**Data Protection Manual**

**Of**

# Nec Money Transfer Limited

## Approved by

Board of Directors dated on **21st August 2023**

# Table of Contents

## Introduction of Data Protection

Data protection is the process of safeguarding personal data from unauthorized or unlawful access, use, disclosure, alteration, or destruction. Data protection is essential for ensuring the privacy, security, and trust of individuals and organizations that share their personal data with others. Data protection is also a legal obligation for any entity that collects, processes, or shares personal data, as there are various laws and regulations that govern how personal data should be handled and protected.

One of the most important and comprehensive data protection laws is the EU General Data Protection Regulation (GDPR), which came into force in May 2018. The GDPR applies to any entity that offers goods or services to individuals in the EU, or monitors their behaviour, regardless of where the entity is located. The GDPR sets out the principles and rights for data protection, such as lawfulness, fairness, transparency, accuracy, security, accountability, access, rectification, erasure, restriction, portability, and objection. The GDPR also imposes strict obligations and penalties for data controllers and processors who fail to comply with the GDPR.

Another important data protection law is the UK Data Protection Act 2018, which supplements and implements the GDPR in the UK. The UK Data Protection Act 2018 also covers some areas that are not covered by the GDPR, such as law enforcement, national security, immigration, and intelligence services. The UK Data Protection Act 2018 also establishes the Information Commissioner's Office (ICO) as the independent authority that oversees and enforces data protection in the UK.

As a company that operates in the UK and the EU, Nec Money Transfer Limited (hereinafter "the Company") is subject to both the GDPR and the UK Data Protection Act 2018. The Company is committed to complying with these laws and regulations and ensuring that it respects and protects the personal data of its customers, employees, directors, representatives, suppliers, partners, and other stakeholders. The Company has developed this Data Protection or GDPR Manual (hereinafter "the Manual") to explain how it complies with the data protection laws and regulations and to provide guidance and procedures for preventing, detecting, and reporting any actual or suspected breaches of data protection by the Company or its employees, directors, or representatives.

## The Purpose and the Scope of the Manual

The purpose of this manual is to explain how Nec Money Transfer Limited (hereinafter "the Company") complies with the data protection laws and regulations, such as the UK Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR). The manual also aims to provide guidance and procedures for preventing, detecting, and reporting any actual or suspected breaches of data protection by the Company or its employees, directors, or representatives.

The scope of this manual covers all activities and transactions of the Company that involve the collection, processing, and sharing of personal data. Personal data is any information that relates to an identified or identifiable individual, such as name, address, phone number, email address, identification number, bank account details, transaction history, or biometric data.

## Types of Data Security Controls

Data security controls are measures that protect data from unauthorized or unlawful access, use, disclosure, alteration, or destruction. Data security controls can be classified into three categories: administrative, physical, and technical.

- Administrative controls are policies and procedures that govern how employees and other authorized persons should handle sensitive data. They include data classification, data retention, data disposal, data breach response, data protection training, and data protection audits. Administrative controls aim to ensure compliance with data protection laws and regulations, such as the UK Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR).

- Physical controls are devices and mechanisms that prevent or limit physical access to data and data storage devices. They include locks, alarms, cameras, guards, fences, safes, shredders, and encryption keys. Physical controls aim to prevent theft, loss, damage, or tampering of data and data storage devices.

- Technical controls are software and hardware tools that prevent or detect unauthorized or malicious access, use, disclosure, alteration, or destruction of data and data systems. They include firewalls, antivirus software, encryption software, authentication systems, access control lists, backup systems, and intrusion detection systems. Technical controls aim to ensure the confidentiality, integrity, and availability of data and data systems.

Data security controls are essential for ensuring the privacy, security, and trust of individuals and organizations that share their data with others. Data security controls also help to avoid or mitigate the risks and costs of data breaches, which can result in financial losses, reputational damage, legal liabilities, and regulatory penalties. Therefore, it is important for organizations to implement and maintain appropriate data security controls according to their business needs and legal obligations.

