GDPR : E.U. Data Protection Harmony -All you need you need to know

Prepared by – Krishnan Sanjeev Nair

Contents

Introduction:

‘’**Regulation (EU) 2016/679** , the Data Protection Law Enforcement Directive, commonly known as **GDPR**, is for the protection of natural persons with regard to the processing of personal data and on the free movement of such data entered into force on 24 May 2016 and applies since 25 May 2018. (EU Commission, EU Charter of Fundamental Rights)

GDPR is reasonable new and wide reaching regulation encompassing entire EU and the first of kind data protection legislation in the market place across the world. The General Data Protection Regulation (GDPR) is considered to be the toughest privacy and security law in the world. Although it is drafted and passed by the European Union (EU) but it imposes obligations onto organizations anywhere in the world so long as they collect data of people in the EU. The background of GDPR is restrict data usage and protection across a sovereign state federation such as the European Union and massively influence usage of any sort of consumer data of software-intensive and data centric IT firms around the EU itself, regardless of its user, or purpose of use. Many non EU countries as well USA, Australia, Singapore, Hong Kong are looking at GDPR as basis for and data protection type.

It is undoubtedly the strictest piece of legislation protecting consumer rights around their data. Some giants Face Book, Tiktok are already in big time trouble with the data commissioned here in Ireland, and thus in Europe. On 13 April 2023, Meta Platforms Ireland Limited (Meta IE) was issued a 1.2 billion euro fine with charge that Facebook failed to protect consumer data as it passed personal information to third parties without any consent. This fine is the largest GDPR fine ever, was imposed for Meta. (EDPB, May’23). On other hand Tiktok infringed the GDPR's principle of fairness when processing personal data relating to children between the ages of 13 and 17. For this act, Tiktok has been reprimanded along with fine of €345 Million imposed on them.(EDPB,15 Sep’23).

This report outlines the implications of the General Data Protection Regulation (GDPR) and addresses some key aspects on the Regulation. It also proposes a roadmap for further enhancing data security posture and ensuring ongoing GDPR adherence. A company must make all effort and be committed to responsible data practices and building strong customer relationships, recognizes the importance of GDPR compliance.

Principles of GDPR:

The GDPR outlines several key principles and requirements that organizations must adhere to when processing customer data. These principles are designed to protect customer privacy and prevent unauthorized access.

Chapter II, Article 5 of the GDPR says that anyone who processes personal data must do so in accordance with seven protection and accountability principles. These principles are as follows:

1. **Lawfulness-** Processing of any personal data must be lawful, fair and transparent to the data subject.
2. **Purpose Limitation-** Data must be processed for specific, explicit and legitimate purposes as outlined to the data subject at the time of collection and not further processed in a way incompatible with those purposes.
3. **Data Minimizations-** Organizations should only collect and process as much data as absolutely necessary, relevant and limited for the stated purposes.
4. **Accuracy-** Data collected and processed must be accurate and wherever necessary to be kept up to date. Organisation has to take every reasonable action to ensure that personal data are accurate in regard to the purposes for which they are processed.
5. **Storage Limitation-** Organisation must store personally identified information as long it is absolutely necessary for the specified purpose as declared to the subject. However Personal data can be retained for extended durations if it is to be exclusively utilized for archival, public interest, scientific, historical research, or statistical purposes as outlined in Article 89(1). This is contingent upon the implementation of requisite technical and organizational measures mandated by this Regulation to uphold the rights and freedoms of the data subject.
6. **Integrity-** Personal data must be processed in a manner that ensures appropriate integrity, security, confidentiality of the personal data for example encryption. Organisation has to also ensure protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

7. **Accountability-** The controller of the organization responsible to follow these principles is also responsible for and must be able to demonstrate the compliance of the GDPR principles as duly followed by the organisation as and when asked for with evidence.

With the looming threat of potentially significant fines, there is also risk of data breach resulting sanctions from EU data protection authorities if organizations fail to comply the requirement under GDPR. Critical requirements that need to be followed are:

Requirements of GDPR:

- **Consent:** Organizations must obtain clear and unambiguous consent from individuals for processing their personal data. This consent must be freely given, specific, informed and unambiguous. Requests for consent must be 'clearly distinguishable from the other matters' and be presented in 'clear and plain language.' There are also specific requirements for obtaining consent from children age 13 or below along with their parents.
- **Data subject rights:** Individuals have a number of rights under the GDPR, including the right to access their personal data, to have it rectified if inaccurate, to have it erased, to restrict processing, and to data portability. Data subjects can withdraw previously given consent whenever they want.
- **Data protection impact assessments (DPIAs):** Organizations may need to conduct a DPIA to assess the impact of certain high-risk processing operations on the rights and freedoms of individuals. They also need to keep documentary evidence of any given consent of the data subjects.
- **Data breaches:** Organizations must notify the supervisory authority and data subjects of a personal data breach in a timely manner.

