
# REPORT ON GDPR COMPLIANCE AND DATA SECURITY MEASURES FOR X

Module Title: Information & Cybersecurity Management

Module code: B9FT102

Module Lecturer: Alexander Victor

Submitted by: Gauri Shingane – 20018204

Submission Date: 10th April 2024

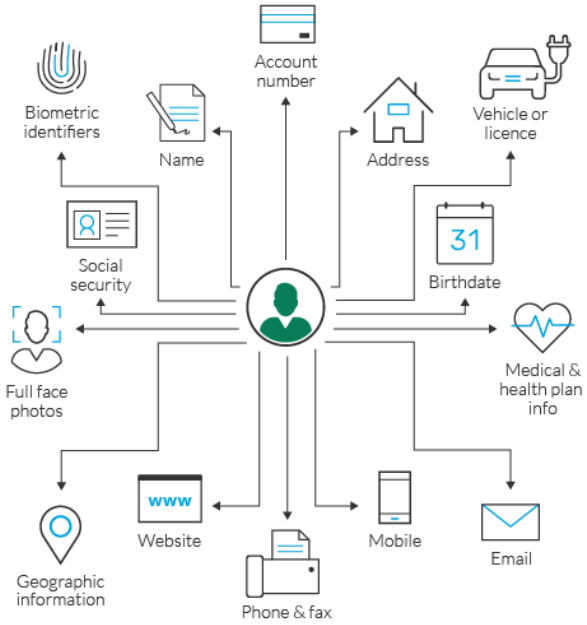
# TABLE OF CONTENTS

# GDPR PRINCIPLES AND REQUIREMENTS RELEVANT TO DATA PROTECTION

The Art. 1(1) of the GDPR (Radley-Gardner, Beale and Zimmermann, 2016) defines personal data as,

> *'personal data' means 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, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

*Figure 1. Elements of Personal Information of an individual*



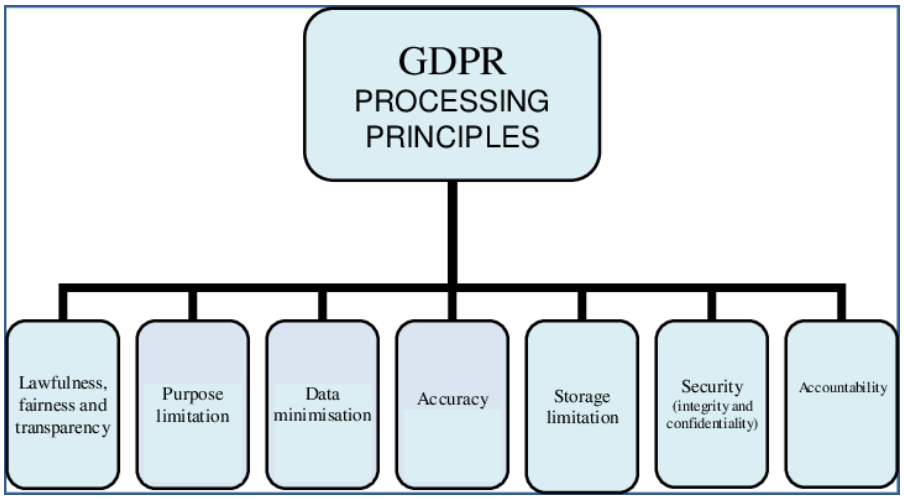

*Source: Imperva*

We at X, store a lot of customer data, so we need to make sure this data is kept safe from malicious elements. Our priority is to make sure the data remains safe during collection and processing, even when we are storing the data for longer periods. Below are a few principles mentioned in the GDPR, which if followed strictly will make sure we are always compliant with the personal data protection principles of GDPR.

## PROTECTION OF CUSTOMER PERSONAL DATA

As mentioned earlier our priority is compliance with GDPR to make sure the personal data of our customer remains protected at all stages of processing and transfer.

*Figure 2. GDPR processing principles.*




*Source: ResearchGate*

## Lawfulness, fairness, and transparency

According to the Art. 5(1)(a) (Radley-Gardner, Beale and Zimmermann, 2016),

> *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*

We at X, need to make sure to implement provisions for the data subjects to be able to have access and the right to get information about how their data is being collected, used, processed, or shared with other data controllers. Also, we need to make sure that the information provided to the data subjects is easy to understand, clear and written in plain language.

