**NCPA's 39th ANNUAL MEETING & SEMINAR**
**April 11, 2019 – April 13, 2019**

# Data Protection & Privacy


## Kristen G. Lingo
## Asst. General Counsel
## FHI 360

April
2019

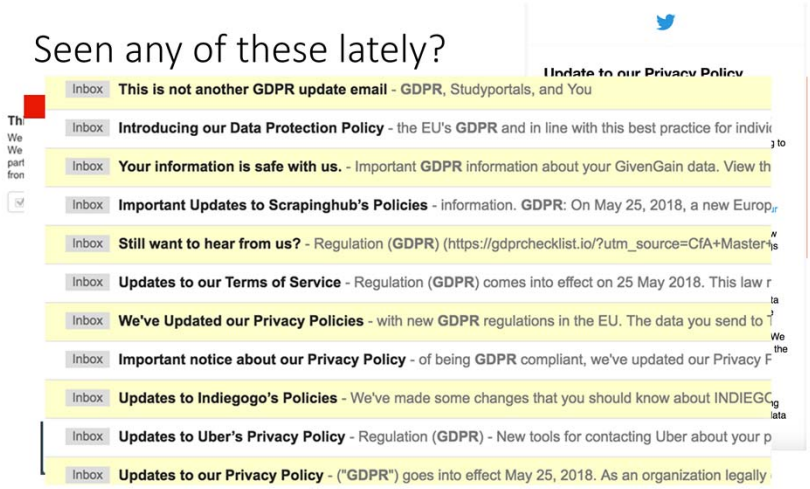
# The European Union's General Data Privacy Regulation

