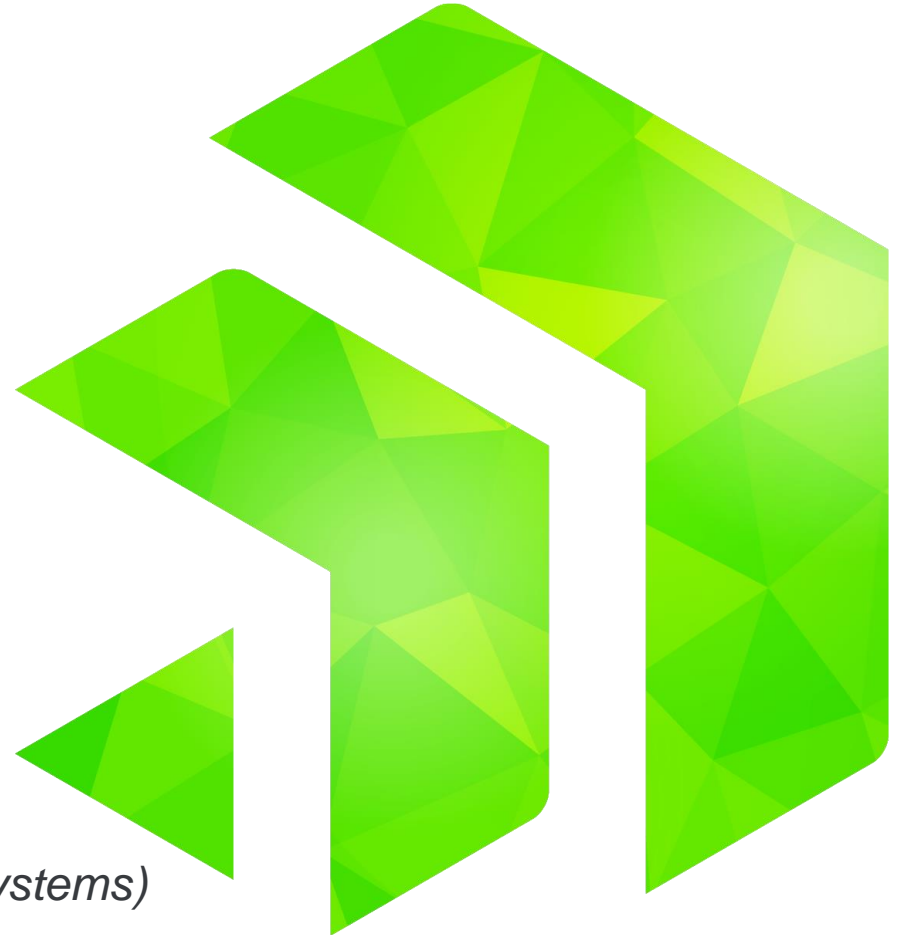




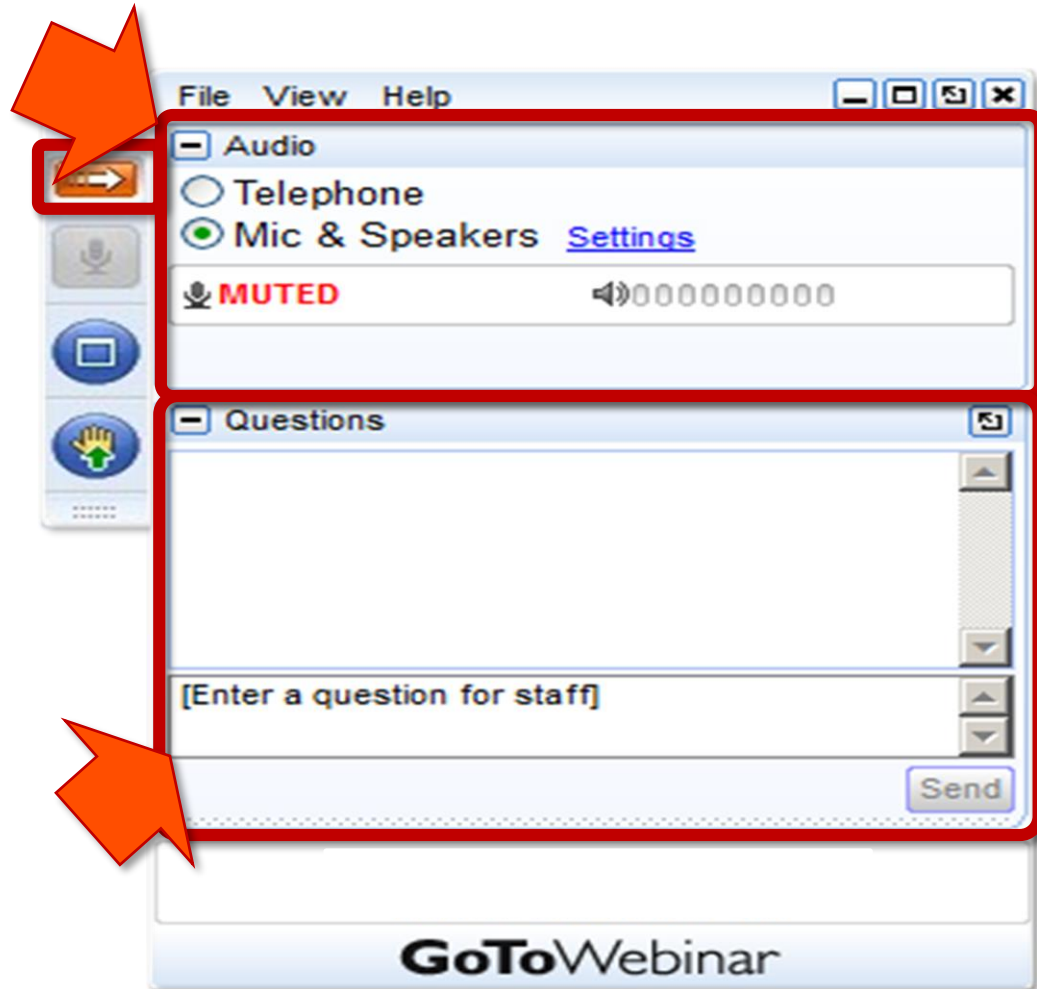
Analytics Continuity During GDPR via Data Masking

Julien Mansier
Sr Solutions Engineer
Progress DataDirect

Rod Welch
BI Consultant (GDPR & MI systems)
Contracted to LV Insurance, UK



Audio Bridge Options & Question Submission



Agenda

- What is GDPR
- GDPR and its impact on analytics
- Leveraging data masking for analytics continuity
- Security best practices for data masking
- Data masking Demo

What is GDPR?

GDPR



COMPLIANCE



PERSONAL DATA



DATA BREACHES



DATA PROTECTION

Gray Area: What is considered PII?

Definition: Under article 4, 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.”

Examples:

- Cookies
- Device Identifiers
- SSN
- Address
- Email
- Login IDs
- Social Media posts
- Digital Images
- IP Addresses
- Geolocation Data *
- Biometric Data *
- Behavioral Data *