## Purpose Limitation and Data Minimization

According to Art. 5(1)(b) (Radley-Gardner, Beale and Zimmermann, 2016),

> *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*

and Art. 5(1)(c),

> *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*

The personal data stored with X should be used adequately and limited to only what is necessary for our purpose. Also, the data subjects should always be aware of their rights to stop their data being stored or processed at any moment, if they feel the need for it.

## Rectification and Erasure

In Art.5(1)(d) of the GDPR (Radley-Gardner, Beale and Zimmermann, 2016), the right of data subjects to keep their data accurate is explained as,

> *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*

We at X, need to ensure that the personal data stored with us is accurate and error-free. If any data subjects request change or correction in their information, it must be done immediately and no other data manipulation should ever be done without the consent of data subject at any point of data processing. Similar rules apply in case of requests for erasure of any data requested by the data subjects.

## Storage Limitation

In Art.5(1)(e) of the GDPR (Radley-Gardner, Beale and Zimmermann, 2016), it explains the need for us to make sure to store data only for the required amount of time,

> *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*

We at X, need to inform the data subjects about the periods for which their data is being stored in our systems and second, we need to make sure to delete the data at the end of the period. The data subjects have the right to complain if the data is being kept longer than necessary. So, we need to establish time limits for the erasure of the personal data of the data subjects and make sure we abide by these time limits.

## Integrity and Confidentiality

In Art.5(1)(f) of the GDPR (Radley-Gardner, Beale and Zimmermann, 2016), the right to confidentiality of personal information of the data subjects is defined as,

> *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

The personal data should be processed in a secure environment making sure that the confidentiality of the data is being maintained. We need to ensure to implement security against any unauthorised access or use of personal data stored in our systems.

### PROCESSING OF CHILDREN'S DATA

In Art. (8), the GDPR (Radley-Gardner, Beale and Zimmermann, 2016) separately mentions the conditions applicable while storing or processing children's data. The personal data of children can be lawfully processed only under two conditions,

1) the child is at least 16 years of age
2) we acquire the consent of the holder of parental responsibility over the child.

We at X need to make sure to abide by these rules as the personal data processing for children is closely and strictly observed by the supervising authority. Also, the member states of the EU can implement additional rules for data processing for children below 13 years, so we need to make sure to check for compliance according to the member state the child resides in. We need to make all possible efforts to make sure the data related to children is only stored or processed after obtaining the appropriate consent from the child or the parental authority. The only exception in gaining parental consent, for children below 16, is if the services offered directly to the child are related to counselling or of a preventive nature.

## RISKS AND CONSEQUENCES OF THE SECURITY BREACH IN GDPR COMPLIANCE

A security breach in the context of GDPR is a security incident with unauthorized exposure of personal data. The Art.4(12) GDPR (Radley-Gardner, Beale and Zimmermann, 2016) defines Personal Data breach as,

> *'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 transmitted, stored or otherwise processed;*

When a personal data breach incident takes place, X is no longer compliant with the Art.5 of the GDPR.

### IMPACT OF DATA BREACHES ON INDIVIDUALS' RIGHTS

#### Unauthorised access to personal data

When a data breach happens the personal information about our users is exposed to unauthenticated, unauthorized personnel who otherwise should never have access to this information. This compromises the rights of individuals as their names, addresses, phone numbers and other such personal information get leaked.(Kolah, 2018, p. 113)

### Risk of identity theft

As the personal and confidential information about individuals is exposed there is a high possibility of identity theft hence leading to fraud. Criminals may use this exposed information to impersonate individuals and do unauthorized financial transactions or even cause reputational damage to the individual using the services at X.(Kolah, 2018, p. 113)

### Loss of control over private data

Once the data is compromised the individuals have little to no control over their personal information and must depend on the X to undertake mitigation actions to reduce further damage.(Kolah, 2018, p. 113)

## GDPR OBLIGATIONS

In the event of a personal data breach, X must notify the supervisory authority and all the data subjects affected by the data breach.

