# Solution highlight: User Interface Logging and Field Masking Solutions by SAP

Erin Hughes, SAP
May 19, 2020

asug

# Your speakers today

Erin Hughes
Cybersecurity Solution Advisor
SAP

 © 2020 ASUG Confidential

# Key Takeaways

•Understand why data masking plays a key part in an overall data security strategy.

•Discover how the UI masking solution can help protect data based on configurable attributes and rules.

•Learn how the UI logging solution complements the UI masking solution by providing a way to record and analyze data that has been displayed in SAP.

 © 2020 ASUG Confidential

# Security challenges are evolving

| | Historical IT Security Perspectives | Today's Leading Cybersecurity Insights |
|---|---|---|
| **Scope of the Challenge** | Limited to your "**four walls**" and extended to the enterprise | Spans your interconnected **global** and business **ecosystem** |
| **Ownership and Accountability** | **IT led** and operated | Business-aligned and owned; **CEO** and **board driven** |
| **Adversaries' Characteristics** | **One-off** and opportunistic; motivated by notoriety, technical challenge and individual gain | **Organized**, funded and **targeted**; motivated by economic, monetary and political gain |
| **Information Asset Protection** | **One-size-fits-all** approach | Prioritize and protect the "**crown jewels**" |
| **Defense Posture** | **Protect the perimeter**; respond if attacked | **Protect the application** and **data** yet plan for a breach, monitor and rapidly respond |
| **Security Intelligence and Information Sharing** | Keep to yourself | Public/private **partnerships**; collaboration with **industry working groups** |


© 2020 ASUG Confidential

# Global data protection regulations are expanding

## Data protection regulations vary globally and are extending their reach

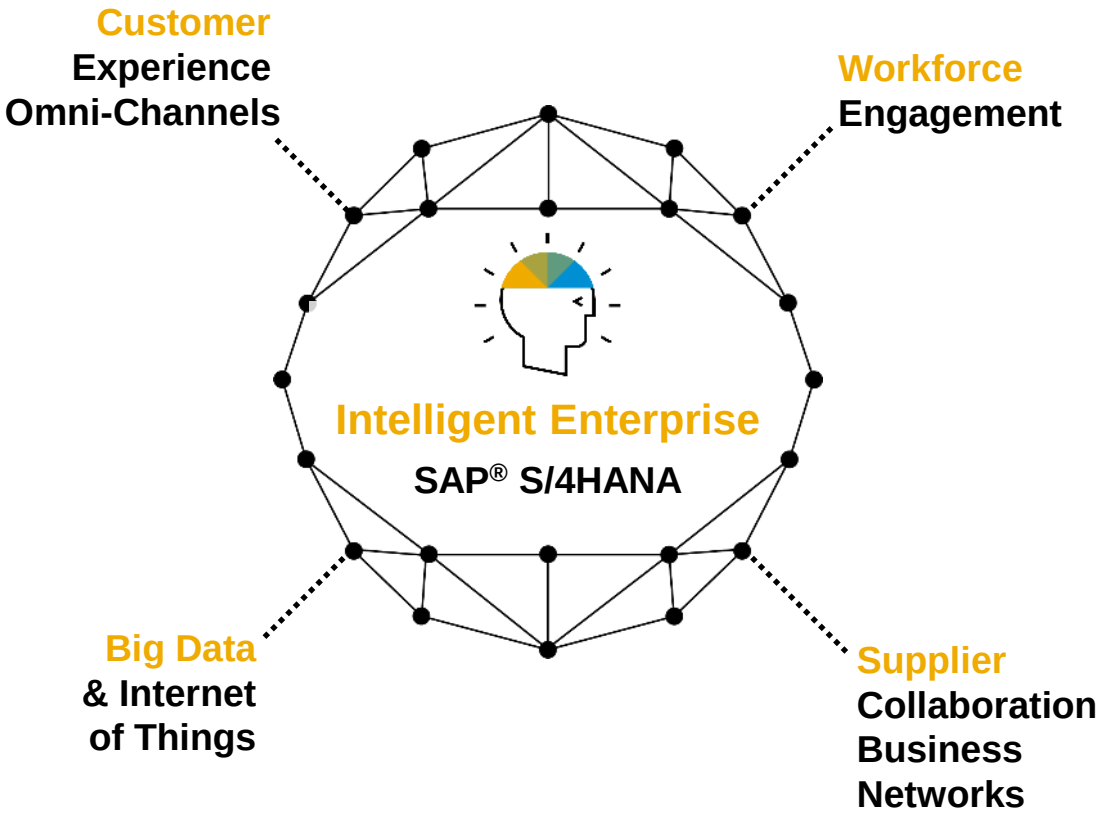
### Global data protection regulations impact cloud vendors and customers

| Country | Regulations |
|---|---|
| **USA** | **USA Patriot Act, Stored Communications Act, EU-US Privacy Shield, California Consumer Privacy Act – 2020** |
| **EU** | EU Data Protection Directive replaced in 2018 by the EU General Data Protection Regulation **(GDPR)** − privacy laws in 28 countries |
| **Germany** | Federal Data Protection Act (FDPA) |
| **Brazil** | **General Data Protection Law (LGPD) – 2020** |
| **Australia** | Privacy Act 1988, Australian state and territory legislation |
| **Singapore** | The Personal Data Protection Act (PDPA) |
| **Canada** | Personal Information Protection Act (PIPA), Personal Information Protection and Electronic Documents Act (PIPEDA), Freedom of Information and Protection of Privacy Act (FIPPA) |
| **Russia** | Federal Law No. 152-FZ on Personal Data |


© 2020 ASUG Confidential

# SAP helps build Digital Trust in digital transformation

## Effectively manage cybersecurity and data protection risk




**Digital transformation requires security to be smarter, automated, and embedded**

1. **Security role design and governance** must be considered early on to minimize cross-system risk and insider threats
2. **Systems and applications** must be monitored and maintained to minimize vulnerabilities and protect against data loss
3. **Manual controls and checks** must be replaced with smarter, AI-driven controls to identify anomalies and potential issues early on
4. **Digital automation** requires even more reliable and effective monitoring of transactions and processes as human intervention is minimized


© 2020 ASUG Confidential

# Data security: What it's all about

## Privacy controls and security should be baked in

### Privacy by design

- Include privacy risk in security risk assessments
- Incorporate data privacy in information security policies
- Maintain procedures to restrict access to personal data – segregation of duties and roles
- Enable identity management and customer identity management processes

### Data security

- Maintain technical security measures
- Maintain measures to encrypt personal data
- Secure and track access to specific application fields

### Data loss prevention

- Maintain a data loss prevention strategy
- Classify and distribute policies
- Conduct testing of security posture
- Maintain security certification
- Maintain business continuity plans


© 2020 ASUG Confidential

# Agenda

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| **What** | **When** | **Where** | **Next Steps** |
| Solution overview | Use cases | Architecture and availability | |

 © 2020 ASUG Confidential

# Agenda

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| **What** | **When** | **Where** | **Next Steps** |
| Solution overview | Use cases | Architecture and availability | |


