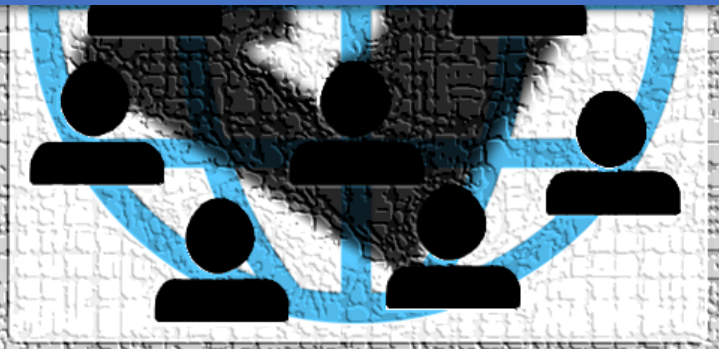
GDPR Readiness Assessment



EHR20.COM
INFO@EHR20.COM
866-276-8309

WHO WE ARE …

EDUCATION

Online Training, Webinars and Customized Workshop

CONSULTING

Professional services to help you with your Compliance needs

DISCLAIMER

This awareness training has been provided for educational and informational purposes only and is not intended and should not be construed to constitute legal advice.

Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

Recording of webinars is available upon request

EHR 2.0
Ensure HIPAA Compliance

Vinay Bansal

CIPP/E, CIPM, CCSP

AWS Certified Professional, GIAC Legal

Vinay's Background

- Principal Engineer, Cisco Systems
- Leads cloud security architectures and strategy (AWS, Google, Azure)
- Privacy and Data Protection Professional
- 24+ years in security and IT industry
- MS Comp Science – Duke Univ
- Interests: Running, teaching kids, healthy living

