What Was In That Data?

Gant Redmon - Program Director, Cyber Security and Privacy, IBM Resilient

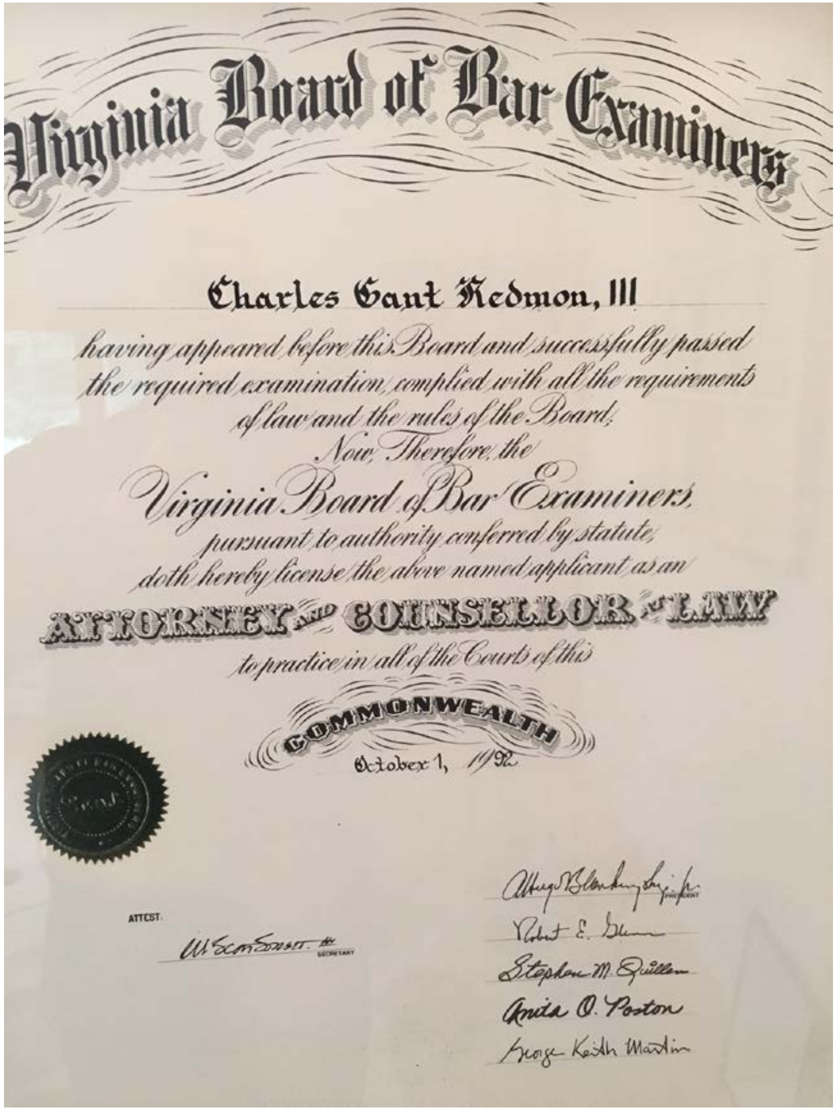
IBM Resilient

File
Main
Identities
Social Security
Credit Card
Password Entry
Bank Account
LOCATION
C:\Docs\application.pdf

General Data Protection Regulation

Data Protection

Data



Virginia Board of Bar Examiners

Charles Gant Redmon, III

having appeared before this Board and successfully passed the required examination, complied with all the requirements of law and the rules of the Board;

Now, Therefore, the

Virginia Board of Bar Examiners,

pursuant to authority conferred by statute, doth hereby license the above named applicant as an

ATTORNEY AND COUNSELLOR AT LAW

to practice in all of the Courts of this

COMMONWEALTH

October 1, 1992

ATTEST:

W. Scott Street, III
SECRETARY

Blankenship, Jr.
PRESIDENT

Robert E. Glenn

Stephen M. Quillen

Anita O. Poston

George Keith Martin

We need you

Reportable?

Data

Personal Data

File
Main
Identities
Social Security
Credit Card
Password Entry
Bank Account
LOCATION
C:\Docs\application.pdf

Article 4 Definition

‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’);

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

Personal Data vs Sensitive Data

Racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures

Under Article 4…

'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **personal data** transmitted, stored or otherwise processed;

Under Article 34…

When the **personal data breach** is likely to result in a high risk to the rights and freedoms of natural persons, the **controller shall communicate** the personal data breach to the data subject without undue delay.

