aspire SYSTEMS
attention. always.

Everyone is talking about GDPR. Is this yet another buzzword that will slowly fade away ?

No, its significance is much bigger than that! GDPR stands for General Data Protection Regulation and came into existence on 27th April 2016. It replaces the earlier Data protection directive 95/46/EC. The main purpose is to provide a standardized data protection law

So, why are people all of a sudden talking about it now?

That’s because every business needs to be GDPR compliant by 25th May 2018. As the date is approaching a number of companies are just waking up to this reality!

Where is all this compliance stored?

There are 11 chapters and 99 articles where the GDPR compliance is stored.

But I’m in India. How does it concern me?

This is the biggest misconception that companies globally outside the EU had — it didn’t concern them as they don’t process personal data. The important point to keep in mind is every business across the world that collects, stores, processes, outsources personal data of EU citizen(s)/resident(s) has to comply with GDPR requirements. It applies to EU citizen’s/resident’s data wherever they reside. Example: Storing EU Client's representative’s name and details.

We are ISO 27001 certified company, are we GDPR compliant?

Not necessarily. It is only if the ISO 27001 certified company's ISMS's A.18.1.4 clause is complying fully with GDPR requirements.

Are small businesses exempted?

No, a firm's size is not a criterion for exemption from GDPR.

Okay, so what happens if businesses don’t comply by 25th May?

Non-compliance fines are very high! It’s 20 million Euros (approximately 150 crores) or 4% of the global turnover, whichever is greater!

How are such fines determined?

Fines are determined in the following ways:

- Nature of infringement
- Preventive measures (available/not available)
- Intention
- Notification to authorities
- Certification of processes

There would also be a potential trust deficit right?

Yes, in addition to the fines, there are other downsides:

- Legal Costs
- Loss of Goodwill
- Loss of Customer Trust

What kind of data are we talking about? There's a Microsoft Office in the EU that I want to reach out to, can I connect with it?

The **Data Subject** governing GDPR involves personal data, not company data. The Data Subject is defined as 'any identifiable natural person'. So you can contact Microsoft, but not Mr. Sebastian who's an EU resident from Microsoft. When an employee data is leaked it becomes a GDPR issue.

What exactly is personal data? In this age, we also put out information on social media, does it qualify?

- Personal data is defined as the following:
- 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. Information that can identify the individual directly or indirectly by reference to an identifier includes:
  - Person's Name
  - Date of Birth
  - Photos
  - Location data like Postal Address
  - Email IDs
  - Online Identifiers (IP Addresses, Cookie Strings etc.)
- It can also relate to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- Even if the person is professionally connected to you on LinkedIn, you cannot use this data. GDPR brings in fundamental changes to the approach of handling personal data of EU residents.

So I understand I can't use that data. What about the person's views or religious faith? Can I quote such a person's views?

There is certain information that qualifies as Sensitive Personal Data. This can be damaging if revealed, for example: Sexual Orientation, Political Views, Religious Faith, Physical Health Information, Psychological Health, Cultural Orientation, Race, Economic Status and so forth.

So GDPR doesn't allow me to contact any EU citizen/resident without taking their permission?

Yes, this permission is called consent.

What does consent imply? Even public information can't be used?

Yes, unless consent is given in clear terms for the purpose the information can be used, it can't be used for that particular purpose.

Consent of the data subject means:

- Data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
- It is specific, informed and unambiguous indication of the data subject's wishes

What if Aspire India takes consent but Aspire Singapore reaches out to an EU client. Does the consent still hold?

Yes, Aspire India has taken consent on behalf of all its locations and this consent still holds. It's important that records are maintained for this purpose.

What if the consent is written in a convoluted or complicated manner resulting in ambiguity?

This doesn't hold as consent as GDPR clearly states that the consent must be given in a specific, informed and unambiguous manner.

Once consent is given, companies can use this data right? How are companies allowed to process this data in GDPR terms?

- Yes. ‘Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as:
- Collection, recording, organization, structuring, storage, adaptation or alteration, retrieval
- Consultation, use, disclosure by transmission, dissemination, or
- Otherwise making available, alignment or combination, restriction, erasure or destruction

What about Profiling? How does GDPR view it?

- Good question. Profiling means any form of automated processing of personal data consisting of the use of personal data:
- To evaluate certain personal aspects relating to a natural person
- In particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements

How about pseudonyms of people?