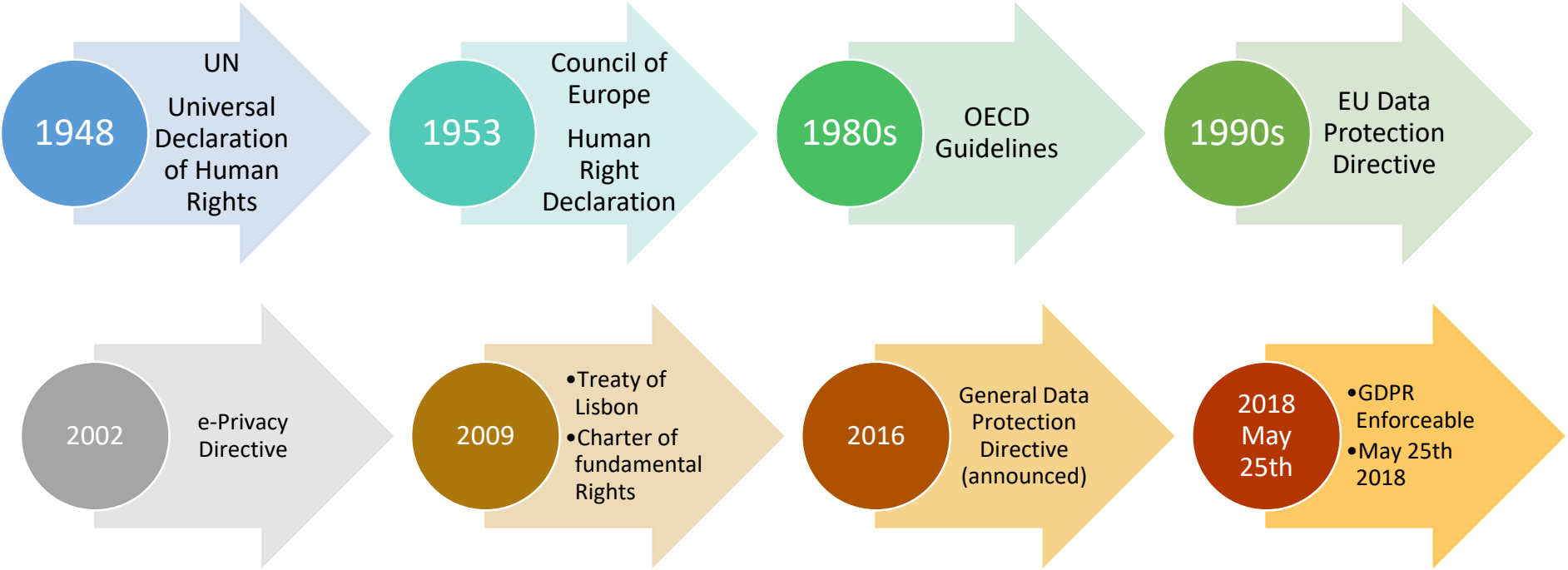
Agenda

1. European Privacy Laws and GDPR
2. Personal Data and Rights
3. Data Protection Roles
4. GDPR Key Principles
5. Ten Steps to GDPR Readiness

What is GDPR?