© 2020 ASUG Confidential

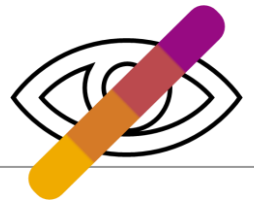
# Key business requirements

1. Reliable control who gets sensitive information displayed in SAP transactions and applications, in a quick and low-effort fashion
2. Introduce a *dynamic* determination of data access authorizations based on the context, at runtime
3. Increase protection of sensitive data against theft and abuse where access must be provided to privileged insiders
4. Detect potentially problematic access to sensitive data rapidly (in near-real time), and conduct a meaningful analysis in order to take the right actions
5. Better comply with business or legal requirements for tracking who accessed sensitive data (PII, BOMs, prices, customer information)


© 2020 ASUG Confidential

# UI Data Security: two step approach to protect data from insiders

## UI Masking



**to conceal specific data (values in fields/columns) – unless required for tasks**

The solution masks sensitive (configured) values **per default**; unmasking requires **explicit access rights** (on top of existing role/authorization setup)

➔ make **data elements unavailable** for data abuse (opportunistic and targeted)

**“the speed limiter”**

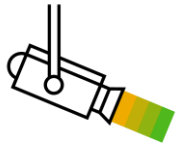
## UI Logging

**to keep data accessible, but log & analyze access, to identify adequate path of action**

The solution provides a **detailed, structured data access log and allows for analysis** who exactly received which data (output), how (input), and in which context (IP…)?

➔ **prevent illegitimate data access and theft** by inducing compliant behavior

➔ **identify & prove** irregular data access



**“the speed camera”**

- awareness for data security (“human firewall”) → protect employees by decreasing inadvertent breaches
- top-of-class protection measures → **trust** (employees, customers, and investors)

 © 2020 ASUG Confidential

# Agenda

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| **What** | **When** | **Where** | **Next Steps** |
| Solution overview | Use cases | Architecture and availability | |

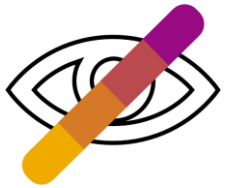

© 2020 ASUG Confidential

# Sample use cases

- **Prevent theft of massive amounts of data** by masking mass access (e.g. from SE16n, and similar transactions, reports)
- **Protect IP in BOMs** (=recipes)
- **Mask specific fields in HR** to protect sensitive private data; specifically Social Security Number
- Mask **pricing/costing information** (conditions, end prices, resulting price list) to avoid leaking to customers/vendors
- **Mask customer data & pricing/costing information** (conditions, end prices, resulting price list) for 3rd parties (usually partners/vendors) working in the system
- "**Divestiture**" – company split of spin offs: virtually segregate data access until systems are physically separated/split
- **Mask data for external/temporary roles** (e.g. call center: show only what is required for the task; e.g. only last names, only parts of identifying numbers like bank accounts, telephone and customer numbers)


© 2020 ASUG Confidential

# UI Masking



## … conceal specific data (values in fields/columns) – unless required for tasks

### Data masking at the UI layer on server side

- data pseudonymization and anonymization
- business and technical transactions
- restriction of data processing (display, change)
- Compliant data transfers (download, export, print)

### Highly configurable – define:

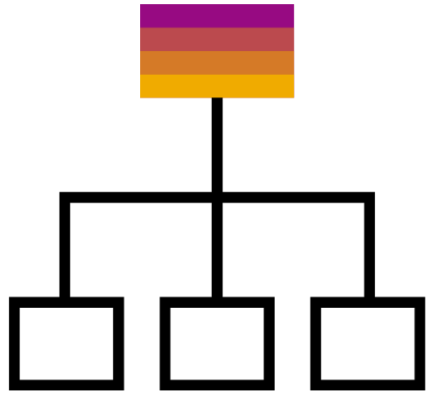
- Which screen fields will appear masked to unauthorized users
- Which users should receive unmasked data for a given field
- When an access trace will be written on access
- Additional logic through BADIs provided by the solution

Based on **SAP NetWeaver** releases 7.00 – 7.50

**Maintenance**: planned until 31.12.2025


© 2020 ASUG Confidential

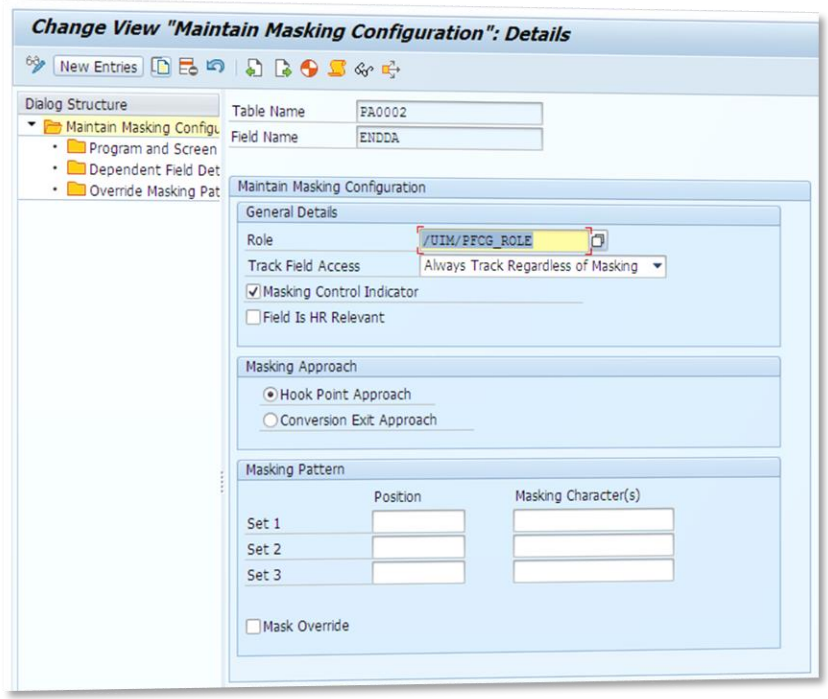
# Role based masking



# UI Masking
## Example: Role based masking

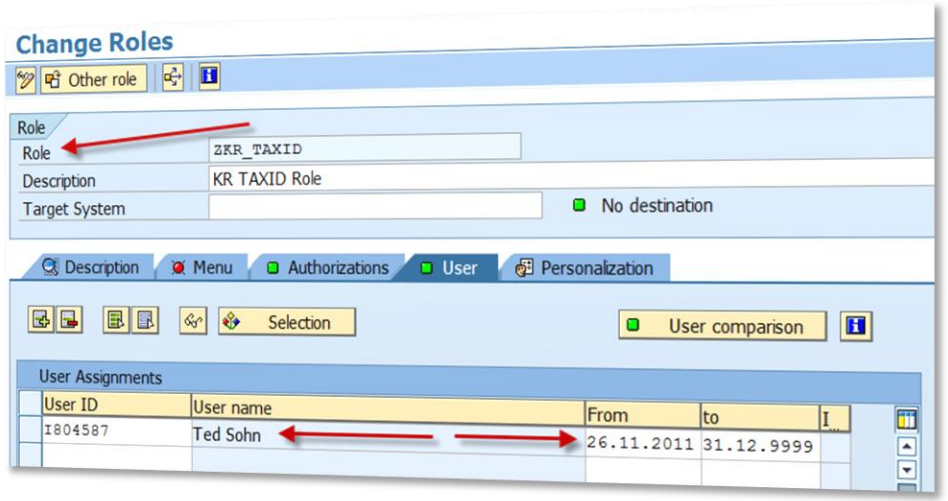
### 1. Define fields to be masked, and rules

- Define which field are masked.
- Configure on field level how a field is displayed. Define on digit base whether and how data are masked.




