Protecting Data Privacy Beyond the Trusted System of Record

Bill White
Mark Moore
Phillip Wilson
Eva Yan
Executive overview

Your sensitive data might already be protected with encryption on a trusted system of record, such as the IBM® Z. However, as soon as that data leaves the confines of the trusted system of record, several questions immediately come to mind:

- **Can data privacy and protection be maintained and enforced?**
  
  Your system of record is trusted to maintain data privacy and protection. When shared, sensitive data that was encrypted is decrypted, copied, and may or may not be reencrypted before it is stored. After it is taken from that system, data protections must remain intact. Adequate controls to retain end-to-end data privacy and protection must be available.

- **Can access to data be revoked?**
  
  Your sensitive data must always be protected, compliance must be guaranteed, and consent must be respected. If conditions that are related to your sensitive data change, such as access or use, the ability to respond and comply must be possible.

- **Is data privacy and protection provable?**
  
  Information about data access, use, and policies must be readily available for auditing purposes. In addition, time that is spent by your security staff, auditors, and developers to administer and prove proper data privacy and protection is in place, should be minimized.

To help you safeguard your sensitive data and provide ease of auditability and control, IBM introduced a new capability for IBM Z® called IBM Data Privacy Passports. It can help minimize the risk and impact of data loss and privacy breaches when collecting and storing sensitive data. Data Privacy Passports can manage how data is shared securely through a central control of user access.

Data Privacy Passports can protect data wherever it goes. Security policies are kept and honored whenever the data is accessed. Future data access may be revoked remotely via Data Privacy Passports, long after data leaves the system of record, and sensitive data may even be made unusable simply by destroying its encryption key.

Data Privacy Passports is designed to help reduce the time that is spent by staff to protect data and ensure privacy throughout its lifecycle via a central point of control.

This IBM Redguide presents a business view of Data Privacy Passports, including how data privacy and protection concerns are addressed. We also explore how value is gained through various business model examples.
Data privacy and protection impact business

Data drives business. The most valuable data (that is, the data that enables business to anticipate needs, predict buying patterns, and better serve customers) often includes personal data. As more personal data is collected and shared, governments and industry regulatory bodies are creating ever more stringent rules for data protection and acceptable data use, with fines for violating those rules. However, this does not represent the greatest financial risk. If data is lost or misused, loss of trust, reputation, and the resulting loss of business are the greatest threats.

There are two broad categories of data risk:

- **Data loss**
  
  Data is stolen or improperly exposed. Probably, most imagine hackers breaking into servers to steal data; however, most data breaches are insider jobs, and many are unintentional. Though a study conducted by the Ponemon Institute, which explored financial impacts and security measures that can help organizations mitigate costs, estimates the chances of any organization experiencing a data loss in the next two years at just under 30%.

- **Privacy violation**
  
  In this case, data is not lost, but misused. If a customer provides consent for a business to use their data but not share it with third parties, accidental sharing could be a violation of that customer’s permitted use. Even within a business, sharing data with staff that are not permitted to use it may represent a violation. Complicating matters, customers may provide consent and later withdraw it.

The annual *Cost of a Data Breach Report*, which is published by the Ponemon Institute and sponsored by IBM Security, goes on to tell us that the worldwide average cost per record that is lost is approximately US $150 and the average size of a breach is more than 30,000 records (costing US $4.5 M). The cost is expected to vary by region and industry with the highest cost per record estimated at US $429 for a healthcare record in the United States. Those estimated costs do not include loss of business.

As businesses look to minimize the risk and impact, they must also find ways to provide end-to-end, data-level protection and privacy. This effort includes not only encrypting data, but granting and revoking access to it, and maintaining and proving control of it, even as it moves off the system of record.

With the launch of pervasive encryption on IBM Z, IBM announced that its hardware can encrypt data at-rest and in-flight while incurring a percentage increase in CPU utilization in the low single digits. With faster encryption and on-chip compression in subsequent generations of IBM Z, that number is even lower.

Pervasive encryption helps reduce the number “non-functional” roles as potential threats of data loss. Non-functional roles are those roles that are not involved in the primary function of workloads that are running on the system. A storage administrator is such a role. The storage administrator needs to be able to move a database from one storage device to another but does not need access to the data that is inside the database. If the database is encrypted and the administrator cannot access the encryption key, that administrator cannot access the data.

