Title	Data Protection Impact Assessment – Redstor Cloud Service
Process Owner	Farid Ouazzani
Date Created	13/07/2022
Publish Date	17/07/2023
Approved By	CEO
Summary	The following document records the Data Protection Impact Assessment (DPIA) process and outcome. It follows the process set out in Information Commissioner's Office (ICO) DPIA guidance.
Classification	Public
Standard	All
Version	1.5

Change Record
Enter any changes to the document within the tag below…
DPIA for Redstor cloud service as of July 2023. Change Comment: Updated to include reference to Azure VM Backup in service description. Change Comment: Also updated sub-processor paragraph to include updated references to sub-processing.
Overwrite the content of the tag, this will create each change you have made to the document and record it in ISOportal

Data Protection Impact Assessment – Redstor Cloud Service

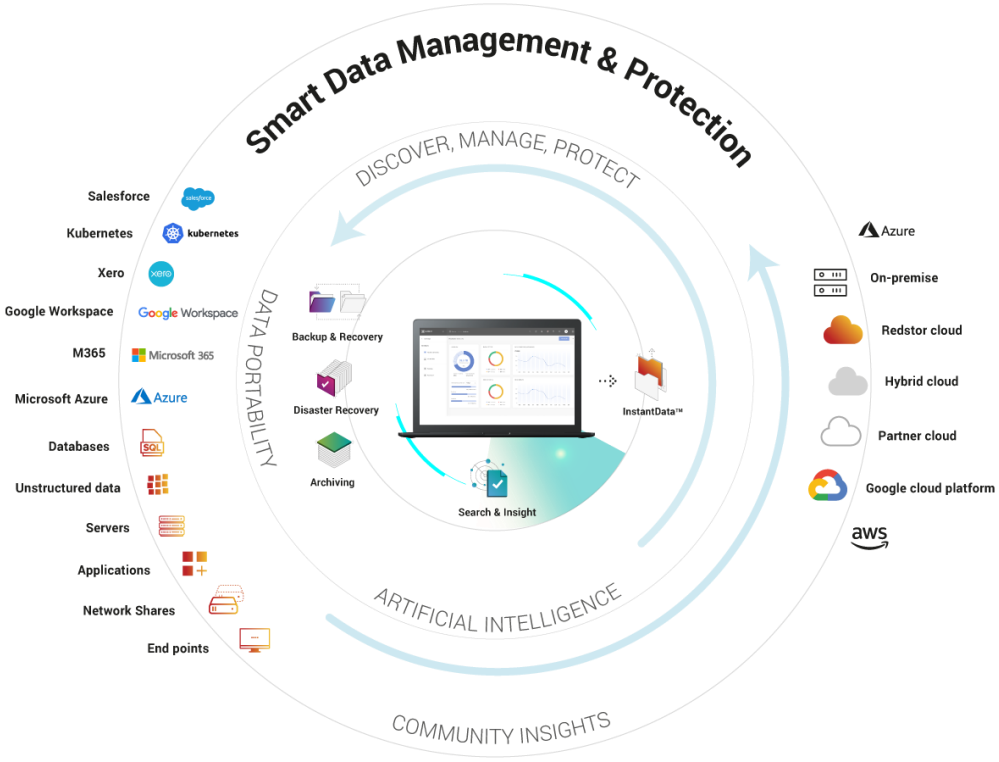
Background and the Identification of Need for DPIA

A determination was made that a DPIA should be completed for the Redstor service given that Redstor serves as a cloud-based data management provider, specialising in backup and recovery. This determination was made given the nature of the Redstor service and the wide range of industry verticals the service is provided to. It was determined that the potential for storing sensitive customer data as part of the service was probable.

"Redstor" is the name given to the Redstor cloud-based service which provides data management services to customers. May also be referred to as "Redstor Pro" or "Redstor Cloud Pro".

Redstor is a disruptive SaaS technology, providing backup and recovery capability for data spanning infrastructure, cloud-native and SaaS environments. AI and machine-learning built into the fabric of the Redstor service automates repetitive tasks, while protecting against the growing risk of ransomware, making backup simpler, safer, and smarter.

