DATA SECURITY POLICY

DATA FOR ALL

Document last Updated on 27.05.2024

Introduction

DFA compiles and uses aggregated, anonymous statistical data to strengthen planning and monitoring across the development sector. This policy describes how DFA ensures that this data is collected, handled, and stored in full compliance with data protection standards.

Why this policy exists

This data protection policy ensures DFA:

- Complies with data protection law and follows good practices
- Protects the rights of institutions and the community
- Is transparent about how the system stores and processes data
- Protects itself from the risks of a data breach

Data protection law

Most countries have data security policies that describe how statistics are to be calculated, managed, stored, and distributed.

These policies apply regardless of whether data is stored electronically, on paper or on other media.

People, risks, and responsibilities

Policy scope

This policy applies to:

- All authorized users involved in the DFA initiative;
- All staff, contractors, volunteers, and other people working on behalf of DFA.

Data protection risks

This policy helps to protect DFA from some data security risks, including:

- Breaches of confidentiality. For instance, information is being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the data are used relating to them.
- Reputational damage. For instance, DFA could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with DFA has the responsibility of ensuring data is collected, stored, and handled appropriately. Each team that handles data must comply with these policies and data protection principles.

Furthermore, people with these DFA roles have key areas of responsibility:

- The DFA Steering Committee is ultimately responsible for ensuring that DFA meets its data security legal obligations.
- The DFA Data Security Officer is responsible for:
    - Keeping the DFA initiative updated about data protection responsibilities, risks, and issues;

    - Reviewing all data protection procedures and related policies, in line with an agreed schedule;
    - Arranging data protection training and advice for the people covered by this policy;
    - Handling data protection questions from staff and anyone else covered by this policy;
    - Responding to requests from individuals to see any data DFA holds about them (also called 'subject access requests');
    - Checking and approving any contracts or agreements with third parties that may handle DFA data.
- The DFA IT Director is responsible for:
    - Ensuring all systems, services, and equipment used for storing data meet acceptable security standards;
    - Performing regular checks and scans to ensure security hardware and software are functioning properly;
    - Evaluating the data security compliance of any third-party services that DFA may use to store or process data, such as cloud computing services;
    - Approving any data protection statements attached to communications, such as emails and letters;
    - Addressing any data protection queries from journalists or media outlets, like newspapers;
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Guidelines

- The only people authorized to access data covered by this policy are those who need the data to carry out their official DFA responsibilities.
- Data should not be shared informally. When access to confidential information is required, authorized users must request approval in writing from their line managers.
- All people handling DFA data need to understand their responsibilities when handling the data.
- All people authorized to access DFA data must ensure that all data are secure, by taking appropriate precautions and following the guidelines herein:
    - In particular, strong passwords must be used and should never be shared.
    - Personal data should not be disclosed to unauthorized people, either within the DFA team or externally.
    - Data should be regularly reviewed and updated if out of date. If no longer required, the data should be deleted and disposed of.
    - Anyone using DFA data should request help from their line manager if they are unsure about any aspect of data security and protection.

Data access

This policy provides guidance on who, how, and what type of data should be accessed:

- The only people authorized to access DFA data covered by this policy are those who require the data to carry out their approved roles and responsibilities;
- DFA data always remains the property of the client and is not authorized for use for any reason without the written consent of the client;
- Access to DFA data is only allowed via approved APIs. Direct access to DFA databases is only authorized to system administrators with the approved roles and responsibilities for managing the backend of the system.

Data storage

These rules describe how and where data must be safely stored. Questions about storing data safely should be directed to the IT director.

When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it. These guidelines also apply to data that are usually stored electronically but have been printed out for any reason.

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared with others.
- If data is stored on removable media (like a CD-ROM or USB drive), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded on approved cloud computing services.
- Servers containing personal data should be situated in a secure location, away from general office space.
- Data should be backed up frequently and securely stored. These backups should be tested regularly, in line with the DFA standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

There is a significant data security risk when DFA data are accessed and used. During this time, there is the greatest risk of loss, corruption, or theft:

- When working with personal data, authorized users should ensure the screens of their computers are always locked when left unattended;
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure;
- Data must be encrypted before being transferred electronically; the IT director can explain how to send data to authorized external contacts;
- Authorized users should not save copies of DFA data to their own computers; – always access and update the centralized instance of the database.

Data Accuracy

The DFA initiative takes reasonable steps to ensure data is kept accurate and up-to-date.

- Data is stored in as few places as necessary and authorized users do not create any unnecessary additional data sets;
- Data is updated as inaccuracies are discovered, and, if no longer required, the data will be removed from the database.

Subject access requests

All individuals who may be the subject of data held by DFA are entitled to:

- Ask what information DFA holds about them and why;
- Ask how to gain access to it;
- Be informed on how to keep it up-to-date;
- Be informed how DFA is meeting its data protection obligations.

If an individual contacts DFA requesting this information, this is called a subject access request. These requests must be made in writing. The identity of anyone making a subject access request will need to be verified and approved before providing any information.

Disclosing data for other reasons

In certain circumstances, laws allow DFA data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, DFA will disclose requested data. However, the DFA team will ensure the request is legitimate, seeking assistance from management and legal advisers when necessary.

Providing information

The DFA initiative aims to ensure that individuals are aware of how data are being processed, and that they understand:

- How the data is being used;
- How to exercise their rights.