- EU General Data Protection Regulations (GDPR)
- Apply across all 28 EU states
- 25th May 2018

European Privacy Laws



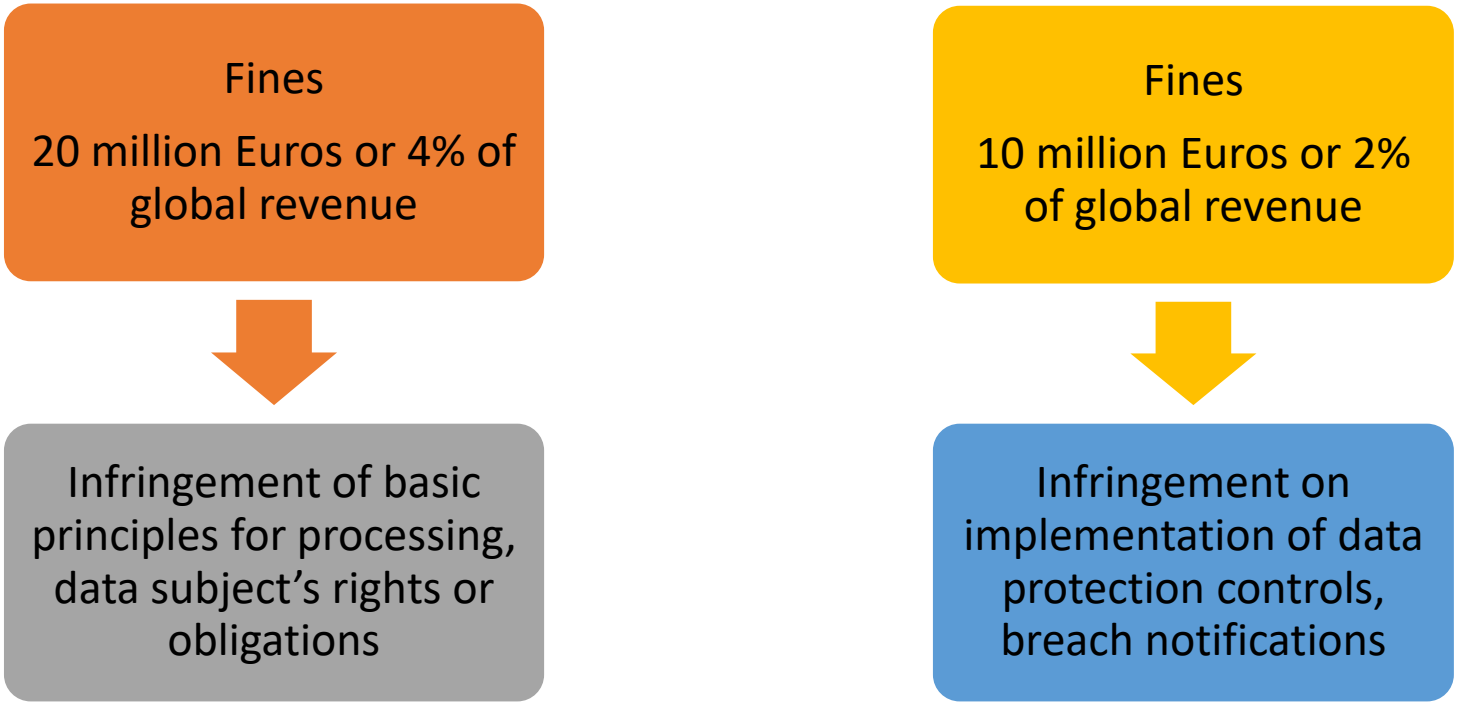
Who needs to comply to GDPR?