---

2. See “Compression and Pervasive Encryption: z15™ Offers the Best of Both Worlds”, published by the IBM IT Economics team.
With this in mind, an information security officer may sleep soundly having implemented pervasive encryption on IBM Z, thus helping to protect their data from loss. However, data must sometimes leave the Z environment.

After the data leaves the demarcations of that trusted system of record, privacy breaches become a possibility as control of the shared data is no longer guaranteed.

Data privacy considerations include functional roles and the minimum amount of data they require to perform their function, and what consent a data subject\(^3\) provided to use their data. With a system of record, interaction with data is constrained by trusted applications. But, outside of that experience, data interaction is less structured. For example, if a data scientist is trying to gain insight from credit card purchases, do they need to see the card number? In short, what does the functional role need to know to get the job done?

It is also important to keep in mind that these questions are answered at a particular time and place, and for a particular role. Rules change. Perhaps today it is permissible to display a full credit card number to a customer service agent, but tomorrow a new regulation requires that it cannot be shown.

Also, data moves. Credit card transactions are collected in an application that is running on IBM Z, but then sent elsewhere in an Extract, Transform, Load (ETL) cycle for analysis by data scientists, for example. Data must be protected wherever it goes and only what is required for a specific role should be exposed given the most recent set of rules available.

In a typical data center, establishing and maintaining rules may require changing code in various applications, altering storage procedures, or even scrubbing over-exposed data and altering the ETL cycle. If the data was sent to a third party, the problems are compounded.

Data Privacy Passports can support the data protection and privacy requirements of businesses, starting by placing data in an encrypted bundle called a Trusted Data Object (TDO). Data is protected in the TDO as it moves from system to system within an enterprise; for example, from a transactional system to a data lake.

Access to the data is governed by policy that determines not only who has access to the data, but what form the data takes for their role. A data scientist may see only a “masked value” of a bit of sensitive data.

When a TDO is opened, a Passport Controller is used to perform that operation. The identity of the person and the data they are accessing are matched to a policy that determines whether they can access the data and in what form.

Information that was masked could be made available in the clear to the data scientist within the organization. In this case, a new policy can be set in the Passport Controller that is used with subsequent queries. If the data was not transformed as the TDO was created, the data does not need to be reloaded in the data lake, as might be the case with a typical ETL tool.

In addition, access to data can be revoked altogether by revoking access to the key that encrypts it. Or, data may be rendered inaccessible remotely by simply destroying the key that is required to decrypt it.

With Data Privacy Passports, audits can be made easier because there is only one place to go to verify data security policies.

---

\(^3\) According to the European Union General Data Protection Regulation (GDPR), a Data Subject is “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 identity of that natural person.”
The administrative costs of maintaining policies in multiple places can be reduced. In a business value assessment of Data Privacy Passports\(^4\), the IBM IT Economics team estimates by reducing the cost of securing data and lowering the risk of a data or privacy breach, Data Privacy Passports is projected to deliver a five-year return on investment (ROI) of approximately 300\%.\(^5\)

This business value assessment accounts for cost of ownership in the form of required hardware, software licensing, and labor. This is balanced against the benefits of reduced risk of fines and lost business, improved efficiency in implementing and auditing policy, and avoiding costs that are associated with in-house implementation of similar measures. Of course, individual circumstances vary.

**Data governance benefits**

There are many benefits that Data Privacy Passports can bring forth as enhancements to a company’s data governance. Data governance is the overall management of data availability, relevancy, usability, integrity, and security in an enterprise. It helps businesses answer questions, such as: “Where did this data come from?”, “Does this data adhere to company policies and rules, such as separation of duties?”, and “Who has access to this data?”.

Data Privacy Passports provides end-to-end encryption and can enhance data governance through a method of data handling that can be demonstrated easily to an outside entity. Data governance with Data Privacy Passports includes demonstrating compliance of internal policies, enforcing data subject requests, and regulating access to personal information.

**Demonstrating compliance of internal policies**

Complying with data access and use policies, and demonstrating that compliance to auditors can be a consuming task. Using Data Privacy Passports can assist in data tracking down to the field-level for personal information. This level of demonstrable granularity should allow audits to proceed smoothly.

**Enforcing data subject requests**

The Passport Controller is a component of Data Privacy Passports that enforces restrictions or access to personal information and provides application owners or business process owners more confidence they can demonstrate compliance with the data subject’s requests. This applies to data access within private and public cloud implementations.