Risks and Consequences of breach:

Data Protection Commission (DPC), the national independent authority responsible for upholding the fundamental right of individuals in the European Union (EU) to have their

personal data protected, has advised to appoint a designated Data Protection Officer (DPO) and publish the details of the DPO (DPC,2022).

As per DPC, Under the GDPR, ‘a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data’ (DPC, 2019).

Keeping in line, a comprehensive framework of questionnaire is prepared to assess the potential risks and consequences of any security breach. A sample structure of such framework is highlighted below to assess the risk and consequence of any breach:

Nature and Scale of the Breach:

- What type of data is breached? How much sensitive are the information (e.g., names, addresses, financial information, passwords)
- How many individuals might be affected? Must be scalable.
- Is the breach accidental, malicious, or unauthorized access? Must be traceable.
- How long will the unauthorized access potentially last?

Impact on Individuals' Privacy Rights:

- Confidentiality: Is any sensitive personal data exposed (e.g. health information, financial data)?
- Integrity: Is the data altered or corrupted?
- Availability: Was access to the data restricted or unavailable? Was there a Role based access?

GDPR Compliance Risks:

- Notification Obligation (GDPR,Art.33): Does the breach pose a high risk to individuals (e.g., financial loss, identity theft, discrimination)?

- If so, notification to the Supervisory Authority (SA) within 72 hours is mandatory.
- If risk is low, notification may not be required.
- Data Subject Rights (GDPR,Art.15-22): Individuals may exercise their rights under GDPR, including:

    i) **Right to Access:** Expect requests for data confirmation and access to breached information.
    ii) **Right to Rectification:** Individuals may request correction of inaccurate data exposed in the breach.
    iii) **Right to Erasure (Right to be Forgotten):** Individuals may request deletion of breached data if applicable. And even withdraw consent given prior.

- Fines and Reputational Damage: Failure to comply with above GDPR obligations or data subject rights can lead to significant fines (up to 4% of annual global turnover or €20 million, whichever is higher) and reputational damage.
- Data Processing Agreements (GDPR,Art.28): Assess if data processors were involved in the breach. Review agreements to ensure processors have appropriate security measures and breach notification obligations.
- Data Protection Impact Assessments (DPIAs): Conduct a DPIAs, review damages to identify any weaknesses exposed by the breach.

By following this framework, organisation can effectively assess the GDPR compliance risks associated with a security breach and take appropriate steps to mitigate them.

Measures to avoid any breach:

With the introduction of GDPR, the responsibilities of the organisation have significantly changed while holding and processing of personal data. There are now real obligations for the way to collect and use personal data in order to protect individuals. Organization is now solely accountable for any lapse and there are significant fines and repercussions on failure.

Considering the previous experience of security breach in respect to GDPR, it is paramount important to strengthen the data security measures and ensure GDPR compliance and prevent future incidents.

Although the Data Protection Act 2018 and the GDPR does not specify any security measures that a data controller or the organisation must have in place however the **GDPR Articles 25 and 32** place an obligation on data controllers and processors of the organisation to implement data protection through **'appropriate technical and organizational measures'** to ensure a level of security appropriate to the risk, taking into account:

- the state of the art;
- the costs of implementation;
- the nature, scope, context and purposes of processing; and
- the likelihood and severity of the risk to the rights and freedoms of individuals.

Considering the above guidelines here is a comprehensive proposal encompassing technical, organizational and legal measures to enhance data security and prevent future security breaches in line with GDPR compliance:

Technical Measures:

1. **Implement data encryption** - The **pseudonymisation** and **encryption** of personal data. Implement data encryption at rest and in transit to protect sensitive personal data even in case of a breach.
2. **Access Controls:** The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. Need to establish a strong access controls with multi-factor authentication along with a **CIA Triad** of such data base access with

proper **User Identity** and **Level of Clearance** by following **Role Based Access Control (RBAC).**

3. **Data Backup and Recovery:** Strong ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. This can be ensured by maintaining **Regular Back up** of client's data and following **Data Redundancy**.