### 2. Register authorized users per field

- In transaction PFCG, assign users to the UI Masking authorization a role.
- Users assigned to these roles will be able to see unmasked values for the applicable fields
- BAdIs available to introduce customized business logic determining who has access




 © 2020 ASUG Confidential

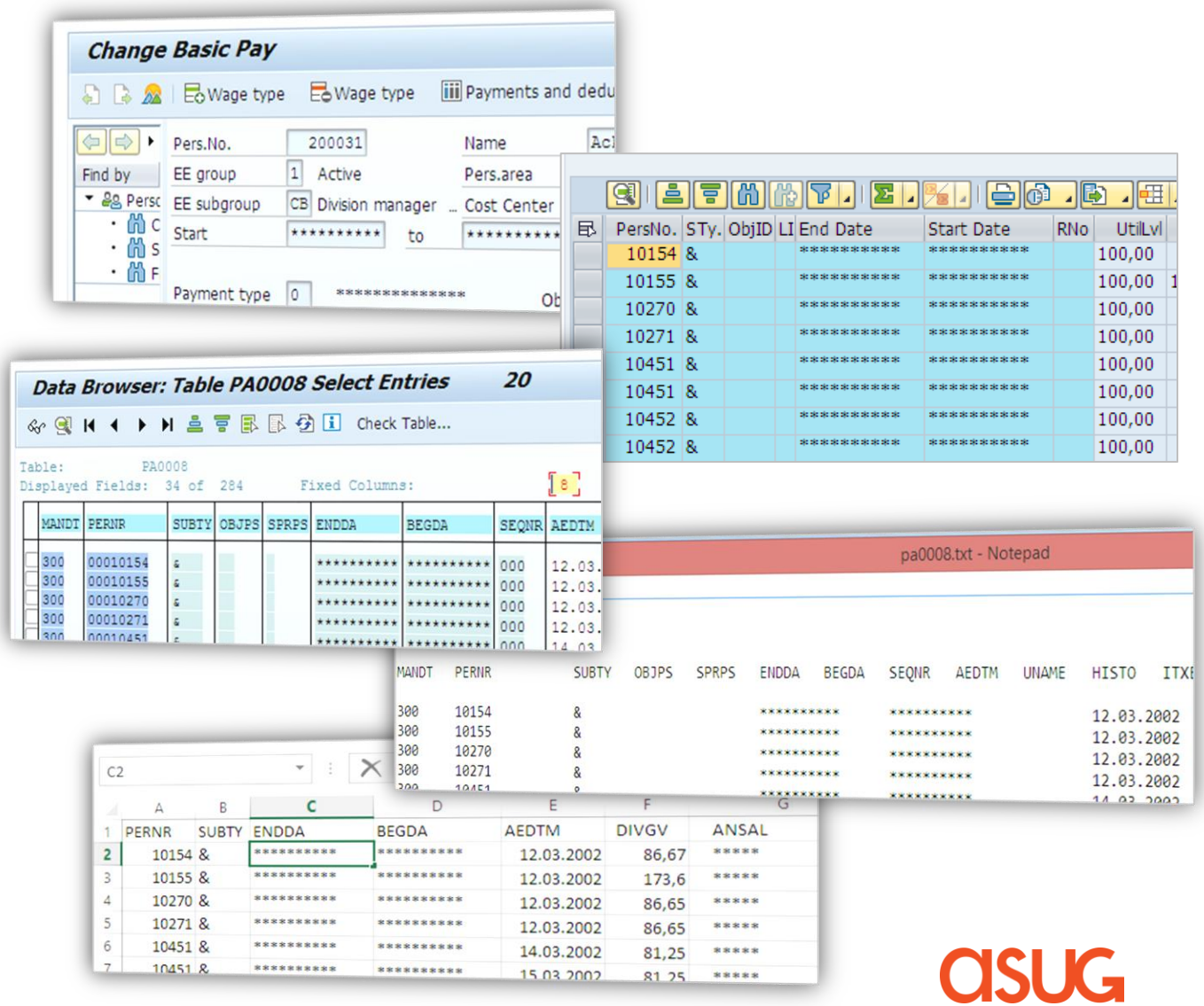
# UI Masking
## Example: Role based masking

### 3. Result: data masking

**Data is masked in GUI transaction** display for un-authorized users.

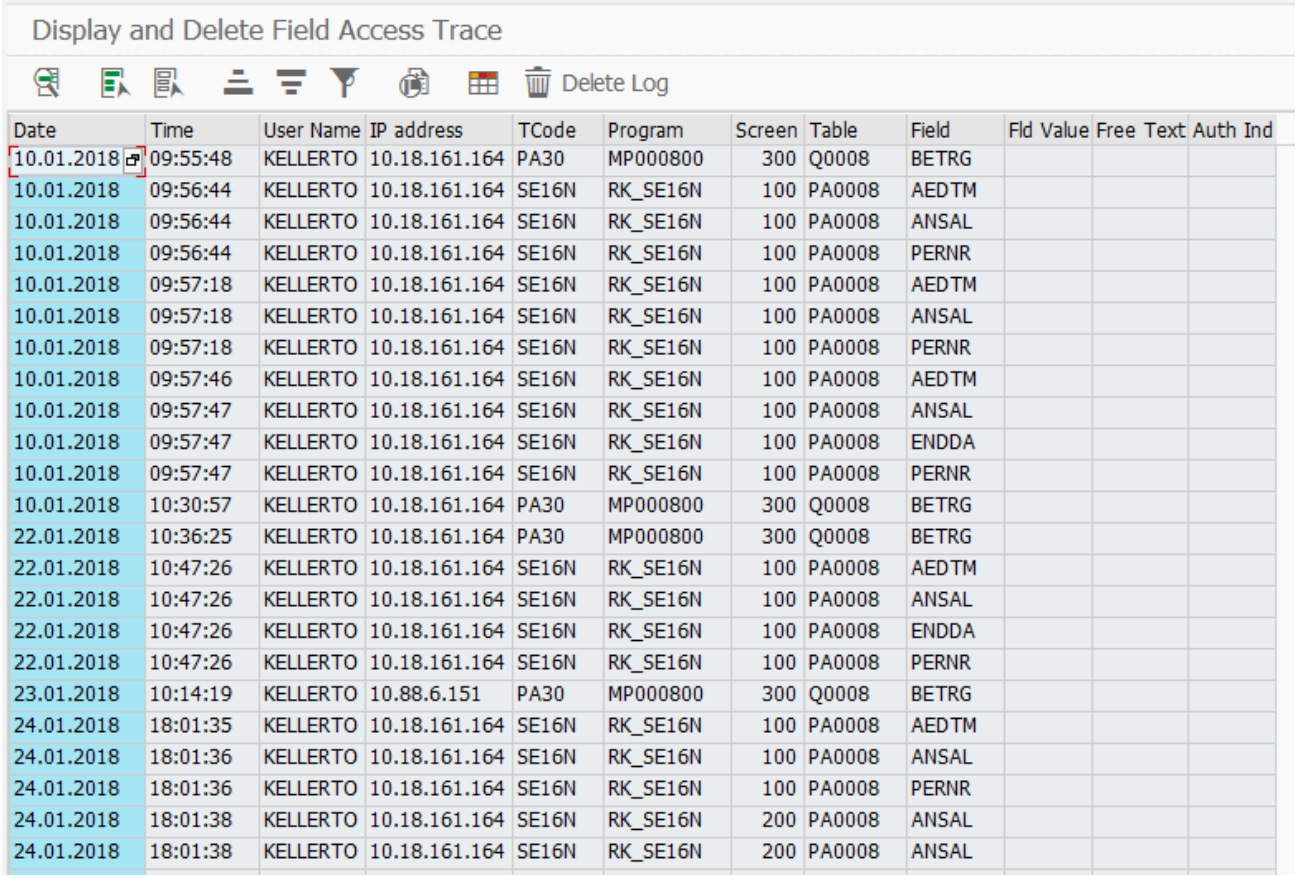
This also **affects high-level "admin" system users** (in dynamic transactions, e.g. SE11, SE12, SE16, SE16n) – unless they are explicitly authorized for a field

