Data Protection Policy

01 December 2020

Metadata

Review

Accountable Director	CTO
Policy Author	CTO
Date Approved	Apr 2019
Date Last Reviewed	Aug 2021
Date of Next Review	Mar 2022

Document history

Version	Date	Author	Description
1	Apr 2019	CTO	Intitial Version
2	May 2020	CTO	Add Metadata section
3	Aug 2020	CTO	Add section ”Responding to SARs as a data processor”
4	Dec 2020	CTO	Add further detail to points in section 4

Contents

1 Policy governance

This policy is the responsibility of PassFort's data protection officer (DPO). The DPO's responsibilities include:

- Ensuring this policy remains up to date
- Ensuring this policy is implemented effectively
- Training our staff and conducting internal audits
- Cooperating with supervisory authorities
- Raising & reporting any breaches of compliance

This policy is also intended to make clear to PassFort's leaders & staff what their data protection responsibilities entail:

- All staff must:
    - ensure that they understand their responsibilities as they relate to this policy
    - ensure that they act in compliance with this policy
- PassFort's leaders are responsible for:
    - ensuring their teams comply with this policy
    - reporting any breach of this policy
    - ensuring their teams have appropriate knowledge and training in relation to this document
- Training our staff and conducting internal audits
- Cooperating with supervisory authorities
- Raising & reporting any breaches of compliance

2 Scope

2.1 What is the purpose of this policy?

This policy articulates PassFort's approach to data protection. It provides details of the approach that PassFort takes in ensuring that it is treating its customers and data subjects fairly.

PassFort is committed to maintaining the rights of data subjects. PassFort is committed to collect, manage and store data on its customers and data subjects in a transparent manner. PassFort will ensures that data is safe, protected and liable to cause no detriment to customers or data subjects.

PassFort understands the importance of designing its products and services in such a way that ensures its customers and data subjects privacy is assured and that they are 'private by default'.

PassFort also understands the importance of ensuring data subjects and customers have effective access to their data and can easily and simply request their data be amended or erased where incorrect or inappropriately collected, managed or stored.

The outcome that this policy is designed to foster is the safe, transparent and effective collection, management and storage of data to ensure the risk of customer and/or data subject detriment is minimised in all PassFort's services, products and activities.

This policy also provides details of how PassFort assures and monitors its data protection activities to ensure it is delivering positive customer outcomes and meeting the Information Commissioner's Office (ICO) and other related regulatory standards.

This policy is based on the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), as amended from time to time. It builds specifically on the eight data principles listed in the DPA and the GDPR.

2.2 What does this policy cover?

This policy applies to everyone who works at PassFort, including full-time employees, part-time employees, consultants, business partners and contractors (staff). This also applies to any suppliers to PassFort.

This policy applies to all geographies that PassFort operates within.

This policy applies to all functional areas within PassFort, including operations, technology, sales, marketing, people, legal & finance.

The key stakeholders of the organisation impacted by this policy are:

- Data subjects
- The board and senior management
- All staff working at PassFort
- The DPO

2.3 What does this policy not cover?

This policy does not cover the following aspects which are covered in other policies and should be read in conjunction with this policy:

- Information security policies
- Product design policies
- Sales and marketing policies

3 Policy statement

This data protection policy is a key reference document for the PassFort staff and key stakeholders.

Collecting, managing and storing personal data in a transparent, safe and effective manner is of real importance to PassFort.

PassFort wishes to ensure that it is effectively collecting and protecting customer and data subject data in a manner that minimises the risk of detriment to those parties.

PassFort wishes to ensure that its staff and key stakeholders have access to this policy and have read and understood its contents and requirements. This is important to PassFort as it expects all its stakeholders to comply with the policy and its guidelines.

PassFort is committed to developing effective data protection processes and procedures to enact the ethos and standards contained within this policy.

PassFort is committed to ensuring that its staff and key stakeholders are appropriately informed of and trained in the data protection activities associated with this policy.

PassFort is committed to identifying, reporting and remediating any significant breaches to this policy to the DPO, the board and any external regulators as detailed in the guidelines within this policy.

PassFort will not tolerate a failure to abide by this policy and will take management action against those who fail to follow this policy and its guidelines.

4 Policy standards

The PassFort data protection policy has the following key policy standards.

4.1 Governance

PassFort commits to put in place effective governance arrangements to ensure the management of data protection activities. These include:

- **Board discussion:** discussion of PassFort data protection activities at board on a quarterly basis
- **Data protection officer:** PassFort has appointed a data protection officer and has established their reporting arrangements in line with the GDPR requirements - specifically they are able to report directly to the Board with independence. They are required to report on compliance with GDPR regulation to the board. They are also required to reporting to ICO following a significant breach, within the timeframe specified by the GDPR.
- **Data protection policy & processes:** The development of and approval by the Board of a PassFort data protection policy and associated processes that comply with the GDPR

4.2 New staff (general)

PassFort commits to provide new staff and stakeholders who are not directly handling personal data with access to the data protection policy and associated training within one week of joining the firm.