**Kristen Lingo**

*Assistant General Counsel*
*and Data Protection Officer*

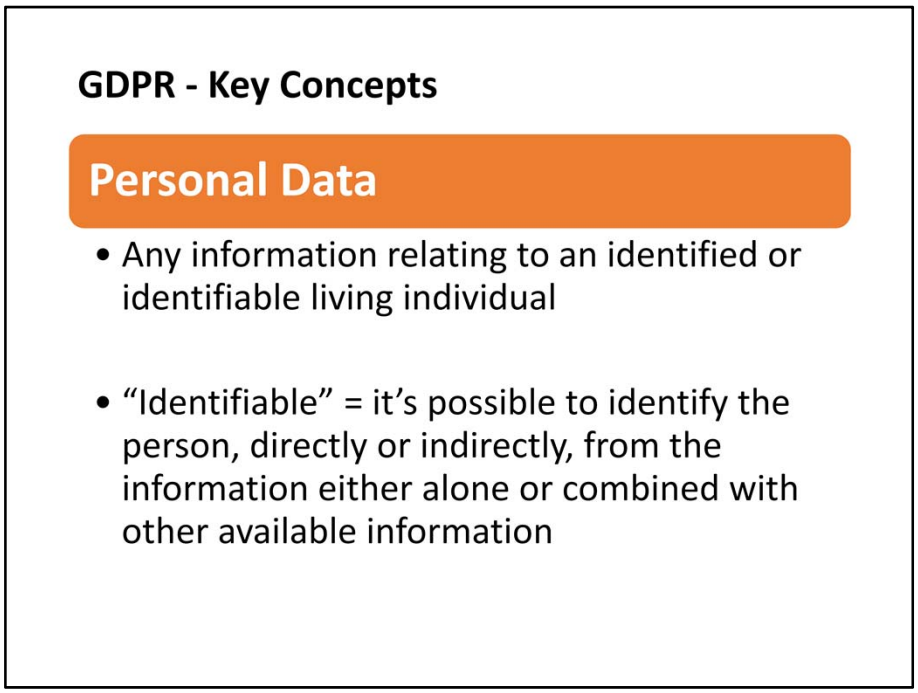
fhi360
THE SCIENCE OF IMPROVING LIVES

# Seen any of these lately?



## General Data Protection Regulation (GDPR)

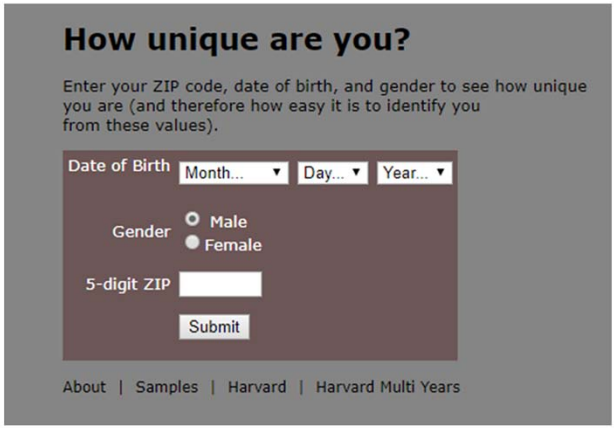
- European Union (EU) law, effective May 2018
- Limits how companies can collect and use personal data
- Gives individuals more control over how their personal data is used
- "[B]iggest change in data protection law for 20 years"



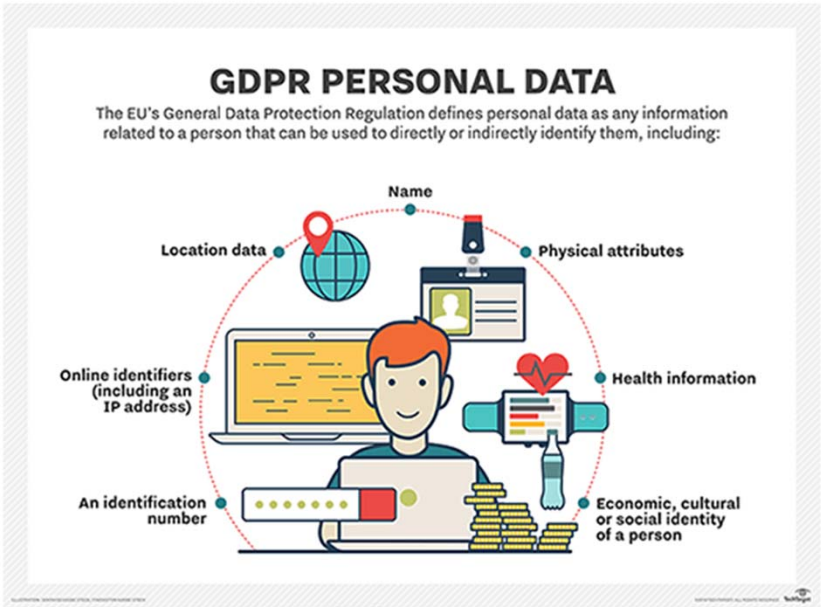

Identifiable – more than a theoretical possibility; there has to be a reasonable likelihood that info can be used to single out an individual

## GDPR – Key Concepts

https://aboutmyinfo.org/




10429 in my zip code
72 born in my birth year
1 born on my birthday


GDPR PERSONAL DATA
The EU's General Data Protection Regulation defines personal data as any information related to a person that can be used to directly or indirectly identify them, including:
Name
Location data
Physical attributes
Online identifiers (including an IP address)
Health information
An identification number
Economic, cultural or social identity of a person

## GDPR – Key Concepts

### Sensitive Personal Data (or Special Category Data)

- Personal data that reveals:
  - Racial or ethnic origin
  - Religious or philosophical beliefs
  - Political opinions
  - Trade union membership
- Genetic data
- Biometric data
- Health data
- Data relating to a person's sex life or sexual orientation

## GDPR – Key Concepts

### Processing

- Collecting, recording, organizing, structuring, storing, adapting, altering, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction of personal data
- Includes hardcopies when part of a “filing system”