UI Masking also protects data during **download, export, and print**




 © 2020 ASUG Confidential

# UI Masking
## Access trace


Display and Delete Field Access Trace

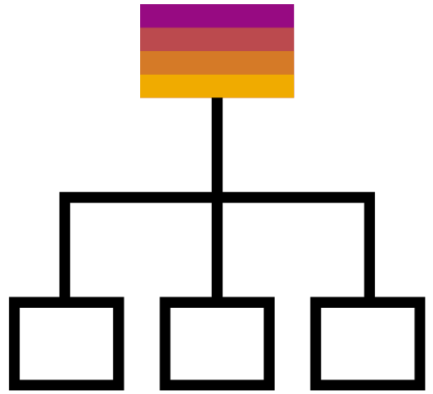
Delete Log

| Date | Time | User Name | IP address | TCode | Program | Screen | Table | Field | Fld Value | Free Text | Auth Ind |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 10.01.2018 | 09:55:48 | KELLERTO | 10.18.161.164 | PA30 | MP000800 | 300 | Q0008 | BETRG | | | |
| 10.01.2018 | 09:56:44 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | AEDTM | | | |
| 10.01.2018 | 09:56:44 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | ANSAL | | | |
| 10.01.2018 | 09:56:44 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | PERNR | | | |
| 10.01.2018 | 09:57:18 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | AEDTM | | | |
| 10.01.2018 | 09:57:18 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | ANSAL | | | |
| 10.01.2018 | 09:57:18 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | PERNR | | | |
| 10.01.2018 | 09:57:46 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | AEDTM | | | |
| 10.01.2018 | 09:57:47 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | ANSAL | | | |
| 10.01.2018 | 09:57:47 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | ENDDA | | | |
| 10.01.2018 | 09:57:47 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | PERNR | | | |
| 10.01.2018 | 10:30:57 | KELLERTO | 10.18.161.164 | PA30 | MP000800 | 300 | Q0008 | BETRG | | | |
| 22.01.2018 | 10:36:25 | KELLERTO | 10.18.161.164 | PA30 | MP000800 | 300 | Q0008 | BETRG | | | |
| 22.01.2018 | 10:47:26 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | AEDTM | | | |
| 22.01.2018 | 10:47:26 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | ANSAL | | | |
| 22.01.2018 | 10:47:26 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | ENDDA | | | |
| 22.01.2018 | 10:47:26 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | PERNR | | | |
| 23.01.2018 | 10:14:19 | KELLERTO | 10.88.6.151 | PA30 | MP000800 | 300 | Q0008 | BETRG | | | |
| 24.01.2018 | 18:01:35 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | AEDTM | | | |
| 24.01.2018 | 18:01:36 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | ANSAL | | | |
| 24.01.2018 | 18:01:36 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 100 | PA0008 | PERNR | | | |
| 24.01.2018 | 18:01:38 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 200 | PA0008 | ANSAL | | | |
| 24.01.2018 | 18:01:38 | KELLERTO | 10.18.161.164 | SE16N | RK_SE16N | 200 | PA0008 | ANSAL | | | |

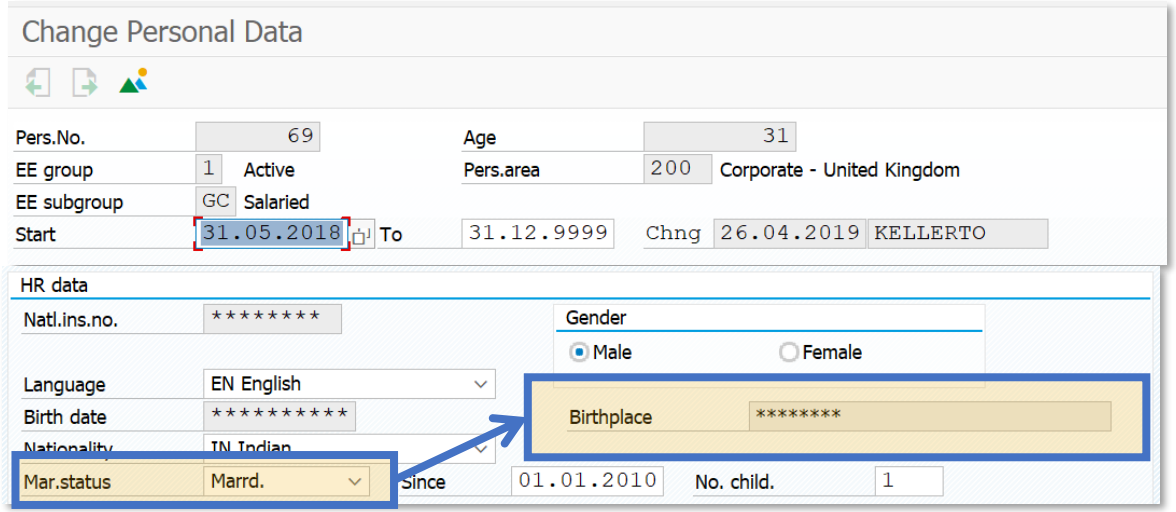
- UI Masking trace functionality gives an overview which data were requested per user, and what information was actually displayed.
- Always, never, only if unmasked
- UIM trace functionality is not comparable to the UI Logging log file. UI Logging is far more detailed, contains context and meta data of the access, and thus is an excellent basis for meaningful analysis of data access.

