GDPR considerations
for your IBM Domino environment

GDPR and Domino: Everything you need to know to become and stay compliant

Speakers: Ben Menesi, Head of Products
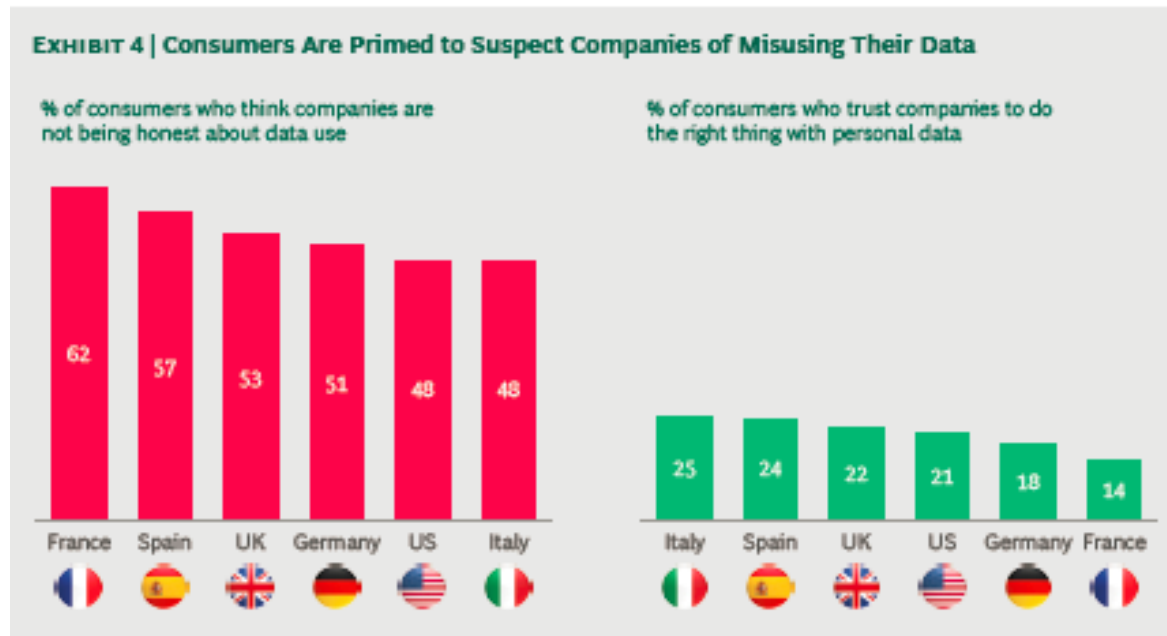
Agenda

Ytria

- GDPR Overview
- Data Subject Rights
- Domino as a Data Container
- Searching Domino
- Ytria tools and how we can help

Introduction

GDPR in a nutshell – a one liner summary

The GDPR Regulation provides the means for
EU citizens to better control their personal and
sensitive data

Introduction

GDPR in a nutshell – reasons

- According to the Boston Consulting Group's recent survey (https://www.bcg.com/publications/2018/leveraging-gdpr-become-trusted-data-steward.aspx)

EXHIBIT 4 | Consumers Are Primed to Suspect Companies of Misusing Their Data

% of consumers who think companies are not being honest about data use

France	Spain	UK	Germany	US	Italy
62	57	53	51	48	48

% of consumers who trust companies to do the right thing with personal data

Italy	Spain	UK	US	Germany	France
25	24	22	21	18	14

Introduction

Ytria

GDPR in a nutshell – Definitions

- **Data Controller**: natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data

- **Data Processor**: a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

- **Data Subject**: A living individual to whom personal data relates / whom personal data identifies.

GDPR in a nutshell – Basics

- Repeals directive 95/46/EC – while principles remain, the GDPR will be much more effective.

- It has been approved by the EU Parliament in April 2016 (already in effect), set to be enforced as of May 25 2018.

- Member states may introduce further provisions as long as they do not weaken the principles outlined in GDPR

- Fines up to 10M EUR or 2& of WW turnover for failing responsibilities, 20M EUR or 4% of WW turnover for personal data

Introduction

GDPR in a nutshell – Consent

- **Consent is key to the GDPR**: Freely given, specific, informed and unambiguous indication of the data subject's wishes by which they agree to the processing of personal data

- **In plain English**: Gone are the days of burying end users in pages and pages of legal mazes for consent (think cookies)

