Understanding the GDPR

Simon Wynn, CIPP/US
Simon Wynn Consulting
www.simonwynn.com

SWC

What is the GDPR?

- The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU)
- Became effective on May, 28th 2018
- Penalties can be up to a maximum fine of €20 million, or four per cent of a company's annual revenue, whichever is greater

What is Personal Information?

From Article 4: *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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;*

Note: 'Personal Information', 'Personal Data', and 'PII' are interchangeable terms

‘Special Categories’ of Personal Information

Sensitive personal data is a specific set of “special categories” that must be treated with extra security. This includes information pertaining to:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where processed to uniquely identify someone)

I'm in the US, does the GDPR Apply to us?

If you are offering good or services to, or monitoring behaviour of, EU residents, the GDPR applies to you.

- It applies if you are 'established' in the EU
- It applies if you are not established in the EU, but are:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union

Examples:

1. You are located in London and you provide an HR SaaS application to global markets - the GDPR applies to you when processing EU user's personal information
2. You are located in San Francisco and provide a CRM SaaS application hosted at AWS us-east-1. Your application and website is translated into French German and Spanish, and you market globally. Your 'starter' tier can be purchased using a credit card in USD, GBP or Euros - the GDPR applies
3. You run a site providing junk removal services in California. You site is in English only and accepts credit cards charged in USD - the GDPR does not apply to you - your web site is clearly is not targeted at EU users

‘Controller’ or a ‘Processor’?

- Under the GDPR you are considered either a ‘Controller’ or a ‘Processor’, or sometimes both. Other privacy regulations have similar designations - for example the CCPA defines a ‘Service Provider’
- **Controller:** *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;*
- **Processor:** *Processor means a natural or legal person, public authority, agency or other body which processes personal data* ***on behalf*** *of the controller*

Controller and Processor Examples:

- A company provides a SaaS project management product. Its users sign up and accept T&Cs and a Privacy Policy. The company may further market to the users about similar products, or those of its partners. If you visit the company site, a tracking pixel is delivered allowing retargeting.
- The company is a **controller**
- It determines the **purpose and means** of processing

Controller and Processor Examples (cont'd):

- A company provides a SaaS log management product - it processes logs that may contain personal information, but does so only based on a binding contract with the Controller which states how it should process personal information, sub-processor restrictions, security requirements, etc. (typically described in a Data Processing Agreement)
- The company is a **processor**
- It does not determine the **purpose and means** of processing, however it does determine the **means** (i.e. it decides to use AWS) - determining just the *means* is fine

Example: Controller and a Processor

- A company can be both - take the previous SaaS log company:
  - Company is a *processor* of log data
  - Company allows admin users to sign up for accounts on its log analysis portal, and uses this information for additional purposes, for example marketing campaigns - for this reason it is also a *controller*

Controllers: Steps to Comply

- Determine if the GDPR applies to you (it probably does)
- Determine if you are established in the EU
- Draft a new Privacy Notice
- Draft a Cookie Policy and implement a cookie banner
- Decide how to manage international transfers of data
- Document key processes and procedures:
  - Data Protection Policy
  - Data Retention Policy
  - Data Processing Agreement (DPA) (if you are a processor)
  - Data Breach Response and Notification Procedure
  - Data Breach Register (aim to keep this blank...)
  - Data Subject Access Rights Procedure
  - Implement an information security program

Controllers: Steps to Comply (cont'd)

- Implement a vendor risk program for your processor and sub-processor vendors
  - At a minimum execute Data Processing Agreements with all of your vendors
- Optional steps:
  - HR documents for EU employees (if you have them)
  - Assigning a Data Privacy Officer and conducting a Data Protection Impact Assessment (a 'DPIA')
    - Only *"where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale".*
- Maintaining Records of Processing
    - *… does not apply to an enterprise or an organisation employing fewer than **250 persons** unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects*

Processors: How to Comply?

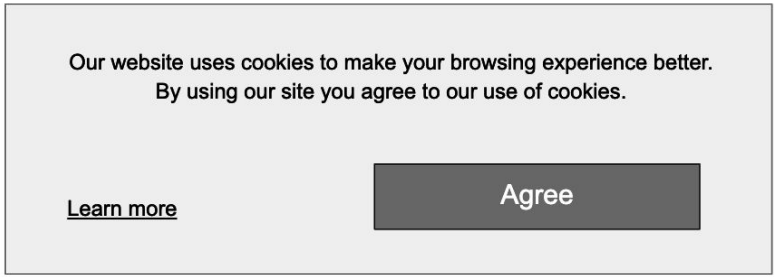
- Much simpler…
- Execute a Data Processing Agreement and follow its obligations:
  - Only processor data based on the controller's instructions
  - Obtain permission to engage sub-processors
  - Return all data at the end of the contract
  - Permit compliance audits
  - Implement an information security program, for example implementing encryption
  - Notify controllers of any data breaches without undue delay
  - Restrict transfers to third countries without adequate protections

Are you 'Established' in the EU?

