Data Breach Response Procedure

CLASSIFICATION: INTERNAL

Attention: The information is intended for the private use of the SBU - Writer Relocations of Writer Business Services Pvt. Ltd. By viewing this document, you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from Writer Relocations. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited.

Document Management Information

Ver. No.	Ver. date	Author	Reviewed By	Approved By	Next Review	Changes
1.0	31-10-2019		Huzefa Bangdiwala	Tarun Ramrakhiani	October 2020	
1.1	30-10-2020		Rohington Kasad	Tarun Ramrakhiani	October 2021	

Table of Contents

1. Definitions and Acronyms

Definitions

Term	Explanation
Information Asset	Anything that has value to the Organization and is either a form of information itself or creates, stores, transmits, or manages information.
Information Security	Preservation of Confidentiality, Integrity and Availability; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved
GDPR	General Data Protection Regulation
Writer Relocations Employee	Person hired to perform a job or service for Writer Relocations, and one who is directly employed or hired on a contract basis
Customers	All the clients of the organization who avail services or products provided by the Writer Relocations.
Third parties	All third parties which includes, but is not limited to vendors, related government authorities, shipping line, airline, partners, volunteers, contractors, consultants, temporaries, and others who have access to, support, administer, manage, or maintain Writer Relocation's information or physical assets
Data Protection Officer (DPO)	A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.
Data Protection	Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes. Data protection is also known as data privacy or information privacy.
Data Breach	A data breach is a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property
Data Processor	The entity that processes data on behalf of the Data Controller
Data Controller	The entity that determines the purposes, conditions and means of the processing of personal data
Data Subject	A natural person whose personal data is processed by a controller or processor
Consent	Freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data

Acronyms

Acronym	Full Name
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
CISO	Chief Information Security Officer
DC	Data Controllers
DP	Data Processors

Acronym	Full Name
DS	Data Subject
BCR	Binding Corporate Rules

2. Scope

This procedure is applicable throughout the SBU – Writer Relocations of Writer Business Services Pvt. Ltd:

- All the Writer Relocations employees including contract employees and temporary staff
- All the third parties working with Writer Relocations including but not limited to suppliers, service providers, consultants etc. where the personal data is made available to third party.

3. Purpose

The purpose of this procedure is to contain any breaches, to minimize the risk associated with the breach and consider what actions are necessary to protect personal data to prevent further breaches. This policy aims to ensure that:

- Breaches are identified, assessed and reported in a timely manner
- Breaches are properly investigated
- Clear roles and responsibilities are defined in an event of data breach
- Breaches are handled properly by skilled individuals
- Escalation procedure is communicated properly
- Breaches are recorded and documented
- Data controllers and data subjects are informed about the data breach
- Data protection officer is informed about the data breach
- Breach response plan is tested regularly
- Evidences are gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- Root cause of the data breach is documented
- Learnings from the data breach are documented to avoid similar incidents

4. Data Processor

The SBU - Writer Relocations of Writer Business Services Pvt. Ltd. is the Data Processor as per the General Data Protection Regulation, which means that it carries out processing of data as per their client required services based on the collected data.

It is also responsible for notifying their customer in case any data breach takes place.

5. Data Controller

The SBU - Writer Relocations of Writer Business Services Pvt. Ltd. is the Data controller as per the General Data Protection Regulation, which means that it determines the purposes, conditions and means of the processing of personal data which is collected from its website or by any other means.

6. Procedure section and clauses

6.1 DEFINING A DATA BREACH

Data breach is a confirmed incident in which sensitive, confidential or protected data has been accessed and/or disclosed in an unauthorized manner.

Data breach includes but is not limited to following:

- Loss of theft of data or equipment on which personal data is stored
- Human error
- Access by an unauthorized third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data. Any circulation of the personal data without the consent of the data subject shall be considered as a data breach.

6.2 ORGANIZATIONAL FRAMEWORK

Writer Relocations shall form an information security incidence response team but not limited to following:

- Data Protection Officer
- Chief Information Security Officer (CISO)
- Representatives from the IT, HR, and other business functions.

6.2.1 Data Protection Officer Responsibilities

Responsibilities of the data protection officer:

- Direct involvement in all the issues pertaining to the protection of the personal data of the data subjects at Writer Relocations.
- To directly advise the people involved in the processing of personal data about the obligations pursuant to the general data protection regulation.
- Monitoring the compliance with the general data protection regulation at Writer Relocations.
- Monitoring the compliance with all the policies pertaining to the data protection including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits at Writer Relocations.
- To advise the Writer Relocations while carrying out the data protection impact assessment.
- To be the single point of contact with the supervisory authority on any issue.
- The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.
- Identifying keys tasks and managing timelines for the response/mitigation efforts.
- Tracking media coverage and devising a strategy to respond to any negative press.
- Data protection officer shall report to the highest management of the organization.