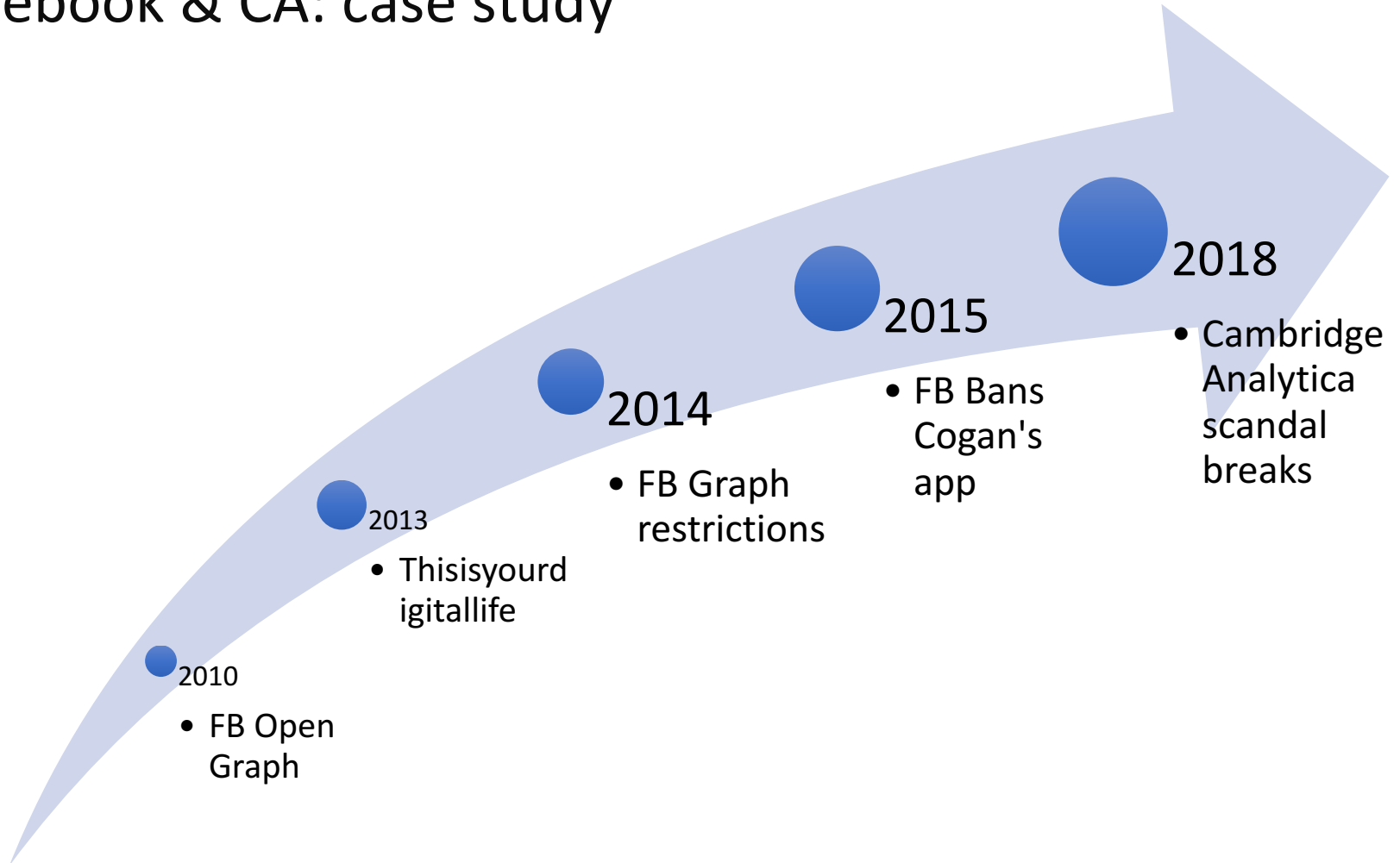- **Out of scope**: This doesn't directly relate to our topic today so we won't be discussing it more in detail. Read more: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/

Introduction

Ytria

GDPR in a nutshell – DPO (Data Protection Officer)

- **Every organization (regardless their size)** must appoint a Data Protection Officer who'll be the face of the organization to the Information Commissioner's Office and to the public.

- **Exceptions:** If processing personal / sensitive data isn't considered to be a core activity (no key operations rely on it)

- **See also:** http://pwc.blogs.com/data_protection/2017/02/data-protection-officer-do-you-need-to-appoint-one.html

- **Conclusion:** It's best to appoint a DPO no matter your company's size, core activities or the scale at which you process personal data.

Introduction

GDPR in a nutshell – Cyber Attacks

- **What is a personal data breach:** Loss of confidentiality that may result in physical, material or non-material damage to natural persons.

- **Report personal data breaches:** within 72 hours of detection

- **Report to the relevant authority:** Contact the ICO and provide a description of the breach including the categories and number of individuals concerned, personal data records, DPO contact information, measures taken to address the breach. (Information may be provided in phases according to article 34(4))

- **About detection:** According to FireEye, global average for intrusion detection is 146 days and **469 days** in the EMEA region. Read more: https://www.fireeye.com/company/press-releases/2016/fireeye-releases-first-mandiant-mtrends-emea-report.html

Cambridge Analytica

Ytria

Facebook & CA: case study

2018
- Cambridge Analytica scandal breaks

2015
- FB Bans Cogan's app

2014
- FB Graph restrictions

2013
- Thisisyourd igitallife

2010
- FB Open Graph

Cambridge Analytica

Ytria

Facebook & CA: In terms of GDPR

- **Facebook:** Data Controller

- **Global Science Research:** Data Processor

- **How to tell if you've been impacted:** One friend is enough:
  https://www.facebook.com/help/1873665312923476?helpref=search&sr=1&query=cambridge

- **Why would (and still might) this be a $480M GDPR Fine**
  - Lack of breach reporting within 72 hours
  - No clear consent or data retention policy
  - Exposing personal data that no data subject consented to