“All companies controlling or processing personal data of EU data subjects”

- Do you offer goods or services to EU data subjects?
- Do you monitor the behavior of EU data subjects?
- Are you data processors of EU data subjects’ personal data?

Note: GDPR applies to **all** companies, including US companies, that collect, store or process personal data of EU data subjects

Impact of Non compliance



Data Protection Roles

- **Data Subject:** Any identified or identifiable natural person
- **Data Controller:** Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data
- **Data Processor:** Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
- **Data Protection Officer:** Natural personal who has expert knowledge of data protection law and practices and who has the ability to advise the controller/processor, monitor compliance and act as the contact point for the supervisory authority on issues relating to personal data processing

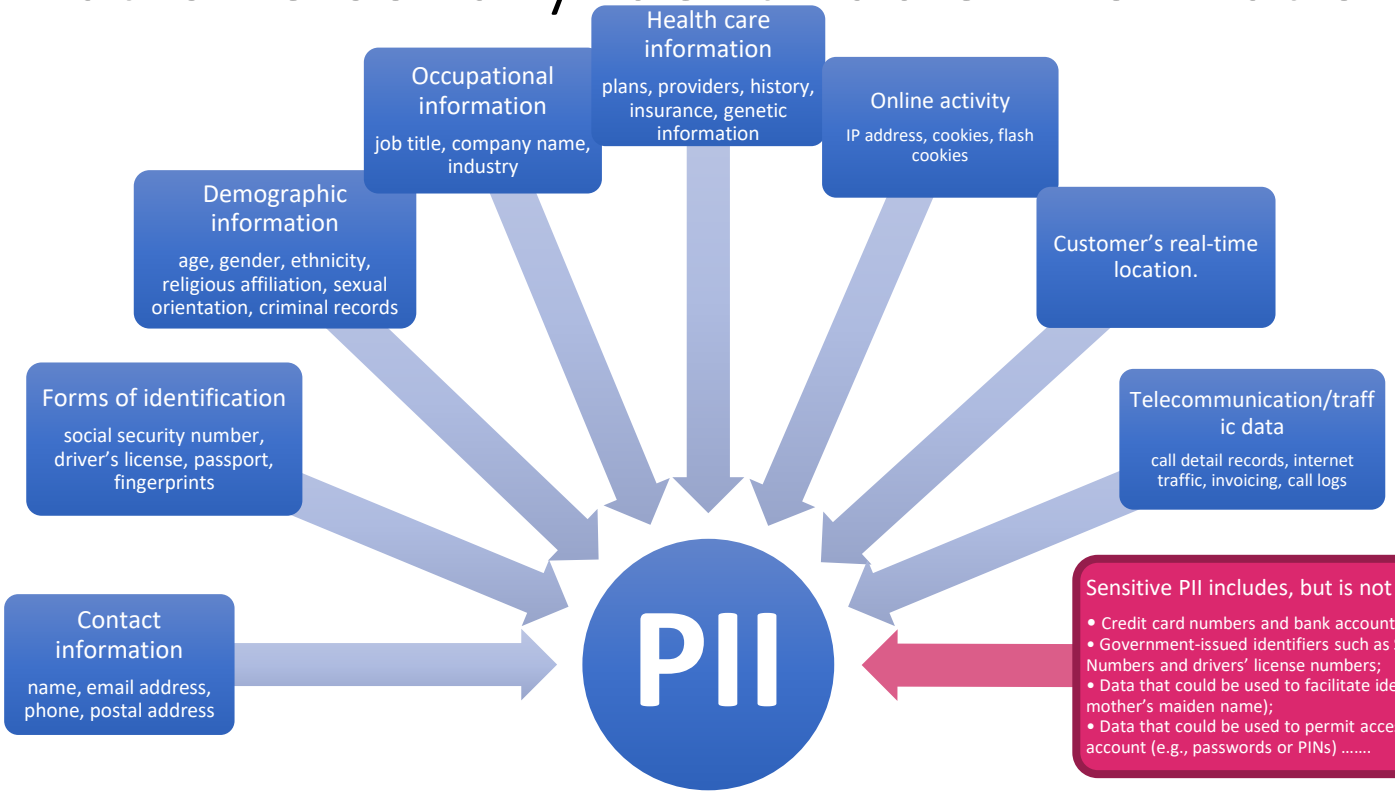
GDPR Key Principles

1. Lawfulness, Fairness & Transparency
2. Purpose Limitation
3. Data Minimization
4. Data Accuracy
5. Storage Limitation
6. Confidentiality & Integrity (Security)
7. Accountability of Data Controller

Ten Steps to GDPR Readiness

Step 1: Data Inventory

What is Personally Identifiable Information?



Sensitive PII: a subset of PII considered to be so important to the individual that it must be specially protected.

SPEACIL CATEGORIES OF DATA

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data and biometric data
- Data concerning health
- Data related to person’s sex life or sexual orientation

Keep an up-to-date list of data elements processed

Data Inventory (Example)

Data Element	System	Is Data PII?	Encrypted ?	Sent to third party?	Geographical Location
Name	**Billing**	**X**	**X**	**X**	**US**
Email address	**Billing**	**X**	**X**	**X**	**US**
Postal address	**Billing**	**X**			**US**
Phone	**Billing**	**X**	**X**		**US**
Occupational information		**X**		**X**	**US**
Online activity (IP address / Geographic location/ Cookies)	**Web Monitoring**	**-**	**X**	**X**	**US**
Government issues forms of identification	**None**	**X**			**US**
Demographic information	**Billing**	**X**			**US**
Health care information	**Healthcare**	**X**			**US**
Credit card numbers and bank account information	**Billing**			**X**	**US**