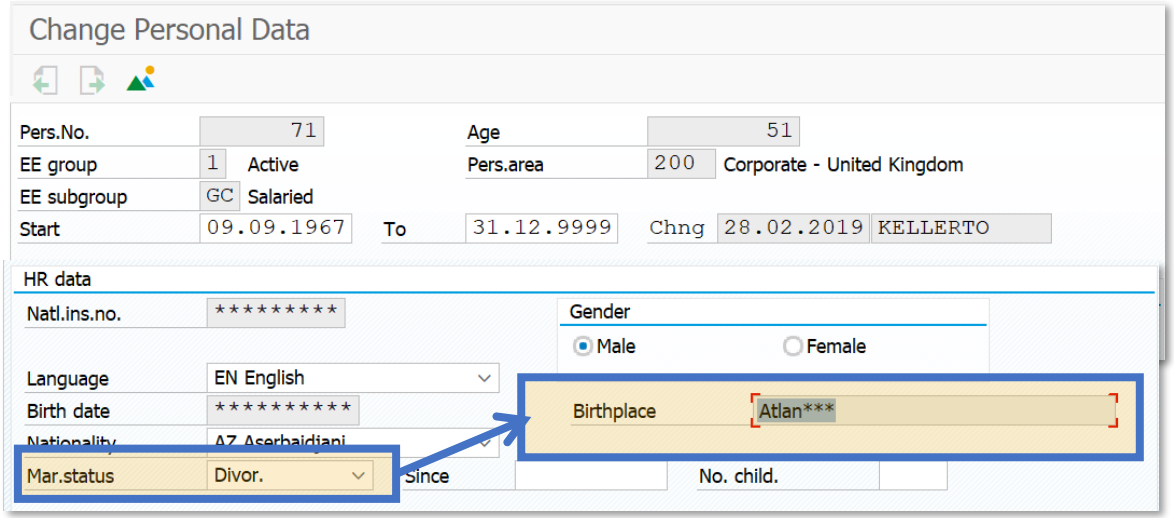

© 2020 ASUG Confidential

# Attribute based masking



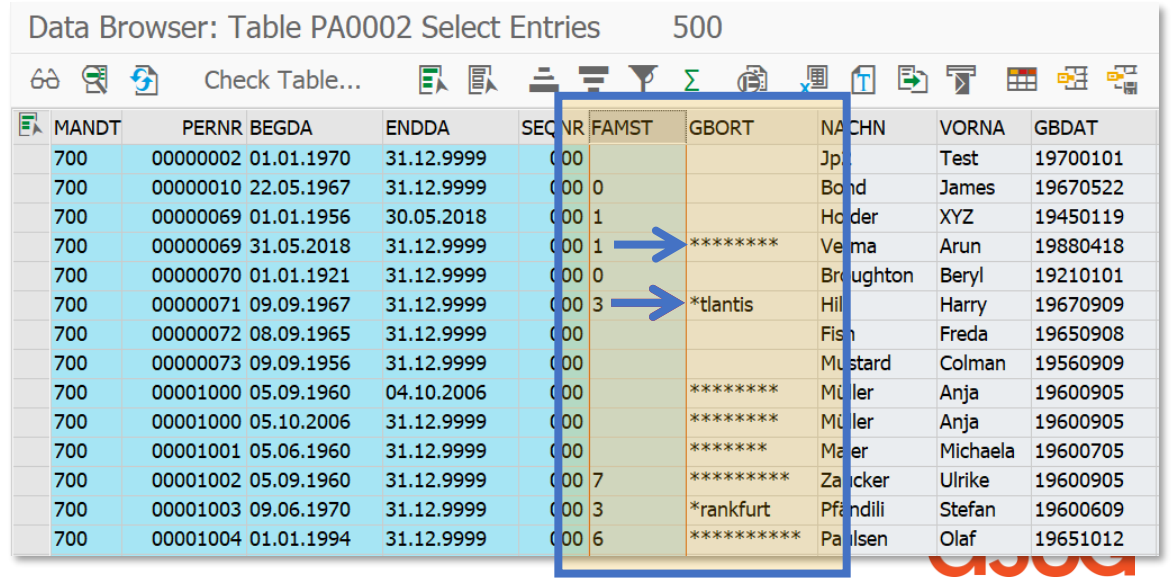
# UI Masking
## Example: Attribute based



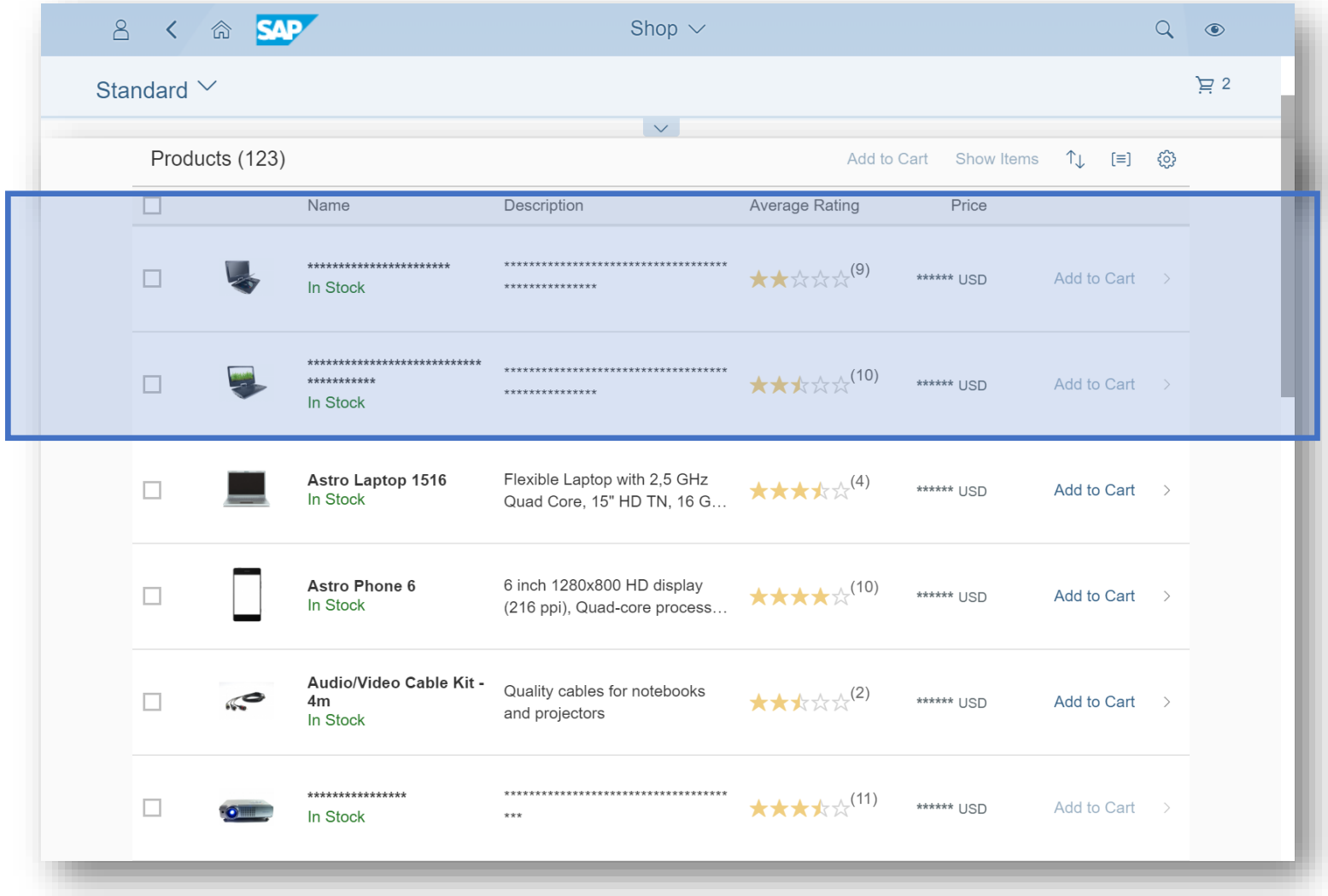

The state of the attribute “marital status” (“family status” determines whether and how the place of birth value is treated.