## Personal Date

Personal data means any information that relates to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, by using an identifier such

as a name, an identification number, location data, an online identifier, or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.

Personal data can include various types of information, such as name, address, phone number, email address, identification number, bank account details, transaction history, biometric data, or cookie ID.

Personal data is subject to the protection requirements set out in the data protection laws and regulations, such as the UK Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR). These laws and regulations aim to ensure the privacy, security, and trust of individuals and organizations that share their personal data with others.

## Sensitive Personal Data

Sensitive personal data and special categories of personal data are terms that refer to types of information that are considered more sensitive or private than other types of personal data. Personal data is any information that relates to an identified or identifiable natural person, such as name, address, phone number, email address, identification number, or online identifier. Sensitive personal data and special categories of personal data are subsets of personal data that may reveal more intimate or confidential aspects of a person's identity, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health status, sexual orientation, biometric or genetic data, or criminal history.

https://gdpr-info.eu/art-9-gdpr/https://www.itgovernance.co.uk/blog/the-gdpr-do-you-know-the-difference-between-personal-data-and-sensitive-data

The terms sensitive personal data and special categories of personal data are often used interchangeably, but they have different origins and meanings in different contexts. Sensitive personal data was a term used in the UK Data Protection Act 1998, which defined it as personal data consisting of information about a person's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health condition, sexual life, commission or alleged commission of any offence, or any proceedings related to any offence.

https://www.gdpreu.org/the-regulation/key-concepts/special-categories-personal-data/

Special categories of personal data is a term used in the EU General Data Protection Regulation (GDPR), which replaced the UK Data Protection Act 1998 in 2018. The GDPR defines special categories of personal data as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

https://www.lawinsider.com/dictionary/sensitive-or-special-category-personal-data

The main difference between the two terms is that the GDPR includes genetic and biometric data as special categories of personal data, whereas the UK Data Protection Act 1998 did not. The GDPR also excludes criminal history from the definition of special categories of personal data, but provides separate rules for processing personal data relating to criminal convictions and offences.

https://www.lawinsider.com/dictionary/sensitive-or-special-category-personal-data

Both sensitive personal data and special categories of personal data are subject to stricter protection requirements than other types of personal data. This means that organisations that collect, process, or share such data must have a valid legal basis for doing so and must implement appropriate safeguards to ensure the privacy and security of the data. For example, organisations may need to obtain explicit consent from the data subjects (the individuals whose personal data is processed), conduct a data protection impact assessment to identify and mitigate any risks associated with the processing, or apply encryption or pseudonymisation techniques to reduce the identifiability of the data.

https://www.lawinsider.com/dictionary/sensitive-or-special-category-personal-data

Sensitive personal data and special categories of personal data are important concepts to understand for anyone who deals with personal information in their professional or personal capacity. By respecting and protecting such data, organisations and individuals can ensure compliance with the relevant laws and regulations and foster trust and confidence among their customers, employees, partners, and other stakeholders.

N.B. Anybody who wants to share these data must also provide adequate safeguards for transferring this data outside the EU, such as adequacy decisions.

## Personal Data, Sensitive Personal Data and Special Categories of Personal Data collection

Personal data and sensitive personal data collection are processes of gathering and evaluating information or data from multiple sources that relate to an identified or identifiable natural person. Personal data is any information that can identify a person, directly or indirectly, such as name, address, phone number, email address, identification number, or online identifier. Sensitive personal data is a subset of personal data that may reveal more intimate or confidential aspects of a person's identity, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health status, sexual orientation, biometric or genetic data, or criminal history.

https://www.itgovernance.co.uk/blog/the-gdpr-do-you-know-the-difference-between-personal-data-and-sensitive-data

https://securityintelligence.com/posts/personal-data-vs-sensitive-data-what-is-the-difference/

Personal data and sensitive personal data collection are essential for ensuring the privacy, security, and trust of individuals and organizations that share their data with others. Personal data and sensitive personal data collection are also legal obligations for any entity that collects, processes, or shares personal data or sensitive personal data, as there are various laws and regulations that govern how personal data and sensitive personal data should be handled and protected. For example, the UK Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR) are two of the most important and comprehensive data protection laws that apply to any entity that offers goods or services to individuals in the UK or the EU, or monitors their behaviour.