- **Cloud Backup and Archiving for Infrastructure -** Rapid cloud backup and recovery for on premise and cloud-based servers, desktops, and laptops, providing instant access to live and archive data.
- **Microsoft 365 Backup -** Back up all Microsoft 365 data within OneDrive, SharePoint, Exchange, Teams, and OneNote, directly from the Microsoft cloud to the Redstor cloud.
- **Google Workspace Backup -** Back up all Google Workspace data within Drive, Gmail, Classroom, Calendar, and Contacts, directly from the Google cloud to the Redstor cloud.
- **Azure VM Backup** - Back up your virtual machines in minutes with Azure VM Pro, the Redstor agentless backup solution for Azure Virtual Machines.
- **Azure Kubernetes (AKS) Backup -** Back up AKS data in minutes with unparalleled operational simplicity.
- **AWS Kubernetes (EKS) Backup -** Back up Amazon Elastic Kubernetes Service (EKS) with powerful simplicity.
- **Salesforce Backup -** Back up Salesforce CRM data and metadata directly from the Salesforce cloud to the Redstor cloud.
- **Xero Backup -** Back up Xero-based accounting data directly from the Xero cloud to the Redstor cloud.
- **Azure Mobility -** Move a virtual machine from its current location to Microsoft Azure.
- **Detect and remove malware from backup data (add-on) -** Deploy AI to remove threats from within backup data, helping to ensure malware-free recoveries. This add-on is available for Redstor's Cloud Backup and Archiving for Infrastructure, Microsoft 365 Backup and Google Workspace Backup services.
- **Data Tagging** - Data tagging provides visibility of how much protected data is highly sensitive or sensitive in nature. This enables organisations to better manage exposure and the concentration of sensitive documents to protect data in the most efficient way.



Description of Processing

In relation to customer data, Redstor will collect, receive, transmit, and store data as per the following.

- **Data Collection** – Data is "collected" using the Redstor software. This includes the on-premise agent known as the ESE client and the cloud native suite known as RedApp. In both cases the "receipt of data" applies.

- **Receipt of Data** - As per the above diagram, customer data will be received from customer environments (*depicted on the right side of the diagram*). This data is encrypted at source prior to being transmitted to Redstor. This data is therefore considered "secured" as to mean it has been rendered unusable, unreadable, or indecipherable to unauthorised individuals.

- **Transmission of Data -** The encrypted data (using AES-256) is securely (using 128-bit TLS) transmitted to the Redstor cloud environment (depicted on the right of the diagram) from the customer environment.

- **Storage of Data** – Once transmitted, data is then stored within the Redstor cloud environment in its encrypted form (AES-256). The data maintains end to end encryption throughout its journey from the customer environment to the Redstor cloud environment.

- **Further Transmission of Data** - Once the data is protected within the Redstor cloud environment it is then available for use by the customer. The customer can interact with or restore data using the available tools which include, the agent, InstantData and the RedApp cloud portal. All these forms of data access require the encryption key which is generated at the point of account creation by the customer. For cloud native backups such as Office365 or Google Workspace the encryption key is

autogenerated at the point of account creation. These keys are not accessible or known to Redstor employees thus preventing unauthorised access to data. Should a customer misplace or forget their encryption key it would not be possible to perform the restore unless the customer has provisioned a "Collection or Group Certificate". Using the aforementioned tools, the customer can restore data from the Redstor cloud environment. This data is transferred to the customer securely using 128bit TLS transmission. The decrypted data is then available to the customer within the customer's environment.

Scope of Processing

- **Data Sources** - The Redstor service protects customer data from a wide range of sources as per the provided background information and description of the service. The nature of the data protected is customer data in its various forms. As the data is encrypted Redstor makes a reasonable assumption that the data under its protection includes personally identifiable information and that it would be considered sensitive in some cases.

- **Use of Data** - Redstor does not use the data it stores for its customers, rather Redstor securely protects the data offsite for the customer in line with the National Cyber Security Centre (NCSC) guidelines regarding the 3-2-1 rule of backup and recovery.

- **Frequency of Collection** - Data is collected from a variety of customer specified sources, typically on a daily cadence, however, backup frequency is configurable and determined by the customer.

- **Retention of Data** - Data is retained as per the retention policy defined or agreed by the customer. Standard data retention is up to two months of daily backups in addition to two month ends (the latest available backup for each of the two prior months). Retention can be increased beyond this as per the customer's retention policy requirements. Any specified retention within a service agreement (contract) will supersede any retention lengths described herein.

- **Deletion of Data** - Data protected using Redstor pertaining to a given customer will be deleted at the end of contract without undue delay. Our standard process at end of contract once the termination period has been observed is to provide the customer with 24 hours' notice that their data will be deleted subject to a final confirmation from the customer after that 24hour period has elapsed. This is known as the "cooling off" period.

