Contents

Introduction

Information privacy, data privacy or data protection laws worldwide provide a legal framework on how to obtain, use and store data on natural persons. There are various laws around the world that describe the rights of natural persons, and they have been designed to protect individuals from having their personal information misused, exploited or mishandled.

Details Management, Ltd. (the “Company”) is subject to the Bermuda privacy legislation, the Personal Information Protection Act (“PIPA”).

The Company collects and uses information about the people with whom it deals. These include the Company’s own employees, suppliers and other third parties with whom the Company conducts business and processes data on their behalf. The information can be factual, such as a name and address, or expressions of opinion about, or intentions towards, individuals. Any information relating to an identified or identifiable natural person is 'Personal Information'. In addition, the Company may occasionally be required to collect and use certain types of information to comply with regulatory requirements. This personal information must be dealt with properly no matter how it is collected, recorded or used, and whether it is recorded on paper or electronically (in a structured or non-structured system).

The Company recognizes that the lawful and correct treatment of Personal Information is important to successful operations and to both maintaining its clients' confidence and enhancing the client experience.

Ownership, Approval and Periodic Review

The document is owned by the Data Privacy Officer (‘DPO’) and will be reviewed at least annually and updated as necessary.

Definitions

Personal Information - means any information relating to an identified or identifiable natural person i.e. this could be any combination of data that enables a living individual to be identified. For example, a name alone may not be sufficient until combined with other data points such as address and gender.

Data Subject - an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person.

Processing - in relation to Personal Information, means carrying out any operation on Personal Information, including collecting, obtaining, recording, holding, storing, organising, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating or otherwise making available, combining, blocking, erasing or destroying it.

Data Controller – a legal entity or other body that determines the purposes of processing personal data and the means of processing it. The Data Controller exercise overall control of the personal data being processed and has the primary responsibility for ensuring that the personal data is processed in accordance with PIPA.

Data Processor – a legal entity or other body which processes personal data on behalf of the Data Controller. The Data Processor may makes its own day-to-day operational decision, but should only processed personal data in line with the Controller's instructions, unless it is required to do otherwise by law.

Breach - means any unauthorized or unlawful Processing, access, accidental loss, disclosure or destruction of or damage to Personal Information, which is likely to adversely affect an individual.

Policy Purpose and Application

The purpose of this Data Privacy Policy (this "Policy") is to ensure that:

- The Company applies a common policy to the treatment of Personal Information, while complying with local legal requirements;
- All Staff are aware of their responsibilities and rights in relation to Personal Information held by the Company; and
- The Company complies with appropriate legislative requirements for any valid requests relating to personal Information.

This Policy apply to all the Company's "Staff', defined as:

- The directors, officers, managers, and employees, whether permanent or temporary; and
- All third-party staff engaged by, for, or on behalf of the Company including but not limited to contractors, secondees, consultants, administrators, project staff, volunteers, whether permanent or temporary.

All Staff are personally responsible for ensuring their understanding of this Policy and its contents and requirements and must adhere to this Policy at all times.

Whilst every effort is made to automate and apply global IT controls to secure the transmission of information, implement access protocols, encryption methodologies and security monitoring, all Staff have a responsibility to ensure their own Personal Information and that of other Staff members to which they legitimately have access, as well as all client, third party Information and corporate Information, is protected at all times.

In addition, Staff must ensure that, inaccurate Personal Information (including client and business contacts) is rectified as soon as possible, and that employee key information is up to date and accurate.

It is important to note that the relevant rules surrounding Personal Information will depend not just on the physical location of the individual Processing the Information, but also where that Information is sent, where the Information is stored, the domicile of the company on whose behalf the Processing is being carried out and the domicile of the Data Subject. Particular care must be taken when transferring Personal Information across jurisdictions.

Policy Principles

The Company recognizes that the lawful and correct treatment of Personal Information is very important to its business and to maintaining clients' and employees' confidence. Accordingly, the Company must adhere to the following general principles of Personal Information protection as a matter of policy. Personal Information must be:

- Processed fairly and lawfully and, in particular, shall not be processed unless specific legal conditions are met (see section 6).
- Obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes, unless specific legal conditions are met (see section 7).
- Collected in a transparent way with individuals' being informed as to how their information will be used (see section 8).
- Adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed (see section 9).
- Accurate and, where necessary, kept up to date (see section 10).
- Kept for no longer than is necessary for the specified purpose or purposes (see section 11).
- Processed in accordance with the rights of Data Subjects (see section 12).
- Subject to appropriate technical and organizational measures to prevent the unauthorized or unlawful Processing of Personal Information, or the accidental loss, destruction or damage to Personal Information (see section 13).
- Not transferred across national / international boundaries unless the recipient country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Information or the Information is otherwise protected using appropriate legal mechanisms (see section 15).