What Do I Need to Know about the Personal Data?

What data do I have?
What data is personal or sensitive?
How did I get it?
Where is it?
Who has access?
Is there adequate security given nature of data?
What is the flow?
When can/should I delete it?

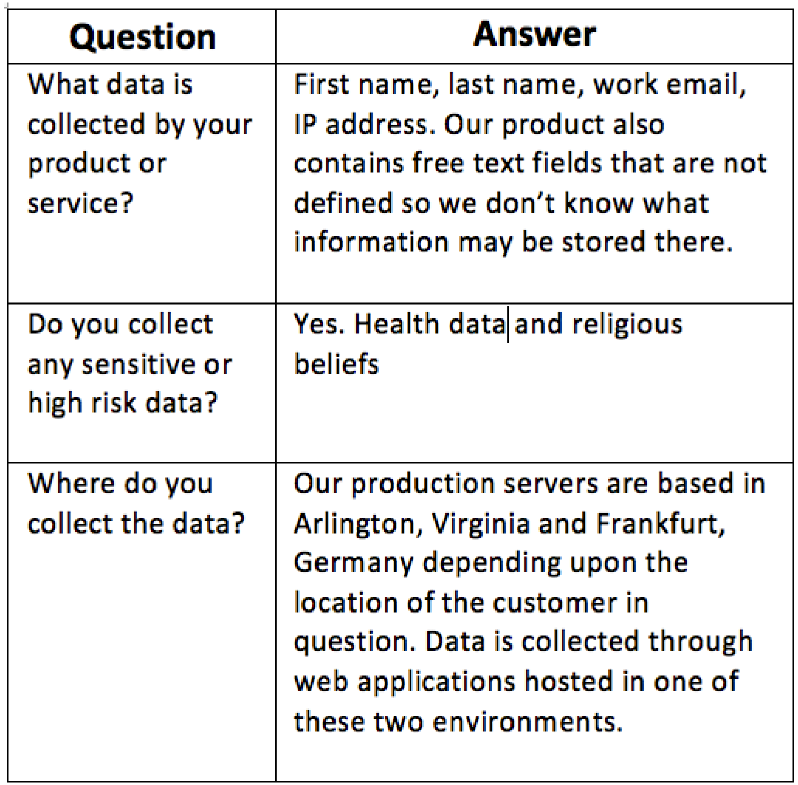
Under Article 5…

Personal data shall be processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

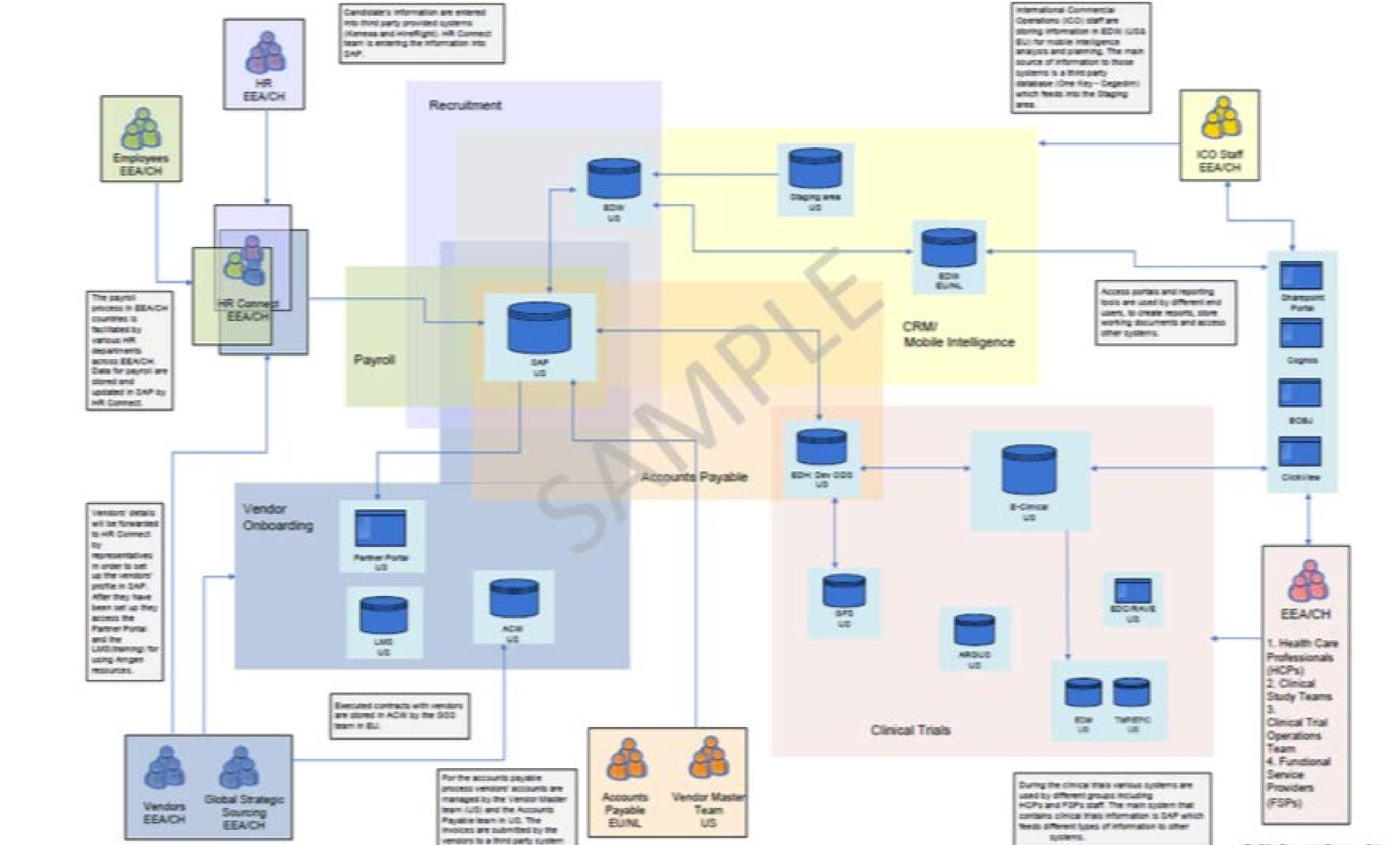
What should we be doing?