**GDPR – Key Concepts**

## Data Controller

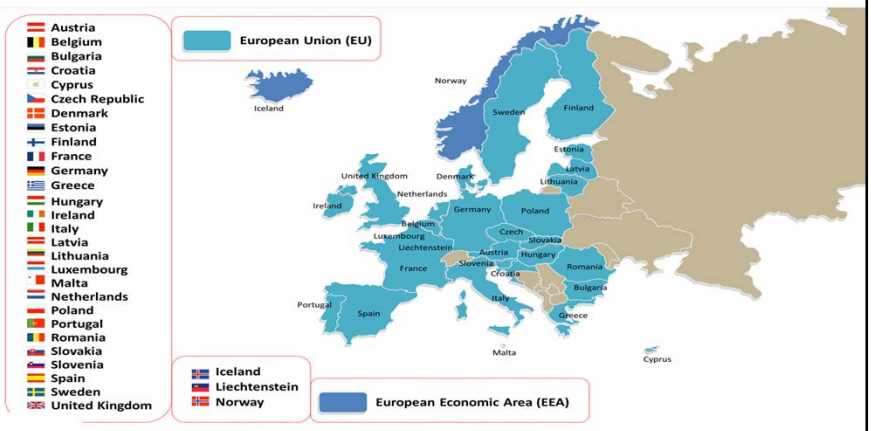
- Decides what personal data to process and the purpose and means of processing

## Data Processor

- Processes personal data on behalf of the data controller

# Where GDPR Applies

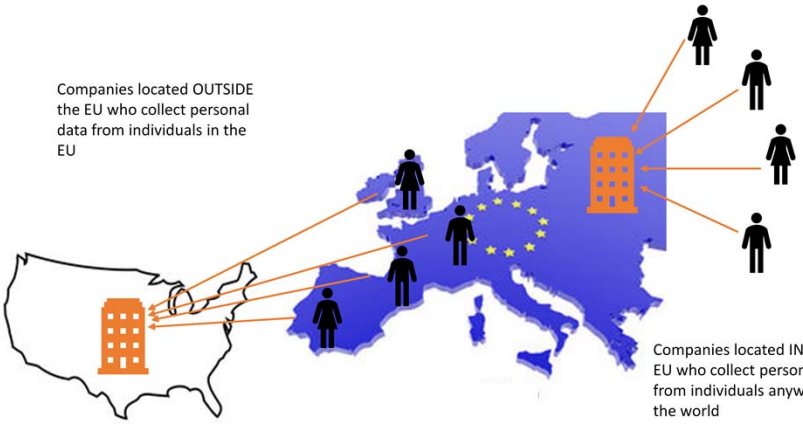
## 28 EU and as well as 3 EEA member states



**Europe?! Why should I care?! This is America!**

## GDPR applies to personal data collected in or collected from the European Union

Companies located OUTSIDE the EU who collect personal data from individuals in the EU