Geographical Areas Covered – Supporting more than 40,000 customers worldwide, Redstor is 100% channel focused and is headquartered in the United Kingdom (UK) with a global footprint, which includes Redstor-owned physical machines located at colocation facilities within the UK and South Africa, as well as cloud environments hosted by Microsoft Azure hosting facilities (US Central, US West, France Central, West Central, East Asia and Australia East) Redstor ensures that sovereignty is maintained for customers that wish to retain their data in region. For example, for our UK based customers, data will reside within our two UK based colocation data centres in Slough and Reading respectively. Should the customer wish to change the region in which their data is stored, a ticket with our support team can be raised where an evaluation of the request can be made.

Context of Processing

In the context of the Redstor data management service and in relation to the protection of customer data, Redstor are considered data processors. Redstor is the service provider of services to downstream customers (resellers or partner organisations) who in turn provide the Redstor service to their customers.

The customer has control over what they choose to protect, how often they wish to protect it, how long they wish to retain it and in which Redstor region they choose to store it. Similarly, the customer has control over when the data is retrieved and who has access to it. Furthermore, the customer has control over when the data is deleted whilst in contract with Redstor. At contract termination the data is deleted. The customer is considered the data controller.

Purpose of Processing

As per the description of service, Redstor processes data on behalf of its customers to provide data management services inclusive of backup and recovery, archiving, malware detection, data tagging and insight. Processing data provides customers with the benefit of peace of mind that they can access, manage, and recover data as and when required from a highly available simple, smart, and safe cloud-based service. Without access to the customer data, it would not be possible to provide such a service to customers.

Description of Processing (and Sub Processors)

Redstor shall ensure that all persons authorised by it (or by any Sub-Processor) to process protected data are subject to an obligation to keep the protected data confidential (except where disclosure is required in accordance with applicable law, in which case Redstor shall, where practicable and not prohibited by applicable law, notify the end user (customer) of any such requirement before such disclosure). Information relating to our use of sub–processors is publicly available here: https://www.redstor.com/sub-processors/

Consultation

In the development of the DPIA the following stakeholders were considered.

- Data Protection Officer (DPO)
- Subject Matter Experts (SMEs)
- Head of Information Security

The DPIA also refers to and has made use of existing documentation.

There are no sub-processors involved with the delivery of the Redstor service therefore consultation with one or more sub-processors is not applicable.

Furthermore, the DPIA will be reviewed by the Data Protection Officer prior to document approval.

Necessity and Proportionality

Redstor will process end user personal data for the purposes of providing the service to customers in accordance with the service agreement. The legal bases we may rely on include:

- Consent: where Redstor has been given clear consent for to process personal information for a specific purpose.

- Contract: where use of personal information is necessary for a contract Redstor has with the customer, or because the customer has asked Redstor to take specific steps before entering into a contract.
- Legal obligation: where our use of personal information is necessary for Redstor to comply with the law (not including contractual obligations)
- Legitimate interests: where the use of personal information is necessary for legitimate interests or the legitimate interests of a third party (unless there is a good reason to protect personal information which overrides our legitimate interests)

It is not possible to provide the services to customers without obtaining a copy of the data albeit in an encrypted state from the customer. Redstor services are designed, developed, implemented, and reviewed with security in mind.

Function Creep

To avoid function creep, changes or additions to the service are carried out with careful consideration of data protection legislation and the duty of care maintained by Redstor on behalf of our customers.

Data quality is maintained through several technical measures in addition to Redstor being ISO9001 (Quality) certified for our business practises. Further detail regarding these measures can be provided on request.

Data minimisation is achieved by ensuring that each element of the Redstor service is designed, developed, and implemented to a specification brief. All aspects of the Redstor are reviewed to ensure purpose fit and relevance to the service offering.

Information Sharing

Redstor will share personal information with law enforcement or other authorities if required by applicable law. Such activities will be carried out as per the Forensic Readiness Policy. Redstor will not share or sell your personal information with any other third party.

Redstor may receive data from third parties, including resellers, but we do not otherwise deal with third party data. Where Redstor receives data, it does so on the basis of a Data Processing Agreement.

Individuals

Redstor adheres to the General Data Protection Regulation (GDPR). Under GDPR individuals have several important rights. For information on each of these rights, including the circumstances in which they apply, see the Guidance from the UK Information Commissioner's Office (ICO) on individuals rights under the General Data Protection Regulation.

Redstor provides contact information and a process should individuals wish to exercise any of these rights. This information is displayed publicly on the Redstor website https://www.redstor.com/privacy-policy/.

International Transfers

Redstor provides the ability for customers to retain data "in country" ensuring that customers can comply with any data sovereignty requirements that they made have. Redstor will not transfer or migrate customer data to another region (country) or geographic territory without communicating such intent, in writing, to the customer in advance of such activity.

