Green Dot

Data Privacy Policy

Contents

1. Introduction 3
2. Purpose 3
3. Scope 3
4. Objective 3
5. Accountability and Management 4
6. Privacy Notice and Transparency 4
7. Choice and Consent 5
8. Collection of Personal Information 6
9. Data Minimization 7
10. Limiting Use, Disclosure and Retention 7
11. Data Subject Rights and Requests 7
12. Transfer Limitation 8
13. Disclosure to Third Parties 8
14. Security Practices for Privacy 9
15. Quality of Personal Information 9
16. Privacy Monitoring and Enforcement 10
17. Personally Identifiable Information (PII) of Green Dot employee 10
18. Staff data processing activities 10
19. Record Keeping (Privacy Register) 12
20. Retention of records 12
21. Data Privacy Impact Assessments (DPIA) 12
22. Data Flow Management 13
23. Monitoring 13
24. CCTV 13
25. Reporting Data Privacy Breach: 14
26. Glossary 14
27. Appendix A: Privacy Principles 16
28. Appendix B: Privacy Organization structure 17
29. Appendix C: Data Privacy Impact Assessment guidelines 20
30. Appendix D: Data breach response guidelines 22

Introduction

Green Dot and affiliated entities (here after "we", "our", "us", "the Company") endeavours to meet leading standards for data protection and privacy. This Privacy policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

While our reasons are founded in ethical and corporate responsibility, our privacy practices as outlined in this policy facilitate the establishment of the following:

- Good Corporate Citizenship: A sound privacy policy is emblematic of reliable corporate citizens that respect data subjects' privacy.
- Business Enablement: Since Green Dot uses adequate volumes of personal information, privacy notices become a prerequisite to building enduring business relationships.
- Legal Protection: Appropriate privacy notices offer an opportunity to eliminate allegations of unlawful usage of personal information.
- Comply with the General Data Protection Regulation (GDPR): failure to comply with the provisions of the GDPR may expose Green Dot to potential fines.

This document (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

1. Purpose

This Policy defines requirements to help ensure compliance with laws and regulations applicable to Green Dot collection, storage, use, transmission, disclosure to third parties and retention of Personal and special categories of personal data (also referred to as personal and sensitive personal information respectively in this policy).

2. Scope

This policy is applicable to all Green Dot employees, contractors, vendors, interns, customers, and business partners who may receive personal information from Green Dot, have access to personal information collected or processed by or on behalf of Green Dot, or who provide information to Green Dot.

This policy covers the treatment of personal information gathered and used by Green Dot for lawful business purposes. This policy also covers the personal information we share with authorized Third Parties or that Third Parties share with us.

3. Objective

The main objectives of the Data Privacy Policy are:

- To ensure that all of the personal information in Green Dot custody is adequately protected against threats to its security.

- To ensure that Green Dot employees are fully aware of the contractual, statutory or regulatory implications of any privacy breaches.
- To limit the use of personal information to identified business purposes for which it is collected.
- To create an awareness of privacy requirements to be an integral part of the day to day operation of every employee and ensure that all employees understand the importance of privacy practices and their responsibilities for maintaining privacy.
- To make all the employees aware about, the processes that need to be followed for collection, lawful usage, disclosure/ transfer, retention, archival and disposal of personal information.
- To ensure that all third parties collecting, storing and processing personal information on behalf of Green Dot provide adequate data protection.
- To ensure that applicable regulations and contracts regarding the maintenance of privacy protection in cross border transfer of personal information are adhered to.

4. Accountability and Management

4.1. A Data Privacy Policy shall be developed and maintained to document the privacy principles and practices followed by Green Dot. (Refer: **Appendix A** – Privacy principles)
4.2. A privacy organization shall be defined for governance of data privacy initiatives. (Refer: **Appendix B** – Privacy organization structure)
4.3. A Data Privacy Officer (DPO) shall be appointed (or DPO function) along with Privacy Coordinators, to process complaints and requests for information related to Green Dot privacy practices.
4.4. Implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects.
4.5. Establish procedures for the identification and classification of personal information.
4.6. The Green Dot Data Privacy Policy shall be communicated to Green Dot internal personnel.
4.7. Procedures shall be established for disciplinary and remedial action for violations of the Data Privacy Policy.
4.8. Changes or updates to the Data Privacy Policy shall be communicated to Green Dot internal personnel when the changes become effective.
4.9. Establish procedures for performing mandatory registration with regulatory bodies.
4.10. Risk Assessment is to be carried out on a periodic basis to ensure risks to personal information are identified and mitigated.
4.11. The potential impact on data privacy is assessed when new processes involving personal information are implemented, or when significant changes are made to such processes. (Refer: **Appendix C** – Privacy Impact Assessment guidelines)

5. Privacy Notice and Transparency

5.1. Appropriate notice shall be provided to data subjects at the time personal information is collected.
5.2. When Green Dot is the Data Controller for PII data it must provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

5.3. The privacy notice or policies and other statements to which they are linked shall provide as full information as is reasonable in the circumstances to inform an individual how their personal information will be used so that Green Dot use is fair and lawful. The following information should be considered for inclusion in a notice (as is appropriate in individual circumstances):

