IBM Consulting

G-Cloud 15
IBM - Privacy - Defensible Data Retention Service

Email: ukcat@uk.ibm.com
Contact: Anne-Marie Wheeler

Contents

Defensible Data Retention Service

Key features of this service

This service is delivered by the IBM Privacy and Data Services team and is a **defensible data retention framework** which results in an organisation being able to store and exploit their data in a cost-effective and resilient way, while reducing operational and cyber-related risk and compliance with data protection laws.

Key features include:

- Delivers robust data retention processes and procedures therefore minimising risk
- Ensures data retention framework meets privacy and compliance rules
- Full service from advisory to design, build and deploy
- Delivered by experts in privacy and data lifecycle management
- Pre-built assets and delivery methodology based on client experience
- Framework decision tree for choosing retention treatment to apply
- Can include use of data management tooling to apply treatments
- Flexible service options from set-up only to full managed service

Key benefits of this service

- Results in total managed view of full end-to-end data landscape
- Tighter control of data lowers operational, cybersecurity and privacy risk
- Minimises cost of data storage
- Delivers complete understanding of data usage and associated privacy management
- Lowers risk of privacy fines and regulatory scrutiny
- Controlling the data landscape improves response to data access requests
- Controlling the data landscape improves response to complaints
- Data transparency demonstrates trustworthiness
- Data minimisation and user access on need to know basis
- Ensures the CPO meets data minimisation and storage limitation obligations

Defensible Data Retention Service

Why is the service needed

Overview

Organisations need to manage their data assets effectively to increase process efficiency, provide accurate and trusted information and improve relationships with users of their services. Data volumes and velocity have grown exponentially. However, this is resulting in large scale expansion of data storage and the accompanying growing complexities of managing that data.

Organisations are drowning in data which is spread across multiple systems and often duplicated many times. Data can be structured or unstructured or a mixture of both. In the past, archive and deletion processes were neglected and not seen as necessary as data storage costs got cheaper.

Several internal and external drivers have now come together to compel organisations to review their data management policies and put in new controls to properly manage the end to end data lifecycle from creation to deletion.

Failure to recognise the need to improve data management could lead to increased operational risks, reputational damage and fines for non-compliance.

1. Data Protection Legislation

The General Data Protection Regulation (GDPR) which is part of the Data Protection Act 2018 in the UK has required organisations to produce a Record of Processing Activity (ROPA) which demonstrates that all stored personal data has a legitimate basis of processing. Any data that is not being processed legitimately must be removed or anonymised.

The Information Commissioner's Office (ICO) is responsible for investigating data breaches and issuing fines and currently, the five largest fines issued by the ICO for breach of data protection law add up to nearly £50 million.

https://ico.org.uk/action-weve-taken/enforcement/

High profile companies such as British Airways, the Post Office and Marriott Hotels are among the organisations that have had serious data breaches. Government departments are not immune and the Cabinet office was fined £500k, reduced for £50k on appeal, for the well-publicised postal address leak of the 2020 New Year Honours recipients. Accordingly, the failure to protect this information led to the leaking of over 1000 home addresses online. Furthermore, many high-profile individuals were among the victims.

2. Operational Resilience

All organisations now rely totally on IT to run their business and operational failure leads to customers being unable to transact business. Recently high-profile IT failures in retail banking have not only caused reputational damage but has also led regulators to insist on financial services organisations demonstrating they are operationally resilient and have robust contingency plans in place to cope with

IT issues. Having to backup and recover legacy data that is no longer required is wasted effort and cost. As more and more organisations rely totally on IT, then they also need to put in more operational controls.

3. Cyber Attacks

Organisations are constantly under threat and in the case of an attack need to minimise the data that is lost. Many Chief Data Officers and Information Security Officers are concerned that they will lose data in an attack that they did not even know they had. Data breaches can result in large fines under data protection legislation.

4. Proliferation of Orphan Data

Many systems hold old legacy data sets which are no longer needed and, in some cases, no longer readily accessible due to broken links, yet they continue to incur both infrastructure and maintenance cost as the data has never been removed.

Summary

In summary Organisations need to reduce their risk exposure and there is now a compelling business case to invest in proper defensible data management and retention. Defensible retention solves the inherent conflict between data consumers such as data scientists demanding more and more data and the Data Protection Officer or the Chief Security Officer trying to minimise risk. Defensible retention provides an agreed and justified policy driven data archive/deletion schedule that the whole business must follow.

This service delivers a defensible data retention framework which results in an organisation being able to store and exploit their data in a cost-effective and resilient way while reducing operational and cyber risk and meeting compliance with data protection laws.

Defensible Data Retention Service

Service description

50-word summary:

IBM’s Defensible Data Retention service helps reduce data privacy risks, comply with data protection laws, and reduce storage costs by establishing a data lifecycle and retention framework. Through advisory, design and implementation, IBM enables classification, treatment and governance of data end-to-end, strengthening operational resilience and delivering transparent, trustworthy data management.

Service options

The IBM scope of service comprises of three sub-offerings.

1. Establish Retention Framework

An 8 to 12 week piece of work that establishes the framework, the decision tree and the treatments and is typically sponsored by the Chief Operating Officer, the Chief Data Officer or the Data Protection Officer.

To kick start the work, IBM uses a framework asset developed over multiple client engagements. The objective is to develop the framework so it can be used with business and technical data owners to decide on the right treatment for their data sets starting with applications that pose the highest risk. While this work typically initially focuses on data sets that contain personal data as these pose the most risk, it can also be applied to all data sets such as those in legacy systems where old data sets are being kept but are no longer used.

Typical activities are:

- Review any current data retention policies and governance that is already in place
- Review existing process documentation such as Record of Processing Activity developed for Article 30 of GDPR
- Adapt the framework, the treatment decision tree and the treatments to suit the organisation
- Review application catalogues to help identify prioritisation areas
- Test the framework and treatment decision tree on one or two business and data owners and revise if required
- Identify the "Top Ten" applications at most risk to start applying treatment.

2. Treatment Rollout

Following the establishment of the retention framework, the next piece of work is applying the treatment to each application. The size and length of the rollout would be dependent on how many applications needed to be treated and the recommendation would be to prioritise the applications by risk level and start with those that are both high risk and easy to treat.

The IBM offering is flexible and for example can consist of a small team of SMEs to guide and support the organisation through to providing teams using a factory model to carry out the treatments. The factory model allows scaling up and down of "pods" - typically one per application - who would use specialist tools and/or bespoke development if required to apply the treatment and to build the on-going scripts to maintain the data minimisation.

Typical activities are:

- Classification - gather all the information on the application that is required to apply the treatment(s)
- Confirm and detail the treatment pattern(s) for the application - work with application owners to determine which treatment patterns and business rules to apply under what circumstances. Produce detailed design document
- Build - Set up an application development environment to build and test the treatment(s) and produce treatment scripts
- Apply- Once fully tested apply treatment(s) to application
- Maintain - Productionise the treatments for the application so that data minimisation is maintained going forward.

3. Application Maintenance Service

If required, IBM can provide on-going maintenance services making sure the application of data minimisation becomes business as usual. This would be a bespoke service depending on the organisation's needs.