Data Protection Measures

Documented herein are some of the core technical and non-technical measures implemented to ensure that customer data is protected. The measures summarised within are some of the measures taken to safeguard data. This is not a definitive account of all measures or controls in place. Further information regarding specific controls can be provided on request.

Certifications and Examinations

Redstor maintains certification in ISO9001 (Quality), ISO27001 (Information Security), ISO22301 (Business Continuity) and has undertaken Type 1 SOC2 (Service and Organisation Controls) examinations. Furthermore, the Redstor service for customers in the Unites States has undertaken a Type 1 HIPAA (Health Insurance Portability Accountability Act) examination.

The certifications and examinations demonstrate that Redstor have the internal processes in place to ensure high levels of service. Furthermore, Redstor undertake annual external audits by accredited and licenced third parties to ensure compliance with the above. In accordance with ISO 27001 and SOC2 Redstor has implemented a number of technical and non-technical controls. These ensure adherence to the requirements of these standards which fundamentally are there to protect the security, availability, integrity and confidentiality of our customers' data.

Awareness Training

In accordance with ISO27001, SOC2 and HIPAA, Redstor has implemented information security and cyber security awareness training for its employees. New employees undertake ISO and related training on commencement of employment and existing employees undertake annual refresher training. Furthermore, interactive cyber security awareness training is provided to all employees on a monthly cadence.

Encryption

Summary

As per the service description, to reduce the risk of unauthorised access to customer data and to ensure the security of the service, Redstor encrypts data at source using 256-bit AES (GCM) encryption. This data is further protected using 128-bit TLS ciphers during transmission. Encryption is managed using keys. Encryption keys are unique to every backup account and are chosen by the customer or generated by the software in the case of cloud native backups. Data cannot be read without the encryption key and at no point are these encryption keys visible to Redstor employees.

ESE Agent Security

Each Redstor account has its own encryption key, which is used to encrypt that account's data during the backup process. The encryption key is essential to recovery and is neither retrievable nor readable unless a Group Certificate is present. If the encryption key is lost or forgotten, there is no way to access the backed-up data, not even for Redstor employees.

During the backup process, data blocks are compressed with LZ4 and then encrypted on the Agent using the user's encryption key specified when the account was created. This encryption occurs prior to data being transferred to the Redstor Cloud. TLS is used to authenticate the data transfer and to create a secure session between the Agent and the Redstor Cloud.

We use a symmetric-key cryptographic block cipher, 256-bit Advanced Encryption Standard (AES) in Galois Counter Mode (GCM) or AES-GCM to ensure authenticated encryption, guaranteeing the integrity of your data. Through AES-GCM, the integrity of each block of data is verified using its inherent checksum before

being stored on the Redstor Cloud. Files that have become corrupt or are missing on the Redstor Cloud (due to disk corruption, for example) are identified by integrity checks and are retransmitted to the Redstor Cloud at the start of each backup.

During a backup, the Agent maintains a rolling buffer of data transmitted to the Redstor Cloud. Whenever a connectivity drop and subsequent reconnection to the Redstor Cloud occurs, the service resumes from the exact position of interruption, seamlessly continuing the backup without having to start at the beginning of the file. This is especially useful when large files are being transferred. For more information on how ESE maintains data integrity, see Article on our support site 1102 https://support.redstor.com/hc/en-gb/articles/360007741113.

Cloud Security

Each Cloud account within a backup set has its own encryption key. Since the Cloud to Cloud backups are run by a single administrator of a tenant with many users, an encryption key is randomly generated for each of these Cloud accounts. The encryption keys are never presented to anyone and cannot be retrieved.

The encryption key is then secured in Azure Key Vault to ensure it is neither available nor visible to anyone. The only entity that has access to this Key Vault is the Cloud to Cloud application itself, which is also hosted in the same Cloud region in Azure.

InstantData recovery requires an account and encryption key to initiate a recovery. However, it is not secure to return an encryption key to an administrator. Instead, a short-lived session is created by the Cloud to Cloud application. A link is generated from this session which allows a user to recover data for a limited period without needing to enter their encryption key. The link is only valid until the session expires.

During the backup process, data blocks are compressed with LZ4 and then encrypted using the encryption key specified when the account was created. This encryption occurs prior to data being transferred to the Redstor Cloud. TLS is used to authenticate the data transfer and to create a secure session between the account and the Redstor Cloud.

Redstor uses a symmetric-key cryptographic block cipher, 256-bit Advanced Encryption Standard (AES) in Galois Counter Mode (GCM) or AES-GCM to ensure authenticated encryption, guaranteeing the integrity of customer data. Through AES-GCM, the integrity of each block of data is verified using its inherent checksum before being stored on the Redstor Cloud. Files that have become corrupt or are missing on the Redstor Cloud (due to disk corruption, for example) are identified by integrity checks and are retransmitted to the Redstor Cloud at the start of each backup.