True Caller

Application to identify unknown caller IDs

- **Yet another GREAT subject for GDPR**

Data Subject Rights

Ytria
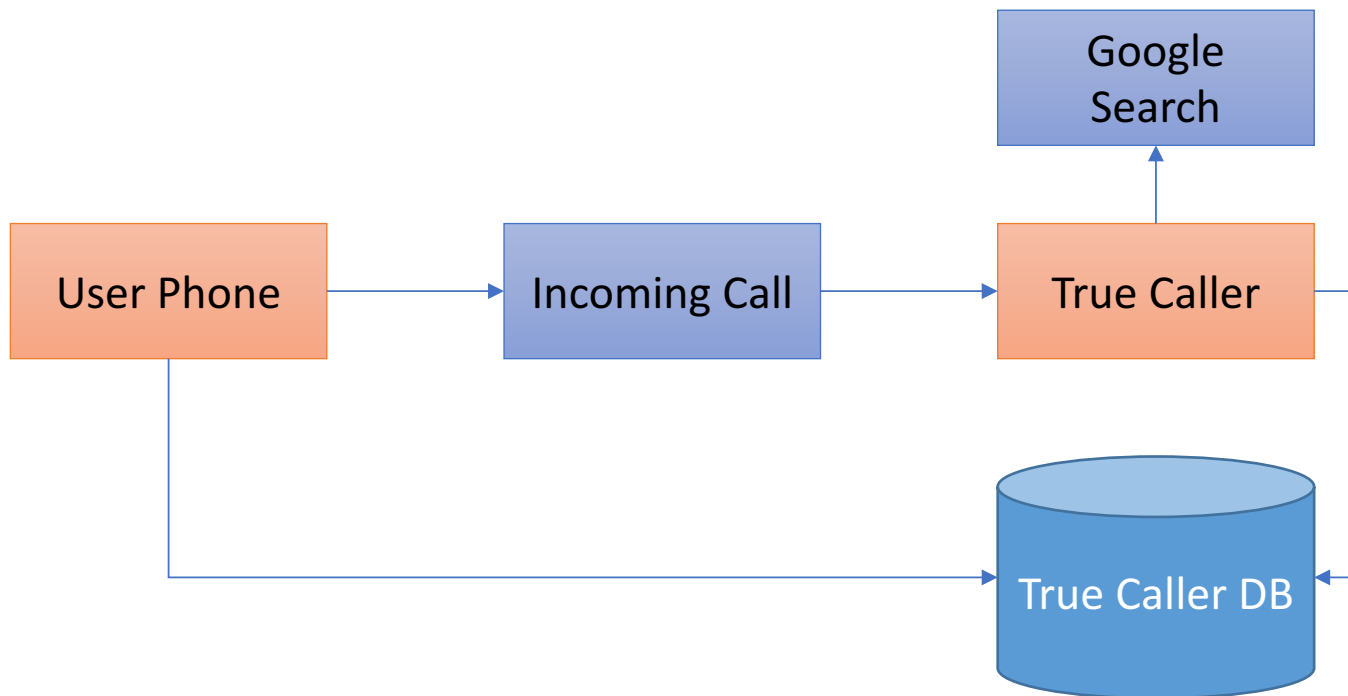
What rights does the GDPR grant to data subjects?

- Right of access: Whether and where my data is processed? For what purposes? Recipients with whom my data is shared? For how long?

- Right of rectification: Is my data accurate? I want it deleted / rectified.

- Right of to be forgotten: You don't need my data anymore. (Google paper: https://drive.google.com/file/d/1H4MKNwf5MgeztG7OnJRnl3ym3gIT3HUK/view)

- Right of data portability: I want a copy of my personal data.

- Right of objection: Stop processing my data unless you can prove you legally need to continue.

- Right to not be evaluated on the basis of automated processing: Do not profile me and make decisions about me unless it's lawfully authorized or I explicitly consented to it.

Domino as a data container

Ytria

Debunking hoaxes about Domino and GDPR

- Some of you might have come across articles such as this one: https://www.realwire.com/releases/Lotus-Notes-and-the-GDPR-conundrum

- Domino is VERY SECURE. (No major data breach in the last decade, last public exploit over 2 years ago)

- Domino can't be made GDPR compliant: FALSE.

- No matter what software you use, complying with the GDPR requires significant legwork. Domino is no exception but it's doable.

Domino as a data container

Ytria

What counts as personal data in an NSF database?

Custom Apps	Mail files	System Databases
• Documents with names • Attachments containing personal information	• Mails from / to / about the data subject • Mails with attachments containing PII	• Logs containing names • IP Address information