4.3 Existing staff (general)

PassFort commits to provide existing staff and stakeholders who are not directly handling personal data with access to the data protection policy and associated recap training annually.

4.4 New staff (data handlers)

PassFort commits to provide new staff and stakeholders who are directly handling personal data with access to the data protection policy and associated training before they handle any client

data.

4.5 Data protection impact assessments

Where there is a possibility that PassFort will be engaging in a potentially high risk data processing activity (see GDPR guidelines) then PassFort commits to undertake a data protection impact assessment (DPIA).

4.6 Lawful basis

PassFort also commits to reviewing, approving and documenting its 'lawful basis' for collecting data prior to collecting or processing new data sets.

4.7 Purpose

PassFort commits to only using the data it collects from data subjects for the purpose(s) it was collected or any other purpose specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data, or as soon as possible thereafter. Further consent will be sought if the data is to be used in a different manner.

Furthermore, we will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

4.8 Rights

PassFort commits to respecting the rights of individuals in relation to the protection of their data as detailed in the GDPR and including:

- **The right to be informed:** PassFort, when collecting data, commits to inform individuals of the following:
  - The firm's identity
  - How the firm will use the information
  - The lawful basis under which the data is being collected
  - The types of third parties, if any, with which we will share or to which we will disclose that personal data

- The means, if any, with which data subjects can limit our use and disclosure of their personal data
- If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter
- That we are the data controller with regard to that data and who the Data Protection Officer is
- The duration the data will be retained for
- The individuals' right to and process for complaining to ICO

- **The right of access:**
  - Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to their line manager or the Data Protection Officer immediately.
  - When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:
  - We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
  - We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked. Our employees will refer a request to their line manager or the Data Protection Officer for assistance in difficult situations. Employees should not be bullied into disclosing personal information.
  - PassFort commits to respond to subject access requests:
    * Within 1 week of receiving a request
    * Without charge unless the request is manifestly unfounded or excessive
    * Without refusal unless a clear and compelling reason for the refusal can be provided and details of the process for complaining are provided with the refusal.
- **The right to rectification:** PassFort commits to rectify any errant information within 1 month of it being acknowledged as errant by PassFort
- **The right to erasure:** PassFort commits to erase any unwarranted information that it holds within 1 month of it being acknowledged as unwarranted by PassFort
- **The right to restrict processing:** PassFort commits to restrict the processing of any information within 1 month of it being acknowledged as necessary to do so by PassFort
- **The right to data portability:** PassFort commits to provide requested personal data in a structured commonly used and 'machine readable' form
- **The right to object:** PassFort commits to ensure that all individuals are provided with details

about how to register a complaint with ICO at the time a complaint is raised

- **Rights in relation to automated decision making and profiling:** PassFort commits to ensure that individuals' data is not used to make automated decisions or complete individual profiling without explicit consent.
- **The right to prevent the processing of their data for direct-marketing purposes.**
- **The right to prevent processing that is likely to cause damage or distress to themselves or anyone else.**

When acting as a data processor, PassFort commits to supporting data controllers in meeting their obligations as defined in the GDPR.

4.9 Consent

PassFort commits to ensure that all data is collected with appropriate consent. Specifically that when data is collected the consent obtained is:

- specific and granular in nature
- clearly articulated in plain English
- prominent within the collection process and documentation
- requires the individual giving consent to opt-in
- properly documented and stored
- easily withdrawn
- not gained from children under the age of 16 without the consent of a parent or guardian

4.10 Duration

PassFort commits to keeping its data in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

4.11 Quality

PassFort commits to keep its data accurate and up to date and will take reasonable steps to ensure that personal data that is inaccurate with regard to the purposes for which it is processed, is erased or rectified within 1 month of being recognised as such.

4.12 Information security

PassFort commits to ensure the appropriate security of the personal data it collects, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by using appropriate technical or organisational measures.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on central computer systems instead of individual PCs.

Security procedures include:

- **Entry controls:** Any stranger seen in entry-controlled areas should be reported.
- **Secure lockable desks and cupboards:** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal:** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
- **Equipment:** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- **Clear desk policy:** All employees need to remove any sensitive or confidential information from their workspace both when not at the workspace, and at the end of each day.
- **Clear screen policy:** All employees are required to lock their computers when leaving their workspace. Additionally, all computers are controlled with screen time out and require password settings.