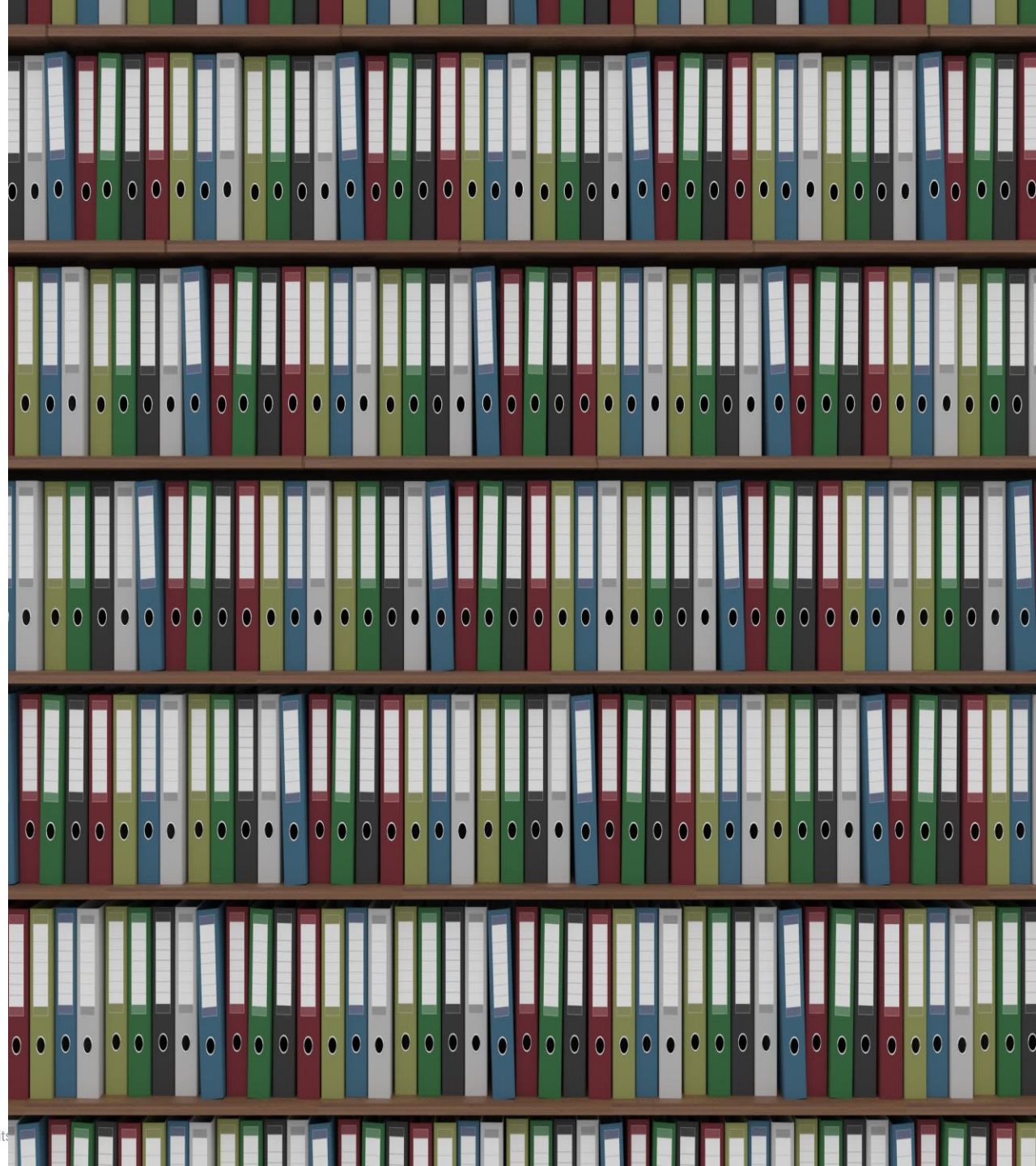
Impact of GDPR on Analytics



Customer data is a
rich source for
demographic and
purchasing analysis



Data teams need large
volumes of historical
and real-time data



Compliance and Fraud
Detection teams will
still need access to
such customer data





Leveraging data masking for analytics continuity



Organizations can retain specific personal data if they have a legitimate business case



Anonymous data is
not subject to
retention restrictions



Security Best Practices



Compliance Needs to be Simplified

- Lawyers and Sec Ops are the compliance experts, not DBAs
- Takes time to create IT ticket to update ACLs on DB
 - If not monitored, this can create privilege creep
 - Or it can create a form of ‘Shadow IT’



Strong Encryption is a Must

- If deletion is not acceptable, use strong encryption with limited key access
 - This encryption is beyond the ‘Always Encrypted’ mechanisms that many DBs have
 - This is assure that few users can view ‘old’ data





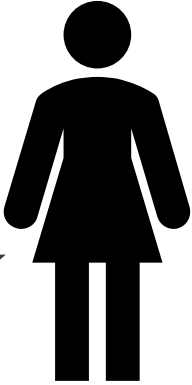
Data masking Demo



Scenario

- Acme Insurance is a **global** insurance company based in New York
- This company was started in the late 1990s
- Acme has many groups including Risk, Fraud, etc.
- As of today, all users authorized to the data via a BI tool, have access to **all** data
- Also, there is project to anonymize data for **closed** claims **older** than 10 years old (beyond encrypting at rest)
- Let's meet our BI users