Domino as a data container

The challenge

Access	Rectification
SEARCH	
Erasure	Portability

Domino as a data container

Ytria
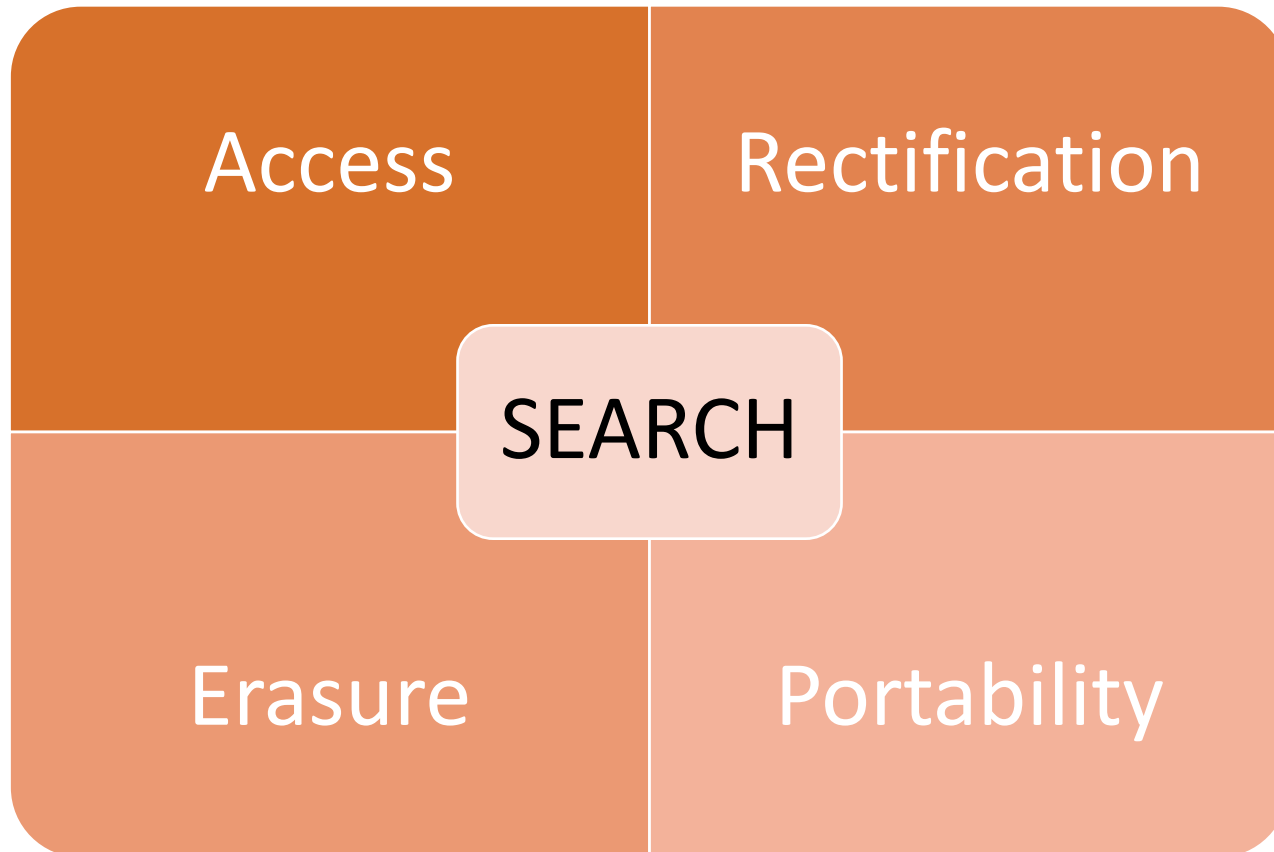
IBM SmartCloud vs. On-premises

	IBM SmartCloud	On-Premises
Data Controller:	Your organization	Your organization
Data Processor:	IBM	Your organization
Domino Data shared with:	3rd party, outside the EU depending on datacenter	Your organization, outside the EU depending on server location & replication
Scope of GDPR compliance	Mail only	Mail & applications (apps. Only if you use IBM SC)

Domino as a data container

Ytria

Ideal GDPR readiness for Domino

Domino as a data container

Ytria
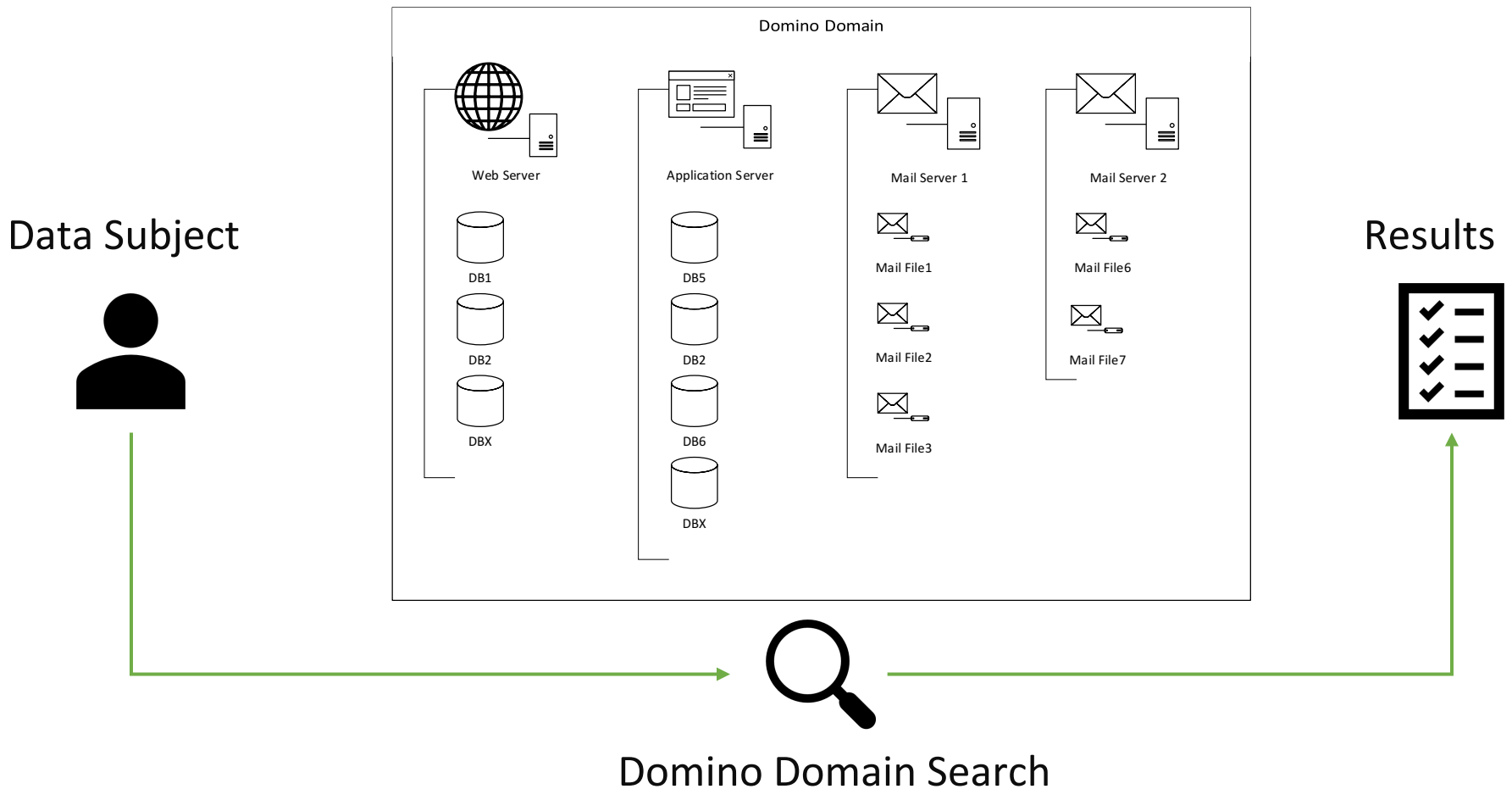
Domino discovery & data mapping phase