5.3.1. Purposes for which personal information is collected, used and disclosed;

5.3.2. Choices available to the individual regarding collection, use and disclosure of personal information, wherever applicable;

5.3.3. Period for which personal information shall be retained as per identified business purpose or as mandated by regulations, whichever is later;

5.3.4. That personal information shall only be collected for the identified purposes;

5.3.5. Methods employed for collection of personal information, including 'cookies' and other tracking techniques, and third-party agencies;

5.3.6. That an individual's personal information shall be disclosed to Third Parties only for identified lawful business purposes and with the consent of the individual, wherever possible;

5.3.7. That an individual's personal information may be transferred within Green Dot entities, globally as per requirement, for business purposes with adequate security measures required by law or as per guidance of provided by industry leading practices;

5.3.8. Consequences of withholding or withdrawing consent to the collection, use and disclosure of personal information for identified purposes;

5.3.9. Data subjects are responsible for providing Green Dot with accurate and complete personal information, and for contacting the entity if correction of such information is required;

5.3.10. Process for an individual to view and update their personal information records;

5.3.11. Process for an individual to register a complaint or grievance with regard to privacy practices at Green Dot;

5.3.12. Contact information of person in charge of privacy practises and responsible for privacy concerns with address at Green Dot;

5.3.13. Process for an individual to withdraw consent for the collection, use and disclosure of their personal information for identified purposes; and

5.3.14. That explicit consent is required to collect, use and disclose personal information, unless a law or regulation specifically requires or allows otherwise.

5.4. Data subjects shall be provided a Privacy Notice in case any new purpose is identified for using or disclosing personal information before such information is used for purposes not previously identified.

5.5. When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

6. Choice and Consent

6.1. A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

6.2. A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient.

6.3. If Consent is given in a document which deals with other matters, then the Consent must be explicit from those other matters.

6.4. A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured.

6.5. Consent may need to be refreshed if there is intention to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.6. Explicit Consent shall be obtained from data subjects at the time of collection of personal information or as soon as practical thereafter.

6.7. Explicit Consent shall be obtained from data subjects for the collection, use and disclosure of their personal information, unless a law or regulation specifically requires or allows otherwise. A record is maintained of explicit consent obtained from data subjects.

6.8. Consent shall be obtained from data subjects before their personal information is used for purposes not previously identified.

6.9. Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

6.10. Green Dot must maintain evidence on types of Consent and keep records of all Consents captured so that the Company can demonstrate compliance with Consent requirements.

6.11. Requests for consent should be designed to be appropriate to the age and capacity of the data subject to consent for themselves and to the particular circumstances (e.g. children who are not older than 16th, vulnerable data subjects unable to understand and consent for themselves).

6.12. Organisation should establish communication guidelines to notify other data controllers (with whom PII was shared) for rectification/deletion/restricting of personal data of data subject.

6.13. Organisation should document guidelines for managing directories of subscribers to electronic services which include the following:

- Guidelines for obtaining consent from the end users.
- What information is to be provided to the data subject at the time of data collection (e.g. purpose, search functions, right to object and information how personal data can be rectified or deleted).

7. Collection of Personal Information

7.1. The collection of personal information shall be limited to the minimum requirement for lawful business purposes.

7.2. The GDPR allows Processing for specific purposes, some of which are set out below:

a. The Data Subject has given his or her Consent;
b. The Processing is necessary for the performance of a contract with the Data Subject;
c. To meet our legal compliance obligations;
d. To protect the Data Subject's vital interests;

7.3. To pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing NoticesMethods of collecting personal information shall be reviewed by the DPO to ensure that personal information is obtained:

7.3.1. Fairly, without intimidation or deception, and

7.3.2. Lawfully, adhering to laws and regulations relating to the collection of personal information.

7.4. DPO shall confirm that Third Parties from whom personal information is collected:

7.4.1. Use fair and lawful information collection methods, and

7.4.2. Comply with the Green Dot Data Privacy Policy and their contractual obligations with respect to the collection, use and transfer of personal information on behalf of Green Dot

7.5. Data subjects shall be notified if additional information is developed or acquired about them.

8. Data Minimization

8.1. Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

9. Limiting Use, Disclosure and Retention

9.1. Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

9.2. Personal information retention shall be only for the duration necessary to fulfil the identified lawful business purposes or as prescribed by law.

9.3. Guidelines and procedures shall be developed for the retention and disposal of personal information. These shall address minimum and maximum retention periods, and modes of storage.

9.4. Upon the expiration of identified lawful business purposes or withdrawal of consent, Green Dot shall either securely erase or Anonymize the data subjects' personal information. Data is anonymized to prevent unique identification of an individual.

10. Data Subject Rights and Requests

10.1. The organisation should ensure that it has established the following:

10.1.1. Mechanism for data subjects to raise requests related to their rights (access/rectification) electronically (especially where personal data are processed by electronic means).

