GDPR - The Essentials
DISCLAIMER

This presentation is meant solely to educate you on GDPR and provides some basic guidelines to help you in your GDPR compliance journey.

Thus the information discussed herein should not be construed as Legal advise or be replaced for Legal advise.

Zoho Corp does not take the responsibility of misinterpretation or misunderstanding of the content by the reader.

Zoho Corp makes no warranties, express, implied, or statutory, as to the information in this material.

Please seek the guidance from a Legal Consultant/Advisor in your compliance project.
Topics

- What is GDPR?
- The augmented privacy principles
- Rights of the Data Subject
- What else does the GDPR say?
- What's new in GDPR?
- Primary Focus of GDPR
- Consequences of non compliance
- Key players/actors in the GDPR

- Examples of Personal Data
- Accountability architecture
- Rights - Explained
- What Zoho is doing about GDPR?
- What our applications would be providing?
- What you should do now?
- Who should be involved?
WHAT IS GDPR (GENERAL DATA PROTECTION REGULATION)?

• It's a law that gives more **power** (control) to an individual over his/her personal data.

• Augments the basic privacy(data protection) **principles**

• Applies when **processing** (using) personal data of EU residents by anyone irrespective of the location of the person/entity performing the processing.

• **Replaces** the data protection directive (officially Directive 95/46/EC).
WHAT ARE THOSE AUGMENTED PRINCIPLES?

- **Lawfulness, fairness and transparency** (the way you handle and manage your customer data)
- **Purpose limitation** (How long have you been keeping the data?)
- **Data Minimization** (What data do you currently hold and for what purposes? Do not keep more than what’s needed)
- **Accuracy** (How accurate is the data you hold?)
- **Data retention** (is the data you hold still necessary for the original purpose of processing?)
- **Security** (How secure is the data you hold?)
OKAY! WHAT DO YOU MEAN BY 'POWER' A.K.A. 'CONTROL'? 

Simply put, more 'Rights'..

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision making including profiling
WHAT ELSE DOES GDPR SAY?

• Stresses on Privacy by Design

• More data security

• Keeping record of the processing activities

• Addresses Cross border data transfers

• And finally, it becomes enforceable from 25th May THIS YEAR!
WHAT'S NEW IN GDPR?

- Increased territorial scope
- Higher penalties
- Consent mechanisms
- Breach Notification
- Enhanced data subject rights
- Data Protection Officers
- Increased accountability for Data Processors
WHAT IS THE PRIMARY FOCUS OF GDPR?

• Control over 'Personal data' (or) 'Personally Identifiable Information (PII)'

• **Definition** - "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..."

• **Example:**
  • **Direct identifiers** - Account information, Identification Numbers, Health information etc.,

  • **Indirect identifiers** - Age, Date of Birth, Gender etc.,
CONSEQUENCE OF NON COMPLIANCE TO GDPR?

- Reputational loss
- Lose existing customers
- Lose new customers
- Fines for violation - can go up to €20 million or 4% of your global annual turnover of the preceding financial year (which ever is higher)
KEY PLAYERS / ACTORS IN THE GDPR

Data Subject - an individual who is the subject of personal data

Data Controller - a 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

Sub Processor / Third party - a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data
KEY PLAYERS / ACTORS IN THE GDPR

Joint Controllers - two or more controllers who jointly determine the purposes and means of processing

Supervisory Authority - independent public authority which is established by a Member State to monitor consistent application of the laws

Representative - a natural or legal person established in the European Union who, designated by the controller or processor represents the controller or processor with regard to their respective obligations
ACCOUNTABILITY ARCHITECTURE
EXAMPLES OF PERSONAL DATA (PII)

- Full Name
- Email address
- Home address
- Data of Birth
- Ethnicity / Race
- Gender
- National ID numbers / Social security number
- Passport number
- Visa permits number
- Driver's license number
- Vehicle registration plate number
- Disability information
- Location information
- What you are doing when / status
- Events attended
- Status
- Sexual orientation

- Education and employment history
- Grades
- Salary
- Job position / title
- Photos
- Anything commercially sensitive
- Political and religious leanings and affiliation
- Views on controversial issues
- History / background
- Mother maiden name
- Place of birth
- Genetic information
- Insurance details
- Medical information
- Criminal record
- Credit score / record
- Sites registered on

- Work details - (Company name, address, colleagues)
- Family members
- Dependents
- Spouse / Partner
- Friends
- Associates
- Usernames / Screen names / aliases
- Email address
- Passwords
- Digital identity
- Bio-metric data - Retina, face, fingerprints, handwriting
- Security tokens
- Password hashes
- Cookies
- Session information and tokens
RIGHTS - EXPLAINED

Right to be informed, Right of access, Right to rectification, Right to Portability

What does it mean?