If the connection to the Redstor Cloud is interrupted, the backup service resumes seamlessly, starting again at the beginning of the interrupted file.

Vulnerability and Penetration Testing

Redstor performs monthly vulnerability and penetration testing to minimise the risk of a data breach. These tests are carried out by a CREST approved, independent third party. Additionally, Redstor has implemented appropriate measures to ensure security by design to meet the requirements of data protection legislation and to protect the rights and freedoms of individuals (data subjects). To mitigate the risks associated with availability and data loss Redstor maintains two offsite copies of customer data, one copy in the primary data centre and another in the secondary data centre. These sites are equipped with redundancy at multiple levels of the data centre and infrastructure stacks.

Patch Management

In accordance with information security compliance requirements, Redstor ensures that all systems, inclusive of those internal to Redstor and our public production services, are patched (updated) monthly as a minimum. Critical updates will be applied as soon as is possible.

Access Control

In accordance with information security compliance requirements, Redstor applies the "principle of least privilege" regarding access rights and access control as per our Access Control Policy. This approach reduces the number of employees with access to restricted systems. It strictly ensures that only those in roles which require access will be authorised for systems use. Ensuring our employees have access to that which is necessary to execute their role's responsibilities is fundamental to our approach to securing identity and access management of our systems. The process is managed through the lifecycle of employment.

Physical Security

Redstor data centre facilities feature an abundance of physical security controls. These include, gated perimeters, number plate recognition for vehicles, 24/7/365 manned security personnel, man traps, surveillance cameras, alarm systems, biometric access control and card-based access control as a second factor of authentication. Further information regarding the security and availability of Redstor data centre locations is available on request.

Redstor office locations, are equipped with physical door locks, card-based access controls, surveillance cameras and an alarm system.

Change Management

In accordance with information security compliance requirements, Redstor maintains a Change Management Policy. Change management helps ensure and protect our customers' data. By carefully considering and assessing changes within Redstor it is possible to identify those changes that may have an impact on customer data either directly or indirectly. Changes are managed as per the policy and consider a risk analysis of the proposed change(s). Changes are reviewed prior to being accepted. Changes are also reviewed having been implemented. Any items or stakeholders associated with a change, such as related documentation, will be updated or in the case of personnel, will be communicated with. Further information regarding change management can be provided on request.

Identification and Assessment of Risk

The table below lists the identified risks and the likelihood and severity of harm to the individual. Based on the combination of the "likelihood of harm" and the "severity of harm" an overall risk value is derived. The risk considers the existing measures and controls when determining the likelihood of harm to an individual and the severity of harm should it take place.

Description of the risk source and nature of potential impact on individuals	**Likelihood of Harm** ***[Remote, Possible, Probable]***	**Severity of Harm** ***[Minimal, Significant, Severe]***	**Overall Risk** ***[Low, Medium, High]***
Encrypted (AES-256) data breach	Remote	Minimal	Low
Metadata breach	Remote	Minimal	Low
Accidental or unauthorised deletion of data (unrecoverable)	Remote	Significant	Low

Compromise of data, recoverable (e.g., ransomware)	Remote	Minimal	Low
Denial of service (cyber-attack)	Remote	Minimal	Low
Prolonged loss of service (business continuity)	Remote	Minimal	Low
Unauthorised access to customer account(s)	Remote	Significant	Low

Results and Recommendations

Based on the identification of the above risks and the determined overall risk scores for each risk, a conclusion has been drawn to accept the risk levels for each item as they are deemed to be low given the existence of many mature existing measures and controls operating within Redstor. Redstor maintains a risk register of risks as part of our approach to Risk Management which this DPIA feeds into.

Given the evaluated risk of harm to data subjects rights and freedoms is low based on current requirements of applicable legislation, it has not been deemed necessary to recommend any treatment plans to reduce risk for any of the above findings. The recommendation is therefore to continue to seek service improvements wherever possible and to review the service within 12 months of the publication of this DPIA.

Review

This DPIA will be reviewed annually and updated as appropriate and where relevant to ensure that control measures up to date and reflect any changes that may have taken place following the completion of this DPIA.

Recommended Review Date:	On or before the 13/07/24
Review To Completed By:	Data Protection Officer

Data Protection Officer Statement

I the DPO for Redstor, can confirm that I have reviewed the DPIA above and am satisfied that Redstor has taken appropriate and proportionate measures to protect customer data.

Signed:	Farid Ouazzani
Date:	13/07/23