DMCS Data Protection and Confidentiality Policy and Procedure

1. Introduction

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data. The DATA Protection Act 2018 and General Data Protection Regulation 2018 ("GDPR") confers rights on individuals as well as responsibilities on those who process personal data. The confidential nature of personal data held by Denis McSweeney practicing under the style of Denis McSweeney Solicitors ("DMCS") makes it all the more imperative that these safeguards are in place.

2. DMCS Data Protection Checklist

- All data subjects are all aware of DMCS's identity as a Solicitors' Practice offering Legal Advice and Services to its clients.
- DMCS has a clear data protection policy in place.
- DMCS clearly informs data subjects what use is made of their data.
- The data held by DMCS is disclosed only for clear legitimate purposes.
- DMCS has appropriate security measures in place both internally and externally to ensure all access to data is appropriate. Manual and electronic records are kept securely and are accessed only for the legitimate purposes of its work.
- DMCS has appropriate procedures in place to ensure that each data item is kept up to date. Data subjects are advised that any changes to their data must be notified to DMCS.
- DMCS has a defined policy in relation to retention periods and this is contained in the within data protection policy.
- Data subjects have the right to access any information which DMCS holds about them. DMCS has procedures for handling access requests from individuals.
- DMCS is not an organisation that is required to register with the Data Protection Commissioner.
- Staff are made aware of the data protection policy and are appropriately trained in data protection. Refresher training will be carried out after the review of this policy every three years.
- DMCS periodically reviews and audits the data which it holds and the manner in which it is processed.

3. Data Protection and Confidentiality Policy

1. DMCS is committed to fulfilling its legal obligations within the provisions of Data Protection legislation.

2. Data Protection is governed by the Data Protection Act 2018 and General Data Protection Regulation 2018 ("GDPR") which replaces the existing Data Protection Legislation namely; Data Protection Act 1988 and the Data Protection (Amendment) Act 2003. The purpose of the Regulation is to protect the rights of individuals whose data is collected, processed, kept, used and disclosed. Data protection is essentially all about the protection of the personal data of individuals whether they are clients, employees, volunteers or donors. Responsibility for ensuring personal data is processed in accordance with data protection legislation lies with the data controller and/or the data processor.

3. Data subjects have the right to access any information which DMCS holds about them.

4. As an employer, DMCS will take all reasonable steps to inform staff about the legislation and to provide appropriate training. Denis McSweeney is assigned to carry out DMCS's obligations under the Act.

5. DMCS holds data relating to the following groups:
    - Clients and former clients
    - Employees, former employees and job applicants
    - Individuals seeking information about the service or seeking to access the service
    - Visitors to website

6. DMCS collects data on a Legitimate Interest basis rather than by consent. Our legitimate interest in gathering an individual's personal information is for the carrying out of work on the individual's behalf only and the individual will be informed of the basis of collection for each matter i.e. property transaction, litigation proceedings or employment. The individual will be informed that 1) there is a valid legitimate interest, 2) the data processing is strictly necessary in pursuit of the legitimate interest, and 3) the processing is not prejudicial to or overridden by the rights of the individual.

7. Staff can be criminally liable if they knowingly or recklessly disclose personal data in breach of the legislation. A serious breach of data protection is also a disciplinary offence and will be dealt with under DMCS's disciplinary procedures. If a member of staff accesses another employee's personnel records without authority this constitutes a gross misconduct offence and could lead to summary dismissal.

8. As a data controller, DMCS undertakes to ensure compliance with the following eight principles:
    - Obtain and process information fairly;
    - Keep it only for one or more specified, explicit and lawful purposes;
    - Use and disclose it only in ways compatible with these purposes;
    - Keep it safe and secure;
    - Keep it accurate, complete and up-to-date;
    - Ensure that it is adequate, relevant and not excessive;
    - Retain it for no longer than is necessary for the purpose or purposes; and
    - Give a copy of his/her personal data to the individual concerned, on request.