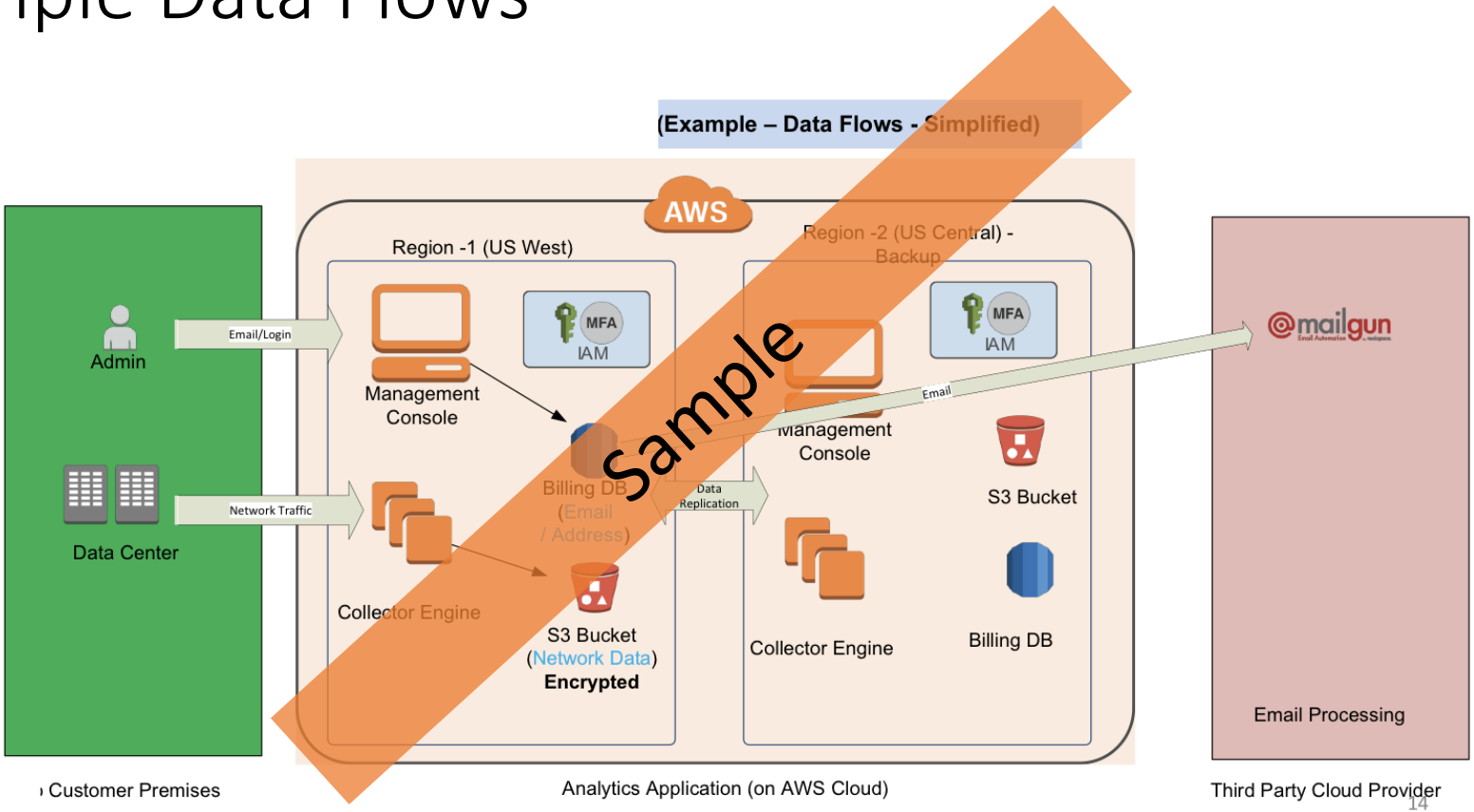
Step 2: Privacy Notice (Transparency)

- GDPR asks for no jargon in the privacy notice.

- What/How/Who/Why is information being collected. How will it be used? Who is it shared with? What will the effects on the individuals concerned? Is the intended use likely to cause individuals to object or complain?

Step 3: Identify Data Flows

Sample Data Flows



Step 4: Perform PIA

Privacy Impact Assessment mandatory when the processing is likely to result in a **high risk** for the rights and freedom of individuals