Personal data and sensitive personal data collection can be done using different methods, such as surveys, interviews, observations, experiments, focus groups, or secondary data analysis. The choice of data collection method depends on the type of data needed, the purpose of the research, the resources available, and the ethical considerations involved. Data collection tools are software and hardware tools that help researchers collect, store, organize, analyze, and visualize data. Data collection tools can include online platforms, mobile applications, web browsers, spreadsheets, databases, statistical software, or data visualization software.

## Personal Data Collection and Sharing

Nec Money Transfer may be able to collect and share personal data from various perspectives, such as:

• From the customers who use their services to send or receive money worldwide. Nec Money Transfer may collect personal data such as name, address, phone number, email address, identification number, bank account details, transaction history, or biometric data. Nec Money Transfer may collect this data to verify the identity of the customers, to comply with the anti-money laundering regulations, to process the transactions, to provide customer service, or to improve their products and services.

https://www.bis.org/fsi/publ/insights33.pdf

• From the employees, directors, and representatives who work for or on behalf of Nec Money Transfer. Nec Money Transfer may collect personal data such as name, address, phone number, email address, identification number, bank account details, payroll information, performance records, or biometric data. Nec Money Transfer may collect this data to manage the employment relationship, to pay salaries and benefits, to monitor and evaluate the performance, to ensure compliance with the data protection laws and regulations, or to protect the interests and assets of the company.

https://edps.europa.eu/sites/edp/files/publication/14-11-25_financial_guidelines_en.pdf

• From the business partners, suppliers, contractors, or joint venture partners who collaborate with Nec Money Transfer. Nec Money Transfer may collect personal data such as name, address, phone number,

email address, identification number, bank account details, contract details, or transaction history. Nec Money Transfer may collect this data to establish and maintain the business relationship, to perform the contractual obligations, to ensure compliance with the data protection laws and regulations, or to protect the interests and assets of the company.

https://edps.europa.eu/sites/edp/files/publication/14-11-25_financial_guidelines_en.pdf

• From the website visitors or mobile app users who access Nec Money Transfer's online platforms. Nec Money Transfer may collect personal data such as IP address, browser type, operating system, device information, location data, cookie ID, or online behavior. Nec Money Transfer may collect this data to provide and improve their online services, to analyze the web traffic and user preferences, to deliver personalized content and advertising, or to enhance the security and privacy of their online platforms.

https://www.bis.org/fsi/publ/insights33.pdfhttps://www.imperva.com/blog/top-security-and-data-privacy-regulations-for-financial-services/

Nec Money Transfer may share personal data with various parties within or outside the EU for different purposes. For example:

• Nec Money Transfer may share personal data with other financial institutions or payment service providers that are involved in facilitating the money transfers. This may include banks, card networks, mobile operators, or other intermediaries that process or execute the payments. Nec Money Transfer may share this data to complete the transactions, to comply with the legal obligations or regulatory requirements in different jurisdictions, or to prevent fraud or money laundering.

https://www.bis.org/fsi/publ/insights33.pdf

• Nec Money Transfer may share personal data with government authorities or law enforcement agencies that request or require access to the data for legitimate purposes. This may include tax authorities, financial regulators, police forces, courts, or other public bodies that have legal powers to obtain the data. Nec Money Transfer may share this data to comply with the legal obligations or regulatory requirements in different jurisdictions, or to cooperate with investigations or enforcement actions.

https://edps.europa.eu/sites/edp/files/publication/14-11-25_financial_guidelines_en.pdf

• Nec Money Transfer may share personal data with third-party service providers that perform functions on behalf of Nec Money Transfer. This may include IT vendors, cloud providers, marketing agencies, auditors, consultants, or other contractors that support Nec Money Transfer's business operations. Nec Money Transfer may share this data to enable these service providers to perform their tasks effectively and efficiently.

https://edps.europa.eu/sites/edp/files/publication/14-11-25_financial_guidelines_en.pdf