- Let’s first define **pseudonymisation**. It means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information*. Ex. ceo@abc.com
- It’s important to remember that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- The other important point is on Anonymization. Anonymization is rendering personal data anonymous in such a way that the data subject is not or no longer identifiable, making it impossible to derive insights on a discreet individual, even by the party that is responsible for the anonymization.

As the power of individual information is emphasized, what rights does the EU citizen/resident hold? Could you give an overview of all the rights involved?

The EU citizen/resident is called the Data Subject. He has the following rights:

Right to information - Right to ask what personal data of theirs is processed and with whom it is shared

Right to access - Right to access their own data as well as request copies of the same

Right to rectification - Right to request for change to their data if it not accurate

Right to withdraw consent - Right to withdraw the previously given consent, so that company does not process their data anymore

Right to object - Right to object when his/her data is processed in variance to committed purposes. This is similar to ‘Withdraw Consent’

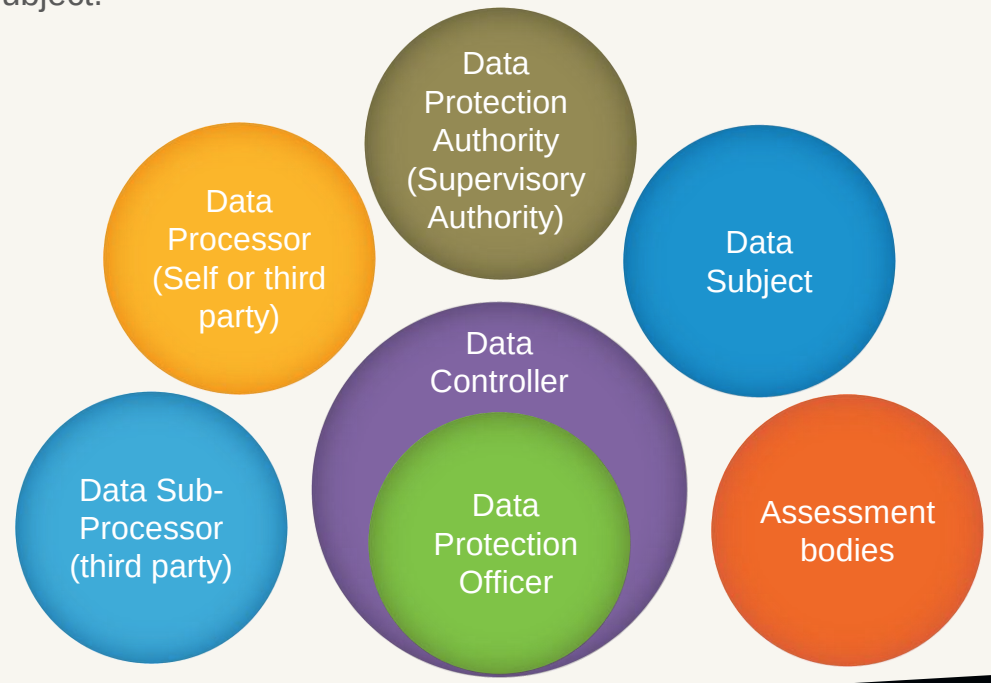
Right to object to automated processing - Right to demand only manual processing to understand the uniqueness of the data subject

Right to be forgotten - Right to request for deletion of their data. To be in conjunction with retention period and retention schedule in-line with applicable laws

Right for data portability - Right to return the data or transfer it to another controller

Who are the different actors in this GDPR ecosystem?

Broadly, this is how the ecosystem looks like: There's a Data Controller that owns the data and then the other actors around it like the Data Processor, Data Protection Authority and Assessment bodies that looks at protecting the data of the Data Subject.



What are the various roles and responsibilities of such actors?

Here are the categories of roles of such an ecosystem:

Data Controller:

- Refers to 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**
- Data Controllers can be **jointly responsible** across entities
- **Accountable** for GDPR compliance
- Upholds Data Subjects' rights

Data Processor:

- A natural person or legal entity that processes personal data on behalf of Data Controller
- Controller and Processor can be the same
- When it is a Third Party, must comply with **Data Processing Agreement**

Data Sub Processor

- A third party natural person or legal entity that processes personal data on behalf of Controller and Processor
- Must comply with **Data Processing Agreement**

Data Subject

- Refers to a natural person who is the subject of personal data
- Holds the rights for providing his/her personal data using consent form
- Has distinct rights under GDPR

Data Protection Officer

- Leadership role required by GDPR
- Exist within companies in EU that processes personal data of EU residents
- DPO oversees approach for data protection, its strategy and implementation. Responsible for GDPR compliance
- DPO' is a mandatory role for an organization.