10.1.2. In relation to the right of access and rectification:

10.1.2.1. Documented process and mechanism for provisioning access to personal data and rectification.

10.1.2.2. Mandatory information to be provided to data subject

10.1.2.3. Guidelines for administrative fees which can only be charged to data subject for subsequent PI access.

10.1.2.4. Personal Data are provided in electronic form unless requested otherwise.

10.1.2.5. Tracking of the received requests from data subjects and appropriate response within 1 month.

10.1.3. Assessments are performed regularly – and at least annually – of whether the rectification of personal data has been performed correctly and without undue delay.

10.1.4. In relation to the right of deletion:

10.1.4.1. Policies and procedures to process/respond to PI deletion requests from data subjects within 1 month.
10.1.4.2. Documentation of the Personal data deletion guidelines considering the grounds for deletion and the applicable exceptions.
10.1.5. Guidelines for restrictions of data processing which address:
10.1.5.1. Documented grounds which are compared with criteria for restricting mentioned in the data subject request and a formal sign-off process to ensure that appropriate decisions are taken and implemented for a defined period of time.
10.1.5.2. Process to inform data subject prior to lifting the restriction of processing of personal data.
10.1.6. Implementation of a mechanism to inform data subjects about alteration, restriction of the processing of or removal of personal data.
10.1.7. Guidelines to process data portability requests from data subjects. The guidelines are compliant with data portability considerations.
10.1.8. Means for data subject to object online.

Refer to procedure "Data Subject Request Management" for further details, request form and response forms.

11. Transfer Limitation

11.1. Green Dot shall limit data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined
11.2. Green Dot may only transfer Personal Data outside the EEA if one of the following conditions applies:
(a) The European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
(c) The Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

12. Disclosure to Third Parties

12.1. Where reasonably possible, management shall ensure that third parties collecting, storing or processing personal information on behalf of Green Dot have:
12.1.1. Signed agreements to protect personal information consistent with Green Dot Data Privacy Policy and information security practices or implemented measures as prescribed by GDPR;
12.1.2. Signed non-disclosure agreements or confidentiality agreements which incorporate privacy clauses in the contract; and
12.1.3. Established procedures to meet the terms of their agreement with Green Dot to protect personal information.

12.2. Personal information may be transferred outside European Union (EU) for storage or processing purposes only in the following cases:
  12.2.1. The individual has given consent to the transfer of information
  12.2.2. The transfer is necessary for the performance of a contract between the individual and Green Dot, or the implementation of pre-contractual measures taken in response to the individual's request.
  12.2.3. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between Green Dot and a third party.
  12.2.4. The transfer is necessary or legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
  12.2.5. The transfer is required by law
  12.2.6. The transfer is necessary in order to protect the vital interests of the individual.
  12.2.7. The transfer is made under a data transfer agreement.
  12.2.8. The transfer is otherwise legitimised by applicable law.
12.3. Remedial action shall be taken in response to the misuse or unauthorized disclosure of personal information by a third party collecting, storing or processing personal information on behalf of Green Dot

13. Security Practices for Privacy

13.1. Green Dot information security policy and procedures shall be documented and implemented to ensure reasonable security for personal information collected, stored, used, transferred and disposed by Green Dot.
13.2. Green Dot shall comply with all applicable aspects of Green Dot Information Security and IT Governance Policy or comply with the administrative, physical and technical safeguards implemented and maintained in accordance with the GDPR and relevant standards to protect Personal Data.
13.3. Information asset labelling and handling guidelines shall include controls specific to the storage, retention and transfer of personal information.
13.4. Green Dot shall establish procedures that maintain the logical and physical security of personal information.
13.5. Green Dot shall establish procedures that ensure protection of personal information against accidental disclosure due to natural disasters and environmental hazards.
13.6. Incident response protocols are established and maintained in order to deal with incidents concerning personal data or privacy practices. (Refer: **Appendix D** – Data breach response guidelines)
13.7. Green Dot must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows: (a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

14. Quality of Personal Information

14.1. Green Dot may perform additional validation procedures to ensure that personal information collected is accurate and complete for the business purposes for which it is to be used.

14.2. Green Dot shall ensure that personal information collected is relevant to the business purposes for which it is to be used.

15. Privacy Monitoring and Enforcement

15.1. Procedures shall be established for recording and responding to complaints/ grievances registered by data subjects.
15.2. Each complaint regarding privacy practices registered by data subjects shall be validated, responses documented and communicated to the individual.
15.3. Annual privacy compliance review shall be performed for identified business processes and their supporting applications.
15.4. A record shall be maintained of non-compliances identified in the annual privacy reviews. Corrective and disciplinary measures shall be initiated and tracked to closure, guided by Green Dot management.
15.5. Procedures shall be established to monitor the effectiveness of controls for personal information and for ensuring corrective actions, as required.
15.6. Any conflicts or disagreements relating to the requirements under this policy or associated privacy practices shall be referred to the Data Privacy Officer for resolution.