Data Identification and Data Mapping and Flow

What A Lot of People Have Today



Question	Answer
What data is collected by your product or service?	First name, last name, work email, IP address. Our product also contains free text fields that are not defined so we don't know what information may be stored there.
Do you collect any sensitive or high risk data?	Yes. Health data and religious beliefs
Where do you collect the data?	Our production servers are based in Arlington, Virginia and Frankfurt, Germany depending upon the location of the customer in question. Data is collected through web applications hosted in one of these two environments.



Candidate's information are entered into third party provided systems (Kenexa and Hirefright). HR Connect team is entering the information into SAP.

International Commercial Operations (ICO) staff are storing information in EDW (USA EU) for mobile intelligence analysis and planning. The main source of information to those systems is a third party database (One Key – Cegedim) which feeds into the Staging area.

The payroll process in EEA/CH countries is facilitated by various HR departments across EEA/CH. Data for payroll are stored and updated in SAP by HR Connect.

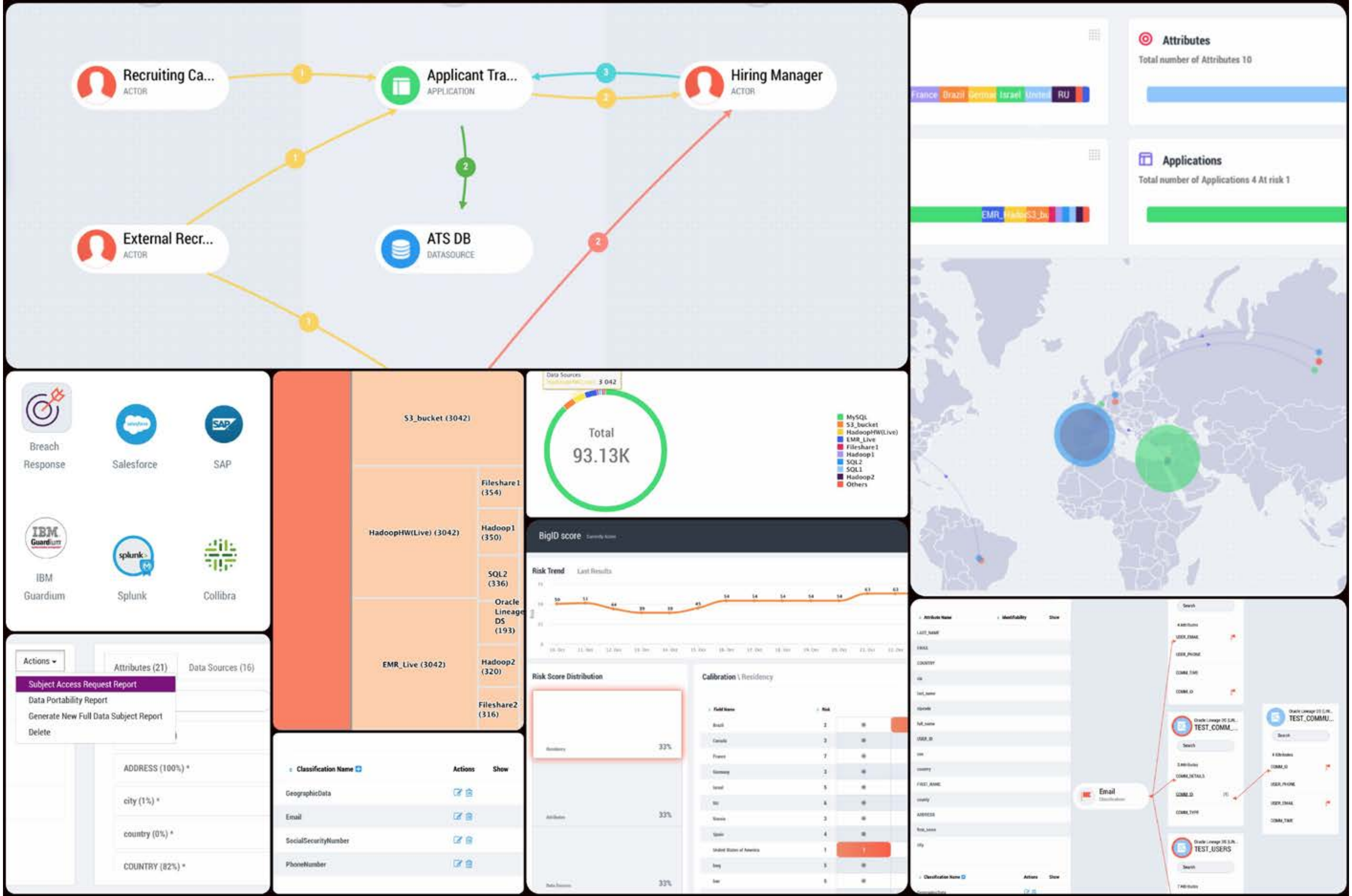
Access portals and reporting tools are used by different end users, to create reports, store working documents and access other systems.

Vendors' details will be forwarded to HR Connect by representatives in order to set up the vendors' profile in SAP. After they have been set up they access the Partner Portal and the LMS(training) for using Amgen resources.

Executed contracts with vendors are stored in ACW by the GSS team in EU.

For the accounts payable process vendors' accounts are managed by the Vendor Master team (US) and the Accounts Payable team in US. The invoices are submitted by the vendors to a third party system (OB10).

During the clinical trials various systems are used by different groups including HCPs and FSPs staff. The main system that contains clinical trials information is SAP which feeds different types of information to other systems.



ADDRESS (100%) *

city (1%) *

country (0%) *

COUNTRY (82%) *

Classification Name	Actions	Show
GeographicData		
Email		
SocialSecurityNumber		
PhoneNumber		

Calibration \ Residency

Field Name	Risk	
Brazil	2	
Canada	3	
France	7	
Germany	3	
Israel	5	
RU	6	
Russia	3	
Spain	4	
United States of America	1	1
Iraq	5	
Iran	5	