### Notification to Supervisory Authority

Art.33(1) of the GDPR (Radley-Gardner, Beale and Zimmermann, 2016) establishes that we at X must inform the supervisory authority within a given timeframe without fail. The GDPR also mentions the information that our company needs to provide to the security authorities in case of a personal data breach in a report called Personal Data Breach Report (PDBR). They are as follows:

1) nature of personal data breaches wherever possible, the types and approximate number of data subjects included in the breach, approximate number of data records exposed due to the breach.
2) contact information of our Data Protection Officer or other contacts to get more information from our company about the data breach.
3) likely effects of the personal data breach
4) measures the data controller takes to address data breaches and possible mitigation steps proposed for reducing further damage.

We at X, also needs to document all the facts related to the data breaches, their consequences and the mitigation steps taken by us. In case we are not able to provide all the information to the supervisory authorities in time, our company also needs to mention the reason for the delay in notifying the authorities.(Radley-Gardner, Beale and Zimmermann, 2016; Kolah, 2018, p. 113)

### Notification to data subjects

In the event of a personal data breach, our company needs to send a notification to all the affected individuals or the data subjects as stated in the Art. 34(1) of the GDPR. The information to be provided to the

data subjects in case of a personal data breach is the same as the type of data needed to be provided to the supervisory authority.

As mentioned in the Art. 12(1) (Radley-Gardner, Beale and Zimmermann, 2016; Kolah, 2018, p. 117), the data provided by our company must be,

- concise
- transparent
- intelligible
- easily accessible
- in plain language

especially in case the data exposed is in regards to children.

The personal data breach notification can be sent to the data subjects through emails, letters or even telephone calls but only if the identity of the data subject can be checked (Radley-Gardner, Beale and Zimmermann, 2016; Kolah, 2018, p. 120).

There are a few conditions that if met our company does not have to report to the data subjects, they are:

1) if our company has implemented measures like encryption that make sure that the personal information leaked during the data breach is inaccessible or unreadable to unauthorized personnel.
2) If our company has taken measures that make sure that the high risk to the rights of data subjects does not occur.
3) It involves a lot of data subjects, in such cases, public communication can be opted for.

## FINES AND REPUTATIONAL DAMAGE

### Reputational Damage

Reputational damage because of personal data breaches can have a significant impact on the image of X among users. (Kolah, 2018, p. 132)

1) Loss of trust: When the personal data of users is compromised it can result in damage to the trust and confidence that the users, partners, and public put in our products and services.
2) Negative perception: When the media lets out negative headlines and articles on media it impacts our company's reputation and can be perceived as if our company is not taking enough measures or is not ready to handle such incidents.

### Fines

The fines imposed by the supervisory authority depend on individual cases and are all laid out in the Art. 83(2) of the GDPR (Radley-Gardner, Beale and Zimmermann, 2016). Some of the outlined figures for penalties are as follows,

1) Administrative fees of €10 million or up to 2% of the total worldwide annual turnover of the preceding financial year of our company, whichever is higher, if the obligations of our company lie within the scope of Art. 8, 11, 25 to 39, 41(1) 42, 43.
2) Administrative fees of €20 million or up to 4% of the annual turnover of the preceding financial year of our company, whichever is higher, if our obligation lies within the scope of Art. 5 to 7, 9, 12 to 22, 44 to 49, 58(1), 58(2). (Radley-Gardner, Beale and Zimmermann, 2016)

## PROPOSED MEASURES TO ENHANCE DATA SECURITY AND PREVENT FUTURE BREACHES

Our company is responsible for making sure that the personal data of the data subjects remains safe, the Art. 24(1) of the GDPR (Radley-Gardner, Beale and Zimmermann, 2016) explains this as,

> *Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*

We need to implement appropriate and effective security measures to ensure the safety of data within our company and make sure we are always compliant with the GDPR principles.

### ORGANISATIONAL MEASURES

#### Data Protection Impact Assessment (DPIA)

Under Art.35 of the GDPR, the Data Protection Impact Assessment (DPIA) helps to comply with the data protection policies and safeguard the rights of users. The DPIA would help X find and solve any privacy or data issues that might appear when making new products or doing anything related to people's personal information. Art.35(3) of the GDPR makes it mandatory for any data controller that handles personal data through automated processing or uses data for monitoring.(Radley-Gardner, Beale and Zimmermann, 2016; Kolah, 2018, p. 90)

## Data Protection Officer

The Data Protection Officer will ensure that X is always compliant with the GDPR. The main objective of a DPO will be to protect the EU users' personal data that we are processing. Art. 37, 38 and 39, of the GDPR explains the position, tasks, and role of DPO in a company. The DPO needs to make sure not to disrupt the operations of X while undertaking the tasks. The DPO could offer suggestions on data protection practices followed by X and DPO's knowledge about the law could help us better our data protection systems as well. (Gobeo, Fowler and Buchanan, 2018, p. 164).