Inventory
- Establish a list of all NSFs
- How and where do they replicate

Data Mapping
- Profile NSFs according to type (mail, app, system)
- Data mapping: which DBs may contain personal data

Structure
- Understand personal data extent and data structure
- Access rights to focus databases
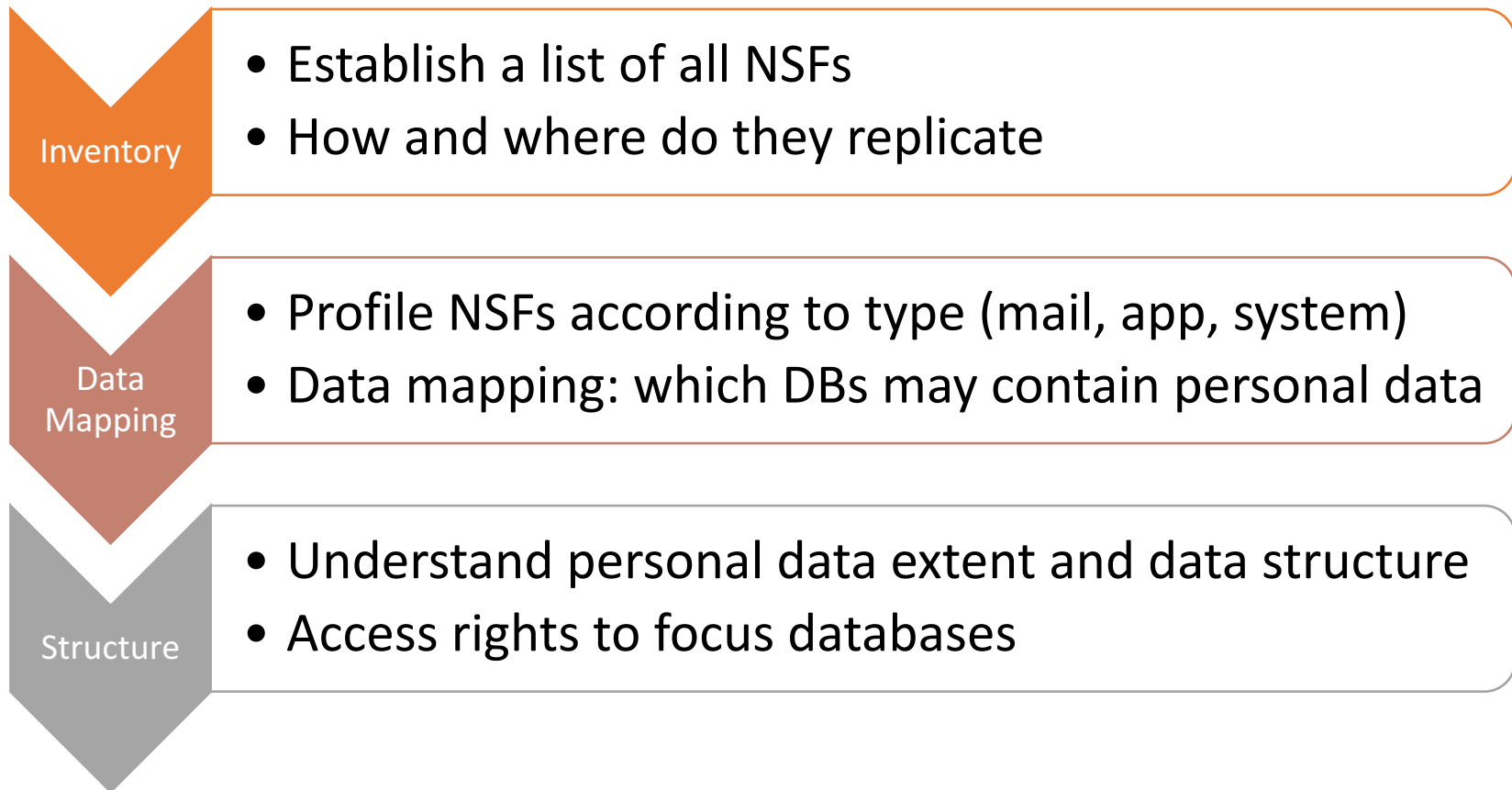
Domino as a data container