Lawful Processing

In order to meet the criteria for lawfulness, Processing must only take place where one of the following requirements has been met:

- the Processing is necessary for compliance with any legal obligation to which the Company is subject that authorizes or requires such use, other than an obligation imposed by a contract;

- the Processing is necessary for the performance of a contract that the Data Subject has entered into or for taking steps at the request of the Data Subject for entering such a contract;
- the Data Subject has given consent to the Processing, where the organization can reasonably demonstrate that the individual has knowingly consented;
- the Personal Information is publicly available information and will be used for a purpose that is consistent with the purpose of its public availability;
- the use of the Personal Information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public;
- the use of the Personal Information is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the organization or in a third party to whom the personal information is disclosed; or
- the use of the Personal Information is necessary in the context of an individual's present, past or potential employment relationship with an organization.

Purpose

Personal Information must not be processed in a manner which is incompatible with the specific purpose for which it was collected, and any information given to an Data Subject explaining the purpose for which Personal Information has been collected.

This does not apply:

- when the use of the Personal Information is with the consent of the individual whose personal information is used;
- when the use of the Personal Information is necessary to provide a service or product required by the individual;
- where the use of Personal Information is required by any rule of law or by the order of the court;
- where the use of the Personal Information is for the purpose of detecting or monitoring fraud or fraudulent misuse of Personal Information; or
- where the Personal Information is used for the purposes of scientific, statistical or historical research subject to the appropriate safeguards for the rights of the individual.

The Company further needs to ensure that Personal Information is adequate, relevant and not excessive in relation to the purposes for which it is used.

Transparency

When collecting Personal Information, the Company needs to provide individuals with a clear and easily accessible statement ("privacy notice") about its practices and policies with respect to personal information, including—

- the fact that personal information is being used;
- the purposes for which personal information is or might be used;
- the identity and types of individuals or organizations to whom personal information might be disclosed;
- the identity and location of the Company, including information on how to contact it about its handling of personal information;
- the name of the DPO;
- the choices and means the Company provides to an individual for limiting the use of, and for accessing, rectifying, blocking, erasing and destroying, the Personal Information.

The Company needs to take all reasonably practicable steps to ensure that the privacy notice is provided either before or at the time of collection of personal information, or, where that is not possible, as soon thereafter as is reasonably practicable. As such, the privacy notice will be posted on the Company's website.

Minimization

The Company collects, stores and processes only small amounts of Personal Information. As the Company grows, protecting this information adequately may become increasingly complex with increasing Information volumes and types. We must therefore reduce or 'minimize' the amount of Personal Information processed as far as possible within the legal framework, whilst maintaining business efficiency and capability.

In order to reduce the amount of Personal Information, in the event that an individual receives Personal Information, only the Information required for the particular purpose should be collected. Any superfluous information should be destroyed, in an appropriate manner, and appropriate security and management controls placed around the Information that is retained. Where possible, collection methods and processes should be reviewed to avoid collecting superfluous information in the first instance.

Information Accuracy

Reasonable steps must be taken by the Company to ensure that Personal Information is accurate and kept up to date. If appropriate, this will include periodic contact with Data Subjects to verify the accuracy of Personal Information.

Retention and Disposition

Personal Information must only be held for as long as is necessary to complete the purpose for which it was collected, or for as long as is necessary to comply with an obligation imposed by law or a regulatory

authority. The Company's Record Retention Policy contains details as to categories of Information, retention periods and disposal triggers, as well as preservation obligations such as litigation holds.

Where Personal Information is to be disposed of, it must be disposed of in an appropriately secure manner to ensure that it is unlikely it can be restored or reconstituted by a third party. In the case of Personal Information held as physical records such records must be disposed of by secure shredding. For electronic records, storage devices used in the Processing of such Information must be securely erased.