4. **Vulnerability Management:** Regular process for testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. Implement Data Loss Prevention (DLP) solutions to prevent unauthorized data exfiltration.

5. **Network Security:** Strengthen network security with **firewalls**, intrusion detection/prevention systems **(IDS/IPS)** and regular security monitoring is essential.

Organizational Measures:

1. **Security Awareness Training:** Need to conduct regular security awareness training to employees to educate them on data security best practices, phishing attempts and social engineering tactics.

2. **Code of Conduct:** Adherence to an approved Code of Conduct as referred to in **Article 40, GDPR** or an approved certification mechanism as referred to in **Article 42** may be used as an element by which to demonstrate compliance as per the requirements of GDPR with regard to following areas:

- Fair and transparent processing.
- The legitimate interests pursued by controllers in specific contexts.
- The collection of personal data.
- The pseudonymisation of personal data.
- The information provided to the public and to data subjects.
- The exercise of the rights of data subjects.

- The information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained.
- The measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32.
- The notification of personal data breaches to supervisory authorities and the communication of such personal data breach to data subjects.
- The transfer of personal data to third countries or international organizations; or
- Out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.
- Develop a comprehensive incident response plan outlining steps for identifying, containing, responding to and recovering from security incidents.

3. **Data Inventory and Classification:** Conduct a data inventory to identify and classify all personal data stored by the company.

4. **Data Retention Policy:** Implement a data retention policy to determine how long data is stored and ensure its deletion when no longer required as per GDPR data retention policy.

5. **Data Protection Officer (DPO):** Consider appointing a DPO to oversee GDPR compliance and act as a point of contact for data subjects.

Legal Measures:

1. **GDPR Compliance Documentation:** Maintain thorough customer data documentation to showcases adherence to GDPR regulations, encompassing data processing procedures, consent protocols, policies for data protection.
2. **Review Data Processing Agreements (DPAs):** Review existing DPAs with third-party vendors to ensure they meet GDPR requirements and hold them accountable for data security.

3. **Privacy Policies and Notices:** Review and update privacy policies and notices to provide clear and transparent information to data subjects about how their personal data is processed, the purposes of processing and their rights under GDPR.
4. **Data Breach Notification Procedures:** Establish clear procedures for notifying the Supervisory Authority and data subjects in case of a personal data breach within the mandated timeframe (72 hours for high-risk breaches).
5. **Regulatory Compliance Monitoring:** Stay informed about updates and changes to GDPR regulations and guidance issued by data protection authorities. Regularly review compliance status and adjust policies and procedures accordingly to mitigate legal risks.

By implementing these technical, organizational and legal measures, Company X can significantly enhance data security, mitigate any future risk of security breaches and demonstrate a commitment to GDPR compliance and data protection. Regular monitoring, review and continuous improvement are essential to adapt to evolving threats and regulatory requirements. . This will not only protect the company from potential fines but also enhance its reputation and build trust with customers and stakeholders.

Post Incidence Remediation:

While setting up above mentioned Technical and Organizational measures, utmost care must be taken to mitigate any risk of incidence. However there are several crucial reasons for conducting and investigating a GDPR incident if at all happens and identification of the root cause and immediate remediation are essential for any organization.

- **"Why"&"How"-** Identifying the root cause of the incident helps identification of weaknesses or vulnerabilities in the organization's data security measures, systems or

processes. This allows addressing the underlying weakness and preventing similar incidents from occurring again.

- **Understanding the Scope and Impact:** Such investigation helps in determining the extent of the incident including the type and amount of data affected and the potential impact on data subjects and the organization. This understanding is crucial for initiating appropriate response measures.
- **Compliance Obligations & Notification-** GDPR mandates organizations has to report certain data breaches to supervisory authorities and in some cases even to the affected data subjects. Conducting the investigation enables the organization to fulfill these legal obligations promptly and accurately.
- **Recovery and Remediation:** Understanding the root cause of the incident facilitates the development and implementation of effective remediation measures to mitigate the impact of the breach. This will enable the organization to restore affected systems, recover lost or compromised data and prevent further unauthorized access.
- **Preserving Evidence:** Proper investigation ensures the preservation of evidence related to the incident, which may be necessary for regulatory inquiries, legal proceedings or internal reviews. Preserving evidence accurately and comprehensively enhances the organization's ability to defend its actions and decisions.
- **Building Trust and Transparency:** Transparently investigating and addressing GDPR incidents demonstrate the organization's commitment to GDPR compliance and accountability. It helps in maintaining trust with customers, partners, regulators and other stakeholders by demonstrating a proactive approach while addressing security incidents.