Data Protection Authority (Supervisory authority)

- It is a public authority in an EU country that monitors compliance to GDPR in its country
- Typically a Privacy Commission
- Enterprises in multiple EU countries may appoint Lead Supervisory Authority for purposes of reporting
- EU organizations can register one DPO for all regions with Lead Supervisory Authority

From Aspire's perspective, who would I be in this ecosystem and would GDPR be applicable?

?

"

It depends on what role you'd be representing Aspire in the following activities:

Aspire has product/service that directly interacts with resident(s) of EU member state.

- You are a **Data Controller/ Data Processor**. GDPR is applicable.

Aspire has operations in EU

- You are a **Data Controller/ Data Processor**. GDPR is applicable.

Aspire is doing an outsourced application development from an EU customer and does not gather data directly from EU resident

- You are a **Data Processor.** GDPR is applicable.

Aspire has outsourced application development from a US customer who had actually got ‘outsourced work’ from an EU customer

- You are a **Data Sub Processor.** GDPR is applicable.

Aspire’s marketing team has bought **data consented telemarketing data** of EU costumer’s personal data

- You are a **Data Controller/Data Processor.** GDPR is applicable

So, what do companies have to know about GDPR? Are there certain guidelines?

Yes, there are certain guiding principles that are required for companies to adhere to:

- **Fairness, lawful and Transparency** – Personal data must be processed in lawful manner, fairly and transparently. It shall be maintained with respect to the data subject
- **Limitation of Purposes** – Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose, or those purposes

- **Adequacy /Data Minimization**– Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
- **Accuracy** - Personal data shall be accurate and, where necessary, kept up to date
- **Retention** - Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes . This also refers to storage limitation.
- **Rights** - Personal data shall be processed in accordance with the rights of data subjects under this Act
- **Integrity & Confidentiality (Security)** - Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- **International transfer** – Personal data shall not be transferred to a country or territory outside the EU unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

How do organizations comply with data protection obligations at such a scale?

- Data Protection Impact Assessment (DPIA) is an effective technique that help organizations to comply with data protection obligations of data subjects
- The DPIA will help organizations to estimate the risk levels involved upfront while handling the data
- In every project the DPIA is carried out in the beginning of the project and appropriate data protection is established. This is referred as ‘ Privacy by design’
- DPIA activity enables the team to make informed decisions on data protection mechanisms and communicate to the stakeholders appropriately
- DPIA documents shall be maintained and shall be demonstrated for compliance with GDPR

What steps can we use to implement DPIA?

- Identify the data for which DPIA shall be carried
- Understand the flow of information
- Estimate risks involved throughout the data life cycle
- Identify data protection mechanisms to mitigate those risks
- Obtain signoff from the data protection officer or an equivalent authority in your organization
- Implement the data protection mechanisms in your process areas

Is there a simple checklist I can use?

- **Q1:** Do I have access to personal data of an EU national?
- **Q2:** Do I have data subject's consent to store/process/outsource data?
- **Q3:** Did I estimate the risk in handling the personal data?
- **Q4:** Do I have proper protection controls to handle the estimated risk level?
- **Q5:** Do I have mechanisms/processes to update/delete data upon data subject's request?
- **Q6:** Do I have monitoring mechanisms to see adequacy of data protection mechanisms?
- **Q7:** Do I have data breach notification process in place (if data breach happens)?
- **Q8:** Do I have mechanisms to minimize the impact of data breach?

Any final advice for me?

Yes, remember most importantly the following points:

- Consent shall be given for each specific purpose(s) by the data subjects
- The data subjects shall have the **Right to withdraw** consent anytime
- The data subjects shall have the **Right to modify** their personal information and same is maintained accurately on relevant places
- The data subjects have the **Right to Access their information** that have been processed
- The data subjects have right to erase and right to restrict data (Exemption only for legal/statutory purposes)
- Notify the data subject and supervisor authority on data breaches within 72 hours
- **Document Everything – Not documenting is considered as not done**

One last question, who would be the First Point of Contact for me to reach out to for any queries related to GDPR ?

?

Your first Point of Contact would be your respective SLO/Department Head.

aspire SYSTEMS
attention. always.