Davka Group Data Protection Policy

Introduction

The Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (PECR) - (March 2019 update) and the United Kingdom Data Protection Regulation (UK GDPR) - hereafter known as Data Protection Legislation, are part of UK law which determines the legal use of personal information and data. This legislation is binding on all UK entities including The Davka Group.

The Data Protection Legislation comprehensively details the requirements and safeguards which must be applied to personal data to ensure the rights and freedoms of living individuals are not compromised.

Personal data is defined as any type of information that can be used to identify or can be linked to an identified living person (data subject). Information to identify a living person is not limited to names and contact details, and part or incomplete information, if it could be collected together with other information to lead to identification, constitutes personal data.

In the UK, Data Protection Legislation is upheld by the Information Commissioners Office (ICO) as the Data Protection Authority. This policy is subordinate in all instances to the Data Protection Legislation as guided by the ICO.

The Davka Group (DG) is a data controller as defined by the ICO as an organisation which determines the purposes and means of the processing of personal data. DG generally also processes data, which it is data controller for. From time-to-time DG may act as a data processor for a third-party organisation.

This policy applies equally and where relevant on all data held as the data processor, however there should be due referral to relevant data sharing agreements in place to apply further requirements of assurance from the data controller.

DG needs to collect and use different types of information about people with whom it engages in operational relationships and associations in order to carry out its purpose and objectives. These include current, past and prospective employees, directors, contractors, suppliers, partners and other service users, and other customers and stakeholders.

There are 6 lawful bases for processing data. At least one of these **must always** apply when data is being processed and DG must process data under a predetermined basis governed by this policy.

- Consent
- Contract
- Legal Obligation
- Vital Interests
- Public Task
- Legitimate Interest

DG will use the lawful basis of Legitimate Interest to process data where legitimate interest can be shown to occur in compliance with ICO guidance. DG will not assume legitimate interest is appropriate for all of its data processing and will use the lawful basis of Consent for all of its processing as default where legitimate interest is inappropriate or indeterminable.

Data protection legislation stipulates that those who record, use and have access to personal information must be transparent about how the information is used and must follow approved data handling processes. It applies to the collection, use, disclosure, retention, access, accuracy, erasure and destruction of data.

It is the obligation of DG, as a data controller and processor, to ensure full compatibility, consistency and compliance with data protection legislation. This policy applies to all personal data held by or on behalf of DG and includes manual/paper records and personal data that is electronically processed by computer systems or other means such as CCTV systems.

Purpose

- To provide a framework for DG to apply all relevant aspects of data protection legislation to its activities. Data protection legislation identifies specific rights in relation to data protection, these are codified in this policy and covered in more detail in the section headed individual rights. Accordingly, this policy must be considered in conjunction with the following additional documents.

    a. Legitimate Interest Assessments (LIA)
    b. Data Breach and Incident Reporting Procedure
    c. Data Protection Impact Assessments (DPIA)
    d. Records Retention Schedule
    e. Privacy Notice (Right to be Informed)
    f. IT Usage and Security Policy
    g. Data Sharing Agreements
    h. Relevant guides on data processing
    i. CCTV Code of Practice

- Communicate the policy of DG with regard to all activities involving the collection, sharing, use and retention of data, and ensure all relevant staff are aware of the policy and refer to it in all instances.
- Comply with the law in respect of the data DG holds about individuals.
- Protect DG's beneficiaries and other service users (partners), customers, donors, staff and other individuals.
- Provide guidance on managing and protecting the organisation from consequences of a breach of its responsibilities.
- Follow best practice.
- Implement all duties in respect of the data protection legislation and ensure that all its relevant external stakeholders understand and can implement all the requirements of data protection legislation.

- Underpin any operational processes and procedures connected with the principles of the legislation.

Scope

This policy will apply to anyone collecting, accessing or using personal information whilst acting on behalf of DG or operating as a representative or associate of DG.
DG requires that all third parties acting as Data Processors will comply with the terms of this data protection policy and other related policies and information.