Rights of the Data Subject

The Data Subject may exercise the following rights (depending on the lawful basis of collection). It is vital that Staff understand what each right means and recognize when it is being invoked. These are the rights to:

- **Access**: including medical records: individuals have the right to submit a request to the Company for copies of their Personal Information that is processed.
- **Correction**: individuals have the right to request that the Company correct any information they believe is inaccurate. They also have the right to request the Company to complete the information they believe is incomplete.
- **Blocking**: to prevent Processing of Personal Information if used for marketing or public relations.
- **Erasure and destruction**: individuals have the right to request that the Company erase their Personal Information if the Company no longer has a valid need to process the Information.

Please refer to Appendix A for the procedures of how to address a Data Rights Request.

Information Security

Appropriate technical and organizational measures must be taken to prevent unauthorized or unlawful Processing of Personal Information and protect against its accidental loss, destruction or damage. These measures shall include but not be limited to:

- limiting access to the Personal Information to those persons that have a legitimate business need or other justification to access that Personal Information;
- holding the Personal Information in a suitably secure environment to minimize the possibility of unauthorized third parties gaining access to the Personal Information;
- not removing, transferring or sharing the Personal Information from the Company's premises unless necessary for the Processing to be carried out; and
- ensuring that any Personal Information that must be removed, transferred or shared from the Company's premises is suitably protected from unauthorized access in transit, Processing and storage; for example, in the case of electronic records of Personal Information, ensuring that such records are encrypted.

Staff must also:

- lock computer screens when not in use or away from the desk;
- operate a clear desk policy and utilize lockable cabinets so that Personal Information is not left on desks
- clear meeting rooms fully following closure of a meeting including whiteboards, meeting documents (presentations, reports etc.) and flipcharts, disposing of any remaining papers in a secure manner
- ensure passwords comply with the Company's guidelines and are not shared
- ensure email chains are only forwarded when appropriate
- ensure that only appropriate recipient email addresses are entered into emails
- only use the Company's corporate email systems, never private / personal email addresses or servers
- consider the most appropriate way to distribute documents in a secure manner depending upon the methods available for the transfer in question. This could include email encryption, encrypted memory sticks or, if none of the stronger methods are available, password protection.

CCTV Policy

The Company uses CCTV for the reasons and purposes described in this policy. The CCTV may be located in reception areas and corridors. All cameras are in a visible location and area clearly signposted to ensure individuals are aware of their location. The CCTV operates on a continual, 24hr basis with the Company using static cameras and motion detector sensors. Only images are captured and there is no audio recording.

The purpose for using CCTV are: -

- For the personal safety of visitors, employees and any other individuals within the Company grounds and buildings
- To prevent crime and protect buildings, business areas and vehicles from damage, disruption, vandalism and any other crime
- To support law enforcement agencies in the prevention, detection and prosecution of crime
- To monitor and enforce regulatory, contractual and/or legal compliance with rules and obligations
- To assist in effective dispute resolution relating to disciplinary or grievance proceedings
- To monitor and protect employees during the provision of their duties

CCTV footage or images are not retained for longer than is necessary and is only used for the above purposes.

Data Breach

A Data Breach is any unauthorized or unlawful Processing, access, accidental loss, disclosure or destruction of or damage to Personal Information, which is likely to adversely affect an individual. Data Breaches may occur for many reasons, including;

- carelessness, such as leaving unprotected documents containing Personal Information in a public place;
- non-adherence to authorized processes, such as emailing Personal Information to one's personal email address;
- accidental omissions, or
- malicious cyber-attack.

The Company recognizes that, whilst it is committed to complying with its obligations to implement appropriate security measures, both organizational and technical, to ensure that Personal Information is protected, it is impossible to completely avoid all Data Breach scenarios.

It is therefore vital that employees report all Breaches or suspected Breaches immediately to the IT Department.

Once reported, the Company will follow procedures to ensure appropriate steps are taken to:

- contain the Breach;
- recover the information compromised;
- assess and mitigate the damage and risks arising from the Breach;
- report externally the Breach, as legally required, and
- implement any necessary improvements to systems, processes and training to mitigate the risk of reoccurrence.

Designated individuals (which will include the DPO and representatives from IT and legal counsel), will make the final determination as to whether a Data Breach has indeed occurred and what, if any, regulatory or Data Subject reporting is necessary. In Bermuda, in case of a reportable Data Breach, the Company will need to, without undue delay:

- notify the Privacy Commissioner of the breach; and
- then notify any individual affected by the breach.