The Art. 37(1) of the GDPR (Radley-Gardner, Beale and Zimmermann, 2016) explains the conditions, which if fulfilled, we need to assign a DPO for X. They are,

> *The controller and the processor shall designate a data protection officer in any case where:*
>
> *(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;*
>
> *(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or*
>
> *(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10. (Radley-Gardner, Beale and Zimmermann, 2016)*

## Incident Response Plan

The Incident Response Plan is a protocol or a risk management plan which X needs to implement in the event of a personal data security breach. The protocol should still be compliant with the GDPR principles and needs to be implemented as soon as the CSIRT in our company is made aware of the breach. The CSIRT, Computer Security Incident Response Team, is an organisational body that mostly deals with the aftermath of the security breach, but they can also help prevent the security breaches. (Gobeo, Fowler and Buchanan, 2018, p. 211,213)

## Employee training

There are several threats to data security because of a lack of security awareness or carelessness of the employees. Non-malicious insider threats are authorized individuals in the company who lack security awareness or refuse to follow the security measures outlined by our company.

*For example, a project manager uses his personal cloud services to process or store the company's data.*

# TECHNICAL MEASURES

## De-identification

1) De-identification of data means removing the identifying elements from the personal information of an individual while sharing data.
2) There are many ways to achieve de-identification like “pseudonymization” and “k-anonymization” as proposed by Fujitsu. (Ito *et al.*, 2016)
3) In pseudonymization the real names are replaced with aliases which act as temporary identifiers, but the biggest drawback is that a combination of features mentioned in data can still lead to identification of the person.
4) In k-anonymization, to make sure a similar issue as with pseudonymization does not occur, it creates a set of features that could indirectly identify an individual called quasi-identifiers (QI) and make sure that there are at least *k* individuals with the same combination of QI. (Ito *et al.*, 2016)

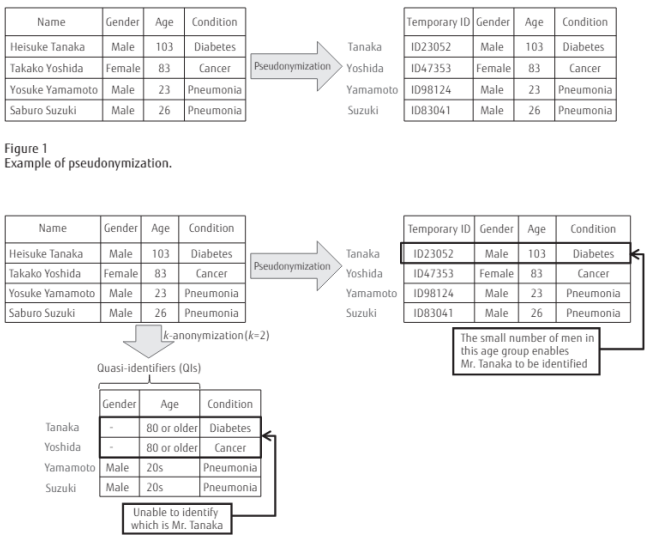
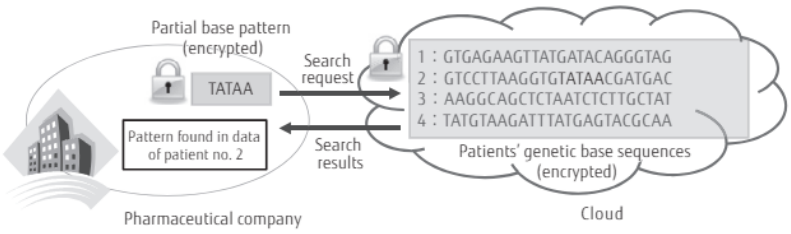



Figure 1
Example of pseudonymization.

