES

- Right to file a Complaint
- Right to Individual Compensation for Material and Non-Material Damages
- Warnings, Reprimands, Ban on Processing, Suspension of Data Flows
- Administrative fines up to the greater of 20 Million EU or 4% Gross Global Revenue

TRANSPARENCY

Transparency = Fair Processing = Disclosure of Data Use = Individual Trust

Transparency must occur **before** data is collected or processed, and **before** any changes to processing. Must be provided in a **Concise** and **Intelligible** manner.

1. Disclose purposes of all data processing, current and future
2. The grounds for legitimate interest if used as lawful method
3. The logic behind any automated decisions, including profiling
4. Disclose any third party processors and third party data appends
5. Data transfers outside of EEA
6. Expected data retention period
7. Disclose all individual rights
8. Disclose data safeguards
9. Make it easy to opt out