The notification to the Commissioner under subsection will need to describe—

- the nature of the breach;
- its likely consequences for the individual; and
- the measures taken and to be taken by the organization to address the breach

so that the Privacy Commissioner can determine whether to order the organization to take further steps and for the Privacy Commissioner to maintain a record of the breach and the measures taken. Agam

In addition, in case of a material breach, the BMA will need to be notified within 72 hours of it occurring, or the suspicion of it occurring.

Data Transfers

Particular care must be taken when transferring Personal Information to another party (irrespective of whether the transfer is to be made to an affiliated company or to a third party) as:

- there is an increased chance of Data Breach
- strict rules apply to transfers across national / international boundaries

Contracts with affiliated entities or Third Parties will need to include appropriate terms to enable transfers across national / international boundaries, and before making any such transfer, the Company will need to assess the level of protection provided by the overseas third party for that Personal Information.

For further information regarding transferring Personal Information internationally both inside and outside of the Company, and any restrictions or conditions that may apply, please contact the DPO.

Third Party Privacy Risk Management

Where the Company proposes to appoint another entity to Process Personal Information on its behalf, the appropriate due diligence must be undertaken, before the appointment is made. This is to ensure the Company can evidence and demonstrate that sufficient and effective safeguards are in place to ensure that Personal Information will be processed in accordance with relevant law.

Data Processor Contracts

When performing services on behalf of our clients (payroll processing, human resource services, etc.), we act as Data Processors of personal information. As such, we act under the instructions of the Data Controller and we do not own or control the data. Each service agreement will have in place clauses specifying the ownership of the data and the purpose and means of processing, including the retention and disposal procedures.

Training

All Staff will be provided with adequate training and guidance on this Policy periodically, to ensure that understanding of the requirements is maintained. Key concepts will also be included as part of the Compliance Induction training for all new staff members. This training will be provided as soon as practicable and not more than one month from being employed by the Company. A register of attendees will be kept on file for audit purposes.

This Policy will be made available and accessible to all Staff.

Record Keeping

Records of breaches, actions taken to rectify and outcomes must be kept by the DPO. Additionally, the DPO is responsible for keeping records of all Data Subject rights requests, including their outcome, and a record of all decisions made in accordance with this Policy.

These records will be held for the period outlined in the Record Retention Policy and maintained on an ongoing basis by the DPO.

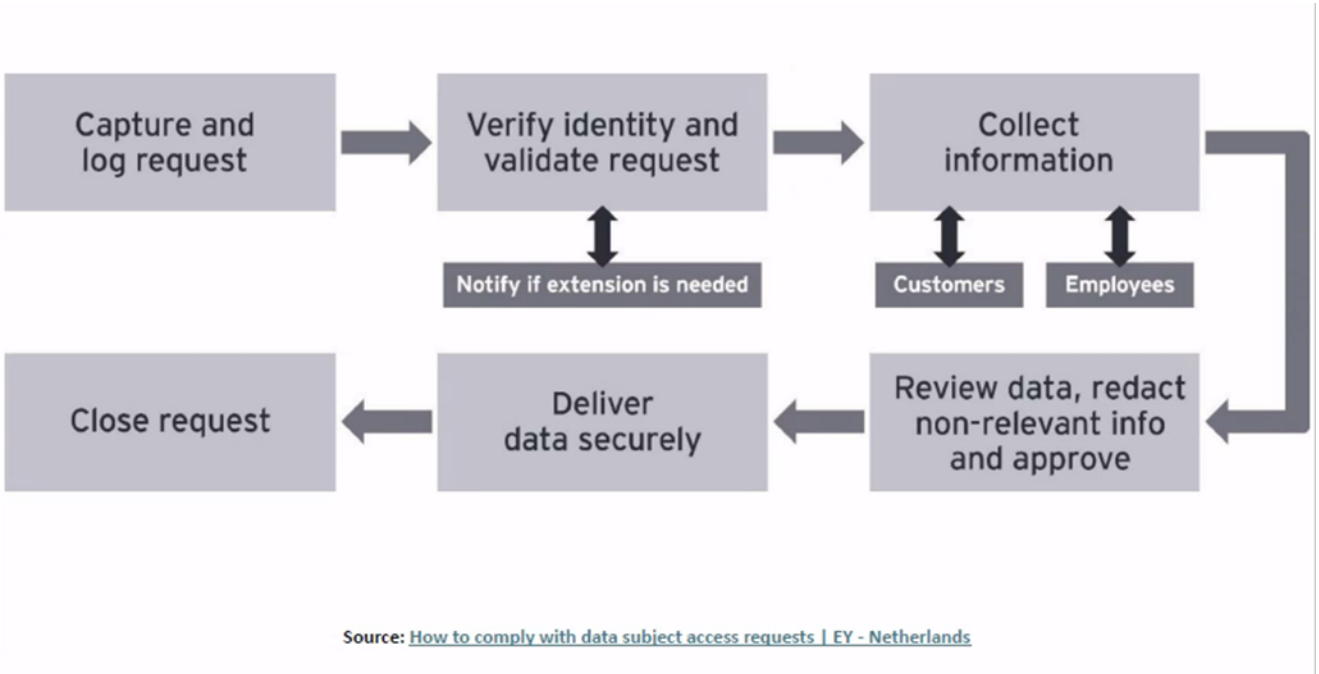
APPENDIX A – DATA RIGHTS REQUEST PROCEDURE