Application of the Policy

DG is committed to ensuring this policy is upheld and embedded within the organisation. To that effect, DG will:

- Incorporate data protection by design and default into all of its operations.
- Process data using the lawful basis of legitimate interest. This does not preclude the processing of data by any other lawful method however must be considered as the primary requirement for processing.
- Apply a legitimate interest assessment (LIA) to all business areas where data is collected, used and retained where legitimate interest is used as the basis for processing to formally Identify the legitimate Interest.
- Show processing is necessary.
- Show balance with individual's rights.
- Assign responsibility to every staff member involved in processing data to ensure there is a relevant LIA completed and authorised before processing any data.
- Consider an opt-out at every practicable opportunity.
- Obtain consent for electronic marketing purposes and anything which might not reasonably be expected under our legitimate interests.
- Apply and comply with conditions regarding the fair collection and use of personal information.
- Meet our legal obligations to specify the purpose for which information is used and the basis under which it is processed.
- Collect and process appropriate information restricted to the extent that it is needed to fulfil operational needs or to comply with legal requirements.
- Document our data processing.
- Ensure the quality and accuracy of any data and information used.
- Apply robust methodology to ensure retention thresholds are complied with.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred outside of the UK without suitable safeguards and regulatory compliance.
- Ensure that the rights of people about whom the information is held can be fully exercised under the legislation.
- Name a person with specific responsibility for data protection in the organisation known as the Data Protection Compliance Officer.
- Provide everyone managing and handling personal information appropriate up to date training, clear instructions and appropriate supervisions.

- Clearly communicate to relevant stakeholders to ensure contractual responsibilities for following good data protection practice are fully understood.
- Ensure that methods of handling personal information are regularly assessed and evaluated.
- Ensure that guidance is in place for robust governance of sharing data with Partners and third parties.
- Demonstrate compliance.

Data Protection Principles

There are seven Data Protection Principles with which DG shall comply. In summary, these are that personal data will be:

- Processed fairly and lawfully in a transparent way.
- Obtained only for specified lawful purposes and not further processed in a manner incompatible with that purpose.
- Adequate, relevant and limited to what is necessary.
- Accurate and where necessary, kept up to date.
- Not be kept for longer than is necessary.
- Protected by appropriate technical and organisational controls.
- Processed in a way with appropriate measures and records to demonstrate accountability.

Application of Principles

DG will apply these principles in accordance with this policy. Specifically, DG will ensure that all data is processed on the authority of a relevant and legitimate LIA and provide access to its privacy notice at all points of collecting data, and grant access to other policies on request.

DG will ensure that data is stored digitally in accordance with its IT policy including system controls to prevent the downloading and storage of information and data to unencrypted removable and transferrable media devices, as well as enforcing prohibition on the use of these devices. All DG computers will require dual factor authentication (DFA) to access DG systems and all data contained on these devices will be password protected and encrypted.

DG will apply and abide by the rights granted to individuals by data protection regulation.

DG will seek to obtain consent for the purposes of electronic marketing in accordance with PECR even where a legitimate interest can be demonstrated.

Individuals Rights

Data protection legislation has introduced a set of rights for individuals. These are summarised below as well as the policy DG has adopted in each case.

The Right to be Informed

DG will provide concise, transparent, intelligible and easily accessible information at the point of collecting personal data which will ensure anybody we are collecting data from will be aware of the scope, purpose and retention of their data.

- Provision of privacy information at the time of collecting data.
- Name and contact details of our organisation.
- Contact details of our DPCO.
- The purposes of processing of personal data.
- The lawful basis for processing of the data.
- The legitimate interest for the processing.
- The categories of personal data obtained.
- The categories of recipients of personal data.
- Details of transfers to international organisations.
- Retention periods for the data.
- Individual rights in respect of processing.
- The right to withdraw consent.
- The right to complain to the ICO.
- The source of the personal data.
- The details of whether individuals are under statutory or contractual obligation to provide their data.
- The existence of automated decision-making, including profiling.