Your domino environment after discovery & data mapping

Domino as a data container

Ytria
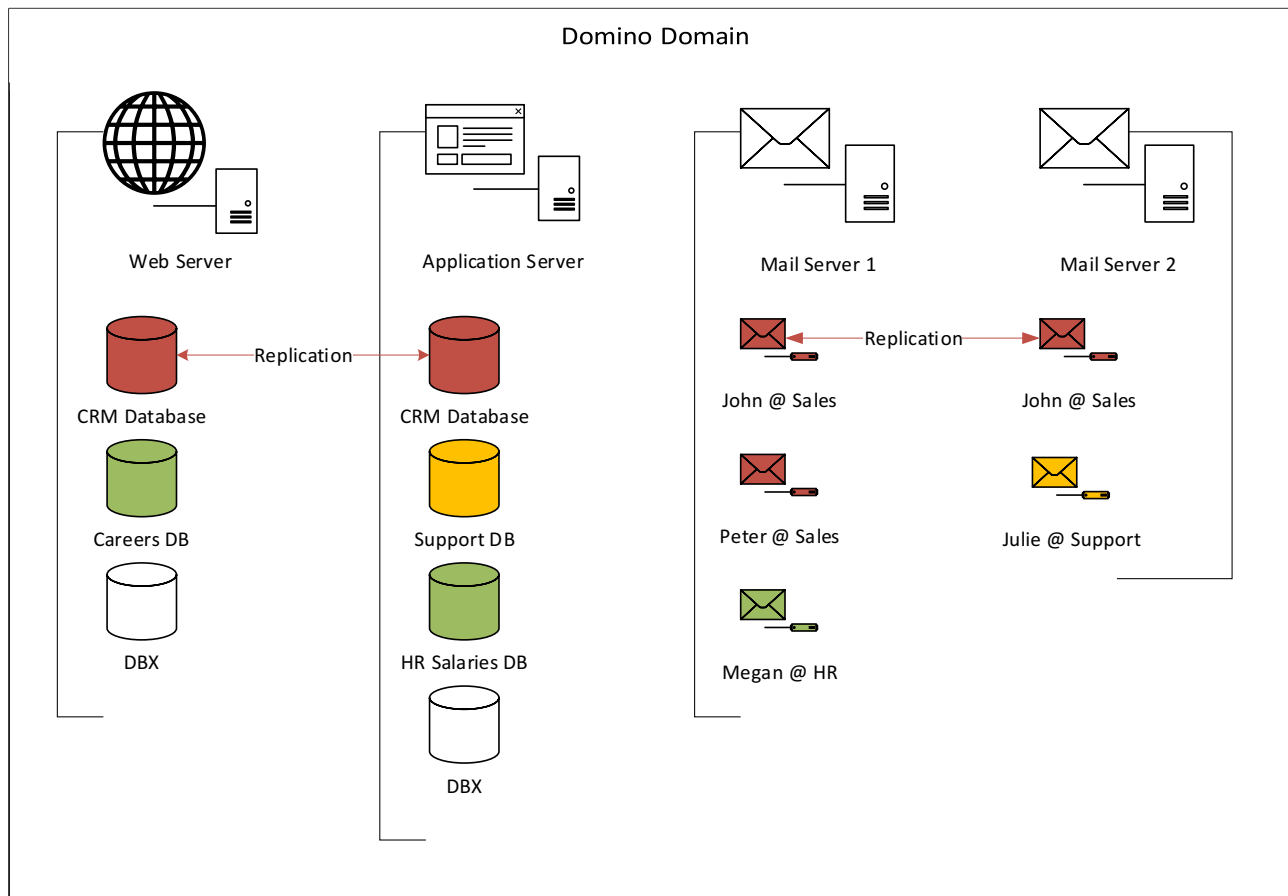
Data mapping in real life

- ■ Example: we've already received our first access request from a customer pertaining to their employers' personal data in our systems

Annual renewal - GDPR Regulation 2018
Hope you are keeping well.

It is almost time for our annual renewal of the scanEZ and databaseEZ licences. I'm sure you are already aware and possibly already been asked GDPR related questions by other customers for the first time this year as the new EU regulation comes into force. On the basis that personal data being processed by Ytria is limited to the name, email address and telephone contact numbers of a small number of [redacted] Staff and the data is processed outside the EEA, I will require the following actions to be completed as part of the renewal process this year:

(a) An appropriate contract should be in place which includes the GDPR compliant clauses and EU model clauses. In particular, the contract must include:-
A clause providing, at [redacted] choice, return or secure & permanent deletion of personal data (at our option) & any copies in accordance with our instructions upon expiry/termination, with certification that destruction has been completed
(b) I will require to review the existing staff information Ytria holds, which has built up to date, to ensure personal data is retained for no longer than is needed for the original support purpose. We can agree to include this information each renewal year to ensure only current staff contact information is being held for the purposes of providing support.

If you can arrange to have a renewal quote together with a list of existing [redacted] staff contact information held and a GDPR compliant support agreement I will be able to progress the renewal Purchase Order.

Searching Domino

Ytria

The key to locating personal data: Search, search and search

- Full Text Indexing is your friend

- When no FTI possible: more work, you need to identify items that can be used to connect documents to data subjects, and then use them for searches via Formulas, LS or Java.

- Database by database search: not enough. You will need a larger framework to comply and make your data subject request response time and resource efficient.