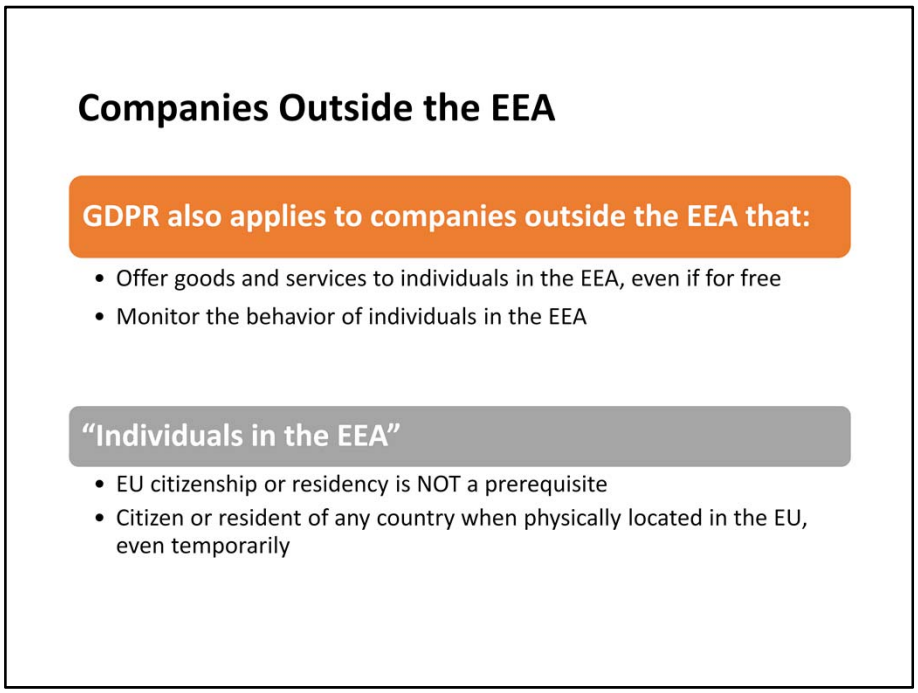


Companies located INSIDE the EU who collect personal data from individuals anywhere in the world

## Companies Inside the EEA

GDPR applies to "EEA-established" companies that process personal data from anyone anywhere in the world

- Not just where an entity is incorporated or registered to do business, or where it is headquartered
- Anywhere a company has "stable arrangements" through which it conducts "effective and real" business activities
  - Owned or leased premises
  - Employees or agents – even a single representative may be enough
  - Bank accounts




Examples

US company that has an online recruiting site and accepts applications from people in the EEA

OK, but we are only providing our service to US tourists whilst on vacation in the EU
This depends on whether there is targeting towards those individuals whilst in the EU or if the fact that they are within the EU is only incidental. If the key feature is to provide the service to individuals because they are within the EU, then GDPR will apply and the fact that they are only there temporarily is irrelevant.
But if the tourists just happen, say, to read a US news website whilst in the EU, that will not make that site subject to GDPR. This is in fact an example given by the EDPB and perhaps inspired to prevent some well publicised US news companies from geo-blocking EU visitors because of GDPR (see a BBC news story here).

## Companies Outside the EEA

### Offering goods and services to individuals in the EEA

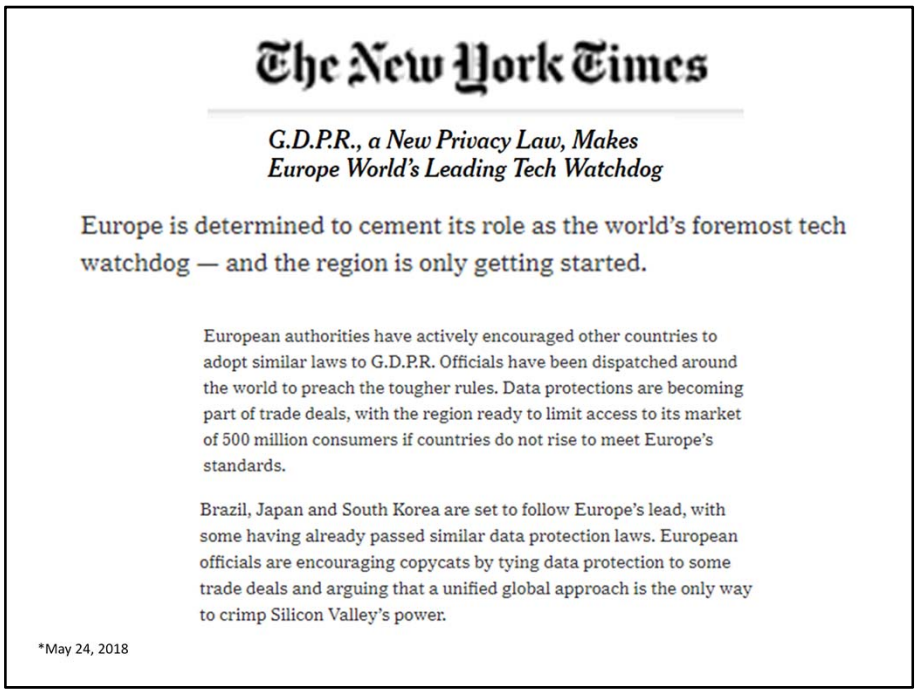
- The fact that your website is accessible to people in the EEA isn't enough
- Are you intentionally targeting people in the EEA? Do you:
  - Use the language of an EU country (that is different from that of your home country)?
  - Display prices in euros, British pounds, Swiss francs, or other currency of an EU member country?
  - Include the US country code in your phone number listing?
  - Use a non-US top level domain name, e.g., companyname.eu or .de?
  - Refer to your international clientele, including customers in EU member states?