**Regulating access to personal information**

When a data subject enters a business relationship, Data Privacy Passports can assist in providing more governance to allow your data to be included in your cloud data lake that can also be used for analytics to enhance the customer experience. However, with Data Privacy Passports, you can regulate the access to personal information in the TDO in the cloud. This includes specific rows and columns in the table, for example.

---

\(^4\) See “IBM z15™ Data Privacy Passports: Protecting data wherever it goes and generating a projected 300% ROI”, published by the IBM IT Economics team

\(^5\) See “Disclaimer for business value assessment” on page 18.
As shown in Figure 1, the data is transformed into a single copy of trusted data objects (TDOs) and enforced data that is shared in the enterprise. This single copy of data can then be accessed by multiple roles or personas, each with a different need to know, for example:

**Data owner**

The data owner has complete access to the data. This persona can resolve TDOs in this protected table. All fields are unencrypted and returned as clear values.

**Data scientist**

The data scientist requires certain fields from the protected table. This persona can resolve TDOs in this protected table. All fields are unencrypted. The s_num field is returned as default mask values. The phone and zip_code fields are returned as clear values.

**Regulator**

The regulator requires only certain fields from the protected table. This persona can resolve TDOs in this protected table. All fields are unencrypted and default mask values are returned.

**Data administrator**

The administrator has permission to create policies and provision data only, but has no need to know any of the data. This persona cannot resolve TDOs. All protected fields are returned as TDOs.

![Figure 1 Consuming protected data by different personas](image)

**Data revocation - enforcing policies**

Data may be transformed into either state as it leaves a system of record. For example, if a full national identification number may never be accessible outside of the system of record, a policy is enforced so that it is masked as it leaves the system.

A great advantage of the Data Privacy Passports approach in safeguarding data is that a policy may be altered after data is circulated. Because data passes through a Passport Controller at the time of consumption, policy may be dynamic. A credit card number that was presented as four digits today may be masked tomorrow on the next access through the Passport Controller. Access to data can be revoked altogether, when required.
Providing a single point of authority

By providing a single point of authority, Data Privacy Passports removes many points of potential failure; that is, separate Extract Transform and Load (ETL) transformations, access control lists, various native encryption options. It replaces them with one point of control and one point to audit.

Its single point of authority also enables Data Privacy Passports, which are facilitated by the Passport Controller, to help manage data privacy audits. Data Privacy Passports could lower the time spent auditing each database. This leaves individuals more time to focus on tasks that create value for a company.

Sharing infrastructure without duplication

Most businesses use the method of ETL to provide data in a format for other uses. Multiple batch jobs that are based on security needs could be used to provide access to data for reports, analytics, or to include within a data lake. This ETL process is costly in terms of system resources.

By using the TDO that is provided by the Data Privacy Passports, one extraction can be done, and different views presented to the user or application based on policy definitions through the Passport Controller.

How does Data Privacy Passports work

Data Privacy Passports provides a new data-centric security model for the protection of eligible data\(^6\) across the enterprise. It is the next logical step from the IBM Z pervasive encryption strategy, extending security to the database level, and protection to data that is resident on IBM Z and also as it moves throughout the enterprise and beyond. Data Privacy Passports does not require IBM Z pervasive encryption to be enabled, although that makes the most sense as it provides end-to-end protection of all data.

Data-centric audit and protection

The idea of data-centric audit and protection (DCAP) is a transition from the current model to which most enterprises are accustom. The way that data is protected today is that each time the data lands, it is secured through a mechanism that is specific to that system. There is little enterprise-wide ability to guarantee a base level of protection, or a centralized way to monitor and audit the access to that data.

In the DCAP model, before the data is moved around the enterprise, it is repackaged into a secure object. In the case of Data Privacy Passports, this is the TDO. Data Privacy Passports does this protection at a field-level, which means that there is a level of granularity to this protection that cannot be obtained from more broad protection techniques.

---

\(^6\) Data Privacy Passports supports data sources that can be accessed through a JDBC connection.
As shown in Figure 2, after the field is wrapped in a TDO, it is the TDO that moves throughout the enterprise to its endpoint.

![Diagram](image)

*Figure 2  Protecting copies of copies of copies*

When any of the original or copies of a TDO need to be opened, that must come back to the Data Privacy Passports infrastructure. At this point, a policy-based view of the clear data can be provided (for example, masking the data) and the access to the data can be audited. A required a trip back to the Data Privacy Passports infrastructure provides a single location for performing data revocation as well.