9. The data collection practices of DMCS are open, transparent and up-front. This means that when DMCS is collecting personal information from individuals, they are made aware of the uses of this information, individual consent has been obtained for any secondary uses of their personal information and individuals are made aware of disclosures of their personal information to third parties.

10. The data protection legislation affords special protection to certain categories of sensitive personal information, including physical or mental health, racial origin, political opinions, religious or other beliefs, sexual life, criminal convictions, alleged commission of offences and trade union membership. Explicit consent must be sought and received from the individual concerned to hold any of the above sensitive personal information

11. Personal data will only be obtained by DMCS for one or more specified and lawful purposes and should not be processed in any manner incompatible with those purposes, which include legal advice and representation and staff administration. Different sets of data may have different purposes and this includes but is not exclusive to the following.

    Contact: Information that allows the individual to be contacted i.e. email address, postal address or telephone number

    Financial: Bank account or credit card information; information on things an individual has owned i.e. house, car, personal possessions;

    Social: Information on an individual's educational or professional career to include job title, salary, employment files and history; information on an individual's criminal activity or convictions; information on an individual's marital status, information on an individual's family, children, siblings, relationships, marriages and divorces; information communicated to or from an individual either by voice recordings, letter or email, application forms.

Historical: Information about an individual's life history, events that happened in an individual's life either to them or around them.

External: Information that uniquely identifies an individual i.e. their name, PPS No., Passport or drivers licence information regarding an individual's physical or mental health, family or personal health history, test results, blood type, prescriptions;

12. DMCS and its staff will only use and disclose information for the purpose specified or compatible with the purposes for which data is collected and kept. This rule is lifted in certain restricted cases, for example where disclosure of the information is required by law or is made to the individual himself/herself or with his/her consent.

13. Any processing of personal data by a data processor on our behalf will be undertaken in compliance with GDPR. This requires that, as a minimum, any such processing takes place subject to a contract between DMCS and the processor which specifies the conditions under which the data may be processed, the security conditions attaching to the processing of the data and that the data be deleted or returned upon completion or termination of the contract. We also take reasonable steps to ensure compliance by the data processor with these requirements.

14. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. DMCS recognises its duty to ensure that these appropriate security measures are in place. This applies to both information technology and manual files. We believe that high standards of security are essential for all personal information.

15. DMCS will only hold personal information which is adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed. This means that the minimum of personal information should be held in order to fulfil its purpose. It is not acceptable to hold information on the basis that it might be useful in the future without a view of how it will be used. DMCS has a responsibility to continually monitor compliance with this principle and to audit what information is kept.

16. DMCS takes reasonable steps to ensure the accuracy of the information processed on our information systems. In collecting information, DMCS takes all reasonable steps to make sure the information is correct and the source of the information is reliable and to check this, if necessary. The significance of the inaccuracy is important. Minor inaccuracies which have no impact are of less importance but the validity of the system and the training and skills of staff inputting data will be checked. Any inaccuracies will be corrected as soon as possible in order to limit the damage and distress caused.

17. Data subjects are responsible for notifying DMCS of any changes to the data DMCS holds about them and advising of any corrections or amendments that need to be made.

18. DMCS will ensure that personal information is not retained any longer than is necessary. This requires DMCS to undertake regular assessment and deletion. Personal data collected will not be retained once the initial purpose has ceased. See section on retention periods for further details.

19. Closed files are regularly destroyed, in accordance with the appropriate retention periods, and personal information is not retained any longer than necessary. DMCS reserves the right to appropriately anonymise personal data after a defined period if there is a need to retain non-personal data.

20. Individuals have a general right of access to their own personal information, which is processed by DMCS in accordance with established procedures. The procedure for data access requests is outlined in this document.

21. For more information on your rights under data protection legislation, please contact the Data Protection Commissioner.

Specific groups of data subjects

Protection of client data

1. Data protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data.

2. The GDPR confers rights on individuals as well as responsibilities on those who process personal data. DMCS takes all reasonable steps to inform its employees and agents about the legislation, to provide appropriate training and to ensure that the necessary safeguards are in place to protect client information.