16. Personally Identifiable Information (PII) of Green Dot employee

Data protection laws govern the use of personally identifiable information. This term means any data relating to a living individual who can be identified using that data. Green Dot may hold the following types of sensitive and non-sensitive PII:

- names, addresses, telephone numbers and other personal contact details;
- gender, date of birth, physical or mental health or condition;
- marital status, next of kin, racial or ethnic origin, sexual orientation, religious, philosophical, political or similar beliefs;
- national insurance or social insurance number, immigration status, trade union membership;
- personnel records including training, appraisal, performance and disciplinary information, and succession planning;
- bank details, salary, bonus, benefits and pension details and other financial information; and
- criminal offences committed (or allegedly committed) including any proceedings and sentencing in relation to any such criminal offence.

17. Staff data processing activities

Personal information about individuals may only be processed for a legitimate purpose. Green Dot may undertake a number of activities with an individual employee's personal information including, but not limited to:

- salary, benefits and pensions administration;
- health and safety records and management;
- security vetting, criminal records checks and clearances (where applicable and allowed by law);

- confirming information on résumés, CVs and covering letters, providing reference letters and performing reference checks;
- training and appraisal, including performance evaluation and disciplinary records;
- staff management and promotions;
- succession planning;
- equal opportunities monitoring;
- any potential change of control of a group company, or any potential transfer of employment relating to a business transfer or change of service provider;
- other disclosures required in the context of staff employment;
- promoting or marketing of Green Dot, its products or services;
- provision of staff or business contact information to customers and agencies in the course of the provision of Green Dot's services;
- CCTV monitoring for security reasons;
- compliance with applicable procedures, laws, regulations, including any related investigations to ensure compliance or of any potential breaches;
- establishing, exercising or defending Green Dot's legal rights;
- disclosures to other companies in the Green Dot group of companies, including companies in other countries to the extent permitted by law, including for the following purposes: as required in connection with the duties of the employee; legal compliance; audit; group level management; in connection with the fulfilment of customer and partner contracts;
- any other reasonable purposes in connection with an individual's employment or engagement by Green Dot;
- providing and managing use of services provided by third parties, such as company provided mobile phones, company credit cards and company cars and billing for such services.

17.1. Green Dot may also collect and process personal information about your next of kin so they can be contacted in an emergency or in connection with use of a company car provided by Green Dot. Their personal information will also be processed in accordance with the data protection laws and as described in the policy.

17.2. In order to fulfil the purposes set out above, Green Dot may disclose personal information to contractors and suppliers that provide services to Green Dot and who may assist in the processing activities set out above and also to law enforcement agencies, regulatory bodies, government agencies and other third parties as required by law or for administration/taxation purposes, to the extent local law allows and requires.

17.3. Green Dot may disclose your personal information to third parties for the purposes of establishing and managing your employment relationship. For example, Green Dot may disclose some of your personal information to:

- benefits providers (for example, pension and insurance providers);
- payroll and data processing suppliers and other service providers who assist us in establishing or managing your employment relationship with us;
- insurance claims and medical related service providers; and
- parties requesting an employment reference.

17.4. Green Dot shall take appropriate measures to ensure that its contractors and suppliers also process personal information in a compliant way and such measures may include a data processing agreement.

17.5. Green Dot may transfer personal information to other group companies, partners, suppliers, law enforcement agencies and to other organisations that are located outside of the country where you are based for the purposes of:

- HR administration (for example, staff recruitment);
- payroll processing for employees working outside the country where they are based;

- employee relocation;
- security clearances;
- visa applications;
- taxation and registrations for employees working outside the country where they are based;
- fulfilling Green Dot's legal requirements;
- fulfilling customer contracts for the provision of Green Dot's services;
- overseas legal proceedings;
- outsourcing Green Dot functions.

17.6. The laws of some jurisdictions may not be as protective as the laws in the country in which you are based. Green Dot may transfer your personal information across provincial or national borders to fulfil any of the above purposes, including to service providers located in countries who may be subject to applicable disclosure laws in those jurisdictions, which may result in that information becoming accessible to law enforcement and national security authorities of those jurisdictions.

18. Record Keeping (Privacy Register)

18.1. Green Dot shall keep full and accurate records of all data Processing activities.

18.2. Green Dot must keep and maintain accurate corporate records reflecting Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

18.3. These records should include, at a minimum, the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

19. Retention of records

19.1. Green Dot has a statutory duty to keep certain records for a minimum period of time. In other cases Green Dot shall not keep personal information for longer than is necessary or as may be required by applicable law.

20. Data Privacy Impact Assessments (DPIA)

20.1. The organisation should conduct Data Privacy Impact Assessment (DPIA) for its business activities for which the processing of personal data is "likely to result in a high risk to the rights and freedoms of natural persons". A DPIA is a process designed to describe the processing, assess its necessity and proportionality, and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.

20.2. The firm should assess all its business processes and define which of them are high-risk. For the purpose of the assessment it should use appropriate risk criteria to help on the factual identification of high-risk business processes. (ie. criteria as set in the Article 29 of GDPR PIA evaluation).

20.3. The organisation should choose a methodology for the implementation of its DPIAs. The DPIA should be compliant with the minimum features described in Annex 2 in Article 29 of GDPR on performing DPIA.

20.4. The company should continuously review and re-assess its business activities as certain changes could increase or decrease their risk.