## Homomorphic Encryption

1) Homomorphic encryption is a cryptographic technique wherein computations can be performed on encrypted data without decrypting.
2) This helps preserve the data and privacy of individuals in case the company wants to analyse the data but makes sure no private information of users can be exposed to anyone handling data.
3) Fujitsu Labs has developed a similar mechanism using a parallel processing method which improves the data processing performance by a lot. (Ito *et al.*, 2016)




## Cyber Essentials

There are certain security controls, which if implemented at X, can prevent maximum cyber-attacks that could lead to personal data breaches. They are,

1) Secure network – the servers and workstations which are used to store or process data at X should always be checked for updates, we should make sure they are always protected.
2) Firewalls and gateways – a firewall prevent attackers from accessing the network and gateways help our users to safely access our services at X online. The Next-generation firewalls help keep our systems safe from intrusions and reduce the time taken to respond to a security incident.
3) Access control – We need to make sure that only the people or systems that are supposed to access our data are the only ones that can access the data at any given time. Even all our X employees should have access to only the data needed to help them complete their tasks. A hierarchical approach for data access will help us segregate the users and employees into categories and only provide necessary access based on their role in our company.
4) Patch management – All the security systems must be timely updated in the form of patches. These security patches can update the security systems at X regularly and help us stay protected from low-level cyberattacks.
5) Malware protection – We need to keep our systems secure from all types of viruses, spyware, botnet software, and Ransomware. (Foulsham, Hitchen and Denley, 2019, p. 49)

## Security Testing and Vulnerability Scanning

It does not matter which security systems we put in place, we must always ensure to test the security systems for the safety of our infrastructure and applications. There are many ways to conduct security tests and these vary in cost and effects, the method we choose depends solely on the nature of our applications and systems. Vulnerability scanning is similar to testing but it does not test the security systems it will give us an estimate of how and where the attackers can target our systems and prepare us better for any future attacks.

# IMPORTANCE OF THOROUGH INVESTIGATION AND ACCOUNTABILITY

Once we have faced the consequences of a personal data breach, we immediately start working on the mitigation of the situation. We have already discussed the steps we at X, need to take on the event of a personal data breach, we will now look at a few steps we need to undertake to make sure we fully understand the cause of the breach, the security weaknesses involved in the breach, prevent further harm and remain compliant with the GDPR.

## Identifying root cause

At X, we need to make sure to fully understand the cause or the point of breach in the event of a personal data breach. This will help us find out the security vulnerabilities in our applications and infrastructure and areas in which we need to focus more in terms of security. The root cause in some cases might be insiders in the company who leaked confidential information related to the company which led to the personal data breach, in such cases we can terminate such individuals and make sure the other employees are trained about the security practices and the consequences of failure to comply with them.

## Assessing the extent of data exposure

Even if the data exposed was or was not encrypted or led to actual exposure of the personal details of the data subjects, the extent of this data leak needs to be examined. We need to understand if the breach targeted the whole data system or just a few servers on the system, also the type of data that was targeted, for example, personal details or financial details we targeted, can help us understand which data is more susceptible to attacks.

## Mitigating further harm

After conducting root-cause analysis and examining the extent of data exposure we can start working on making our systems more robust and ensure the security remains intact in case of another such attempt at a security breach. We can put up

## Facilitating regulatory compliance

According to GDPR, we need to take responsibility for the personal data exposed during the breach and make sure to comply with the principles. We need to make sure to notify the relevant supervisory authority and the data subjects affected by the breach not later than 72 hours after becoming aware of the breach. Conducting a thorough investigation can help us align with the accountability principles of GDPR and also demonstrate proactive efforts to make sure to identify and address security concerns and protect personal data from future attacks.

# LEGAL AND FINANCIAL CONSEQUENCES OF NON-COMPLIANCE

## Penalties

The fines imposed by the supervisory authority depend on individual cases and are all laid out in the Art. 83(2) of the GDPR (Radley-Gardner, Beale and Zimmermann, 2016; Foulsham, Hitchen and Denley, 2019, p. 83),

> *Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.*

Depending on the circumstances, the GDPR has laid out the conditions, which if fulfilled, a penalty can be imposed on us by the supervisory authority. When deciding whether to impose any penalty and how much penalty to be imposed, the following points are taken into consideration: (Radley-Gardner, Beale and Zimmermann, 2016)

1) the number of data subjects affected including the extent of damage suffered, the type and duration of violation that took place, and the reason the data was being processed when data was violated.
2) careless nature of the violation
3) the steps taken by our company to reduce the damage caused to the data subjects
4) the level of accountability shown by our company concerning implementing technical and organisational prevention against violation
5) any previous records of violation of our company
6) the amount of support and help shown towards the supervisory authority to reverse the damage and reduce further effects on the data subjects
7) the categories of personal data affected by the breach or violation
8) if our company made a timely notification to the supervisory authority and how the news about the incident reached the supervisory authority. (GDPR Art. 83(2))

The GDPR imposes penalties in case of non-compliance on two levels as mentioned here.