3. The confidential nature of client data makes it all the more imperative that these safeguards are in place.

4. As a Data Controller DMCS are obliged to only hold personal information of an individual for which we have a legitimate reason for doing so. The reasons that we can rely on for holding information are the following:

    a. If they pertain to a current matter and are specifically required for the effective processing of that matter.

b. If the matter has now closed but we must retain it for specific length of time as recommended by the Law Society; these timelines are as follows:
    i. 7 years for litigation files
    ii. 12 years for all conveyancing files (discretionary for Vendor files, can be disposed of previous to 12 years)
    iii. 12 years for Probate files however where there is a trust the file must be kept for the lifetime of the trust plus 12 years.
    iv. Indefinitely for all files relating to the drafting of Wills and those of a mentally incapacitated person.

5. Once a file is archived, the year for destruction should be clearly marked on the outside of each file and recorded in a file closing register. Once marked for destruction all files will be destroyed by a reputable shredding company onsite and under the supervision of DMCS staff to ensure safety of our clients' data.

6. Clients have the right to access any information which DMCS holds about them, in accordance with GDPR.

7. DMCS collects all information fairly and all clients are provided with adequate notice of how their personal data will be processed. Clients are clearly informed of their rights under the Act to gain access to a copy of their personal data.

8. If DMCS holds information about individuals and wishes to use it for a new purpose, an option will be given to individuals to indicate whether or not they wish their information to be used for the new purpose.

9. DMCS seeks only the minimum necessary personal data from clients.

10. DMCS has a security policy and set of procedures which explicitly address the security aspects of any personal data held by DMCS or any personal data disclosed to third parties.

11. As part of DMCS's contract of engagement, all clients agree and give permission to DMCS to collect certain personal information on a legitimate interest basis through engagement of DMCS services. DMCS takes all reasonable steps to ensure that it remains up to date.

12. Should the client's information change, the client must notify DMCS immediately so that personal data is accurate and up to date.

Protection of employee data

1. DMCS collects all information fairly and all employees are provided with adequate notice of how their personal data will be processed. Employees are clearly informed of their rights under the Act to gain access to a copy of their personal data.

2. If DMCS holds information about individuals and wishes to use it for a new purpose, an option will be given to individuals to indicate whether or not they wish their information to be used for the new purpose.

3. DMCS seeks only the minimum necessary personal data from employees.

4. DMCS does not retain employees' PPSNs and personal financial information other than for remuneration and taxation purposes.

5. DMCS does not retain personal data from unsuccessful applicants for jobs in DMCS after the individual has been advised of the outcome of the recruitment process for them.

6. DMCS has a security policy and set of procedures which explicitly address the security aspects of any personal data held by DMCS or any personal data disclosed to third parties.

7. As part of DMCS's terms and conditions of employment, all employees agree and give permission to DMCS to collect, retain and process information about employees, such as age, gender and ethnic origin and any illness/disabilities. DMCS takes all reasonable steps to ensure that it remains up to date.

8. Should the employee's personal circumstances change, the employee must notify DMCS immediately so that personal data is accurate and up to date.

9. DMCS maintains a personnel file for each employee. Each employee may review the content of his or her own file, except for letters of reference and certain other limited kinds of information, at reasonable times and intervals. The individual requesting access to his or her file may make copies of papers in the file bearing his or her signature. Each file will contain annual leave request forms, contract of employment, sick leave records (dates & reasons), medical notes, personal contact information, salary details, start date, PPSN, next of kin, a record of the original application form, Curriculum Vitae, written performance reviews, a history of time keeping, etc.

10. The personnel files are maintained by DMCS and under the control of the Practice Administrator. Access to any of these records is only by written authority of Denis McSweeney and this written authority will become part of that individual's personnel records.