21. Data Flow Management
    21.1. For all high-risk business procedures as defined in the 'Data Privacy Impact Assessment'
    21.2. Organisation should define guidelines for data mapping. Data mapping addresses below mentioned:
    21.3. Documenting the data processing activities.
    21.4. Type of personal data used for each processing activity along with personal data storage location.
    21.5. The organisation should identify and document data flows specific to how personal information is moving through the underlying systems and software within the organization (including third party operations).

22. Monitoring

    22.1. Green Dot IT and communications systems are intended to promote effective communication and working practices within our organisation.
    22.2. For business reasons, and in order to carry out legal obligations in our role as an employer, use of Green Dot systems on whatever platform including the telephone (mobile and fixed) and computer systems (including email and internet access), and any personal use of them, is monitored. If you access services by the use of passwords and login names on Green Dot IT and communication systems this might mean that your personal access details are seen by Green Dot.
    22.3. Monitoring is only carried out if and to the extent permitted or as required by law and as necessary and justifiable for business purposes. The resulting log files may be used so that instances of attempted misuse and other security events can be detected and that information is available to support any subsequent investigation. To the extent permitted by law and, where breaches of this and other Green Dot policies or applicable law are found, action may be taken under the disciplinary procedure.
    22.4. The employees are informed that the telephone system used by the Company allows identification of all dialled numbers and received calls.
    22.5. Green Dot reserves the right to retrieve the contents of messages, check searches which have been made on the internet, require the immediate return of devices supplied by Green Dot and access data stored on such devices for the following purposes (this list is not exhaustive):
        - to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy (and employees acknowledge that the Company can use software to monitor the identity of senders and receivers of emails);
        - to find lost messages or to retrieve messages lost due to computer failure;
        - to assist in the investigation of wrongful acts; or
        - to comply with any legal obligation.
    22.6. If evidence of misuse of Green Dot IT systems is found, Green Dot may undertake a more detailed investigation in accordance with Green Dot disciplinary procedures, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the disciplinary procedure. If necessary such information may be handed to the police in connection with a criminal investigation. Investigations and disclosure of information to the relevant authorities shall be carried out only to the extent permitted by law.

23. CCTV

23.1. Some of Green Dot's buildings and sites use CCTV systems to monitor their exterior and interior 24 hours a day for security reasons. This data is recorded. Use of CCTV and recording of CCTV data is only carried in accordance with Green Dot approved guidelines.
23.2. Green Dot shall take reasonable efforts to alert the individual that the area is under electronic surveillance.

24. Reporting Data Privacy Breach:
24.1. The GDPR requires Data Controllers to notify any Personal Data Breach to the Cyprus Data Protection regulatory authority and, in certain instances, the Data Subject.
24.2. Green Dot shall put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where is legally required to do so.
24.3. Where there is a suspicion of a Personal Data Breach occurrence, the DPO, the information technology or security department should be notified immediately and should follow the Green Dot Data Breach Management Procedure. All evidence relating to the potential Personal Data Breach should be preserved.

25. Glossary

Term	Definition
Anonymize	To process a collection of personal data or information such that a natural person cannot be identified on the basis of the output collection of data or information
Data subject	A living individual about whom personal information is processed by or on behalf of Green Dot
Personal Identifiable Information (PII)	PII refers to the combination of personal data that identify a specific individual
Data Controller	The 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; where the purposes and means of such processing are determined by Union or Member State law.
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Vulnerable data subject	A Data subject that may be over the age of 16 however do not have the competence to understand and consent for themselves
“Green Dot”, “we”, “our”, “us”, “the Company”	Green Dot / its Subsidiaries / its Group Companies / its affiliates, its directors, employees (excluding the User/affirming employee in this context), assigns and successors.
Information security	Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Personal Data or personal information	Any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person

Sensitive personal data or sensitive personal information	Sensitive personal data means personal data consisting of information as to: 1) the racial or ethnic origin of the data subject, 2) his political opinions, 3) his religious beliefs or other beliefs of a similar nature, 4) whether he is a member of a trade union, 5) his physical or mental health or condition, 6) his sexual life, 7) the commission or alleged commission by him of any offence, or 8) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
Third party	All external parties – including without limitation contractors, interns, summer trainees, vendors, service providers and partners – who have access to Green Dot information assets, information systems or who are pass personal information from them.