Alice



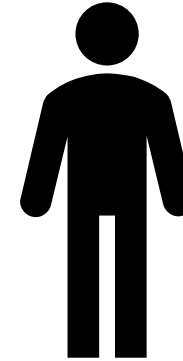
Role: Sr. Risk
Advisor

Group: Risk
Management

Organization:
InfoSec

Region: Global

Bob



Role: Fraud Analyst

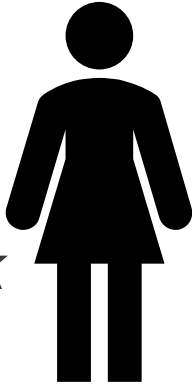
Group: Fraud

Organization: Legal

Region: EMEA

Name	Address	Gender	SSN	Claim Date
John	123 NY	Male	123-45-6789	2/3/2018
Jane	456 CA	Female	987-65-4321	1/1/2002

Alice



Role: Sr. Risk
Advisor

Group: Risk
Management

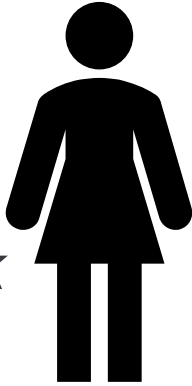
Organization:
InfoSec

Region: Global

A diagram showing five green arrows originating from a single point above Alice's silhouette and pointing to the five columns of the table below: Name, Address, Gender, SSN, and Claim Date.

Name	Address	Gender	SSN	Claim Date
John	123 NY	Male	123-45-6789	2/3/2018
Jane	456 CA	Female	987-65-4321	1/1/2002

Alice



Role: Sr. Risk
Advisor

Group: Risk
Management

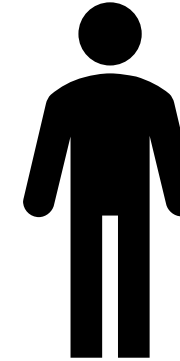
Organization:
InfoSec

Region: Global

MASKED

Name	Address	Gender	SSN	Claim Date
MASKED	123 NY	Male	**MASKED**	2/3/2018
MASKED	456 CA	Female	**MASKED**	1/1/2002

Bob



Role: Fraud Analyst

Group: Fraud

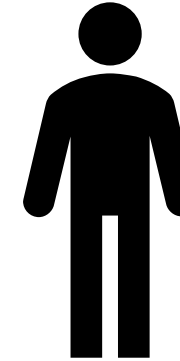
Organization: Legal

Region: EMEA

Four red arrows originate from a single point near Bob's silhouette and point to the 'Name', 'Address', 'Gender', and 'SSN' columns of the table below.

Name	Address	Gender	SSN	Claim Date
John	123 NY	Male	123-45-6789	2/3/2018
Jane	456 CA	Female	987-65-4321	1/1/2002

Bob



Role: Fraud Analyst

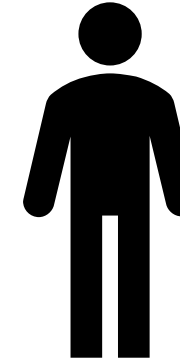
Group: Fraud

Organization: Legal

Region: **EMEA**

Name	Address	Gender	SSN	Claim Date
John	123 NY	Male	123-45-6789	2/3/2018
Jane	456 CA	Female	987-65-4321	1/1/2002

Bob



Role: Fraud Analyst

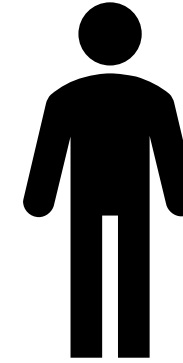
Group: Fraud

Organization: Legal

Region: **EMEA**

Name	Address	Gender	SSN	Claim Date
John	123 NY	Male	123-45-6789	2/3/2018
Jane	456 CA	Female	987-65-4321	1/1/2002

Bob



Role: Fraud Analyst

Group: Fraud

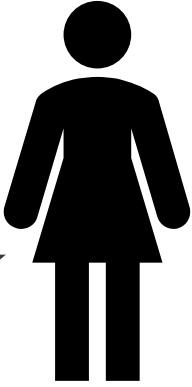
Organization: Legal

Region: EMEA

The diagram illustrates access paths from Bob to a data table. Four red arrows originate from a point above Bob's silhouette and point to specific columns in the table: a solid arrow to 'Name', a dotted arrow to 'Address' labeled 'EMEA Only', a solid arrow to 'Gender', and a solid arrow to 'Claim Date'.