11. Certain personal information concerning all employees must be obtained and kept accurate and up to date for administrative, emergency, compensation, and other needs of DMCS, including addresses, telephone numbers, tax withholding information (including PPSN, change in marital status, or number of dependents) and other information necessary for DMCS and governmental reporting purposes.

12. Each employee must report any changes to the Practice Administrator promptly so that these records can be maintained as accurately as possible. DMCS will not release any such personal information to third parties except as necessary in accordance with the applicable data protection legislation. If a written release is given, DMCS will provide dates of employment, job title, and the fact of employment to a prospective employer or to another person requesting a verification of employment.

13. DMCS will publish the name, address, and contact telephone number of each solicitor and staff member solely for use by DMCS personnel in order to enable solicitors and staff to contact others in times of emergency or other extenuating circumstances. Under no circumstances will DMCS use this information for general announcements, solicitations, or other reasons except to the extent specifically permitted, in writing, by an individual DMCS solicitor or staff member.

14. DMCS may from time to time in the course of administering our business need to process both personal data and sensitive personal data in relation to employees. DMCS will process such data in accordance with the applicable data protection legislation.

4. Data Protection and Confidentiality Internal Policy and Procedure

Procedure for handling data access requests

1. Individuals can ask for a copy of all their personal details held by DMCS in computer or in manual form making a data access request to DMCS, as governed by data protection legislation.

2. Individuals are informed that they have the following rights with regard to their personal data:

    - Right to access the data - you have the right to request a copy of the personal data that we hold about you, together with other information about our processing of that personal data.

    - Right to rectification- you have the right to request that any inaccurate data that is held about you is corrected, or if we have incomplete information you may request that we update the information such that it is complete.

    - Right to erasure - you have the right to request us to delete personal data that we hold about you. This is sometimes referred to as the right to be forgotten.

    - Right to restriction of processing or to object to processing - you have the right to request that we no longer process your personal data for particular purposes, or to object to our processing of your personal data for particular purposes.

    - Right to data portability - you have the right to request us to provide you, or a third party, with a copy of your personal data in a structured, commonly used machine readable format.

3. DMCS deals with data access requests in a timely and transparent manner and in accordance with data protection legislation.

4. On making an access request, any individual whose personal data DMCS holds is entitled to:
    - a copy of the data held in relation to them;
    - know what data DMCS holds in relation to them and DMCS's purpose for processing it;
    - know the identity of those to whom DMCS discloses the data;
    - know the source of the data, unless it is contrary to public interest;
    - know the logic involved in automated decisions;

- data held in the form of opinions, except where such opinions were given in confidence and even in such cases where the person's fundamental rights suggest that they should access the data in question it should be given;

5. DMCS does not charge an access fee.

6. To make an access request the data subject must:
   - apply to DMCS in writing using the DMCS Data Access Request Form or by letter;
   - give any details which might be needed to help DMCS identify him/her and locate all the information DMCS may keep about him/her, for example previous addresses, date of birth;

7. Within five days of receiving an access request, DMCS will arrange a meeting between the individual charged with responsibility for data access requests and any other employees it may deem appropriate.

8. At this meeting, a strategy will be agreed to ensure that all relevant manual files and computers are checked for the data in respect of which the access request is being made.

9. DMCS will return information to the individual promptly and in accordance with data protection legislation and the guidelines mentioned above, within 30 days of receiving the request;

10. DMCS will provide the information in a form which will be clear to the ordinary person, e.g. any codes must be explained.

11. If DMCS's investigations show that it does not keep any information about the individual making the request, will be informed within the 30 days.

12. If DMCS decides to restrict the individual's right of access in accordance with one of the very limited restrictions set down in the Acts, the data subject must be notified in writing within 30 days and must be provided with a statement of the reasons for refusal. DMCS will also inform the individual of his/her entitlement to complain to the Data Protection Commissioner about the refusal.

13. Once the information has been collated according to the within policy and data protection legislation, it will be approved by the individual with responsibility for data access requests, and will be submitted to the Denis McSweeney for approval. Denis McSweeney must approve the information before it is sent to the individual exercising their right of access.