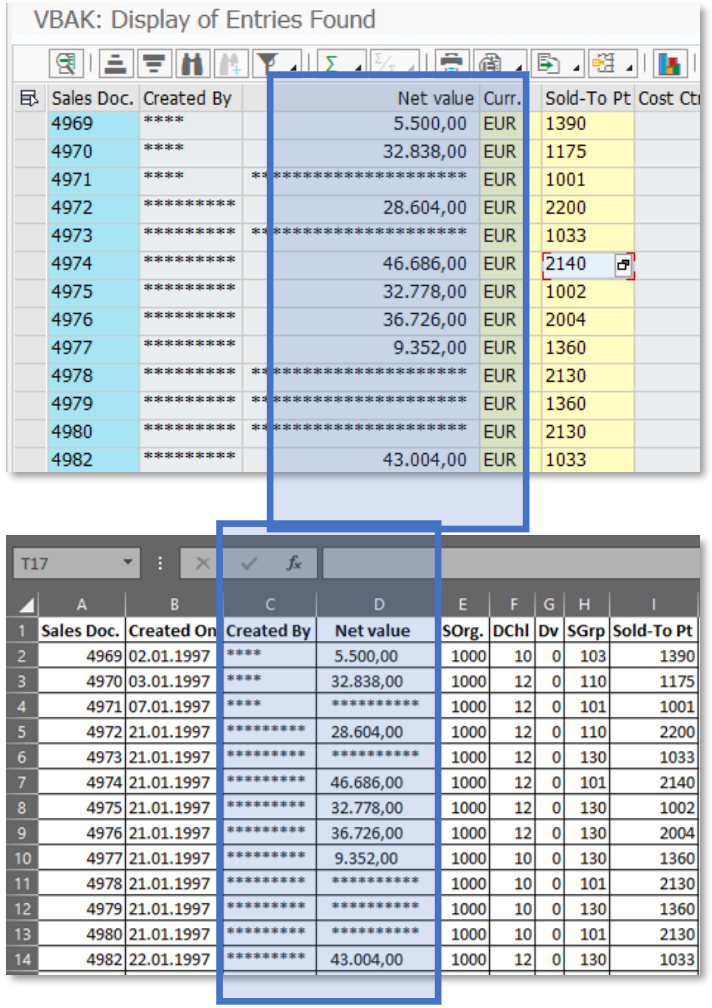
The logic is configured in “policies”, which are highly versatile and enable more differentiated treatment of field values based on additional attributes – pertaining to the user (e.g. HR employee associated to the company code), the data object ((e.g. employee older than 65 years), or other system-borne as well as external variables.




 © 2020 ASUG Confidential

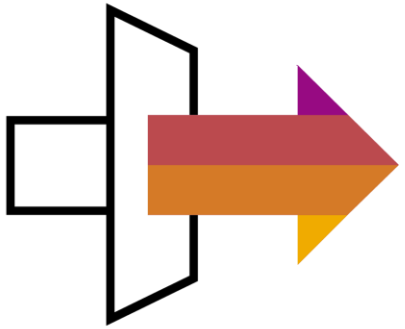
# UI Masking
## Example: Attribute based




 © 2020 ASUG Confidential

# Reveal on Demand



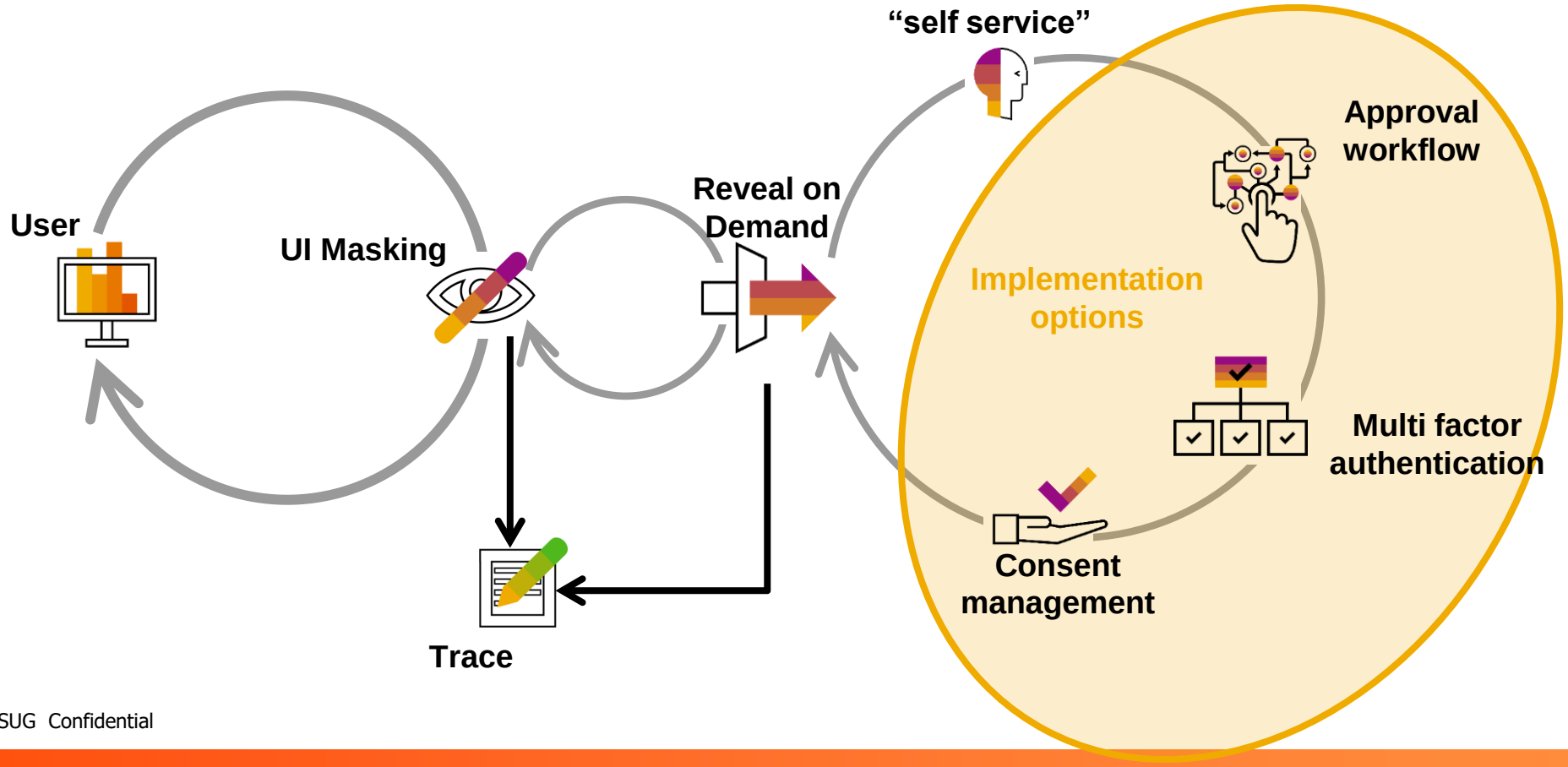
# UI Masking: “Reveal on Demand”

UI Masking introduces an intercept point for a user’s access to data based on a determination of authorization.

“Reveal on Demand” constitutes a second intercept, refining and basing authorization on additional conditions.