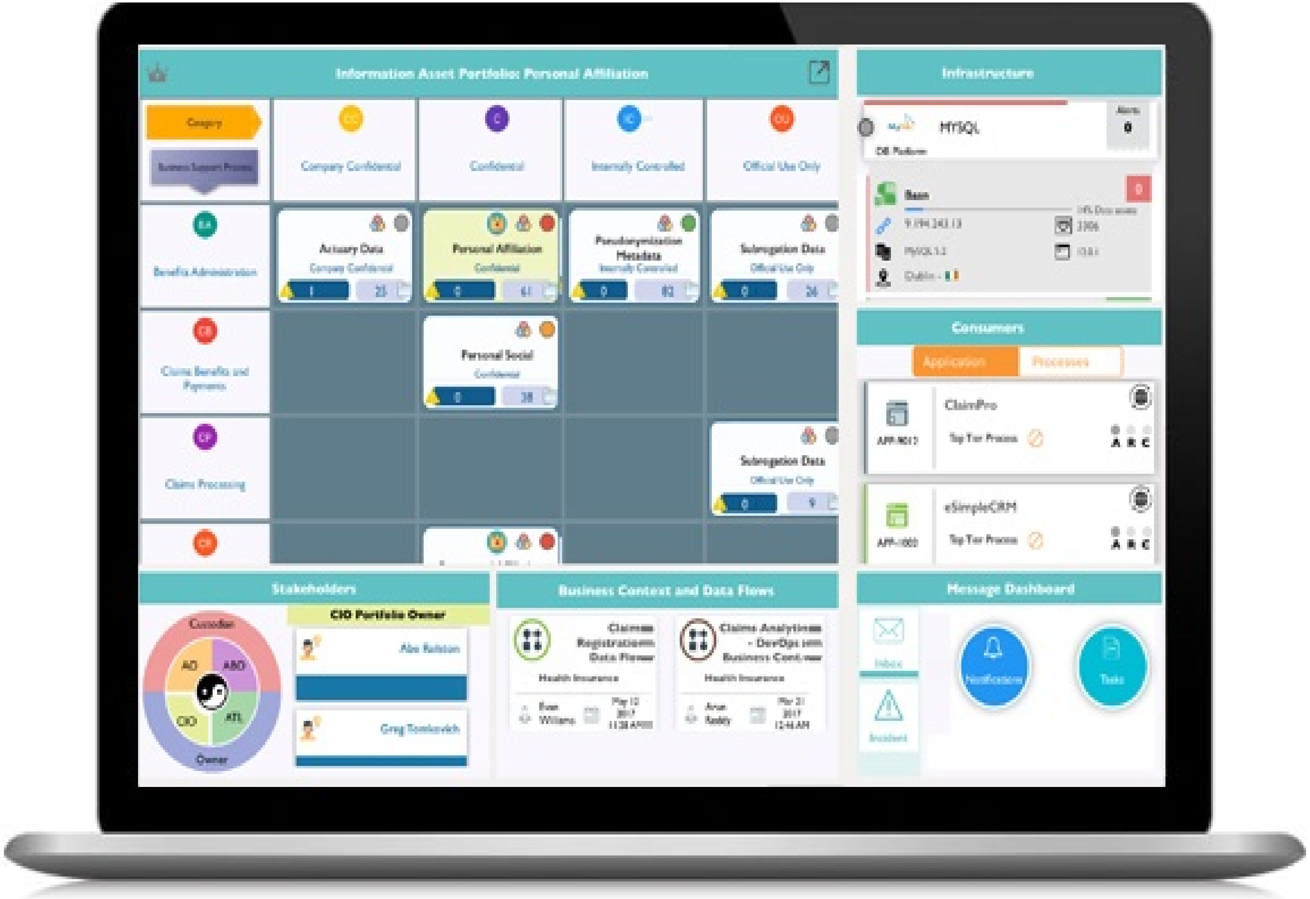
Attribute Name	Identifiability	Show
LAST_NAME		
EMAIL		
COUNTRY		
city		
last_name		
zipcode		
full_name		
USER_ID		
ssn		
country		
FIRST_NAME		
county		
ADDRESS		
first_name		
city		

Classification Name	Actions	Show
GeographicData		

4 Attributes
USER_EMAIL
USER_PHONE
COMM_TIME
COMM_ID

TEST_COMM_... 3 Attributes
COMM_DETAILS
COMM_ID
COMM_TYPE

TEST_COMMU... 4 Attributes
COMM_ID
USER_PHONE
USER_EMAIL
COMM_TIME


Information Asset Portfolio: Personal Affiliation
Category
Business Support Process
CC
Company Confidential
C
Confidential
IC
Internally Controlled
OU
Official Use Only
BA
Benefits Administration
Actuary Data
Company Confidential
1
25
Personal Affiliation
Confidential
0
61
Pseudonymization Metadata
Internally Controlled
0
82
Subrogation Data
Official Use Only
0
26
CB
Claims Benefits and Payments
Personal Social
Confidential
0
38
CP
Claims Processing
Subrogation Data
Official Use Only
0
9
Infrastructure
MYSQL
DB Platform
Alerts
0
Baan
0
9.194.243.13
2306
MySQL 5.2
10.8.1
Dublin -
Consumers
Application
Processes
ClaimPro
APP-9012
Top Tier Process
A B C
eSimpleCRM
APP-1003
Top Tier Process
A B C
Stakeholders
CIO Portfolio Owner
Custodian
AO
ABO
CIO
ATL
Owner
Abe Ralston
Greg Tomkovich
Business Context and Data Flows
Claims Registration Data Flow
Health Insurance
Evan Williams
May 12 2017 11:38 AM
Claims Analytics - DevOps Business Context
Health Insurance
Arun Reddy
May 21 2017 12:46 AM
Message Dashboard
Inbox
Incident
Notifications
Tasks

Vendors

Data Discovery and Mapping

Guardium Analyzer - Assess security and compliance risks associated with GDPR personal data by using next-generation classification techniques and performing vulnerability scanning to prioritize databases with at-risk data.