Example: Privacy Impact Assessment Results

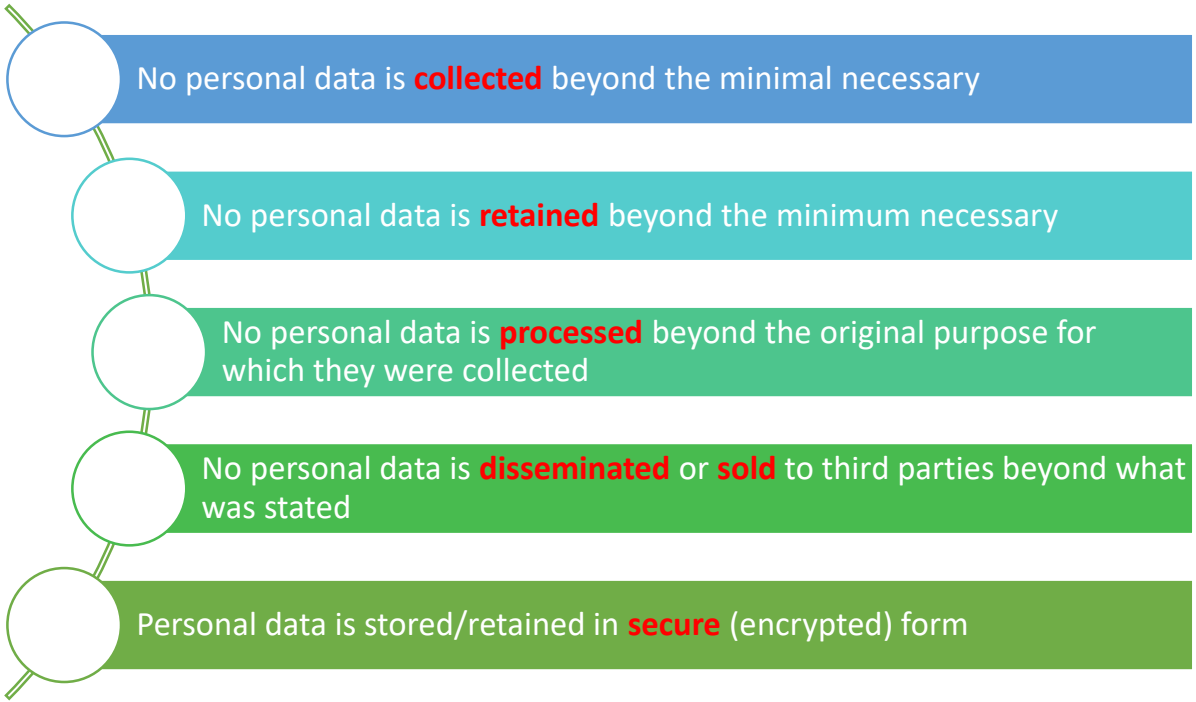
Area	Description	Example Findings from Privacy Assessment
Notice	Data subjects should be **given notice what** data is being collected, **when** their data is being collected, and the **purpose** it serves in the offering	Link to Privacy Statement present. Privacy supplement to be added.
Purpose	Data should only be **used for the purpose stated** and not for any other purposes.	Additional details on data usage to be captured in a separate Privacy Supplement.
Consent	Data **should not be disclosed** without the data subject's consent, The consent of the data subject should be captured	Opt-In exists. Need to formally capture consent record in database.
Protection & Security	Collected data should be **kept secure** from any potential abuses using the following: Secure processing to maintain confidentiality; security controls for Storage, Transmission/Communication; Promoting compliance and awareness; Restricted trans-border data flows	Adequate technical security protection in system. Trainings for operations/support staff not completed.
Disclosure, Transparency, & Trust	Data subjects should be **informed** as to who is collecting their data; How that data will be used; With whom Cisco will share this privacy data; Data breach notifications in case of unauthorized access	Marketplace Partners, privacy data sharing agreement to be signed.
Access & Accountability	Data subjects should be **allowed to access their data and make corrections** to any inaccurate data; Data subjects should also be provided the ability to object and deny privacy data being collected	Users can update privacy related information via user profile.
Data removal	Privacy data should not be retained beyond its purpose (**Limited retention**)	Privacy data is not completely deleted after the customer closes the account. (Keep transactional information for financial records, remove customer PII

Sample Data Impact Assessment & Prioritization

		Likelihood		
		High	Medium	Low
Impact	High	Unencrypted laptop ePHI	Lack of auditing on EHR systems	Missing security patches on web server hosting patient information
	Medium	Unsecured wireless network in doctor's office	Outdated anti-virus software	External hard drives not being backed up
	Low	Sales presentation on USB thumb drive	Web server backup tape not stored in a secured location	Weak password on internal document server

Updated risk management plan to be maintained

Step 5: Privacy by Design (Data handling)



Data Subject Rights

- Data access and rectification
- Data portability
- Data Erasure
- Restriction of data processing
- Right to object to data processing
- Decisions based on automated data processing

Establish Data Handling Processes

- Don't hold data unnecessarily
- Strong data deletion processes
  - Procedural Controls
  - Technical Measure

- Allow data subjects to positively opt-in to allow usage of personal information
  - you can not have a pre-ticked box.