This changes the requirement from monitoring every location data is stored. Instead, you can focus on the data usage and monitoring when, where, and who accessed the data.

**Protected and enforced modes**

There are two ways to get the data into a policy specified view:

- Protected mode

  A TDO is created and stored along with the data in a protected table in a target database management system (DBMS). This data can be accessed through ad hoc queries or as a utility process through the Data Privacy Passports infrastructure.

  A different enforced view, as shown in Figure 3, is returned to the data consumer based on the credentials of that user and the need-to-know that is defined in the data policy.

![Diagram](image)

*Figure 3  Enforced views that are generated from the protected table*
Enforced mode

The protected phase is skipped and policy enforced views of data from the clear source are created. In this case, there are no TDOs (protected tables) created, as shown in Figure 4.

![Figure 4 Enforce views that are generated from the source table](image)

Enforced mode is required for applications that cannot support changing of the table schema. A format preserved view needs to be used and can be generated directly from the clear data.

Deployment

Figure 5 shows that Data Privacy Passports uses the IBM Hyper Protect Virtual Servers support for deployment, which is built on the IBM Secure Service Container framework. This allows trusted application, such as Data Privacy Passports, to be deployed in the IBM Z environment with the utmost protection.

![Figure 5 Data Privacy Passports deployment on IBM Z](image)

Data Privacy Passports components

Next, we examine the different components that are inside of the Data Privacy Passports solution.

---

7 Requires an IBM z15 or later generation.
**Passport Controller**
As shown in Figure 6, Data Privacy Passports consists of a single component that is known as the Passport Controller. This provides all the protection, enforcement, policy, and key management for the solution.

![Passport Controller components](image)

**Figure 6  Passport Controller components**

**Internal key storage**
The encryption that is performed by Data Privacy Passports is symmetric encryption using the Advanced Encryption Standard (AES) with a key length of 256 bits (AES 256). The keys are stored internally and managed by the Passports Controller.

**Data policy**
A policy describes how the Passport Controller should operate. There is specific means for mapping users and groups to personas such that a need to know for data can be established. Think about these elements as the following types:

- **Groups**: Provides connections of Enterprise LDAP users to personas.
- **Data Elements**: Rules that govern the need to know for specific fields.
- **Users**: Defined in Enterprise LDAP.
- **Personas**: Also known as a functional role, provides information that is required for personas to work with TDOs and used for specific enforcement in Data Elements.
- **Trust Zones**: Virtual data perimeters, scoped to the Passport Controller.
These different policy elements fit together to form a complete view of how data is accessed and processed. Figure 7 shows these policy elements.

![Figure 7: Visual representation of policy elements](image)

**Administrator and user interactions**

The programming interface for interacting with Data Privacy Passports is through a REST API or a Java Database Connectivity (JDBC) connection for issuing the SQL SELECT statement.

As shown in Figure 8, the administrator interacts with the Passport Controller using REST APIs. Some example administrative tasks are uploading policies, activating policies, and performing data provisioning activities.

There are two ways for a user to interact with the Passport Controller. To perform ad hoc SQL queries, send the SQL statements via JDBC requests directly to the Passport Controller. The user can also use REST APIs to perform functions, such as provisioning views of data.

![Figure 8: Administrator and user interactions with the Passport Controller](image)
Using Data Privacy Passports

There are several architectural patterns that can be deployed that service a set of use cases, including the following examples:

- Data segmentation and brokering
- Embedded data retention and revocation policies
- Single data source for multiple views

Data segmentation and brokering

Privacy legislation is being enacted globally, with far-reaching effects on businesses that collect personal data. Solutions solving geographic segmentation of data can be highly useful in global companies that operate in multiple countries. How can data be shared while respecting the data residency and privacy requirements of various countries?

Business problem

A large multi-national corporation has disjointed human resource systems in each of its geographic locations and wants to allow for new analytics on employee retention, motivation, and job satisfaction across the entire global workforce. The corporation must adhere to the data privacy requirements of each employee’s country. How can they federate their corporate data systems and maintain confidentiality of their employees’ personal data?

Solution

Data Privacy Passports allows the organization to define Trust Zones, which can access open a subset of TDOs. This allows a group of users to continue to access the data, while other users see only the protected TDO. For example, only authorized members of the Trust Zone can open the PII portions of HR records of employees in their specific country. A data scientist can analyze the records from all countries to gain new insights while being restricted from viewing individual record fields.