This is the procedure and protocols followed by Details Management, Ltd. *(hereinafter referred to as* ***" the Company"*** when such a request is received.

The the Company need to collect personal information to carry out our everyday business functions and services effectively and compliantly and, in some circumstances, to comply with the requirements of the law and/or regulations.

As the the Company processes personal information regarding individuals, we are obligated under Bermuda's Personal Information Protection Act, 2016 (PIPA) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with the Act and its principles.

The the Company will follow this 6 step process when handling Data Rights Request (DRR).



Source: How to comply with data subject access requests | EY - Netherlands

STEP 1 - Capture request

An individual rights requests must be made in writing to privacy@details.bm. The components required are:

- Individuals full name
- Individuals address and phone number
- What action they would like performed
- Any specific documents requesting
- What time period of information they are looking for, if applicable

When logging the request, also determine which right(s), the request falls under:

- Right to Access
- Right to Correction
- Right to Erasure
- Right to Blocking

For definitions of these rights, please refer to the Data Privacy Policy above.

STEP 2 - Verify Identity and Validate Request

Acknowledge receipt of the request in writing. The individual must be verified one of the following methods:

- Request a copy of a drivers licence to validate personal information
- Establish that the request is from a regular email address that they use to correspond with you and not newly made up
- Phone the individual using the phone number in your database, not the one they provide

If a third party, relative or representative is requesting the information on behalf of individual, verify their authority to act on behalf of individual by contacting the individual in one of the manners to confirm their identity and gain authorisation prior to actioning any request.

If the request could not be verified of the third party could not be authorized, then the request should be refused. See Sample Letter 1 below.

STEP 3 - Information Collection

Perform searches and/or assign responsibility to relevant departments to undertake searches. Use the Data Map as a guide to understand where the information requested is located. Gather all documents relating to request and ensure that the information required is provided in an acceptable format.

Perform searches and/or contact relevant departments to undertake searches.

Under PIPA, the Company have a duty to disclose all relevant personal data, unless an exemption or a specific overriding argument applies, such as it would breach a duty of confidence or would undermine your own data protection rights causing damage or distress.

When identifying the personal data of an individual, a balance should be struck between the requestor's rights and the rights of other parties personal data that we hold. Those making decisions in respect of DRRs need to balance the right of access alongside the legitimate privacy or data protection expectations of professionals. Personal data relating to professionals routinely shared as part of everyday business (i.e. the names of employees in public facing roles, work/business contact details, professional opinions etc.) are unlikely to attract a level of consequence if the data was disclosed as part of a DRR. However, as in all instances, this should be judged upon a case-by-case determination. The same principles apply in respect of those which do not work for your company, but in determining any level of risk, you may wish to consult with these 3rd parties to present their own evidence for you to consider. Determining whether it is reasonable to disclose the information, consider all the relevant circumstances, including:

- Any duty of confidentiality to the Company or other individuals. Examples of confidential content:
    - Details of information originating for confidential complainant which would allow the identification of the source
    - Information which may jeopardise commercial confidences (such as trade secrets, commercial rates, intellectual property etc.)
    - Information gathered as part of a confidential relationship (such as lawyer or doctor)
    - Information covered as part of a non-disclosure agreement

- Whether it is appropriate to seek consent from other individuals. It is not appropriate to seek consent from other individuals if seeking consent could prejudice the data rights of the requestor, subsequent harm could arise from seeking consent (ie. From a victim of a crime, an estranged partner going through divorce proceedings, insufficient capacity to provide consent).
- If any steps are taken to seek consent from the other individuals, document steps (see Sample letter #2 below)

For example, if data subject A provides a witness statement as part of data subject B's disciplinary investigation, it would not be appropriate to provide any internal analysis of data subject A's evidence to data subject B as part of a Rights Request.