### Monitoring the behavior of individuals that occurs in the EEA

- Tracking individuals online to create profiles and using them to analyze or predict their personal preferences, behaviors, and attitudes

**Another reason. . .**


Europe is determined to cement its role as the world's foremost tech watchdog — and the region is only getting started.



The New York Times

*G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*

Europe is determined to cement its role as the world's foremost tech watchdog — and the region is only getting started.

European authorities have actively encouraged other countries to adopt similar laws to G.D.P.R. Officials have been dispatched around the world to preach the tougher rules. Data protections are becoming part of trade deals, with the region ready to limit access to its market of 500 million consumers if countries do not rise to meet Europe's standards.

Brazil, Japan and South Korea are set to follow Europe's lead, with some having already passed similar data protection laws. European officials are encouraging copycats by tying data protection to some trade deals and arguing that a unified global approach is the only way to crimp Silicon Valley's power.

*May 24, 2018

"If we can export this to the world, I will be happy," said Vera Jourova, the European commissioner in charge of consumer protection and privacy who helped draft G.D.P.R. She said she planned to travel to Japan and South Korea in the next few weeks for talks about data protection. Regulating technology, she added, is a "global challenge." Europe's influence can be seen in Brazil, which has sought advice from Brussels on its own privacy legislation.

Other countries that either already have or are are considering new data privacy regimes that share elements with the GDPR – Chile , South Africa,Agentina, Isreal, New Zealand Nigeria

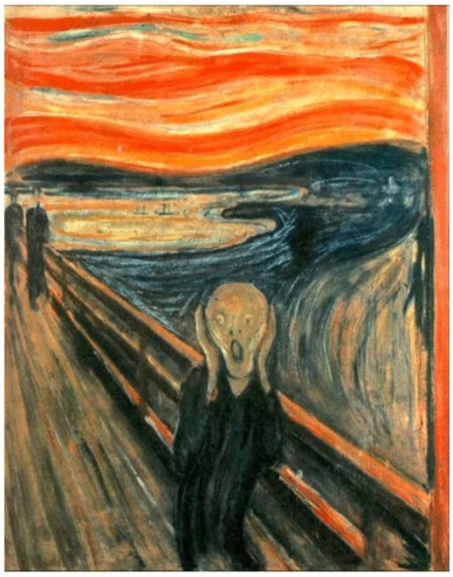
Kl what drives this is the restriction on transferring personal data outside the EEA. Ity is ILLEGAL. Can only do it if the EU has determined the country has privacy protections that adequately protect EU citizens (Privacy Shield)

## Coming to America. . .


**California Consumer Privacy Act follows in the GDPR's footsteps**

**While no one was looking, California passed its own GDPR**

The California Consumer Privacy Act of 2018 is similar to the EU's GDPR. Companies that hold data on more than 50,000 people and do business in California must comply.