Make Opt-Out easy

- Unsubscribe button or how to stop receiving mail.
- Have a process to provide information stored of a consumer
- Must be done in 1 month and free of charge

Step 6: Agreements/Contracts: Manage Third Party Processors

- Contractual Obligations for Sub-Processors
  - Written agreements in place between your organization and the data processors that outline how personal data should be handled
- Cross Border Data transfer
- Controller must establish
  - Types of personal data and categories of data subjects
  - Nature, purpose and duration of processing
  - Obligations and rights for controllers

Step 7: Data Protection Officer (DPO)

- Data Protection Officer Must
  - Report to the highest management level of an organization
  - Is not dismissed or penalized for performing their tasks
  - Inform and advise data controllers or processors
  - Monitor compliance with data protection laws
  - Contact person for supervisory authorities

Mandatory for

- Public authority company
- Companies with Large Scale systematic monitoring of individual
- Large scale processing of special categories of data
- Data relating to criminal convictions and offences

Even if it is not mandatory

- Recommended
- Consider virtual (part time) DPO

Step 8: Breach Notification

Personal Data Breach

" a breach leading to accidental or unlawful disclosure, destruction, loss , alteration or access, to personal data transmitted, stored or otherwise processed"

Data Subject Notification

- Notification without undue delay in case of high risk to the rights and freedom of individuals
- Notification may not be necessary if data is encrypted or appropriate technical measures in place

Data Protection Authority Notification

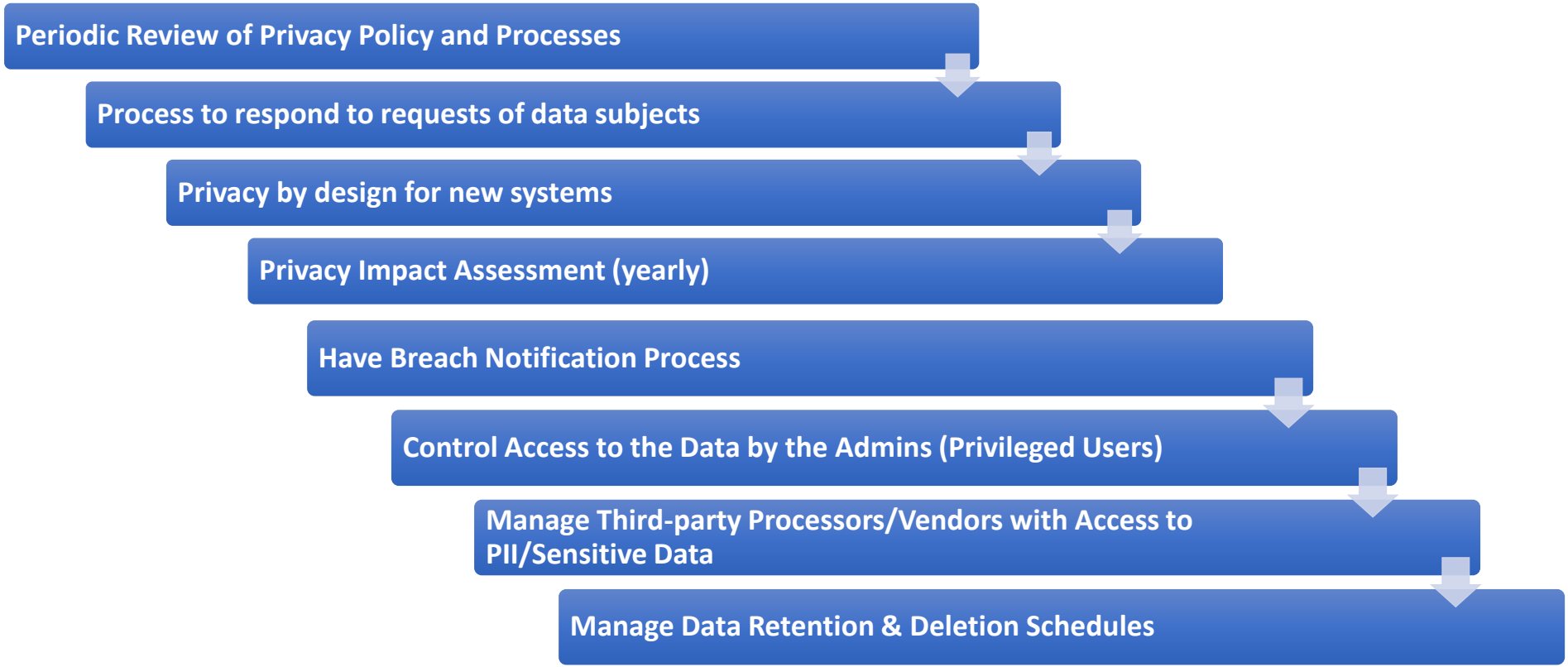
- Within 72 hours of becoming aware of breach
- Nature of Breach
- Consequences of breach
- Details of DPO
- Measures taken for remediation