Nec Money Transfer must ensure that it has a valid legal basis for collecting and sharing personal data in accordance with the UK Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR). The possible legal bases include consent from the data subjects (the individuals whose personal data is processed), contract performance (the processing is necessary for fulfilling a contract with the data subjects), legal obligation (the processing is necessary for complying with a legal duty), vital interest (the processing is necessary for protecting someone's life), public interest (the processing is necessary for performing a task in the public interest), or legitimate interest (the processing is necessary for pursuing a legitimate interest of Nec Money Transfer or a third party).

https://edps.europa.eu/sites/edp/files/publication/14-11-25_financial_guidelines_en.pdf

Nec Money Transfer must also ensure that it provides adequate safeguards for transferring personal data outside the EU in accordance with the UK Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR). The possible safeguards include adequacy decisions from the UK government or the European Commission (the transfer is made to a country that provides an adequate level of protection for personal data), standard contractual clauses (the transfer is made under a contract that contains specific clauses approved by the UK government or the European Commission), binding corporate rules (the transfer is made within a group of companies that have adopted common rules approved by the UK government or the European Commission), codes of conduct or certification mechanisms (the transfer is made under a code of conduct or a certification scheme approved by the UK government or the European Commission), or derogations for specific situations (the transfer is made under exceptional circumstances that justify the transfer).

https://edps.europa.eu/sites/edp/files/publication/14-11-25_financial_guidelines_en.pdf

## Lawful Bases for Data Processing

the lawful bases for processing are set out in Article 6 of the UK GDPR. There are six available lawful bases for processing. No single basis is better or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual. The six lawful bases are:

- Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

- Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

• Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

• Vital interests: the processing is necessary to protect someone's life.

• Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

• Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Most lawful bases require that processing is necessary for a specific purpose. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis. You must determine your lawful basis before you begin processing, and you should document it. You should also include information about both the purposes of the processing and the lawful basis for the processing in your privacy notice.

https://www.itgovernance.co.uk/blog/gdpr-lawful-bases-for-processing-with-examples

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/

## Access Requests

By law, people can ask you for a copy of any information that's to do with them. It might be saved on your system, but if it's about them, it's their personal data, and they have a right to see it. If they ask you for a copy of it, by phone, in person, or in writing, they have made a 'subject access request' (SAR), and you need to take following steps link below for more understanding:
https://ico.org.uk/for-organisations/sme-web-hub/how-to-deal-with-a-request-for-information-a-step-by-step-guide/

## Data Storing, Quality, Confidentiality and Security

Nec Money Transfer Limited follows the principles of data storage, which means that it aims to ensure that the personal data it holds is stored for as long as is necessary, considering the purposes for which it was collected and applicable legal storing periods.

Personal data quality, confidentiality and security are important aspects of data protection that Nec Money Transfer Limited strives to uphold. According to its privacy policy, the Company collects, processes, and transfers personal data of its customers and employees for various purposes, such as providing money transfer services, complying with legal obligations, and improving its products and services. The Company respects the rights and preferences of its data subjects and ensures that their personal data is treated in a fair and lawful manner.

The Company follows the principles of data quality, which means that it aims to ensure that the personal data it holds is accurate, complete, relevant, and up to date. The Company also implements appropriate security measures to protect the personal data from unauthorized access, disclosure, or loss. The Company uses encryption, authentication, access control, and other technical and organizational safeguards to prevent data breaches and ensure data integrity. The Company also monitors and audits its data processing activities to identify and address any risks or issues.

The Company also respects the confidentiality of the personal data it processes. Nec only collects and uses personal data for the purposes that it has informed the data subjects about or that are compatible with those purposes. Nec does not disclose or transfer personal data to third parties without a legitimate basis and sufficient protective measures. Nec also complies with the applicable laws and regulations regarding the transfer of personal data to countries outside the European Economic Area (EEA), such as using standard contractual clauses or adequacy decisions.