As shown in Figure 9, a user who is authenticated with Passport Controller 1 can access data only in Protected Database 1, based on the need-to-know definition in its policy. To access data in Protected Database 2, the user must first authenticate with Passport Controller 2.

Figure 9   Data segmentation and brokering
Embedded data retention and revocation policies

Each industry has its own regulations and best practices for data retention. Data owners today must request erasure of data to anyone who could have a copy, and may be limited in their ability to audit compliance. How can access control to all copies of the data be put back in the hands of the owner?

Business problem
A company provided their customer historical data to multiple departments during a company-sponsored internal 30-day hackathon, which focused on “go to market” innovation.

Solution
Data Privacy Passports provides cryptographic erasure of data in all copies of the database that may have been taken by a department. With the key deleted and the source data rekeyed, Passport Controller no longer opens any TDOs with the old key, which ensures that any copies of data that are held by any department is rendered unusable.

Figure 10 shows one example of data revocation. Copies of protected data that contain TDOs exist throughout the enterprise. All TDOs are encrypted by using a specific key (or set of keys). When source data is updated, the old data can be invalidated by deleting the key. With validation, the old copies cannot be opened ever again. New protected data can then be provisioned and a new set of keys is used to encrypt the TDOs.

![Figure 10 Data revocation example](image)

Single data source for multiple views

To perform effective analysis, data is often copied and massaged to fit into the parameters that are required by the data scientist. The security team is tasked with making sure that the data is properly safeguarded in all of these various environments without knowledge about who should have what type of access. This results in broad data protection mandates that are forced to be one size fits all. How can data control remain in the hands of the data owner or custodian who is most knowledgeable about who should have what types of access?

Business problem
An insurance company needs to share details about their customers to a data scientist, the customer themselves via a web portal, and a regulator. The customer should always be able to view all of their data. The data scientist does not need exact values, but needs tokens that are consistent representations of the actual data. The regulator needs to see certain data, but is a third party to the company.
Solution
IBM Data Privacy Passports can create a single protected table of data from policies that allow multiple views of data varying by needs.

As shown in Figure 11, source databases are replicated and protected with TDOs to a target DBMS. There are two ways a data consumer can access the protected data. First, by accessing the protected data directly. This means that no enforcement is done, which returns TDOs for protected elements to the user. The second method is to use REST APIs to access the protected data via the Passport Controller. The user sees an enforced view of the protected elements based on their need to know.

Figure 11  Single data source for multiple views

Line-of-business use case

An example of this use case could be a collaboration between two line-of-business departments within a company. The marketing department is working to enhance their client experience and has asked their IT department to provide them with a copy of the company’s customer data. Their goal is to use analytics to target new offerings to drive incremental sales.

In many cases, the IT department could have many levels of security approvals from the Chief Security Officer (CSO), and multiple query iterations on the source data could impact production processing.

Using Data Privacy Passports for this case, the IT department can create a protected table where sensitive information is wrapped with TDOs. Different views can be defined in a data policy based on functional roles and need-to-know. For example:

- The user testing in the marketing department would allow a customer to access their account with full access
- The data scientist in the marketing department performing analytics to provide insights for new offerings to clients can access enforced data that is format that is preserved and stable for analysis.
- The IT department and Chief Security Officer can monitor or audit as needed. The IT department can also provide access to regulators to ensure auditability of the data outside of their production systems.

With this solution, the IT department can ensure that access that is based on their security guidelines are consistent, even when the data moved outside the walls of the production system, which they manage.

8 No other enforcement is needed because the data elements were encrypted or masked.
Finally, after a successful completion of the line-of-business effort, the IT department can revoke future access to the protected table or individual data elements through one of several ways:

- **Policy changes**
  
  Policy activations are dynamically supported in Data Privacy Passports. This provides the ability to change the enforcement for specific fields for specific users that are defined in the policy at any time for any future accesses.

- **Identify management changes**

  The user assignments in the enterprise identify management system, such as LDAP, can be changed to remove users from groups and alter how the Data Privacy Passports policy applies to that user.

- **Cryptographic erasure**

  The data encryption key that is used to create a TDO are all internally stored inside of the Data Privacy Passports infrastructure. When a TDO is presented to a Passport Controller, that data encryption key material is found, using the key label that is provided in the TDO, and then that key material is used to perform the decryption operation. If that key is deleted, any TDOs that are created by using that data encryption key no longer can be opened, which provides a means to revoke any future access to those TDOs.