DG will update and monitor this policy in line with ICO guidance on the right to be informed as found here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UKGDPR/individual-rights/right-to-be-informed/

The Right of Access

Any person whose details are collected, processed and held by DG has a general right to receive on request a copy of their own information. DG recognises that there may be some exceptions to this rule, such as data held on safeguarding.

- All Subject Access Requests (SAR) are logged, acknowledged within a reasonable timeframe of the request being made and fully responded to normally within 1 month.
- All requests are coordinated by the DPCO.
- Appropriate identification of a requesting individual is always obtained.
- DG will issue a standard form for receiving SARs however recognises all requests whether the form is used or not.

DG will follow the ICO guidance on handling SARs which can be found here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UKGDPR/individual-rights/right-of-access/?q=privacy+notices

The Right of Rectification

An individual has the right to have their data rectified if it is inaccurate or incomplete.

- All requests are logged, acknowledged within a reasonable timeframe of the request being made and fully responded to normally within 1 month.

- All requests are coordinated by the DPCO.
- Appropriate identification of a requesting individual is always obtained.
- Inform third parties we have shared our data with so that they can rectify what they hold.
- If asked, inform the requester who we have shared their data with.
- DG recognises all requests whether verbally or in writing.

DG will follow the ICO guidance on handling requests for rectification which can be found here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UKGDPR/individual-rights/right-to-rectification/?q=privacy+notices

The Right to Erasure

This is also known as the right to be forgotten and is the basis against which any request by the data subject to remove all or part of any data on the data subject is considered.

The reasons to erase may be as follows:

- Where the data is no longer necessary in relation to the purpose it was collected for.
- It is being unlawfully processed.
- The individual withdraws consent.
- It must be erased to meet a legal obligation.
- The individual objects to the processing and there is no overriding legitimate interest.

DG retains the right to override any requests made under the right to erasure where the legitimate interests of DG justify the override.

- All requests are logged, acknowledged within a reasonable timeframe of the request being made and fully responded to normally within 1 month.
- DG recognises all requests whether verbally or in writing.
- All requests are coordinated by the DPCO.
- Where data has been shared DG will inform the recipient of the erasure.
- If asked, inform the requester who we have shared their data with.

DG will follow the ICO guidance on handling requests for erasure which can be found here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UKGDPR/individual-rights/right-to-erasure/

The Right to Restrict Processing

This is effectively an alternative to the right to erasure where a data subject may request that their data is restricted in use. Data may be processed in the authorised way but on granting this right, may only be used according to the restrictions.
This right may also be exercised to extend the retention of data under certain circumstances.

The right applies when a request is made under the following conditions:

- There is a question over data accuracy, or a request is received to rectify data.

- Data has been processed unlawfully where erasure is not requested.
- There is an objection to lawful data processing while legitimate grounds are considered.
- Data may be required for future legal reasons.
- DG will ensure all requests are logged, acknowledged within a reasonable timeframe of the request being made and fully responded to normally within 1 month.
- Inform third parties we have shared our data with so that they can apply the same restriction on what they hold.
- If asked, inform the requester who we have shared their data with.

DG will follow the ICO guidance on handling requests to restrict processing which can be found here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UKGDPR/individual-rights/right-to-restrict-processing/

DG will automatically restrict the processing of data where it receives a request for erasure, request for rectification, request for restriction or any objection to processing for the duration of the time given to consider each request, which is normally one month.

The Right to Data Portability

This is a right which allows people to obtain and reuse their data for their own purposes. It allows them to move, copy or transfer personal data from one IT system to another securely. It applies to:

- Data provided by the subject where it is based on consent or in performance of a contract and;
- If carried out by automated means.

DG currently doesn't operate a system of capturing data compatible with the requirements to comply with requests under the rights of data portability. In any event of compatibility, DG will apply ICO guidance on data portability as found here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UKGDPR/individual-rights/right-to-data-portability/

The Right to Object

An individual can object to the processing of their data where it is processed for the following:

- Our legitimate interest of lawfully processing.
- Public interest or exercise of official authority.
- Direct marketing.
- Purposes of scientific/historical research and statistics.