Searching Domino

Ytria

Locating personal data in Domino

Data Subject Request

Scan focus databases

Identify focus mail files & mail-in DBs

Locate focus databases

Access and delegation report for any matching DBs

Access Report for any DBs with matches

Scan focus mail files & mail-in DBs

Response to Request

< 1 month*

How we can help you
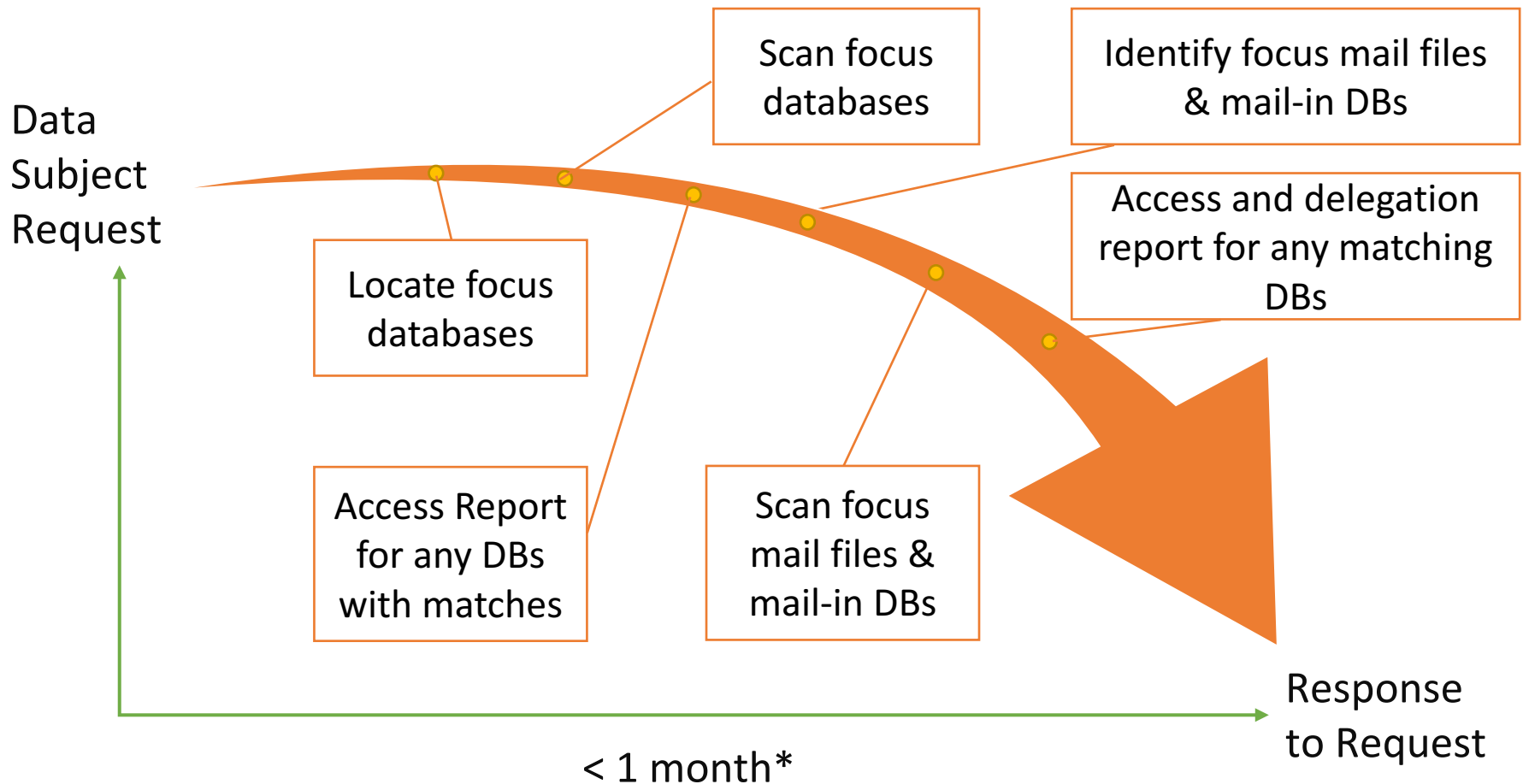
Ytria

Using Ytria to extend database operations

Discovery
- Environment overview
- Replication analysis

Extended Search
- Multi-DB FTI, Formula, Mail & attachment search
- Extended Custom Application Search

Access Documentation
- Cross-server ACL Reporting
- Effective Access reporting across servers

Ytria – Discovery

Ytria

replicationEZ: cross-server database overview

Ytria - Discovery

With replicationEZ you can

- List every single database across all servers and find out where and when they replicated

- Easily identify focus databases with personal information based on their template inheritance or any other database information

- Filter out templates and non-relevant, standard IBM databases to focus on what really matters.

Ytria - Discovery

Ytria

databaseEZ: In-depth server-wide database analysis

Ytria - Discovery

With databaseEZ you can

- Analyze all apps server by server including 130+ database properties

- Classify databases by type, template, amount of documents and more

- Analyze user activity across multiple databases to establish usage patterns and locate focus databases.

scanEZ search automation

- Use databaseEZ for database selection and process selected databases using scanEZ automation XML scripts

- Find all pre-made scripts here:
  http://www.ytria.com/WebSite.nsf/WebPageRequest/GDPR-considerationsen

- Easily edit your XMLs to modify / add search terms.

- Load server using databaseEZ, select databases to scan and use 'Execute Automation Scripts on' > scanEZ before selecting the appropriate XML file.

Ytria

Running scanEZ automation scripts

Ytria – Extended Search

Multi-database FTI search using scanEZ automation

- Edit the XML to modify the search term

```xml
<!--Full Text Index search term to look for. Copy and paste the entire line to add more terms -->
<List name="vFTISearchTerms" Action="SetVar" vFTISearchKeyword="GDPRFTI"/>
```

- Duplicate and edit line to add more search terms

```xml
<!--Full Text Index search term to look for. Copy and paste the entire line to add more terms -->
<List name="vFTISearchTerms" Action="SetVar" vFTISearchKeyword="GDPRFTI"/>
<List name="vFTISearchTerms" Action="SetVar" vFTISearchKeyword="Sensitive Data"/>
<List name="vFTISearchTerms" Action="SetVar" vFTISearchKeyword="Gender"/>
```

- Find the script here:
  http://www.ytria.com/WebSite.nsf/WebPageRequest/GDPR-considerationsen

Ytria – Extended Search

Ytria

Multi-database Mail search using scanEZ automation

- Edit the XML to modify the search term

```
<!-- USER INPUT: Please define your variables here. Define a file name including its extension -->
<List name="vDataSubjectNames" Action="SetVar" vDataSubjectName="John Admin"/>
```