## Compensation

The Art. 82(1), of the GDPR (Radley-Gardner, Beale and Zimmermann, 2016) states that,

> *Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.*

The GDPR also states that, if the data processor is not found guilty of being responsible for the data breach, it can be exempted from the compensation, so we need to make sure to implement all necessary infrastructure to make sure the data security is indeed in place. According to the Art. 82, if the data breach happened because of another data controller our company is eligible to get compensation from the controller as well.(Foulsham, Hitchen and Denley, 2019, p. 84)

## Loss of Business

The company can lose a lot of business, because of a personal data breach, due to reputational damage, legalities involved and operational disturbances. Once the user trust is damaged, the users lose confidence in the company's data protection policies. The legal proceedings would also cost a lot of money and other resources which would damage the growth of our company. Also, the most damaging consequence would be a decline in our company's stock value or market capitalization which would heavily damage us financially.(Kolah, 2018, fig. 6.1)

## Remediation costs

The only way for our company to get back the customers it has lost to a personal data breach is to reinforce all the security measures and make sure to add to the data protection policies. We would need to implement data clean-ups to remove any malware or unauthorized access points from the systems. We will also have to enhance the security controls by implementing encryption to the data, applying multi-factor authentication, and training the employees on the latest security practices. The cost of implementing new data policies, conducting security audits, and giving proper compensation to the affected users is going to cost a lot which leads to further damage to the financial aspect of our company.(Kolah, 2018, fig. 6.1)

# CONCLUSION

The report explains the importance of following the rules of GDPR for our company X, to ensure the personal data of our users remains safe. It will help us implement principles like being transparent about the data collected and limiting the time and amount for which the data is stored. Also, it emphasizes the sensitivity with which we must handle the children's data.

If we ever encounter a personal data breach and data gets exposed it causes issues like identity theft and loss of control for the data subjects. We will need to make sure to notify the security authorities and the affected data subjects promptly according to the GDPR. Not complying can lead to heavy fines imposed on X and damage our company's reputation, so we need to appoint a Data Protection Officer to help us comply with the GDPR. We can use various organisational and technical measures to improve our defence against breaches and take steps to mitigate harm in case of a breach.

We need to investigate the personal data breach thoroughly and fix all the security vulnerabilities to make sure it does not happen again. So, it is crucial to maintain compliance with the GDPR principles and make sure the personal data of our users is kept safe.

# REFERENCES


Foulsham, M., Hitchen, B. and Denley, A. (2019) *GDPR: how to achieve and maintain compliance*. London ; New York: Routledge, Taylor & Francis Group.

Gobeo, A., Fowler, C. and Buchanan, W. (2018) *GDPR and cyber security for business information systems*. Denmark: River Publishers.

Ito, K. *et al.* (2016) 'De-identification and encryption technologies to protect personal information', *Fujitsu Scientific & Technical Journal*, 52(3), pp. 28–36.

Kolah, A. (2018) *The GDPR handbook: a guide to implementing the EU general data protection regulation*. London ; New York: Kogan Page Limited.

Radley-Gardner, O., Beale, H. and Zimmermann, R. (eds) (2016) *Fundamental Texts On European Private Law*. Hart Publishing. Available at: https://doi.org/10.5040/9781782258674.

'What is Personally Identifiable Information | PII Data Security | Imperva' (no date) *Learning Center*. Available at: https://www.imperva.com/learn/data-security/personally-identifiable-information-pii/ (Accessed: 9 April 2024).

Figure 1, 'What is Personally Identifiable Information | PII Data Security | Imperva' (no date) *Learning Center*. Available at: https://www.imperva.com/learn/data-security/personally-identifiable-information-pii/ (Accessed: 9 April 2024).

Figure 2, GDPR interference with next generation 5G and IoT networks - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/GDPR-processing-principles_fig1_342017058 [accessed 9 Apr, 2024]