DG will stop processing data as soon as practicable on receiving an objection unless we have compelling legitimate grounds by which to override the objection.

- The Right to Object will be made clear to all individuals from whom DG will collect and process data. This includes CCTV and other image capturing.

- All requests are logged, acknowledged within a reasonable timeframe of the request being made and fully responded to normally within 1 month.
- All requests are responded to by the DPCO.

DG will follow the ICO guidance on handling objections which can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UKGDPR/individual-rights/right-to-object/

Rights related to automated decision making including profiling

An individual has the right to not be the subject of a decision if it is based on automated processing and it produces a legal or similar impact on the subject.

DG currently does not operate any decision making or profiling by ways of automated software. This policy will be reviewed periodically, and data protection legislation relevantly applied in any instances where the above requires updating.

In any eventuality, DG will follow the ICO guidance on handling requests to grant the right related to automated decision-making including profiling which can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UKGDPR/individual-rights/rights-related-to-automated-decision-making-including-profiling/

Rights of Employees

Rights of employees as data subjects are upheld as per other data subjects. HR data may be considered special category data and is subject to its own retention schedule.
All staff who have access to employee data must abide by this policy in relation to that data and ensure that DG has the controls in place to ensure the privacy of its employees is upheld to the highest standard.

Data Incidents and Breaches

The Davka Group holds a large and varied amount of data which includes personal and special category data and information.

- DG commits to ensuring that every care is taken to avoid a data breach by protecting personal information and following authorised processes to avoid the breach of any data.
- In the unlikely event of a data breach, DG will always ensure that appropriate action is taken to mitigate any repercussions, minimise any associated risk, and comply with data protection legislation requirements around reporting of the breach within the timescales stipulated.
- DG has incorporated into this policy its approach to Data Incident Reporting which covers the process of recognition, reporting, recording and escalation of all data incidents without exception.
- All data incidents are ultimately the responsibility of DG as an organisation however DG will apply its disciplinary policy proportionately in all instances of data incident or breach.

- This part of the policy must be considered in conjunction with the Data Breach and Incident Reporting Procedure.

Recognition of Data Breach

A data incident is any incident where data, be it personal or otherwise is involved. A data incident does not automatically indicate a breach. DG recognises a data breach where a data incident occurs which is systematically evaluated in seriousness and impact to be a breach.

A data breach is the descriptive term used for a data incident where the following might occur-

- Any private/confidential information or data controlled by DG where that control is lost as an intentional or unintentional release to an untrusted environment.
- Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to protected data.
- Any action taken by DG or its employees and associates which is not compatible or compliant with data protection legislation such as where data is processed or held contrary to general ICO guidance.
- Unauthorised cross-departmental access to data, especially special category data.
- An identified weakness in the controls in place to prevent loss of data or actions where any part of this policy on data protection is not adhered to or complied with or any activity occurs not in good faith of DG's policies, guidance and information.
- Any event, or risk of event which results in perceived or actual damage to an individual's rights and freedoms, where data is a factor in the event.
- A data breach also refers to any non-compliance with data protection regulation and for the purpose of this policy is not restricted to events which are likely to cause damage to an individual.
- A breach will generally be attributed only to data that DG is either the data controller of, or data that it is in the power of DG to be disclosed.
- Data received by DG from external organisations which is in appearance a breach of ICO rules on lawful processing is dealt with in the Breaches by Other Organisations section.
- Any processes designed to communicate, embed, report and monitor data protection at DG are not followed appropriately.

Detecting a Data Breach

Data is processed by a number of different departments and staff at DG. Generally, it is the responsibility and duty of all staff employed by DG to be aware of this policy and their individual responsibilities under this policy. This includes understanding a duty for reporting a data incident or where there is perceived risk of an incident or breach occurring and by following the Data Breach and Incident Reporting Procedure.

This applies to perceived actions of others but also a requirement for self-reporting.
On detection of an incident, immediate appropriate action must be taken to mitigate or remedy the situation by whoever detects it.