Further examples for consideration:

CONSIDERATION	EXAMPLE	OUTCOME
Does the content relate to special characteristic personal data? (i.e. medical or health conditions, ethnicity, criminal offences etc.).	An email from employee A to their manager explaining that they cannot visit the data subject as they are having a pregnancy scan.	There would be an expectation this would primarily constitute personal data relevant to the employee, not necessarily that of the data subject and would be redacted.
Would the disclosure have unjustified significant consequences on the professional?	An email from employee B (an undercover investigator) outlining the evidence they have captured about the data subject.	If the investigation has been concluded and there is no prejudicial effect, it may be appropriate to share the content with the data subject. However, it may be appropriate to redact the undercover investigator's name to preserve their covert role or to protect their identity in the event that the data subject may seek revenge.
Is there a reasonable expectation that their personal data will be released? You should consider whether it relates to the personal data in a professional capacity, their seniority and the public facing nature of their role.	An email from the HR Director containing interview feedback concerning a potential candidate.	There is a reasonable expectation that those making decisions about individuals in key roles should be accountable and open to scrutiny. A potential candidate has a legitimate expectation that they should be able to receive constructive feedback about their interview. There would be less of an expectation for the disclosure of the name of the reception staff who welcomed the candidate into the building.

Source: DPOCentre

STEP 4 - review data, redact/anonymize data, and approve

Once all the data is gathered, subject to the above, a review of the data is performed. There are a number of exemptions from the rights available to data subjects. The the Company can restrict access to data subject rights including DRRs whereby it is necessary to safeguard the following:

• Crime and taxation • Crime and taxation risk assessments • Information required to be disclosed by law or in connection with legal proceedings • Legal professional privilege • Self-incrimination • Disclosure prohibited or restricted by an enactment • Immigration • Functions designed to protect the public • Audit functions • Bank of England functions • Regulatory functions relating to legal services, the health service and children's services • Other regulatory functions • Parliamentary privilege • Judicial appointments, independence and proceedings • Crown honours, dignities and appointments • Journalism, academia, art and literature • Research and statistics • Archiving in the public interest • Health data • Social work data • Education data • Child abuse data • Corporate finance • Management forecasts • Negotiations • Confidential references • Exam scripts and exam Personal or household activities (as personal data processed in the course of a purely personal or household activity, with no connection to a professional or commercial activity, is outside the PIPA's scope) • Law enforcement • Safeguarding national security or defence

If any of these exemptions apply, determine whether it is possible to anonymize the data. If it is not possible to anonymize the data, the information is to be redacted. Redaction can be completely electronically or by hand. One of the most adopted methods is by using the full version of Adobe Acrobat (not just Adobe Reader). There are other tools on the market which are similar. Adobe allows for content to be scanned by Optical Character Recognition (OCR), allowing for text searching and automatic redaction, but it also gives you a tool to redact content manually. Redaction within Microsoft Word is not recommended as the content can be copied and pasted with formatting removed allowing the original content to be revealed.

Another secure method is to undertake the redaction manually by hand. Before undertaking redacting activity, it is important that your disclosure bundle is printed out single sided. Manual redaction can be completed by clearly colouring over or marking over the protected content, preferably with a straight line. You do not need to be concerned by the fact that the marked over content can potentially be read through on the flip side, as this can be alleviated on completion by photocopying or scanning the disclosure bundle on the darkest brightness setting and sending the output instead.

Once we have collated all the personal information relevant to the request, obtain approval from DPO and/or Compliance Officer for approval before final response sent to requestor.

STEP 5 - Deliver Data Securely

The Company is required to provide information in a concise, transparent, intelligible and easily accessible form, using clear and plain language so that the content can be understood by the average person.

If you redacted information as part of the disclosure, the Company is obligated to explain the rationale for this as well as any exemptions used.

If an individual made a request electronically, then the response should be provided electronically, unless otherwise specified).