The Company is committed to maintaining a high level of personal data quality, confidentiality and security in accordance with its data protection manual https://necmoney.com/pdf-file/GDPR_Manual_Final_30_11_2022_002.pdfhttps://necmoney.com/pdf-file/GDPR_Manual_Final_30_11_2022_002.pdf and the relevant laws and regulations, such as the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The Company also provides adequate training and guidance for its employees, agents, and partners on how to handle personal data in a responsible and compliant manner. Nec also responds to any requests, complaints, or inquiries from its data subjects or supervisory authorities in a timely and cooperative way.

An employee who has access to personal data must only process the data in accordance with the purpose of the processing, and may not share, distribute, or otherwise disclose the personal data to a third party unless instructed to do so by Nec Money Transfer Limited.

Security breaches, which jeopardise the confidentiality or security of personal data processed by Nec Money Transfer should be reported immediately to a supervisor and the Risk Management officer.

## Notification of Data Processing Activities

Each company within NEC Money Transfer is obliged to notify its data processing activities to the applicable supervisory authority, unless an exception from the notification obligation applies.

If the data processing activities change, an assessment should be made as to whether notifications made to the applicable supervisory authority should be updated or amended.

## Penalties

Penalties to violate GDPR and the Data Protection Act 2018 in the UK are severe and can have a significant impact on the reputation and finances of any organisation that fails to comply with the data protection laws. There are two levels of fines that can be imposed by the supervisory authorities, such as the Information Commissioner's Office (ICO) in the UK, depending on the type and severity of the infringement:

- The lower level of fines can be up to £8.7 million or 2% of annual global turnover, whichever is higher, for infringements of articles such as those related to data security, data breach notification, data protection by design and default, data protection impact assessment, and records of processing activities.

- The higher level of fines can be up to £17.5 million or 4% of annual global turnover, whichever is higher, for infringements of articles such as those related to the data protection principles, the rights of data subjects, the lawful basis for processing, the transfer of personal data to third countries or international organisations, and the obligations of controllers and processors.

In addition to fines, the supervisory authorities can also take other actions against non-compliant organisations, such as issuing warnings and reprimands, imposing a temporary or permanent ban on data processing, ordering the rectification, restriction or erasure of data, and suspending data transfers to third countries.

Some examples of GDPR fines that have been issued so far in the UK and other EU countries. For instance:

- In July 2019, the ICO announced its intention to fine British Airways £183.39 million for a cyberattack that compromised the personal data of approximately 500,000 customers. https://www.lawtonslaw.co.uk/resources/data-protection-act-offences-and-penalties/

• In October 2019, the ICO announced its intention to fine Marriott International £99.2 million for a cyberattack that exposed the personal data of approximately 339 million guests worldwide. https://www.lawtonslaw.co.uk/resources/data-protection-act-offences-and-penalties/

• In January 2019, the French supervisory authority (CNIL) fined Google €50 million for lack of transparency, inadequate information and lack of valid consent regarding its ads personalization. https://www.itgovernance.co.uk/dpa-and-gdpr-penalties

• In December 2018, the Portuguese supervisory authority (CNPD) fined a hospital €400,000 for insufficient access controls and inadequate technical and organisational measures to protect patient data. https://www.itgovernance.co.uk/dpa-and-gdpr-penalties

These examples show that GDPR fines can vary widely depending on the nature, gravity and duration of the infringement, as well as other factors such as the degree of cooperation, remediation and prevention measures taken by the organisation.

## Do's and Don'ts

Personal data collection and processing are essential activities for Nec Money Transfer Limited to provide money transfer services, comply with legal obligations, and improve its products and services. However, these activities also involve certain risks and responsibilities that Nec must be aware of and address accordingly. To help Nec ensure that its personal data collection and processing are compliant, secure, and respectful of the rights and preferences of its data subjects, I have searched the web for some do's and don'ts regarding personal data collection and processing. Here are some of the main points that I found:

• Do: Identify a clear purpose and legal basis for your personal data collection and processing. You should know why you are collecting and processing personal data, what kind of personal data you need, how much personal data you need, how you will use and analyse the personal data, and what outcomes you expect from the personal data. Having a clear purpose and legal basis will help you align your personal data collection and processing with your business goals and avoid unnecessary or irrelevant personal data collection or processing.