Reporting of Data Breach

Any member of staff who is party to identifying a potential or actual data incident must refer to and comply with the procedures on Data Breach and Incident Reporting. In all instances the following will apply.

- All incidences must be reported to an appropriate line manager and the DPCO or their delegated person.
- Incidences can be reported through the designated channels as stated in the Whistleblowing.
- The manager must ensure the incident is contained.
- All incidences involving data are assumed to be a data incident.
- All data incidences are assumed to be a data breach until fully evaluated.
- An individual observing (discovering or committing) an incident will not be responsible for evaluating the incident.
- An individual observing an incident is critically and personally responsible for reporting the incident as soon as they are aware of it.
- All data incidences are reported to the DPCO using the authorised Incident Reporting Form, and in person or by phone directly to the DPCO.
- All data incidences are evaluated by the Data Protection Compliance Officer which includes conducting a full risk assessment.
- All data incidents involving special category data, specifically those which relate or might relate to safeguarding must always be notified to the safeguarding lead officer as per the safeguarding.
- The DPCO holds responsibility for escalating an incident.

Investigating a Data Incident or Breach

All data incidents and breaches will be subject to proportional investigation. This investigation will be co-ordinated the DPCO in conjunction or collaboration with management of any relevant or involved departments or parties.

In all instances the investigation must be overseen by an appropriate senior manager who will be the investigating manager. This requirement will be advised on by the DPCO in all instances.

All evidence and findings will be recorded and held by the DPCO.
Any lessons learnt from the investigation in relation to any individuals involved will be the responsibility of an appropriate line manager to implement supported by the DPCO.

The investigation into the breach is a separate investigation to that of the involved individual's conduct.

The investigation of the circumstances of a breach should always lead to documented learning from the incident and positive change to ensure the risk of a similar incident occurring is mitigated.

Recording of Data Breach

All data incidences are recorded appropriately by the DPCO. The record will include a description of the nature of the personal data breach including:

- The categories and number of individuals concerned.
- The categories and number of personal data records concerned.
- The name and contact details of the investigating manager and other individuals involved and a report of their investigation.
- Data Incident Reporting Form.
- Assessment of seriousness of breach.
- A description of the likely consequences of the data incident.
- A description of the measures taken, or proposed to be taken, to deal with the data incident.
- The measures taken to mitigate any possible adverse effects.
- Details on escalation or other actions.
- Confirmation that the data subject has been informed of the ongoing right to complain to the ICO.
- Final outcome, process/policy changes and learning.

Assessment and Escalation of Data Incidents

Assessment & escalation of data incidents refers to the reporting requirements for certain types of breach to the ICO, Data Controllers where we are the Data Processor, and to the Data Subjects involved.

All incidents go through an assessment process to determine level of seriousness which then determines the level of escalation required. This is detailed in the Data Breach and Incident Reporting procedure and will comply with ICO guidelines.
The assessment will be carried out with due attention to:

- Whether any control has been lost over personal data.
- The potential harm or risks to the data subject as a result of the incident, including any distress the data subject may suffer as a result of the incident.
- The impact of the breach in relation to-
    - Limitations of an individual's rights & freedoms
    - Discrimination against an individual
    - Identity theft or fraud
    - Financial loss
    - Damage to reputation
    - Loss of confidentiality
    - Volume
    - Sensitivity
    - Severity of any other consequences

As data processor, DG is required to report any breach as soon as it is aware of the breach, regardless of the impact and risk, to the relevant data controller.

- Informing the ICO.
- Informing the affected individual (data subject).

- The decision on the escalation of any data breaches ultimately rests with the Head of the Organisation (CEO) or in their absence the Director of Finance and Resources (DFR), or Directors, under the advice of the DPCO.
- DG will not report any incidences to the ICO, data subjects or data controllers without the express permission and/or knowledge of the CEO, DFR and/or Directors.
- In any even an incident in escalated to the ICO, the CEO or DFR must inform the Chair or Deputy Chair of Directors as soon as practicable.

All escalations will be co-ordinated and conducted by the DPCO strictly in line with ICO requirements, timelines and guidelines found here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UKGDPR/personal-data-breaches/

As far as is reasonable, DG will err on the side of caution in deciding whether to report breaches.