26. Appendix A: Privacy Principles

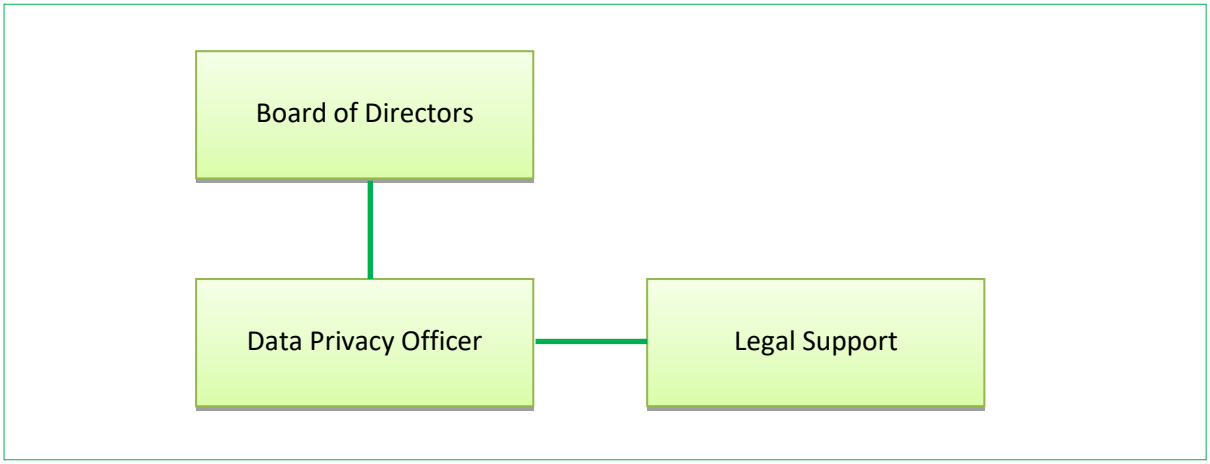
Green Dot Data Privacy Policy aligns with Generally Accepted Privacy Principles. In view of the changing legislative and technological environment for data privacy, the Data Privacy Policy will undergo revisions. The guiding privacy principles articulated in this policy document are as follows:

- Management:
  Define, document, communicate, and assign accountability for Green Dot Data Privacy policy and procedures
- Notice:
  Provide notice about Green Dot Data Privacy policy and procedures and identify the purposes for which personal information is collected, used, retained, and disclosed
- Choice and Consent:
  Describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information
- Collection of personal information:
  Collect personal information only for the purposes identified in the notice
- Limiting Use, Disclosure and Retention:
  Limit the use, storage and retention of personal information to the purposes identified in the data privacy notice and for which the individual has provided implicit or explicit consent. Retain personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately dispose of such information
- Access for review and update:
  Provide data subjects with access to their personal information for review and update
- Disclosure to third parties:
  Disclose personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual
- Security practices for privacy:
  Protect personal information against unauthorized access (both physical and logical)
- Quality of personal information:
  Maintain accurate, complete, and relevant personal information for the purposes identified in the notice
- Monitoring and enforcement:
  Monitor compliance with Green Dot Data Privacy policy and procedures, and have procedures to address privacy related complaints and disputes

27. Appendix B: Privacy Organization structure

The privacy organization has been designed keeping in mind the various business units across locations where Green Dot operates. Stakeholders, and oversight from key business functions and senior leadership, provides sustainable and practical guidance for the privacy framework.

27.1. Privacy organization structure



27.2. Board of Directors

The role of the Board of Directors is to channel resources and address organizational issues related to privacy.

Responsibilities of Board of Directors:

- Review and approve the Data Privacy Policy at least on an annual basis.
- Establish a process for the enforcement of Data Privacy Policy.
- Ensure the implementation of a data privacy program that enables compliance with the Data Privacy Policy and applicable regulations with respect to data protection.
- Define processes to address grievances and handling complaints from data subjects with respect to their personal information held by Green Dot.
- Determine the action to be taken against grievances and information request cases presented by the Data Protection Officer.
- Review the findings from periodic privacy compliance reviews and sanction the implementation of corrective actions if applicable.
- Ensure that privacy impact assessments and measures to address privacy risks are aligned with the enterprise risk management framework.
- Monitor the data privacy program effectiveness.
- Identify and appoint a Data Privacy Officer.
- Ensure that the Data Protection Officer receives all support necessary in order for him/her to perform the tasks as determined in the GDPR and does not perform other tasks or has other duties which may result in a conflict of interest with the tasks and duties of the DPO.

27.3. Legal Support

The role of the Legal Support is to guide and monitor the data privacy program and present timely reports to the Board

Responsibilities of Legal Support:

- Provide legal assistance to the Data Privacy Officer for identifying applicable regulations relations related to data privacy.

27.4. Data Privacy Officer

The role of Data Privacy Officer (DPO) is to act as a central authority for the implementation and enforcement of Green Dot privacy program. The DPO is required to advocate for the privacy program, articulate and communicate the organization's privacy goals, and lead enforcement of the Data Privacy Policy. To achieve this, the appointed DPO should have the organizational credibility to facilitate decision making and resource allocation. DPO's contact details should be communicated to public and supervisory authority.

Responsibilities of Data Privacy Officer:

- Develop and maintain the Data Privacy Policy.
- Conduct annual review of the Data Privacy Policy and recommend changes or policy updates to the Board.
- Ensure compliance with the Data Privacy Policy and associated privacy practices.
- Facilitate privacy awareness training for all employees of Green Dot. The privacy awareness training should be designed with the following considerations:
    - Providing briefings, information and resources for employees to keep them apprised of current and emerging privacy requirements;
    - Providing employees with adequate guidance on identifying and appropriately handling data protection issues that may affect the performance of their job; and
    - Sensitizing employees to the importance of data privacy to data subjects and the organization.
- Establish contact with appropriate professional bodies, supervisory authorities and governmental agencies related to data protection and privacy.
- Ensure that appropriate certification of the privacy practices is obtained and maintained.
- Support the employees on Data Privacy Policy and organizational issues.
- Provide counsel relating to privacy aspects of business contracts and partnerships.
- Facilitate periodic privacy compliance reviews.
- Establish procedures for disciplinary and remedial actions for Data Privacy Policy violations.
- Ensure that privacy impact assessments are undertaken to understand the risks to privacy raised by new or modified products, services, facilities, technologies and business processes, and to mitigate those risks.
- Ensure that an inventory is developed and maintained for personal information in Green Dot.
- Provide inputs for privacy risk mitigation strategies.
- Define and communicate the privacy data breach response plan.
- Coordinate with the offices of governmental agencies and supervisory authorities during the investigation of a privacy complaint against the organization.
- Handle requests for information made by individuals and third-party agencies (including law enforcement agencies).
- Participate in audits
- Liaising with works councils in countries where consent to process is conditional upon clearance from such bodies
- Overseeing the operation of company whistleblowing schemes and policies.

- Implement processes to address grievances and handling complaints from data subjects with respect to their personal information held by Green Dot.
- Respond to requests for access to and correction of personal information and general issues concerning personal information held by Green Dot.
- Maintain a record of all grievances and inquires registered by data subjects.
- Collate all grievances and information requests along with relevant and share with DPO and present with relevant details to the Board for exceptions to established response processes

28. Appendix C: Data Privacy Impact Assessment guidelines

A Data Privacy Impact Assessment (DPIA) can be used to demonstrate that the system owners and functional management have applied data privacy controls throughout the system development lifecycle. In addition, performing a DPIA for proposed changes identifies any conflicts between the post-implementation state and the privacy framework. For example, the DPIA prior to introducing a new business application will identify if the way personal information is shared by the new application is in violation of the Data Privacy Policy.

A DPIA should be triggered by events that significantly change the privacy environment of the company or if an existing process which significantly affects the privacy rights of data subjects is identified. For example, the introduction of new technology may change the manner in which personal information is stored and processed. In some cases, the technology may only collect personally identifiable information for a moment. For example, a security camera stream may capture the movements of an individual. While a record may not be maintained for later use, the initial capture and viewing may raise privacy concerns and a DPIA could be required. Other instances of technology with privacy implications include: systems utilizing radio frequency identification devices (RFID), biometric scans, data mining, or location tracking.

In other cases, the technology may not be changing, but a program or system opts to use data from a new source such as a commercial aggregator of information. A DPIA is required when such new sources of information are used.

The introduction of a new business process and notable changes to existing business processes may trigger a DPIA for various reasons. New business processes may introduce new uses of personal information, new information systems and infrastructure supporting the changed processes, and new methods of collection, processing and disclosure. Some new business processes may require updates to agreements and contracts, potentially impacting the management of personal information.

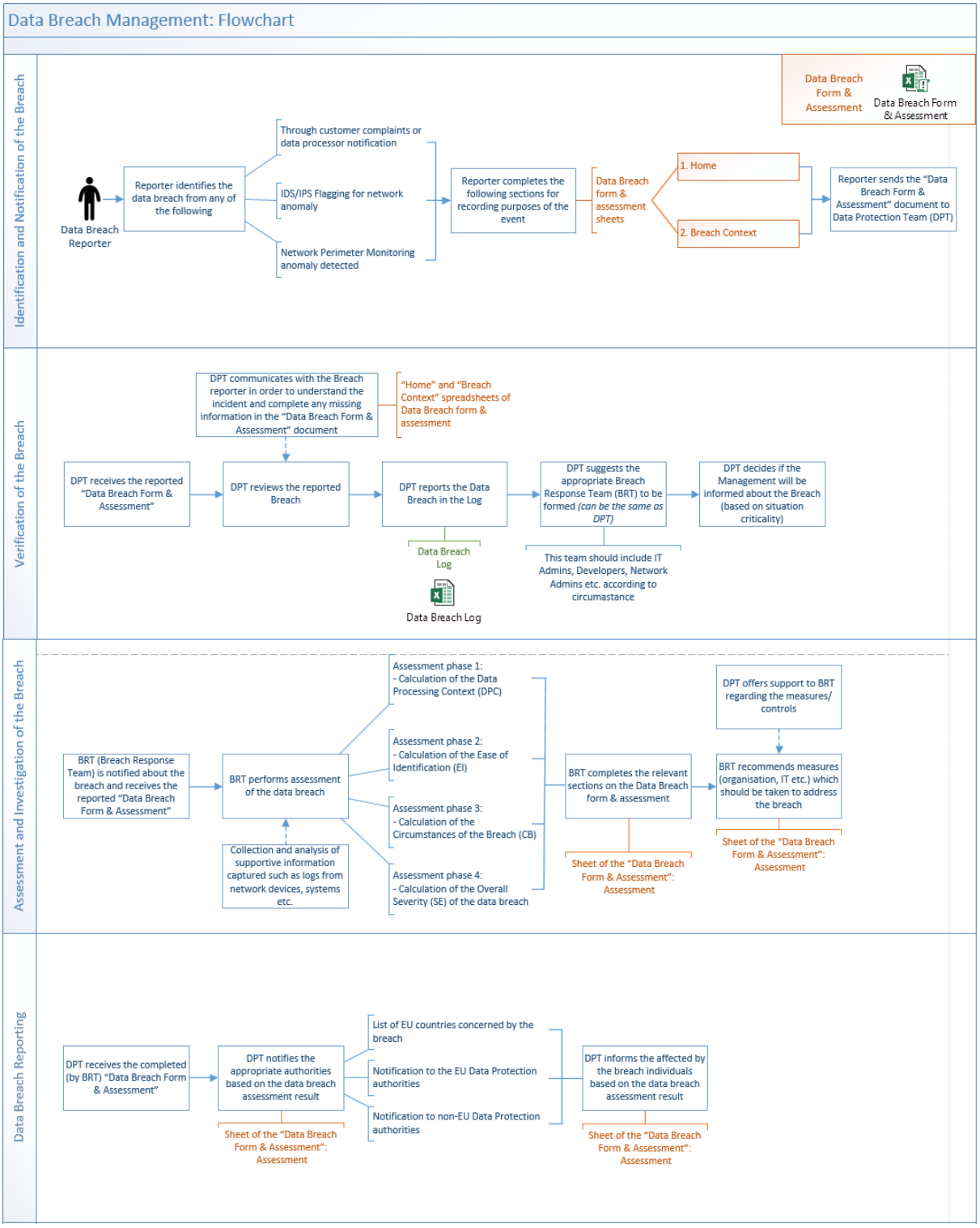
At minimum, the following triggers should be considered:

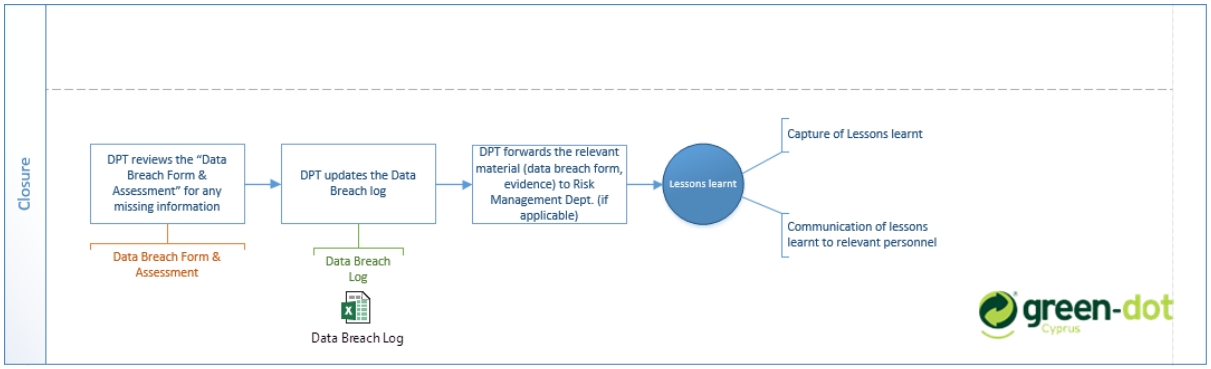
PIA Trigger	**Description**
Digitization of records	Converting paper-based records to electronic systems.
Anonymous to Non-Anonymous	Operations performed on existing personal information database changes anonymous information into Sensitive Personal Information (SPI) or personal information (PII).
Significant System Management Changes	New uses of existing IT systems, including application of new technologies, significantly changes how SPI or PII is managed in the system. For example, when the company employs new relational database technologies or web-based processing to access multiple data stores, such additions could create a more open environment and avenues for exposure of data that previously did not exist.
Significant Merging	The company adopts or alters business processes so that databases holding PII are merged, centralized, matched with other databases or otherwise significantly manipulated. For example, when databases are merged to create one central source of information, such a link may aggregate data in ways that create privacy concerns not previously an issue.
New User Access Mechanism	User-authentication technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by users (including Third Party users).

PIA Trigger	Description
External Sources	The company systematically incorporates into existing information systems, databases of personally identifiable information purchased or obtained from third parties or public sources. An exception to this trigger would be merely querying such a source on an ad hoc basis using existing technology.
New Uses	Business partners work together on initiatives involving significant new uses or exchanges of information in identifiable form, such as marketing for products and solutions developed as joint ventures. In such cases, the Green Dot Data Privacy Officer should be consulted and prepare the DPIA.
Internal Flow or Collection	Alteration of a business process that results in significant new uses or disclosures of information, including incorporation into the system of additional PII.
Alteration in Character of Data	New PII is added to a database or information collection and thus, raises the risks to personal privacy. For example, the addition of health or financial information may lead to additional privacy concerns that otherwise would not arise.
New Processes	Introduction of new business process that results in multiple triggers and changes to business agreements impacting management of personal information.

29. Appendix D: Data breach response guidelines

The immediate response upon discovery of a data breach leading to compromise of personal information records should align with the information security incident response plan. This document provides guidelines on the procedural steps to be taken at minimum:





Refer to procedure "Data Breach Management" for detailed steps, data breach form and assessment methodology.