6.2.2 Representatives from other teams

- Assessing the breach and reaching out to a decision whether it is a data breach.
- Supporting in identifying the root cause of the breach.
- Securing affected systems and/or taking affected systems offline.
- Collecting and preserving evidences.
- Coordinating with internal and external forensics team.
- Closing the data breach in co-ordination with the data protection officer, legal and HR representatives.
- Ensuring that learnings from the data breach is documented.
- Ensuring that all the unpatched vulnerabilities are patched within the defined timelines.
- To carry out organization wide data protection impact assessment on quarterly basis and immediately after the data breach.

6.2.3 Legal representative's responsibilities

- Determining how and when to notify the affected individuals, the media, law enforcement and government agencies, and other necessary parties
- Coordinating with external counsel
- Serving as a resource for data breach notification requirements and other legal obligations under applicable federal and state laws
- Identifying what aspects of the response/mitigation efforts should be protected by the attorney-client privilege (e.g., documents and telephone conferences)

6.2.4 HR representative's responsibilities

- Coordinate with employees to direct communication/questions related to breach to company's DPO

6.2.4 All authorized user's responsibilities

- Reporting an actual or suspected data breach via designated channel
- Supporting the investigation by providing relevant support and evidences on actual or suspected breach

6.3 REPORTING A DATA BREACH

- Any individual who accesses, uses or manages the personal data collected, stored or transmitted by Writer Relocations is responsible for and shall report actual or suspected data breach immediately to the data protection officer at huz.ban@writerrelocations.com
- If the breach occurs or is discovered outside normal working hours, it shall be reported as soon as is practicable
- The report shall include full and accurate details of the breach in Breach Reporting Form. (**Refer Appendix A**)

6.4 PRELIMINARY ASSESSMENT OF THE DATA BREACH

- Once a breach has been reported, a preliminary assessment shall be carried out by DPO to evaluate the severity of breach.
- The severity shall be established based on the levels defined in this policy (**Refer Appendix B**)

6.5 DATA BREACH RESPONSE PLAN

The data breach response to any reported breach shall undergo following phases:

- Containment and Recovery
- Investigation and Data Protection Impact Assessment (DPIA)
- Notification
- Evaluation and Response

6.5.1 Containment and Recovery

- The DPO shall firstly determine if the data breach is still ongoing, if so the appropriate steps shall be taken immediately to minimize the impact of the data breach
- Basis the severity and type of breach the data protection officer shall identify relevant representatives who shall lead the breach investigation
- The data protection officer and investigation representatives shall identify potential ways to limit the damage the breach could cause and/or to recover any losses occurred due the breach
- The data protection officer shall identify which all parties need to be notified as part of the initial containment and shall inform such parties on immediate basis
- The data protection officer in liaison with the investigating representative shall determine the suitable course of action to be taken to ensure resolution of the incident
- Advise from internal process owners or external experts may be sought in resolving the breach

6.5.2 Investigation and Data Protection Impact Assessment (DPIA)

- An immediate investigation shall be initiated by data protection officer and identified investigation representative and wherever possible within 24 hours of the breach being identified or reported
- The data protection officer and investigation representative shall investigate the breach and assess the risk associated with the consequences of the breach
- The investigation shall at least take following into consideration:
    - The personal data involved
    - The severity of personal data and the number of individuals affected
    - The existing protections or security controls in place for protecting the data
    - What happened to personal data such as whether it is lost, modified, accessed etc.
    - Whether the data could be put to any illegal use
    - Whether there are wider consequences of the data breach

6.5.3 Notification

- The data protection officer in consultation with the legal representative and CEO of Writer Relocations shall identify the parties who needs to be notified of the breach
- For GDPR, Writer Relocations shall notify the data controller, supervisory authority and/or Information commissioner's office (ICO) without any undue delay or not later than 72 hours from the discovery of breach.
- While identifying the parties who needs to be notified at least following shall be considered:
    - Any legal, regulatory, contractual notification requirements
    - Whether the notification would assist the affected the individual to mitigate their risks
    - If many individuals are affected and the breach has very serious consequence, then the ICO shall be notified at security breach helpline **0303 123 1113** or via email at **casework@ico.org.uk** using the breach notification form available at **https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/**.
    - The ICO can also be notified by sending breach notification form via post **to Wycliffe House, Water Lane, Wilmslow, Cheshire SK95AF**
    - Alternatively, ICO can be informed by filling up their online form and submitting it: https://ico.org.uk/media/2258298/personal-data-breach-report-form-web-dpa-2018.doc
- The affected individuals shall be notified with a description of how and when the breach has occurred and what personal data has been breached.
- Clear advice shall be given to affected individuals on what they can do to protect themselves, and include what mitigation actions has already been taken to mitigate the risks
- The affected individuals shall be given a mechanism to contact to Writer Relocations for further questions and clarifications.
- The data protection officer shall notify external third parties such as but not limited to service providers, police, banks, insurers etc. when it is identified that illegal activities may be performed using personal data
- The data protection officer shall prepare to address incoming media queries
- All the actions shall be recorded by Data protection officer