- *Establishment* exists when there is a ***real and effective activity*** exercised through ***stable arrangements***
- Anything from a single EU employee to a registered subsidiary qualify as *establishment,* however, the EU personnel must be directly related to the business in Europe, for example, a salesperson or sales office would qualify. A remote software development team would not!
- Why is it good to be established:
  - Establishment means you don't need a obtain a local legal 'representative' and can benefit from the 'one-stop-shop', meaning you only need to work with one Data Protection Authority in the country you are established in; otherwise..
  - You need a designate a local legal representative, typically through a law firm specializing in this service to comply with Article 27 of the GDPR

What About Cookies?

- Regulations regarding cookies are not part of the GDPR - they are part of country-specific implementations of the *ePrivacy Directive*
- An example of a country-specific regulation is the UK *Privacy and Electronic Communications Regulation (PECR)*
- To be 100% compliant, you should give users the choice of disabling all non-essential and third-party cookies **before** they are stored in the user's browser
- The *Informational Cookie Notice* is generally adequate though:



Data Subject Access Rights

- GDPR give users ‘Access Rights’ as follows:
  - Right of access. The right to obtain access to your personal data.
  - Right to rectification. The right to correct your personal data
  - Right to erasure. The right ‘to be forgotten’
  - Right to restriction. The right to obtain the restriction of the processing
  - Right to portability. The right to portability allows you to move, copy or transfer personal data easily from one organization to another.
  - Right to object. You have a right to object to processing based on legitimate interests and direct marketing.
  - Right to object to automated decision making, including profiling

Data Subject Access Rights (cont'd)

- Critically important a Data Subject Access Rights Procedure (DSAR procedure) is developed and communicated with the organization
- Requests typically handled by the Customer Success team
- Strict timescales to respond
- CCPA and other emerging privacy regulation all have similar provisions

International Transfers

- The GDPR permits transfers to countries outside of the EU who have an *adequate level of data protection,* as determined by the European Commision:
  - Andorra
  - Argentina
  - Canada (commercial organisations)
  - Faroe Islands
  - Guernsey
  - Israel
  - Isle of Man
  - Japan
  - Jersey
  - New Zealand
  - Switzerland
  - Uruguay
- Note that the US is missing!

International Transfers (cont'd)

- Options for legal transfer of EU personal information to the US:
  - *Consent* - Add language in your privacy policy telling users they consent to transfers
  - Avoid this! Complexity of providing and withdrawing consent means this is not a good option
- Binding Corporate Rules (BCRs)
  - A custom agreement typically implemented by a multi-national - must be approved by EU regulators - don't go this route unless you are Facebook!
- Model Clause Contract (MCCs)
  - Standard contractual clauses drafted by the European Commision - they cannot be changed (typically)
  - Cumbersome if you have a large number of EU users, for example a B2C product

International Transfers (cont'd)

- The US Privacy Shield Framework
  - *Designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.*
- Decide if you want EU-US, Swiss-US Privacy Shield, and if you want to cover HR data
- Update your Privacy Notice
- Pick an independent recourse mechanism (an arbitrator)
- Agree to the Privacy Shield Principles
- Pay the fees
- Renew each year

Digital Marketing

- All EU countries (an most other countries except the US) require consent **prior** to sending marketing emails to consumers (B2C)
- Many EU countries require consent when sending marketing emails to business users (B2B)
    - An exception would be the UK
- Exceptions:
    - *The email address was collected during the sale of goods or services, and;*
    - *The marketing communications must be about similar goods or services to those purchased or enquired about;*
    - ***Most importantly, someone must be given an opportunity to object to electronic marketing, each time they are sent a marketing message, as well as at the time the data was collected.***
- Each country has its own regulations based on the ePrivacy Directive (not the GDPR)

Issues Ahead...

- The European Court of Justice (ECJ) may invalidate the US Privacy SHield and the Model Clause Contracts
  - Various legal challenges including ‘Schrems’ are challenging existing frameworks
  - Issues center around US Government surveillance laws
- Brexit
  - A no-deal Brexit leaves the UK as a ‘third-country’ without any frameworks for international transfers in place
  - Complex issue for US companies with establishment in the UK

Other Privacy Regulations

- The California Consumer Privacy Act (CCPA):
  - Went into effect on 1/1/2020
  - A business (a for profit business…) is subject to the CCPA if:
    - The business must generate annual gross revenue in excess of $25 million;
    - The business must receive or share personal information of more than 50,000 California residents annually; or
    - The business must derive at least 50 percent of its annual revenue by **selling** the personal information of California residents.
- Many other states and countries are planning similar regulations
  - Most are ‘GDPR like’
- Regulations at the Federal level may happen at some point

Useful Resources

- International Association of Privacy Professionals (IAPP)
  - https://iapp.org
- Certikit
  - Compliance toolkits, including the GDPR
  - https://certikit.com
  - **Use our discount code: AF10SWC**
- OneTrust Data Guidance
  - Privacy compliance guidance
  - https://www.dataguidance.com
  - Annual subscription
- The Data Protection Network
  - https://www.dpnetwork.org.uk
- The UK Information Commissioner's Office (the “ICO”)
  - https://ico.org.uk

Thank You!