14. Individuals have a strong right of access to see their personal data. However, section 5 of the Data Protection Acts provides that individuals do not have a right to see information relating to them in certain circumstances.
    a. If the information is kept for certain anti-fraud functions: but only in cases where allowing the right of access would be likely to impede any such functions
    b. If the information concerns an estimate of damages or compensation in respect of a claim against the organisation, where granting the right of access would be likely to harm the interests of the organisation, DMCS can restrict that information.
    c. If the information would be subject to legal professional privilege in court, DMCS can restrict that information.
    d. If the information is kept only for the purpose of statistics or carrying out research, but only where the information is not disclosed to anyone else, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved, DMCS can restrict that information.

15. DMCS is not obliged to retrieve back-up copies of its personal information in responding to an access request. However, it should be noted that back-up data is not necessarily the same as old or archived data. Such archive data is subject to an individual's right of access in the normal way.

16. Information about other individuals: Under GDPR a data controller is not obliged to comply with an access request if that would result in disclosing data about another individual, unless that other individual has consented to the disclosure. However, the data controller is obliged to disclose so much of the information as can be supplied without identifying the other individual, e.g. by omitting names or other identifying particulars. In this regard, DMCS will redact information as appropriate.

17. Where personal data consists of an expression of opinion about the data subject by another person, the data subject has a right to access that opinion except if that opinion was given in confidence. If the opinion was not given in confidence then the possible identification of the individual who gave it does not exempt it from access.

18. Disproportionate effort: GDPR provides that the obligation on a data controller to comply with an access request, should normally be met by supplying a copy in permanent form, unless the supply of such a copy is not possible or would involve disproportionate effort.

19. Repeated Access Requests: If a data controller has complied with an access request he does not have to comply with an identical or similar request.

Data protection and confidentiality policy and procedure for employees

1. The employee shall observe client confidentiality at all times as a matter of priority. Any information regarding clients or any other confidential information which becomes known to the employee in the course of his/her employment may not be disclosed other than in the normal course of business, according to exceptions as prescribed by law or as expressly authorised by the Denis McSweeney as the case may be. The employee may not make any public statements or publish material without such authorisation.

2. This rule of confidentiality should be regarded as absolute, save for as required by law, and a breach of the confidentiality rules is regarded by us as a most serious matter.

3. All individuals working with DMCS must also ensure that confidential waste is properly disposed of in the confidential waste bin, located on the first floor and basement. The contents of this waste bin are collected weekly and shredded on site.

4. All closed hardcopy files must be stored in our Archive location and according to our archiving procedures and held for the time recommended by the Law Society of Ireland. No hardcopy files will be kept beyond the recommended time and will thereafter be properly disposed of.

5. All electronic files will be held on our central database for the time recommended by the Law Society of Ireland and will then be deleted from our system.

6. All client files should be kept in filing cabinets provided in each office for this purpose. DMCS operates a Clean Desk Policy which is communicated to Employees in a separate document.

7. Client files should only be removed from the office when absolutely necessary to do so, i.e. going to consultations with Counsel, settlement meetings, home visits or Court/Tribunal appearances. All care must be taken when solicitors remove a client file from the office to protect against loss or theft of the file. The file should be carried in a secure bag/briefcase and kept with the solicitor at all times. If the solicitor is travelling by car the file should be locked securely in the boot of the car. Files must never be left overnight in a car and should instead be removed to the residence of the solicitor for that time and stored securely, safely and confidentially. Files should be returned to the office at the earliest opportunity.

8. When out of the office certain staff may with the approval of Denis McSweeney remotely access the office computer system. Staff must ensure that remote access is exercised through a secure network. Remote access is only permitted from a secure system and network. Staff using remote access privileges must ensure that laptops, computers or any other electronic devices have adequate security to protect the confidentiality of DMCS and its clients, that all care is taken to ensure that screens and information cannot be seen by any

third party. All DMCS laptops are encrypted to ensure information contained therein is secure. Staff cannot remove any client information from the DMCS offices on any portable electronic recording device.