**What’s next: How IBM can help**

Protecting data, ensuring policy compliance, and maintaining control of the data are crucial to the success of any business. Data Privacy Passports simplifies the process of demonstrating regulatory or business process compliance through the policies you implement.

Data Privacy Passports is a data-centric audit and protection (DCAP) solution that enables data to play an active role in its own protection and ensures that data remains encrypted or masked, even if it leaves the enterprise.

With Data Privacy Passports, data protection through IBM Z allows you to take advantage of privacy control policies to help ensure that your data is always protected.

To learn more about Data Privacy Passports or how to get started, IBM offers the following resources:

- IBM Marketplace provides more information about Data Privacy Passports, its uses and how it can help your business. For more information, see this web page.

- IBM Systems Lab Services offers services for Data Privacy Passports, these include:
  - A planning workshop, which consists of training and a readiness assessment. The readiness assessment shows any deficiencies in your environment that are related to the deployment and use of Data Privacy Passports.
  - A jump-start, which focuses on building, verifying, and using a Data Privacy Passports test environment. This can be extended further with a production deployment.

  For more information, email ibmsls@us.ibm.com.

- IBM Z Content Solutions provides a comprehensive set of information to help you understand, implement, and use Data Privacy Passports. For more information, see this web page.
Authors

This guide was produced by a team of specialists working with IBM Redbooks.

Bill White is an IBM Redbooks® Project Leader and Senior IT Infrastructure Specialist at IBM Redbooks, Poughkeepsie Center.

Mark Moore is a software architect in the IBM IT Economics Consulting and Research team, focusing on IBM Z pervasive encryption, Data Privacy Passports, and IBM LinuxONE. He has also performed extensive research comparing IBM social and mobile solutions to major competitors. Before joining the CPO, Mark was a technical and management consultant. He has spent 30 years in the software industry working on operating systems, compilers, public key infrastructure, e-commerce, portals, and database publishing.

Phillip Wilson is a Client Technical Specialist with IBM North America. He has 10 years of experience with IBM Z. He has worked at IBM for 34 years. His areas of expertise include Linux, MicroSoft Windows, Nodejs, and system architectures.

Eva Yan is an Executive I/T Specialist at IBM where she leads a global team in creating technical collateral to help drive IBM Z and LinuxONE adoptions. In this role, her primary focus is hardware and solution offerings including IBM z15, IBM Hyper Protect Virtual Servers, IBM Data Privacy Passports, Red Hat OpenShift, and Cloud Paks. Before her current position, Eva was the chief architect for the IBM LinuxONE Community Cloud, which provides no-charge, open access to the public for skills building and innovations.

Thanks to the following people for their contributions to this project:

Jessica Doherty
Barbara Sannerud
Anthony Sofia
IBM Poughkeepsie

Now you can become a published author, too!

Here’s an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at: ibm.com/redbooks/residencies.html
Stay connected to IBM Redbooks

- Find us on Facebook:
  http://www.facebook.com/IBMRedbooks
- Follow us on Twitter:
  http://twitter.com/ibmredbooks
- Look for us on LinkedIn:
  http://www.linkedin.com/groups?home=&gid=2130806
- Explore new publications, residencies, and workshops with the IBM Redbooks weekly newsletter:
- Stay current on recent Redbooks publications with RSS Feeds:
  http://www.redbooks.ibm.com/rss.html
Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided “AS IS”, without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.
Disclaimer for business value assessment

Analysis based on a hypothetical ROI projection for IBM Data Privacy Passports, including the reduced risk of a data privacy breach, reduced risk of industry fines and regulatory penalties, policy enforcement efficiency and audit labor reduction, and the cost avoidance of an in-house equivalent implementation.

Data breach risk is taken from the IBM-sponsored Ponemon report, “2019 Cost of a Data Breach”. Potential industry fine or regulatory penalty data is based on a blended combination of penalties across several recent GDPR, HIPAA, and PCI DSS publicly disclosed violations. Costs associated with labor savings in policy enforcement, audit, and in-house implementation and maintenance of a comparable solution are derived from IBM IT Economics data aggregated from client engagements.

A range of values for risk reduction, industry and regulatory fines, and efficiency were considered, producing an ROI between 284% and 332%. Actual ROI will vary by geography, industry, and individual client circumstance.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

IBM®
IBM Z®
IBM z15™
IBM Redbooks®
Redbooks (logo) ®
z15™

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

OpenShift, Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.