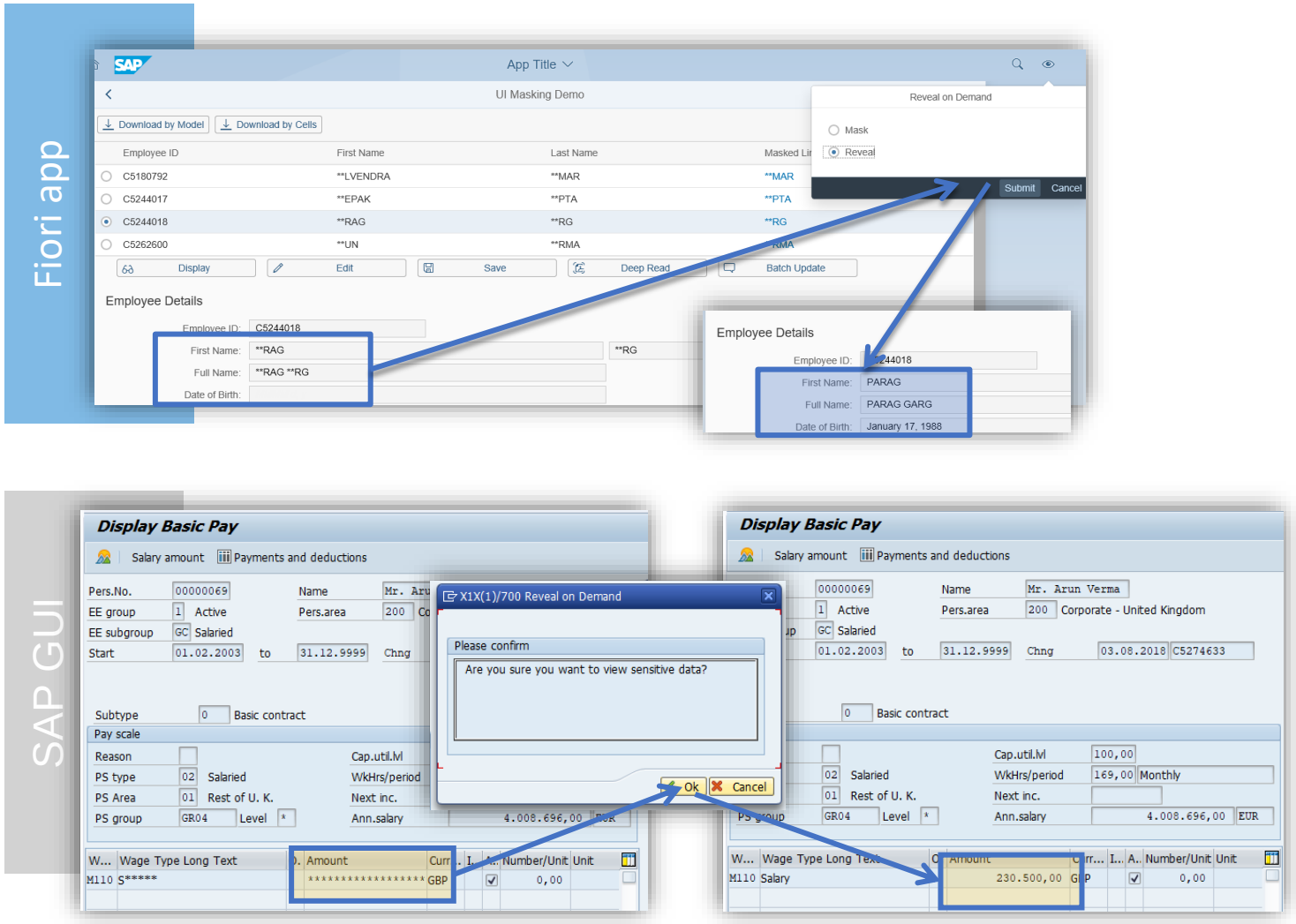
In an RoD scenario, data are always protected initially. A user action triggers an additional determination of authorization including a bespoke trace of the event and result.

RoD authorization could be based e.g. on approval, additional authentication or, in a case the data subject of PII has given her consent for her data to be used under the given conditions.



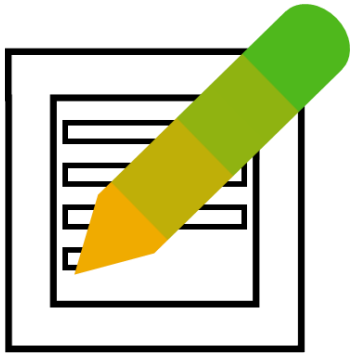

 © 2020 ASUG Confidential

# UI Masking: “Reveal on Demand”




 © 2020 ASUG Confidential

# UI Logging



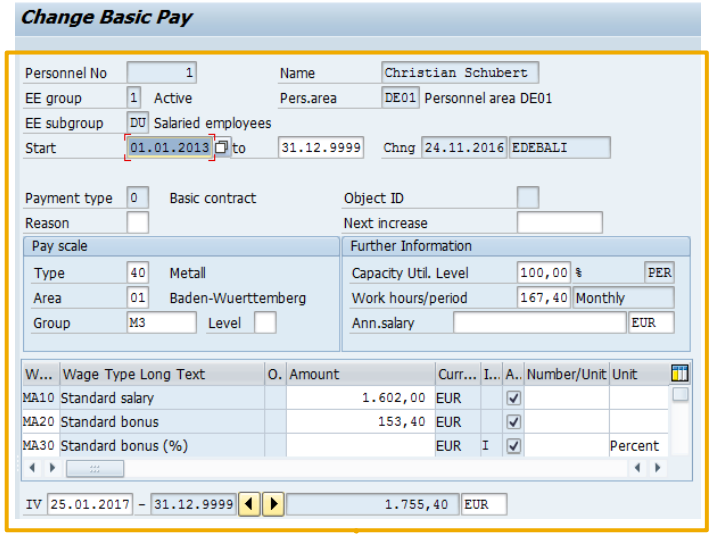
# UI Logging: configurable logging of data access in SAP UIs

- configurable scope of data to be protected on transaction/application/service level
- configurable list of users subjected to logging
- configurable alerts on specific (critical) data accesses
- configurable log reasons and retention time
- Log Analyser UI for researching the log file
- Integration with SAP Enterprise Threat Detection