4.13 International data

PassFort commits to the guidelines provided in GDPR and the DPA with regard to sharing data internationally and recognises that the level of protection afforded by GDPR must not be undermined if any personal data is transferred outside of the European Union.

We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The data subject has given his consent.
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements outlined above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

4.14 Disclosure and Sharing

We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

We may also disclose personal data we hold to third parties:

- In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.
- If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

- If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

4.15 Responding to SARs as a Data Processor

Due to the nature of PassFort's business, PassFort occasionally receives SARs where it is a "processor" rather than "controller" (as defined within the GDPR) of the data requested. In these cases, PassFort commits to:

- Supporting the requester with identifying the controller of their data. This might require the collection of specific information from the requester to positively identify them. For individuals we require as standard a full name, date of birth and current address.
- Providing the requester with contact information to the data controller.
- Supporting the data controller in meeting their obligations under the GDPR.

All correspondence relating to the above should happen over email or via letter, to support a fully auditable paper trail.

5 Policy controls and processes

5.1 Monitoring structure

It is the responsibility of the first line of defence to ensure that it is enacting and following the policy guidelines and meeting the policy standards.

It is also the responsibility of the first line of defence to raise and report any breaches to the operation or application of the policy to the DPO and the board.

To support the first line of defence the data compliance team (the second line of defence) will carry out additional monitoring activities on both a scheduled and unscheduled basis:

The scheduled monitoring will take place on a half yearly basis as detailed in the data compliance monitoring plan and will review the performance of the first line of defence

The unscheduled monitoring is likely to be triggered by a specific incident (e.g. a specific breach) and will review and assess compliance with any relevant aspects of the data protection policy or process.

5.2 Reporting procedures

PassFort takes very seriously the reporting of management information in relation to the carrying out of its data protection activities. In particular it is very aware of the need to and is committed to reporting significant breaches of the regulations to ICO as soon as is possible after the breach has come to the attention of the DPO, the CEO or the board. The standards for reporting data breaches are contained within PassFort's breach management policy and associated guidelines and procedures.

PassFort also acknowledges that on occasions it may also need to inform data subjects if they are impacted by a data breach and that PassFort is committed to ensuring it has the procedures in place to be able to carry this out if required.

PassFort expects a half yearly written report from the data compliance team detailing the risks and issues generated by the monitoring it has completed in relation to PassFort's data protection activities. This is in addition to the normal flow of management information.

5.3 Policy communication and training

This data protection policy is stored at the PassFort HQ and on the PassFort intranet. It can be accessed directly by all key stakeholders.

In addition to the initial post-recruitment training provided by the People Team to all staff and the additional training provided to those staff handling data, PassFort commits to provide annual refresher training in data protection for all its staff and further commits to keep key stakeholders informed of (and if necessary trained in) any changes made to the data protection policy.

The data compliance team will be asked to provide evidence on the quality and coverage of the requisite training as part of its reports to the board.

6 Policy review and update process

6.1 When do we make changes?

Broadly there are two categories of event which will trigger a review of this policy.

Standard triggers:

- We review this policy on an annual basis
- In response to changes in our business

Emergency triggers:

- In response to an incident – if we identify a major issue (either through monitoring or in response to a breach)
- In response to regulatory change

7. Definitions and glossary

7 Key Terms

List of the key technical terms used within the policy document and a simple explanation of their meaning:

Controller: A person or an organisation who determines the purposes and means of the processing of personal data. The processing may be carried out jointly or in common with other persons.

Data protection impact assessment (DPIA): The assessment required to be carried out by the organisation if its planned data collection/processing activity carries an inflated risk of detriment to customers or data subjects. See GDPR legislation for specific risk triggers.

Data protection officer: An individual who has responsibility for informing and advising the firm and its employees about their obligations to comply with the GDPR and other data protection requirements; monitoring compliance with the GDPR; and acting as the first point of contact for supervisory authorities.

Data services: Services related to the collection, management, processing or storing of data.

Data subject: An identified, or identifiable natural person to whom data collected, stored or processed refers.

First line of defence: A term that derives from the three lines of defence model where the first line of defence is the business, the second is the compliance function and the third is the audit function and board.

Information security policies: The specific policies that relate directly to the securing and storage of data by the organisation.

Policy: This specific data protection policy.

Processor: A person or an organisation who processes data on behalf of the controller.

Personal data: Information relating to an identified or identifiable person (data subject). An identifiable person is one who can be identified directly or indirectly in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

Special categories of personal data: Article 9 of the GDPR sets out special categories of personal data. The processing of such personal data (which includes a) racial or ethnic origin; b) political opinions; c) religious or philosophical beliefs; and d) trade union membership) is prohibited, except where the data subject has given their explicit consent. There are other select circumstances.