Datavantage by Varonis - "scan all my filesystems, then categorize & add metadata to determine breach"

CA Data Content Discovery - By discovering where the data is located, classifying the data based on sensitivity level and providing comprehensive reporting on the scan results, mission essential data can be protected and exposure risks can be mitigated.

BigID - Know your data without moving your data. Graph your data relationships without building another data warehouse or lake. Discover identity relationships across your data stores with no language or meta data dependencies.

Prifender - Prifender's ability to track the identities of the data subjects that the organization is responsible for across repositories and networks provides a mechanism to associate the GDPR requirements with the relevant data, rather than only rely on policy, training and contracts.

Agile 3 - Leveraging inputs from IBM Security Guardium, IBM Information Governance Catalog and Symantec DLP, Data Risk Manager is an integration platform that provides an end-to-end view of all business metadata associated with sensitive information assets, including applications, processes, policies, procedures, controls, ownership and more.

Data Loss Prevention

Symantec DLP - Symantec DLP is configured to identify sensitive data (including that defined by GDPR) and uses a variety of advanced data detection techniques to identify data in many forms.

Digital Guardian - Industry leading DLP plus data-centric Endpoint Detection and Response (EDR) all from a single cloud-delivered, big-data analytics service. See, understand, and stop threats to your sensitive data from insiders and outside attackers.

Spiron - Spirion strengthens existing data loss prevention (DLP) solutions by accurately discovering, classifying, and protecting sensitive data at the source. Data stored anywhere, in any format, and at any time—from PII, PCI, ePHI data to company confidential information.

CipherCloud - Sophisticated compliance scanning lets you easily discover and classify new and existing content. Out-of-the-box policies scan for content relevant to GDPR, PCI, GLBA, SOX, and HIPAA compliance regulations, credit card numbers, national IDs, social security numbers, bank routing codes, national drug codes, and more.

Clearswift - Information hidden inside the network or shared in the cloud can be immediately detected, secured and brought into compliance with industry regulations (GDPR, HIPAA, PCI, SOX, etc.) - without complexity and disruptions to your business.

Data Discovery and Mapping

Microsoft Azure Data Catalog - Azure Data Catalog is an enterprise-wide metadata catalog that makes data asset discovery straightforward. It’s a fully-managed service that lets you—from analyst to data scientist to data developer—register, enrich, discover, understand, and consume data sources.

HyTrust CloudAdvisor for Data - enables you to define policies to automatically discover the data that’s valuable to you, detect anomalous user access behaviors, and defend your organization against careless exposure, data loss, malicious users, and regulatory noncompliance.

Cognigo - DataSense’s content-aware search and control engine results in radically faster, more accurate and scalable data security than traditional solutions. Using groundbreaking machine learning technologies, DataSense is able to classify data, ensure compliance, enforce data policies and actively mitigate data at risk in real-time.

Global IDs - In contrast to traditional approaches which focus on governing data silos, Global IDs allows organizations to govern data ecosystems. This perspective allows organizations to see their data in a holistic manner, allowing visibility into the way in which business is conducted across the enterprise.

Informatica - A machine-learning-based data catalog lets you classify and organize data assets across cloud, on-premises, and big data. It provides maximum value and reuse of data across your enterprise.

Integris Software - Our software gives you the ability to visualize where personal information is located across the organization, prove adherence to regulatory standards, and fuel strategic decision making.

Forensic and eDiscovery Solutions

Guidance Software/EnCase/OpenText - Whether a corporate or legal investigator, you need to be confident that you can gather all data pertinent to your investigation, analyze it at the deepest forensic level, and produce trusted reports.

Concordance by Lexis/Nexus - Used by more than 70,000 attorneys and litigation support professionals, Concordance provides an effective, cost-efficient way to manage and review the high volumes of documents generated during litigation—scanned paper, email, PDFs, etc.

How about you?

GDPR is not the end all be all…

NISD, ePrivacy, etc.

Thank you.

Questions?

75 Binney Street
Cambridge, MA 02142
WWW.RESILIENTSYSTEMS.COM
888.426.4968

IBM Resilient