- Current script searches expression in items SendTo, Copyto and From. Modify XML to change / add / remove item names to search custom applications

```
<!--This script block will perform the search for the documents.-->
<SearchBy Type="Formula">
    <Setparam Field="SetFormula" Value="@Contains(FirstName:LastName:Mgr:Customer:c_Gender;&quot;{%vDataSubjectName%}&quot;)"/>
    <Setparam Field="SearchDocuments" Value="true"/>
    <Setparam Field="SearchDesigns" Value="false"/>
    <Setparam Field="PutSearchInSelCreateName" Value="{%vDataSubjectName%}"/>
</SearchBy>
```

- Find the script here:
  http://www.ytria.com/WebSite.nsf/WebPageRequest/GDPR-considerationsen

Ytria – Extended Search

Multi-database Attachment search using scanEZ automation

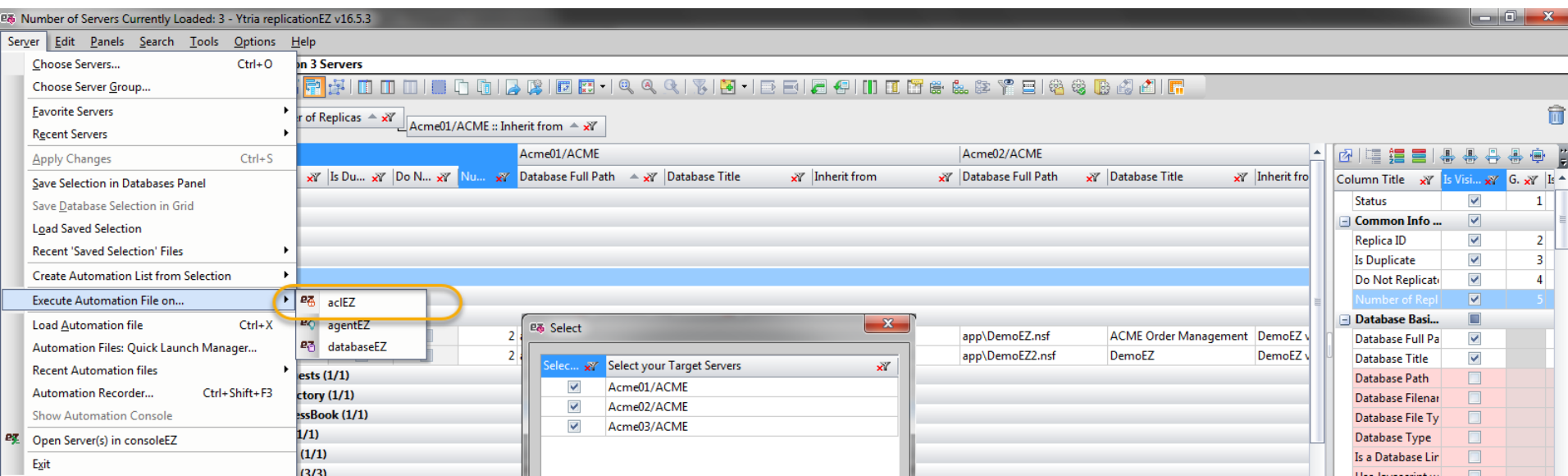- Edit the XML to modify / add attachment names to locate

```xml
<!-- USER INPUT: Please define your variables here. Define a file name including its extension -->
<List name="vAttachmentSearchObjects" Action="SetVar" vAttachmentName="Sensitive_CV.pdf"/>
<List name="vAttachmentSearchObjects" Action="SetVar" vAttachmentName="CV.pdf"/>
```

- Find the script here:
  http://www.ytria.com/WebSite.nsf/WebPageRequest/GDPR-considerationsen

Ytria – Access Documentation

Multi-server effective access reporting automation

- aclEZ can calculate effective access for multiple users, across all databases.

- Using replicationEZ load multiple servers, then select 'Server' > 'Execute automation file on' > 'aclEZ' and select servers to report Effective access from.

Ytria – Extended Search

Multi-server effective access reporting automation

- Edit the XML to modify / add / remove users whose effective access will be calculated across all databases and servers.

```
<ShowEffectiveAccess RemoveAll="true">
    <!-- Modify the Value field to match any user of interest, and feel free to remove or add lines for less / more users -->
    <SetParam Field="Added" Value="Anonymous"/>
    <SetParam Field="Added" Value="Dorothee Parker/ACME"/>
</ShowEffectiveAccess>
<Select />
```

- Set the 'RemoveAll' parameter to "false" and remove user names to calculate effective access for all users across all databases (warning: this will take time!)

```
    <ShowEffectiveAccess RemoveAll="false">
</ShowEffectiveAccess>
<Select />
```

- Find the script here:
  http://www.ytria.com/WebSite.nsf/WebPageRequest/GDPR-considerationsen

Need Help?

Ytria

Ytria Tandem Jump

- 2h remote session with one of our engineers using the Ytria tools

- Includes temporary licenses and help with Automation script configuration

- Flat pricing at USD $500

- More info: http://www.ytria.com/tandem

"Taking the tandem jump with Ytria's help let us discover so much about our environment, that it would've probably taken us about 2 weeks to get the same results ourselves—even if we already had the Ytria tools..."

- Anatol Lizik, Domino admin, Solaris

Next Webinar…

Free webcast on Domino Security

- External Domino security and all that's involved

- Mitigating internal risks from application design flaws to agent security

- Real life attack scenarios and how to defend yourself against them

Apr 18, 2018 9:00 AM in Eastern Time (US and Canada)

www.ytria.com/ibmdominosecurity

Thank you

Ytria

Thank you for attending our webinar

Any feedback or questions:

support@ytria.com

Recording available:

https://youtu.be/ELOO4RU6ss4