Provide a covering letter as part of your response (see sample letter 2 below). If refusing the request in its entirety on excessive or manifestly unfounded grounds, explain reasons for refusal, the right to complain to the Privacy Commissioner and the ability to enforce rights through judicial remedy.

STEP 6 – Close Request

Document and close the request on internal log. Include information containing the date the DRR was responded to, the method of delivery, any exemptions and rationale. By maintaining a detailed log of individuals DRR, the Company can demonstrate transparency, accountability, and compliance with PIPA regulations.

Fees and Timeframes

All access requests are to be completed within PIPA's requirements (45 days from the date the request is received). However, where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended as set out in the PIPA. If this is the case, we will write to you within 30 days and keep you informed of the delay and provide the reasons.

Under PIPA, a fee may be charged to cover our administrative costs for responding to a subject access request.

SAMPLE LETTERS

1 – SAMPLE 3rd Party REQUEST DENIED LETTER

Dear [NAME],

I write in connection with your request received on [DATE] seeking access to [DESCRIPTION OF THE REQUEST]. It is not possible to fulfil your request. This is because it is the company's view that the disclosure of the information sought would be prejudicial to the data protection rights of the individual concerned and would breach our obligations under Personal Information Protection Act, 2016.

If you feel that this is incorrect, you may wish to outline your request to [INSERT RELEVANT DEPARTMENT] for reconsideration. As part of this it is important that you clearly define any relevant rationale or legal provisions being relied upon to support this request.

2 - Sample content for a letter seeking consent

Dear [NAME],

[COMPANY] has recently received a Data Rights Request from a third party. Under the provisions of the Personal Information Protection Act, 2016 (PIPA) individuals have a right to access personal data relating to them. Whilst collating the relevant data, we have located the following records which relate to yourself too (a copy of which has been enclosed for your perusal). As part of our decision-making process, we are required to balance the individual's right to a Data Rights Request, against any privacy or data protection rights that you may have. In responding to such a request, [COMPANY] has a duty to disclose all relevant personal data, unless an exemption or a specific overriding argument applies, such as it would breach a duty of confidence or would undermine your own data protection rights causing damage or distress. If you feel this is applicable in this case, please reply to me, outlining why you feel this is the case. Under data protection law we are required to process a Data Rights Request within 45 days of receipt. As such, it is vitally important that you give this matter your urgent attention. If [COMPANY] has not received any feedback from you by [GIVE TWO WEEKS], [COMPANY] will assume that you have no outstanding concerns and you are happy for [COMPANY] to make appropriate decisions around disclosing or withholding your data. If you wish to discuss further, I am available on the following contact details:

3 – Data Subject Response Cover Letter or Email

Dear [NAME],

Data Subject Access Request – Reference:

I write in connection with your request received on [DATE] seeking access to [DESCRIPTION OF THE REQUEST].

Your request has been considered in line with Personal Information Protection Act, 2016, and the personal data you are entitled to has been included with this letter. Additional to the provision of your personal data, I can confirm that [Company] processes your personal data and for more details surrounding the purposes and scope of this can be found within our Privacy Notice [PROVIDE LINK OR COPY OF PRIVACY NOTICE].

You may note that certain parts of your disclosure have been redacted (i.e. removed with black marks), this is because it contains…

[LIST OF EXEMPTIONS]:

Information relating to 3rd parties:
Under the right of access, Data Subjects are only entitled to their own personal data and not necessarily that relating to any 3rd parties. As part of providing information we have had to consider your right of access and balance that against any other rights that other individuals such as protecting their own data protection or privacy rights.

Information provided in confidence:
There will often be occasions whereby information is provided in confidence to the company and release of such would undermine that duty of confidence potentially resulting in legal consequences for the company. Furthermore, it is important that such confidences are respected and that individuals can share matters with the company in confidence without fear that their confidence will be breached. Please rest assured that what we can share in respect of these instances will have been shared or anonymised appropriately.

I hope that you find the enclosed information useful. [COMPANY] now consider your request fulfilled and the matter to be closed. Should you feel this is not the case, in the first instance please let me know. If you remain dissatisfied following this, please note that you have the right to raise the issue with the Privacy Commission Office who can be contacted by the following methods:

You also may wish to seek to enforce your rights through the Courts. If your concerns related to procedural matters rather than the provision of information, please can I politely suggest that such matters are taken up with the relevant departments or via our complaints processes.