Breaches by Other Organisations

This section refers to

- Data controlled by DG that is shared with an authorised data processor where the data processor has disclosed that data unlawfully or experienced any kind of breach.
- Data received by DG from a third-party organisation or individual which appears in breach of data protection legislation.
- Where a data processor processing data on behalf of DG has a breach, it is their legal responsibility to report it to DG as soon as they become aware. All processors must have clear breach reporting requirements written into a data sharing agreement. DG is thereafter responsible for treating the breach in accordance with this policy. The processor takes no responsibility for reporting or escalating the breach to the ICO.
- DG does not recognise any legal obligation towards data received which appears in breach of data protection legislation, however, will take limited action depending on the circumstances.

Examples might be:

- Data or information including Special Category Data is received by the wrong person.
- Unprotected information is received.
- Shared or generic mailboxes receive unprotected data.
- Information received is excessive to requirements.
- Where data is received by DG from a third-party data controller which appears inconsistent with data protection legislation, the following applies.
- The incident is to be considered a data incident.
- The incident must be reported following the Data Breach and Incident Reporting procedure.
- The recipient must not respond unless under the instruction of the DPCO.

Third party complaints to the ICO

In the event of a complaint being made to the ICO in regard to how DG is processing data, this complaint will be investigated by the DPCO, and a response provided under the authority of the CEO.

Sharing Data

The sharing of data specifically means where DG, as the data controller holding data for a legitimate interest, allows access to that data by either an external individual or organisation, or internal departments or members of staff who may or may not be part of the legitimate interest.

Information can only be shared where DG has a recognised and approved legitimate interest, or where that legitimate interest is not sufficient, by an appropriate lawful basis, ordinarily consent.

Consent can only be granted by the data subject or by somebody acting on their behalf in a legal capacity. Consent cannot be granted by DG as the data controller, nor by anybody else regardless of their trusted status with the data subject's data.
Where DG shares data, DG remains the data controller whilst the recipient is the data processor. For data to be transferred between the two, there must **always** be a data sharing agreement in place.

Examples of where DG may share data include:

- Data returns to funders & government departments or agencies.
- Shared information with beneficiaries or health authorities.
- Sharing data with Local Authorities.
- Internal cross-departmental sharing.

Disclosures permitted by law

- Data sharing for safeguarding purposes.
- Requests by the police or other enforcement agencies.
- DG will always seek a written request confirming the reason for the disclosure where consent has not been obtained and will evaluate that request before responding.

The sharing of data must comply with the LIA for the processing and be in line with ICT policy of secure document sharing. Where practicable or available this must be by authorised secure means such as a secure file sharing system.
Data that is authorised to be shared must-

- In an authorised format and route.
- Only be sent to a confirmed designated and authorised recipient.
- In a protected format, physical or password.
- Never sent in the same communication as the method of accessing the data.

Circumstances where data cannot be shared.

- Where it is sent to a personal mailbox belong to a staff member.
- Where it is sent to a family member or other associate of a staff member.
- Using a generic email address of an organisation or DG.

- Cannot be sent in a secure way.
- Using unsecured WiFi or other networks when off premises.

Data sharing agreements.

Any sharing of personal information between DG and other organisations will be subject to an information sharing protocol that commits the partners to an agreed data transfer process that meets the requirements of Data Protection legislation.

Any data sharing agreements entered into must be approved by the DPCO prior to the information being shared. Data Protection Impact Assessments will be carried out whenever there are projects, new or changed service activities, or new ICT that could potentially impact on the privacy of individuals. The results of assessments will be conducted by and reported on by the DPCO to the project lead and other relevant staff.

Document Retention & Deletion

This part of the policy must be considered in conjunction with the Document Retention Schedule.

DG will hold a clear schedule identifying all data processes and show the intended retention for every processed data. DG will complete a legitimate interest assessment for each data stream it processes including an identification of the retention requirements and intention.