# What's so different about GDPR?

## Different approaches

- Patchwork of federal sectoral laws addressing different types of personal data, such as:
  - HIPAA – health information
  - Gramm-Leach-Bliley – financial information
  - Family Educational Rights and Privacy Act – education information
  - Children's Online Privacy Protection Act – children's information
- And 48 state data breach notification laws

- Single omnibus law that covers <u>all</u> personal data

## Different underlying philosophies

- Harm-based
- Protect information to shield people from social, economic, or physical harm that could result from its misuse
  - Identity theft, loss of money, damage to credit
  - Threats and harassment
  - Embarrassment
  - Improper denial of government benefits
  - Blackmail
  - Discrimination

- Privacy-based
- Protect information to preserve people's fundamental right to privacy

## The biggest reason GDPR is different

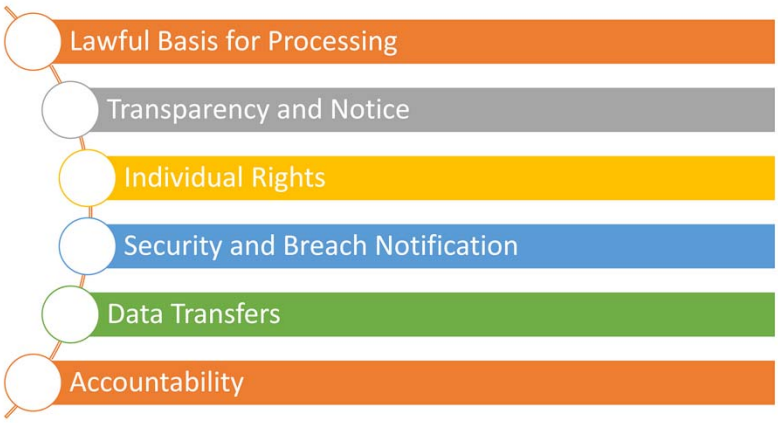
### Consequences of noncompliance

- Liability to data subjects for damages
- Investigations and audits by administrative agencies
- Administrative warnings, reprimands, and compliance orders
- Suspension or termination of data processing activities
- MAJOR administrative fines
  - Determined on a case-by-case basis as "effective, proportionate, and dissuasive"
  - **Up to € 20 million or 4% of annual global revenue, whichever is higher**

## GDPR Privacy Principles

| | |
|---|---|
| Lawfulness, fairness, and transparency | • Only process personal data for lawful reasons, with full disclosure of the purpose and use of the data and notice of the subject's rights |
| Purpose limitation | • Only process personal data for a specified, explicit, and legitimate purpose |
| Data minimization | • Only collect or use the personal data that is necessary to achieve the stated purpose |
| Accuracy | • Keep personal data accurate and up-to-date, and correct or delete inaccurate data promptly |
| Storage limitation | • Don't keep identifiable data any longer than absolutely necessary |
| Integrity and confidentiality | • Protect personal data against unauthorized use or accidental loss |
| Accountability | • Fully document data processing and be able to demonstrate GDPR compliance |

## GDPR Requirements



# Lawful Basis for Processing

It is illegal to process personal data unless one of the six lawful bases for processing applies

| Contract | Legal Obligation | Vital Interest | Public Interest | Legitimate Interest | Consent |
|---|---|---|---|---|---|
| • Processing is necessary to enter into or perform a contract with a data subject | • Processing is necessary for compliance with legal obligations under law applicable to the data subject | • Processing is necessary to protect the vital interests of the data subject | • Processing is necessary for performance of a task carried out in the public interest in the exercise of official authority | • Processing is necessary for the purposes of the legitimate interests of the data controller or a third party, unless outweighed by the interests or fundamental rights of the data subject | • The data subject has consented to processing. |

## Consent

Consent to processing of personal data must be:

- Freely given
- Specific
- Informed
- And unambiguous, as indicated by a clear affirmative action
  - Opt in, not opt out
  - Do NOT pre-check the box

Data subject must have the option to refuse or withdraw consent without adverse consequences

Consent must be as easy to withdraw as it was to grant

Avoid relying on consent alone where possible

## Transparency and Notice

Data subjects must, at the time their personal data is collected, be notified of:

- The name and contact information of the data controller
- The lawful basis for processing data
- The purpose for which the data will be processed
- Who will receive the data
- The data retention period
- The data subject's individual rights and how to exercise them

The notice must be given in clear, plain, easy to understand language.