Name	Address	Gender	SSN	Claim Date
John	123 NY	Male	**MASKED**	2/3/2018
Jane	456 CA	Female	**MASKED**	1/1/2002

Alice



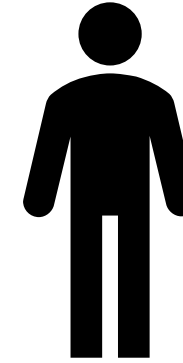
Role: Sr. Risk
Advisor

Group: Risk
Management

Organization:
InfoSec

Region: Global

Bob



Role: Fraud Analyst

Group: Fraud

Organization: Legal

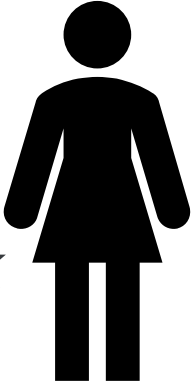
Region: EMEA

MASKED

EMEA Only

Name	Address	Gender	SSN	Claim Date
John	123 NY	Male	123-45-6789	2/3/2018
Jane	456 CA	Female	987-65-4321	1/1/2002

Alice



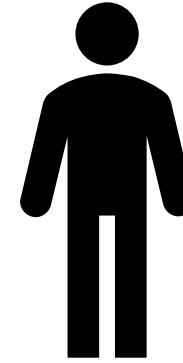
Role: Sr. Risk
Advisor

Group: Risk
Management

Organization:
InfoSec

Region: Global

Bob



Role: Fraud Analyst

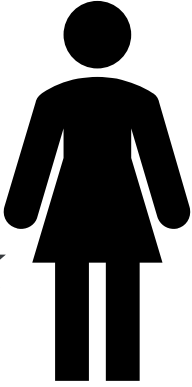
Group: Fraud

Organization: Legal

Region: EMEA

Name	Address	Gender	SSN	Claim Date
John	123 NY	Male	**MASKED**	2/3/2018
Jane	456 CA	Female	987-65-4321	1/1/2002

Alice



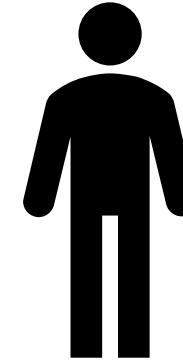
Role: Sr. Risk
Advisor

Group: Risk
Management

Organization:
InfoSec

Region: Global

Bob



Role: Fraud Analyst

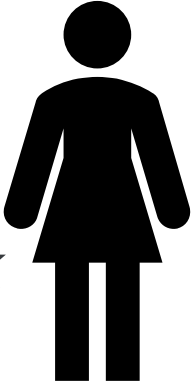
Group: Fraud

Organization: Legal

Region: EMEA

Name	Address	Gender	SSN	Claim Date
John	123 NY	Male	**MASKED**	2/3/2018
Jane	456 CA	Female	987-65-4321	1/1/2002

Alice



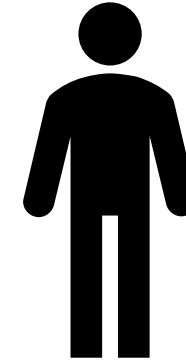
Role: Sr. Risk
Advisor

Group: Risk
Management

Organization:
InfoSec

Region: Global

Bob



Role: Fraud Analyst

Group: Fraud

Organization: Legal

Region: EMEA

MASKED

EMEA Only

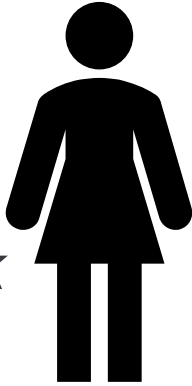
Name	Address	Gender	SSN	Claim Date
John	123 NY	Male	**MASKED**	2/3/2018
ENCRYPTED	ENCRYPTED	ENCRYPTED	ENCRYPTED	1/1/2002



Demo



Alice



Role: Sr. Risk
Advisor

Group: Risk
Management

Organization:
InfoSec

Region: Global

MASKED

Name	Address	Gender	SSN	Claim Date
MASKED	123 NY	Male	**MASKED**	2/3/2018
ENCRYPTED	ENCRYPTED	ENCRYPTED	ENCRYPTED	1/1/2002

Wrap up

- This type of access control is known as Attribute Based Access Control
- This is meant to define access beyond just a user's role
- Example Attributes:
 - Role
 - Location
 - Time of Day
 - Normal Access Pattern (Read vs Write)
- Next Steps: Add one-time passcode to decrypt older claims for a set amount of time



QnA