It is the responsibility of all staff members processing data to ensure that the LIA for that data includes information on the retention of that data. Data must not be processed unless there is a clear retention period available. The retention will be determined by the periodical and time-based question, do we need this data? If yes, this might be due to:

- Regulatory or legislative reasons.
- Public interest, archives, scientific or historical research.
- Statistical purposes.
- Operational reasons.
- Confirmation of existence of a relationship

There are 2 basic rules DG will follow:

- That we can justify the retention period internally.
- We can explain the retention period externally.

Where there is no fair and lawful basis for retaining data, it must be either deleted or anonymised securely and completely.

Definitions

Data Controller

The Davka Group is the data controller and is fully responsible for ensuring compliance with the legislation.

Data Processor

A data processor is the person or organisation who process personal data which has been shared with them legitimately by a data controller. A data processor does not own the data and cannot use it for purposes other than stated in the contract or where a legal gateway exists. Any use or sharing of data should not be done without the written consent of the data controller.

For the most part, DG is the data controller and the data processor.

Data Controller/Processor Relationship

Where the controller and processor are not the same i.e. The Davka Group and a partner organisation, the relationship must be underpinned by a contract including a data sharing agreement. This contract must include detailed schedules of the data to be processed as well as the clauses regarding the arrangements for the use, storage, retention and deletion of data by that external party. All contracts must be reviewed by the DPCO to ensure that they meet requirements. The contract between DG and the processor will make plain the liabilities and duties arising from data protection legislation that the processor must comply with.

Personal Information

Personal information is defined as information relating to a living individual who can be identified directly or indirectly from that information. It may also be possible to identify an individual from that and other information which is in the possession of, or likely to come into the possession of DG. It also includes any expression of opinion about the individual and any indication of the intentions of DG or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the information held and partly on other information (not necessarily data), the information held will still be personal.

Special Category Data

This is data identified as being more sensitive therefore requiring more protection. In general, any data which could create a greater risk to a person's fundamental rights and freedom is considered special category. For example-

- Race
- Ethnic Origin
- Politics
- Religion
- Trade Union Membership
- Genetics
- Biometrics
- Health
- Sex Life
- Sexual Orientation

In addition, any data which if compromised could cause undue significant harm to an individual should be treated in the same way.

- Criminal Records
- Financial Information
- Disciplinary Information

It is important to emphasise that special category data is identified as such as it is data which could be used in an unauthorised way to cause significant harm to an individual. It is the duty of DG to ensure that wherever data under these or similar categories is processed that suitable and effective safeguards are in place.

Roles and Responsibilities

CEO

The CEO has overall accountability and responsibility for all aspects of data protection in their capacity as the senior executive officer for DG. This accountability is to the board of Directors of DG, the ICO, third party data controllers, and all data subjects of DG.

The CEO is required to provide assurance to Directors that all risks to DG relating to data protection and information security are effectively managed and mitigated.
The CEO is supported in this responsibility in accordance with the normal operational structure and hierarchy of DG.

The CEO will delegate responsibility for compliance with Data Protection Legislation (including the implementation of this policy and other related documents) to the DPCO.

Data Protection Compliance Officer (DPCO)

The DPCO is responsible for internal compliance, informing and advising on data protection obligations at strategic level, providing advice on all aspects of data protection and being the point of contact for data subjects and the ICO.

The DPCO is responsible for ensuring that The Davka Group is registered with the ICO for data processing, that the registration accurately reflects the data processing activities undertaken by DG and that the registration is maintained and renewed as required.

Responsibilities of Each Company

Each company is responsible for ensuring it has completed LIAs for each unique type of data it processes or where relevant the necessary consent can be obtained. LIAs must be submitted to the DPCO for review and approval.

Each department is responsible for ensuring that every opportunity for an opt out is offered where processing data for legitimate interests.

Responsibilities of Managers

All managers are required to ensure that they (and their staff) understand and adhere to this policy and any associated procedures. They are responsible for ensuring that staff are informed and updated on any changes made to this policy.

They are also responsible for ensuring their staff are aware of where data protection information is held.