• Don't: Collect or process personal data without informing the data subjects or obtaining their consent, unless there is another lawful justification. Data subjects have the right to be informed of your reasons for collecting and processing their personal data and of their data protection rights by way of a privacy notice. They also have the right to give or withdraw their consent for certain types of personal data processing, such as direct marketing or profiling. You should respect their rights and preferences and provide them with clear and easy ways to exercise them.

• Do: Implement appropriate security measures to protect your personal data from unauthorized access, disclosure, or loss. Personal data security is essential for ensuring personal data confidentiality, integrity,

and availability. You should use encryption, authentication, access control, and other technical and organizational safeguards to prevent personal data breaches and ensure personal data integrity. You should also monitor and audit your personal data collection and processing activities to identify and address any risks or issues.

• Don't: Disclose or transfer your personal data to third parties without a legitimate basis and sufficient protective measures. Personal data disclosure or transfer can expose your personal data to potential misuse or abuse by third parties who may not have the same level of security or compliance as you. You should only disclose or transfer your personal data when there is a lawful justification and enough protective measures in place, such as a data processing agreement, a consent form, or a privacy notice. You should also comply with the applicable laws and regulations regarding the transfer of personal data to countries outside the European Economic Area (EEA), such as using standard contractual clauses or adequacy decisions.

• Do: Provide information to individuals and respond to access requests regarding their personal data. If you are processing personal data of individuals, such as customers or employees, you should respect their rights and preferences regarding their personal data. You should inform them of your reasons for collecting and processing their personal data and of their data protection rights by way of a privacy notice. You should also respond to their requests to access, rectify, erase, restrict, or object to the processing of their personal data in a timely and cooperative.

• Don't: Keep or use personal data for longer than necessary or for purposes that are incompatible with those for which they were collected. Personal data retention and deletion are important aspects of personal data quality and minimisation. You should only keep or use personal data for as long as is necessary, considering the purposes for which they were collected and applicable legal retention periods. When the retention period of personal data has expired, you should erase them in a permanent and secure way.

## Reporting

Employees who suspect that a violation of this policy or of relevant data protection laws has occurred within Nec Money Transfer should contact the Data Protection officer.

## Training

Nec Money Transfer Limited provides adequate training for all employees consistent with Nec Money Transfer's risk profile and appropriate to employee responsibilities.

## Internal Audit

The Data Protection Officer is responsible for conducting objective, comprehensive audits of data protection, on a periodic basis.

## Contact Information of Responsible Officers

The CEO is responsible for the overall oversight and implementation of the Corporate Compliance Programme.

## Conclusion

The GDPR manual of Nec Money Transfer Limited is a document that explains how the company complies with the data protection laws and regulations in the EU and other countries where it operates. The manual covers the following topics:

Data protection is the process of safeguarding important information from corruption, compromise or loss. The GDPR is the toughest privacy and security law in the world, which imposes obligations onto organizations that target or collect data from people in the EU.

Nec Money Transfer Limited processes personal data daily, such as sender and receiver information, bank account details, mobile phone numbers, etc. Protecting customers' personal data is very important for the company to make it more practical for everyone.

The manual applies to everyone at all levels of Nec Money Transfer Limited, including their branches, agents, managers, executives, and all employees who may have access to data. The company has implemented various types of data security controls, such as authentication, access control, encryption, data masking, tokenisation, deletions and erasure.

The company has to document the legal basis and purpose of data processing, such as consent, contract, legitimate interest, public interest, etc. The company also has to inform data subjects about their rights and how to exercise them, such as right to access, right to rectification, right to erasure, right to object, etc.

The company has to establish procedures for responding to data subject requests and supervisory authority inquiries within the required time frames. The company also has to review and update contracts and agreements with third parties that process personal data on behalf of the company, such as payment network partners, agents, or recipients in third countries.

- The company has to conduct regular training and awareness programs for its staff and stakeholders on GDPR compliance and best practices.