9. Employees are not allowed to copy any document or information whether from any computer application or otherwise except as is necessary or required for your work with us. Special care should be taken in relation to the storing and sending of any material to clients. Information on the computer system should be at all times properly protected and any other material generally on your desk should be properly secured at all times.

10. DMCS staff may not at any time during their employment (except insofar as is necessary and proper in the course of employment) or afterwards disclose to any person any information as to DMCS's practice, business dealings, affairs or any of our clients, or as to any other matters which may come to their knowledge during the course of employment. This obligation continues after termination of employment.

11. At no time should a client's affairs be discussed at Reception, either at the desk or in the waiting area. Computer screens on which confidential information may appear should not be visible to visitors. Papers should not be left unattended in places to which the public has access.

12. DMCS's Email Policy within the DMCS Information Systems Policy must be observed at all times.

Security policy

1. DMCS takes appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of all data it holds and against its accidental loss or destruction.

2. The security of personal information is all-important, but the key word here is appropriate, in that it is more significant in some situations than in others, depending on such matters as confidentiality and sensitivity and the harm that might result from an unauthorised disclosure. High standards of security are, nevertheless, essential for all personal information.

3. The nature of security used may take into account what is available technologically, the cost of implementation and the sensitivity of the data in question.

4. DMCS restricts access to central IT servers in a secure location to a limited number of staff with appropriate procedures for the accompaniment of any non-authorised staff or contractors.

5. DMCS restricts access to any personal data within an organisation to authorised staff on a 'need-to-know' basis in accordance with its data protection and confidentiality procedure.

6. Access to computer systems is password protected with other factors of authentication as appropriate to the sensitivity of the information.

7. DMCS takes all reasonable measures to ensure that information on computer screens and manual files is kept hidden from callers to our offices.

8. DMCS operates a back-up procedure for computer held data, including off-site back-up.

9. DMCS takes reasonable measures to ensure that staff are made aware of the organisation's security measures, and comply with them.

10. DMCS disposes carefully of all waste papers, printouts, particularly those containing sensitive personal information and maintains and destroys its files, as appropriate, in accordance with the DMCS policy on the retention or destruction of files and other papers and electronic storage.

11. DMCS designates Maeve Moloney as having responsibility for security and for periodic reviews of the measures and practices in place.

Procedure for handling data breaches

1. Breaches of Data can be categorised as follows:

   Confidentiality breach – where there is an unauthorised or accidental *disclosure* of, or *access* to, personal data.

   Integrity breach – where there is an unauthorised or accidental *alteration* of personal data.

   Availability breach – where there is an accidental or unauthorised *loss* of access to, or *destruction* of, personal data.

2. Once an Employee becomes aware of a data breach they must immediately report the breach to Denis McSweeney.

3. Denis McSweeney then has 72 hours to investigate the nature and severity of the data breach.

4. Denis McSweeney will assess the potential risk to individuals from the data breach, and subsequently determine if it is necessary to notify the relevant supervisory authority and or the individuals concerned with the breach.

Review

This policy will be reviewed every three years.

Glossary

Data: Information in a form in which it can be processed, manually or automatically.

Personal data: Data relating to a living individual who can be identified either from the data, or from the data in conjunction with other information in the possession of the data controller.

Data controller: A person who, either alone or with others, controls the contents and use of personal data.

Data processor: A person who processes personal data on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment.

Data subject: Individual person who is the subject of any relevant personal data.

Third party: Someone other than the data subject, controller, processor and persons with authority of the controller or processor to process the data.

Recipient: Person to whom data is disclosed. This would include employees. The data subject has to be informed of the recipients of the data.

Data subject's consent: Any freely given specific and informed indication of his/her wishes by which the data subject signifies his agreement to personal data to him/her being processed.