The Principle of Accountability in GDPR aims to guarantee compliance with the Data Protection Principles. This requires the organizations not only to put in place an appropriate technical and organizational measure as we detailed above, but at same time also able to demonstrate what action they have taken to counter any incidence and effectiveness of such measures undertaken. The GDPR requires that the controller/security officer of the organisation is responsible for making sure all privacy principles are adhered to.

By complying with all stated Technical and Organizational measures, our organisation will demonstrate that we are compliant with the law and our measures include:

- Adequate documentation of all personal data as processed;
- How and to what purpose and how long data will be processed for;
- Documented processes and procedures aiming at tackling data protection issues at an early state; and
- How fast organisation can remediate and recover from any incidence.
- The presence of a Data Protection Officer who is integrated in the organisation planning and operations etc and under full control of all measures.

Legal and financial Consequences for non-compliance:

Legal Consequences:

There are several avenues for legal actions against a GDPR violation, with potential consequences for both the data subject and the data controller of the alleged organization. Supervisory Authorities have the power to take various legal actions beyond fines such as issuing warnings, reprimands or orders to restrict data processing. Individuals whose data has been compromised due to a GDPR violation have the right to take legal action against the organization. This can result to payment of compensation for damages (material or non-material) from the data controller of the company including financial losses, emotional distress, or reputational damage caused by the violation. Data subjects may seek injunctions from courts to prevent further processing of their data or to have inaccurate data rectified.

Aside any GDPR violation news in media will significantly damage the organization's reputation, leading to a loss of customer trust and potential business opportunities. Negative publicity surrounding privacy violations can lead to loss of business, brand devaluation, and long-term reputational harm.

Non-compliance with GDPR may restrict the organization's scope to conduct business in various EU market. This might even lead to barriers to enter into contracts or partnerships with EU-based companies, limiting their market reach and growth opportunities.

Financial Consequences:

The Supervisory Authorities and EU Commission have the task to ensure compliance of GDPR and to be able to fulfill these tasks they have rights to undertake investigation and corrective powers. The most severe form of sanctioning from a company perspective is the administrative fines. **Article 83(5) GDPR,** states the severe violation of the Regulation where the maximum amount of penalty can be up to EUR 20 million or up to 4% of the total worldwide turnover of preceding fiscal year, whichever is higher. **Article 83(4) GDPR** sets forth fines for less severe violations with penalty up to EUR 10 million, or, in the case of an undertaking, up to 2% of its entire global turnover of the preceding fiscal year, whichever is higher. The GDPR, in addition, gives right to each Member State to lay down rules on other penalties for infringements of the Regulation which are not already covered by Article 83.

Apart from administrative sanctions, entities might have to pay compensation to data subjects. In this regard, it should be noted that, for the first time, the processor will be facing its own civil liability for infringements of the GDPR. (Josephine Wolff et al. 2021). GDPR fines are designed to make non-compliance a costly mistake for both large and small businesses. And this implies to all types of businesses, from multi-nationals down to micro-enterprises. The fines are effective, proportionate and dissuasive for each individual case.

Overall, it can be stated that organisation must consider the GDPR compliance seriously and implementing appropriate measures can significantly reduce the risk of facing legal and financial repercussions for non-compliance and violations. A proactive approach to data protection is not only essential but also strengthens trust among customer and stakeholders and fosters a positive reputation for the organization.

Bibliography

1. **GDPR fines and penalties- https://gdpr-info.eu/issues/fines-penalties/** (Accessed 30th Mar,2024)
2. **GDPR Top Ten #2: Accountability principle- https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-accountability-principle.html** (Accessed 28th Mar,2024)
3. **Know your obligations - https://www.dataprotection.ie/en/organisations/know-your-obligations/data-security-guidance** (Accessed 25th Mar,2024)
4. **Security of processing- https://gdpr-info.eu/art-32-gdpr/** (Accessed 25th Mar,2024)
5. **Two tiers of GDPR fines- https://gdpr.eu/fines/** (Accessed 30th Mar,2024)
6. **What if companies fail to comply with data protection rules ?- https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_en** (Accessed 28th Mar,2024)

7. **What is GDPR-** https://gdpr.eu/what-is-gdpr/ (Accessed 28th Mar,2024)

END OF REPORT