- People that you hold identifiable information about will now have the right to ask about
  - what information you hold about them,
  - why you hold it,
  - how long you’ve had it,
  - how long you intend to hold it,
  - what you intend to do with it and
  - ensure that data held about them is accurate.
RIGHTS - EXPLAINED

Right to be informed, Right of access, Right to rectification, Right to Portability

What does it mean?

• If someone finds out that a company holds incorrect data on them,
  • they have a right to contact the company and
  • have them make any necessary corrections immediately.

• EU citizens will also have a “right to data portability”, which means that they have a right to request a digital copy of any data held about them; companies will have to provide this within a month of receiving the request.
RIGHTS - EXPLAINED

Right to Objection, Right to Restriction and Right to Erasure (Right to be forgotten)

What does it mean?

• Along with the right to give informed consent, they also have a right to retract/withdraw that consent at any point.

• They also have a right to object to certain uses of their data that they disagree. Eg: sharing their details with a third party.
RIGHTS - EXPLAINED

Right to Objection, Right to Restriction and Right to Erasure (Right to be forgotten)

What does it mean? Continued..

• There is also the “right to restrict processing” in which due to various reasons, a data subject may request the data controller to restrict their personal data from being processed until they give their consent again.

• Also part of the GDPR legislation is the “right to erasure”, which means that you should be able to delete all of an individual’s personally identifiable data should they request it, provided there’s no “compelling reason” for you to continue storing/processing that data.
WHAT ZOHO IS DOING ABOUT GDPR?

- Reviewing our data inventory and data flows
- Revisiting & amending contracts with our third party service providers
- Conducting employee awareness trainings
- Privacy Risk & Impact Assessments
- Enhancing our data handling processes and procedures
- Revising our customer data protection agreements to meet the requirements of the GDPR
WHAT DOES ZOHOL ALREADY HAVE?

• ISO 27001:2013 - Information Security Management Systems

• SOC 2 Type II

• EU-US Privacy Shield framework
WHAT OUR APPLICATIONS WOULD BE PROVIDING?

• Provisions within our Apps for Data Controllers to cater to the Rights of the data subjects

• Stronger data security measures like
  • Encryption
  • More Access Controls
  • Anomaly detection

• Enhanced audit logs of activities with the Apps

• Better data administration & governance provisions for Data Controllers

The above mentioned points may vary in the implementation for each application. For more information on how each application addresses them, send us a mail to security@zohocorp.com
THAT'S AMAZING! NOW, TELL ME WHAT I SHOULD DO NOW?

• Buy-in from the Top (Board level)
• Raise awareness among your colleagues
• Data Mapping & Inventory (Types of data & their whereabouts)
• Identify what measures you already have in place
• Understand & document the legal basis from the every processing you are carrying out
THAT'S AMAZING ! NOW, TELL ME WHAT I SHOULD DO NOW?

• Assess third parties in your data flow chain on their GDPR readiness & amend contracts where required

• Establish procedures to respond to data subjects when they exercise their rights

• Clean up old unused data from your systems

• Establish & conduct Privacy Impact Assessment (PIA) for high risk processing operations

• Establish a process for Breach Notification
GOT IT! SO WHO NEEDS TO BE INVOLVED?

**Marketing teams** - Check if you need to get consent from your customers/clients for processing their personal data

**Product Engineering & Management teams** - Build privacy into your products & processes. Work to process data more securely.

**Legal, Privacy & Compliance teams** - Review the existing contracts with your third party providers & constantly monitor compliance.

**Senior Management & Board** - They will have to provide the necessary support & back you up in this journey
Resources - Zoho

- Privacy Policy - https://www.zoho.com/privacy.html
- Our public statement on our GDPR readiness - https://www.zoho.com/gdpr.html
Resources - ManageEngine

- Privacy Policy - https://www.manageengine.com/privacy.html
- Our resources for your GDPR compliance - https://www.manageengine.com/gdpr/index.html
Get started, now!

For more information on our compliance journey, mail us at security@zohocorp.com