Managers must ensure that through the induction process or otherwise that all members of their team confirm that they have read, understand, and will comply with this policy.

All managers must clearly understand the requirements around reporting data incidents and ensure they and their staff comply with those requirements. They must also embed a positive reporting culture and operate in a way that incorporates data protection into everything that is done by default and design.

All managers must ensure that their staff undertake training in data protection, which is specific and relevant to their role, they must also uphold the element of personal responsibility for all staff around data protection.

Responsibilities of Staff

All staff, whether permanent or temporary, are required to read, understand and accept this data protection policy and associated procedures that relate to personal data that they may handle in the course of their work.

All staff have a responsibility for data protection and are required to adhere to this policy, any associated procedures and to attend any associated training.

All staff must:

- Understand the main concepts within the Data Protection legislation.
- Identify and report any risks to the security of data processed by DG to their line manager and the DPCO.
- Assist their customers/service users to understand their rights and DG's responsibilities in regard to data protection.
- Identify and report any requests relating to data to the Data Protection Compliance Officer so that they can be processed in accordance with the Data Protection Act.
- Taker personal responsibility for ensuring the data they collect, and access is in full compliance with this policy and legislation.

All staff including those on temporary contracts, agency staff, and their line managers must confirm that they have read, understand, accept and will comply with this policy before they are permitted access to personal data held by DG.

Training & Induction

Reading, understanding and signing in agreement to this policy is a mandatory part of the induction process at DG and must be documented as completed within the induction period.

The DPCO will lead on the development of staff training either through e-learning modules, face to face or third-party training. The training will be developed to meet the specific needs of individuals and the organisation.

It is the responsibility of individual line managers to ensure that they and their staff have sufficient training to ensure they are able to meet their obligations under this policy.

Quick Rules

- Check that you have a completed LIA to process data.
- Check that you have an information sharing agreement in place if you need to share data externally to DG.
- Think about data as if it were your data. Would you be comfortable with your data being processed in the way you or DG are processing other's data?
- Hold data only for as long as it is needed.
- Discard and delete files correctly and confidentially.
- Make sure you have accurate data.
- Keep your passwords safe and secure, they are not to be shared with anyone else.
- Lock your PC whenever you leave it unattended, even for a minute.
- Make sure any documents are not left on your desk if they contain personal or sensitive information.
- Do not disclose personal information unless you are **sure** you can, and you know who is asking for it.
- Suspect an incident? Report it straight away.
- Above all, if in any doubt, ask for advice.

Legal bases of processing data

Legitimate Interest

The UK GDPR does not define what factors to take into account when deciding if your purpose is a legitimate interest. Generally, it means that Data can only be processed if it is in the genuine interest of an organisation to do the processing and it is fundamental to the operations, purpose or prospects of the organisation. It may be summarised as what may be reasonably expected by a data subject when entrusting their data to an organisation.

All data processed must have a clear and specific benefit and I precise purpose to the processing in mind, this is documented in a legitimate interest assessment (LIA) which determines that a legitimate interest exists prior to processing.

Consent
Consent is required for some specific types of data processing; generally, where other lawful bases are not appropriate. This is where explicit consent is given by a data subject before any processing occurs. This is generally necessary for some electronic marketing activities and sometimes where special category data is processed.

Responsibilities Summary

Scope
Users of DG services and members of staff and Directors are entitled to assume that any personal information which is collected or recorded during the course of their involvement with the organisation will not be disclosed inappropriately by any person or persons working within the organisation.

All staff, including permanent staff, temporary staff, agency staff and all Directors of DG are in a position of trust. Any abuse of this trust will be construed as misconduct and may result in disciplinary or legal action.

It is a requirement of DG that all staff and all Managers requesting access to systems for these staff members, should read, and undertake to comply with, these compliance guidelines in accordance DG's Data Protection Policy.

General Principles

It is the responsibility of Managers and Supervisors of all staff, including temporary staff, agency staff and any other person who has access to personal information (including sensitive personal information) to ensure that these workers understand and comply with the need for confidentiality under Data Protection legislation.