Step 9: Privacy Training

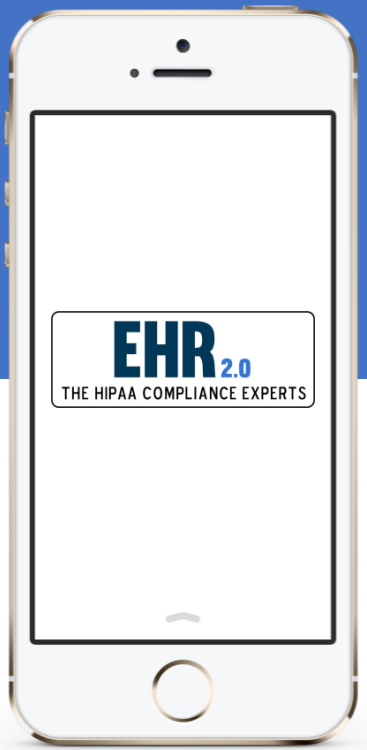
- All Employees handling personal data
- IT Team/Administrators (privileged access)
- Senior Management

Frequent user awareness training and assessment

Step 10: Continuous Privacy Governance Program



FIND US



CALL US
866-276 8309

SERVICE
info@ehr20.com

LOCATION
150, Cornerstone Dr.
Cary, NC

SOCIALIZE
Facebook
Twitter

Twitter: @ehr_20

Facebook: ehr20

Questions

Please don’t hesitate to ask

Thank You

for your attention!

GDPR Principles - Description

- **Personal information shall be processed lawfully, fairly and in a transparent manner;** Clear Consent/Opt-in for data subjects; ability to be demonstrably forgotten
- **Personal information shall be collected for specified, explicit and legitimate purposes;** Organizations must be clear with data subjects about how their personal information is going to be lawfully used and information may only be used that way
- **Personal information shall be adequate, relevant, and limited to what is necessary;** The data controller must only collect personal information that is absolutely required for the specified purpose
- **Personal information shall be accurate and, where necessary, kept up-to-date;** The data controller must ensure – to the best of their abilities – that the information collected is correct
- **Personal information shall be retained only for as long as necessary;** All personal information must now have an expiration date applied appropriate to its collected purpose
- **Personal information shall be processed in an appropriate manner to maintain security;** The data controllers and processers must ensure that the confidentiality, integrity, and availability of the information is maintained