The data cannot be processed for any other purpose unless provided with new notice specifying the new purpose and the lawful basis that applies

# Individual Rights

**Data subjects in the EEA have the following rights:**

| | |
|---|---|
| Withdrawal of consent | • Data subjects can withdraw consent to future processing at any time |
| Access | • Data subjects can access a copy of their personal data and obtain a copy on a commonly used electronic format |
| Portability | • Data subjects can have their personal data transferred to another processor in a common used machine readable format |
| Rectification | • Data subjects can require the controller to correct inaccuracies in personal data |
| Objections/Restriction | • Data subjects can object to or restrict processing of their personal data for certain purposes |
| Erasure, or "The Right to Be Forgotten" | • Data subjects can require the controller to erase their personal data |

## Security and Breach Notification

Data controllers must implement "appropriate technical and organizational measures" to protect personal data from unauthorized or unlawful processing or accidental loss, destruction, or damage

- Pseudonymization and encryption
- Disaster recovery processes
- Access control
- Firewalls
- Procedures for testing and evaluating security measures

In the event of a data breach, data controllers must:

- Notify the relevant data protection authority of any personal data breach within 72 hours were possible, or without undue delay
- Notify the data subject without undue delay if the breach is likely to result in a high risk to the rights and freedoms of individuals

## Accountability and Compliance

Data controllers must:

- Maintain records of all data processing activities and be prepared to demonstrate compliance with GDPR
- Have data privacy awareness and training programs
- Adopt the principle of privacy by design – conduct data privacy risk assessments, and ensure data privacy risks and data protection are taken into account from the early stages of designing new products and services
- Adopt the principle of privacy by default – setting up systems so that privacy is default option and sharing personal information is an affirmative choice
- Conduct regular audits of data privacy systems and processes to evaluate effectiveness
- Require data processing vendors to sign contracts obligating them to abide by the same requirements, only process personal data in accordance with written instructions, and assist data controller with data subject request.
- Appoint a data protection officer where required

## Processing Special Category Data

To process special category data, one of the following conditions must apply (in addition to having a lawful basis for processing):

- Processing is necessary to fulfill statutory or regulatory obligations of an employer
- Processing is necessary for the exercise or defense of legal claims
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for reasons of medical treatment or public health reasons
- Processing is necessary for scientific, historical, or statistical research purposes.
- Data subject has given explicit consent for the processing of sensitive personal data

## Steps To GDPR Compliance

| | |
|---|---|
| Inventory your data | • Find out what personal data you collect, where you store it, how you use it, who you share it with, how long you store it, etc. |
| Establish lawful basis for processing | • Once you know what personal data you have, ensure that you can articulate which of the six lawful bases for processing applies<br>• If relying on consent, make sure it's freely given, specific, informed, unambiguous, and affirmative |
| Send privacy notices | • Notify data subjects about the data you hold, the purposes of processing, data retention and destruction periods, their individual rights, and other required info |
| Develop data retention and record-keeping policies and systems | • Review your personal data and delete anything you no longer need; develop time frames for reviewing and deleting data |

## Steps to GDPR Compliance

| | |
|---|---|
| Develop a system for responding to data subject requests | • Determine who will handle such requests, make sure you have the technical ability to locate, provide, and delete data |
| Implement a data breach response plan | Train employees to report breaches, know what steps you'll take to contain and limit the damage, and plan how you'll notify data subjects and supervisory authorities |
| Implement system for vetting and contracting with data processors | • Ensure that they handle personal data appropriately and revise templates to include data processing language |
| Develop training and awareness program for employees | • Educate employees about data protection obligations and build a culture of privacy |

## Data Protection Resources

- DLA Piper: A Guide to the General Data Protection Regulation
- Top Ten Operational Responses to GDPR
- Supplemental Guide to GDPR for HR Professionals
- A Practical Guide to the GDPR
- GDPR: A Primer for US-Based Organizations
- Getting Ready for the GDPR
- GDPR Checklist
- UK Information Commissioner's Office Guide to the GDPR