6.5.4 Evaluation and Response

- After the breach is contained, the data protection officer shall carry out a complete review of the root causes, effectiveness of response, and whether any changes are required in policies, procedures and infrastructure
- The data protection officer shall review existing security controls to determine accuracy and effectiveness of the implemented controls and identify whether any corrective action needs to be taken
- The review by the data protection officer shall at least consider following:
    - Where and how the personal data is collected and stored
    - Identify major risk areas and potential weak points within existing controls
    - Evaluating personal data transmission and sharing mechanism for its effectiveness

- Evaluating the awareness of employees handling personal data or systems where the personal data is collected, processed or stored
- Evaluating the adequacy and effectiveness of breach response plan

- A report recommending reasonable changes to infrastructure, policies and procedures shall be submitted by data protection officer to management

7. Special situations and Exceptions

Writer Relocations top management, government or any other regulatory body or norms thereof may override Writer Relocations policies / procedures at any time.

8. References

- General Data Protection Regulation (2016)

9. Appendix A: Data Breach Reporting Form

Notification of Data Security Breach	To be filled by person reporting the data breach or by data protection officer
Unique ID / Number of the data breach	
Date & time when the breach was discovered	
Place of the data breach	
Date & time when the breach was reported to data protection officer	
Name & designation of person reporting the data breach	
Contact details of the person reporting the data breach (email and phone number)	
Confirmed or suspected data breach?	
Is the breach contained or ongoing?	
Brief description of the data breach or details of personal data lost	
Volume of the personal data involved; if known	
Number of affected data subjects; if known	
Type of data subjects	
Severity of the breach (as per the severity classification mentioned in **Appendix B**)	
Brief description of any actions taken when the data breach was discovered	
Who all have been informed of the data breach in Writer Relocations?	
Details of the IT systems, equipment, devices, or media involved in data breach	
If the breach is ongoing, what actions are being taken to contain the data breach?	
If the breach is ongoing, what actions are being taken to recover the data?	
Actions taken by respective investigating officer	

Follow up actions required / recommendation	
Only to be filled by data protection officer	
Reported to internal stakeholders	Yes / No, if yes; notified on: Details of notification:
Reported to data subjects	Yes / No, if yes; notified on: Details of notification:
Reported to data controller	Yes / No, if yes; notified on: Details of notification:
Reported to Supervisory Authority	Yes / No, if yes; notified on: Details of notification:
Reported to ICO	Yes / No, if yes; notified on: Details of notification:
Reported to Media	Yes / No, if yes; notified on: Details of notification:
Reported to other applicable regulatory bodies and external stakeholders	Yes / No, if yes; notified on: Details of notification:
Reported to Police	Yes / No, if yes; notified on: Details of notification:
Reported to external third parties such as but not limited to service providers, banks etc.	Yes / No, if yes; notified on: Details of notification:
Reported to insurers	Yes / No, if yes; notified on: Details of notification:

10. Appendix B: Data Breach Severity Evaluation Form

Data Breach Severity Assessment	To be filled by Data Protection Officer
Details of the IT systems, equipment, devices, or media involved in data breach	
How much personal data has been affected?	
How many data subjects are affected?	
What is sensitivity of personal data affected? Please list down all type of personal data which has been affected.	
Is sensitive personal data such as but not limited to following involved: • Racial origin • Ethnic origin • Political opinions • Religious belief • Physical and/or mental health • Sexual life • Criminal proceedings, offences	
Is personal data which can be used to commit illegal activities such as identify fraud involved? For example: SSN, national ID, bank account numbers, passports, visas etc.	
Is the personal data which could cause distress to affected individual if disclosed; involved? For example: Salary information, work performance etc.	
Are there any contractual security requirements which are bound for the affected personal data?	
High Severity: Major Data Breach	
The severity of the data breach shall be classified as **"High"** if any of the below conditions are met: • Sensitive personal data is involved • Number of affected data subjects >>> • Third party data is involved • Consequences of data breach are irreversible • Likely media coverage • Immediate breach response is required regardless of whether the breach is contained or not • The breach requires response beyond normal working hours	**Final Severity Rating:** **Justification for assigning the severity:** **Designated Investigating officer:** **Contact Details of Investigating officer:** **Other relevant internal / external contacts:**

Moderate Severity: Serious Data Breach	
The severity of the data breach shall be classified as **"Moderate"** if any of the below conditions are met: • Personal data is involved • Number of affected data subjects > • The data of third party is not involved • Significant inconvenience will be caused to affected data subjects • If the breach may not yet be contained	**Final Severity Rating:** **Justification for assigning the severity:** **Designated Investigating officer:** **Contact Details of Investigating officer:** **Other relevant internal / external contacts:**
Low Severity: Minor Data Breach	
The severity of the data breach shall be classified as **"Low"** if any of the below conditions are met: • Personal data is not involved • Number of affected data subjects < • Slight inconvenience will be caused to affected data subjects • Affected data is duly protected using encryption • Incident can be responded during normal working hours	**Final Severity Rating:** **Justification for assigning the severity:** **Designated Investigating officer:** **Contact Details of Investigating officer:** **Other relevant internal / external contacts:**