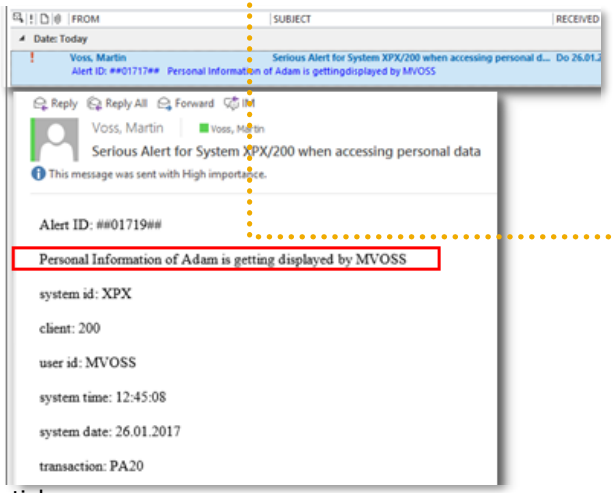
 © 2020 ASUG Confidential

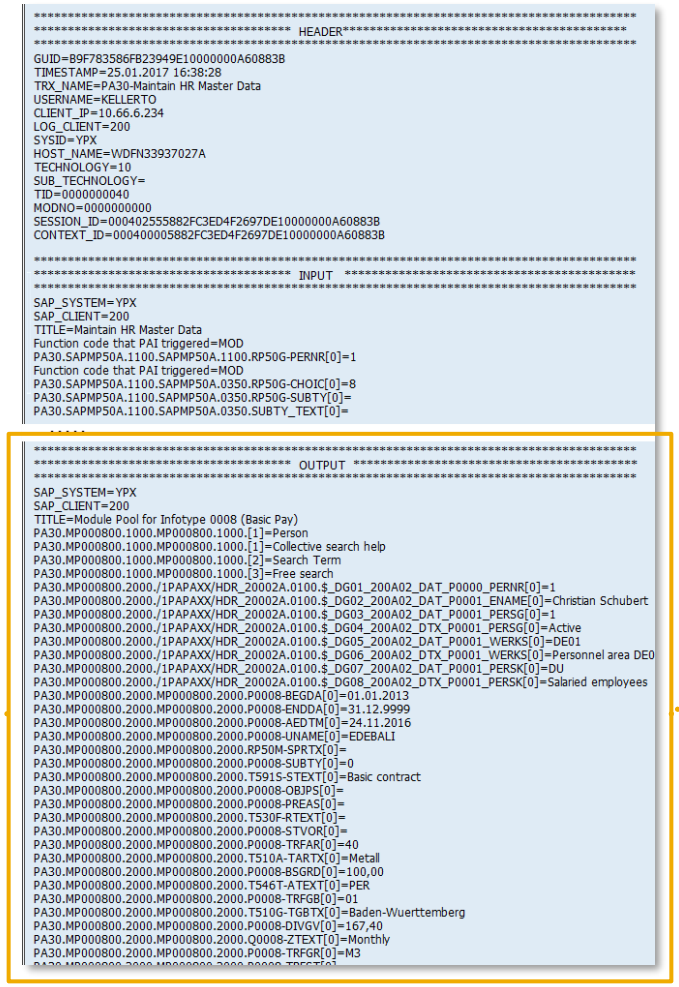
# UI Logging: Log access, get notified, take action

## 1. Log data access



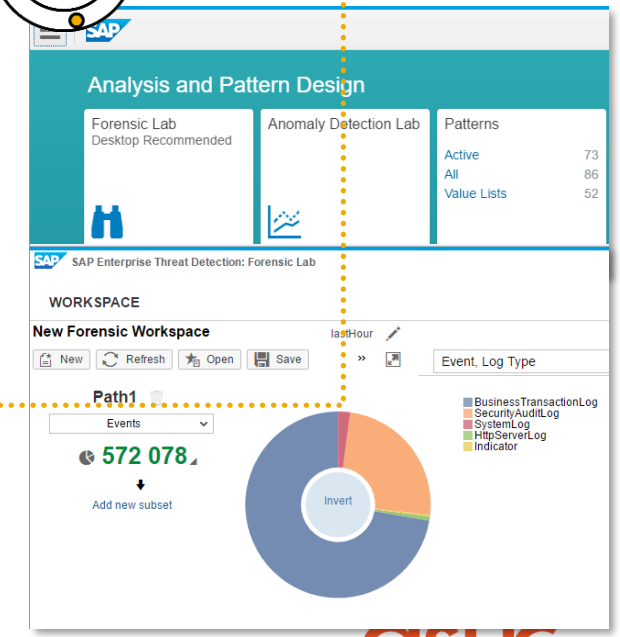

## 2. Automatic alert



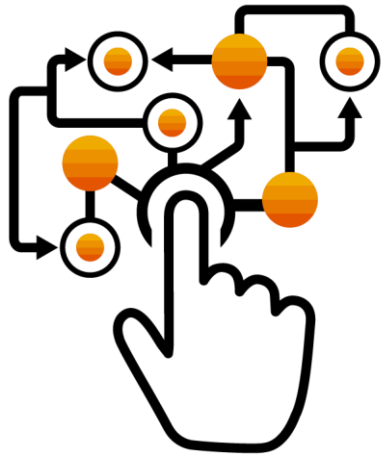

## 3. in-depth analysis

## 4. Aggregate & detect (SAP ETD)



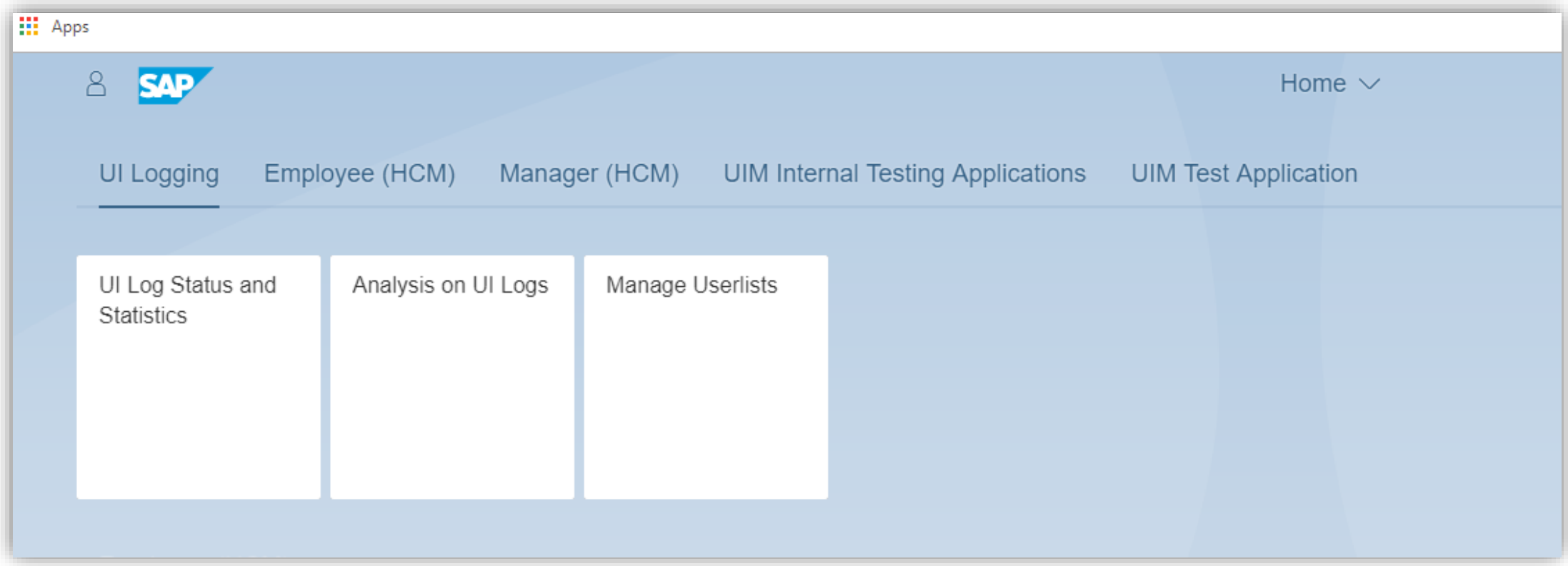

 © 2020 ASUG Confidential

# UI Logging
# Analysis Apps Screen View



# UI Logging: Fiori Applications for the DPO (Data Protection Officer)

“Security personnel” (e.g., security office, data protection officer running UI Logging and working on its logs) leverage Fiori apps for keeping an overview, conducting deep dive analysis into data usage, and managing lists of users whose data access they have identified as noteworthy.

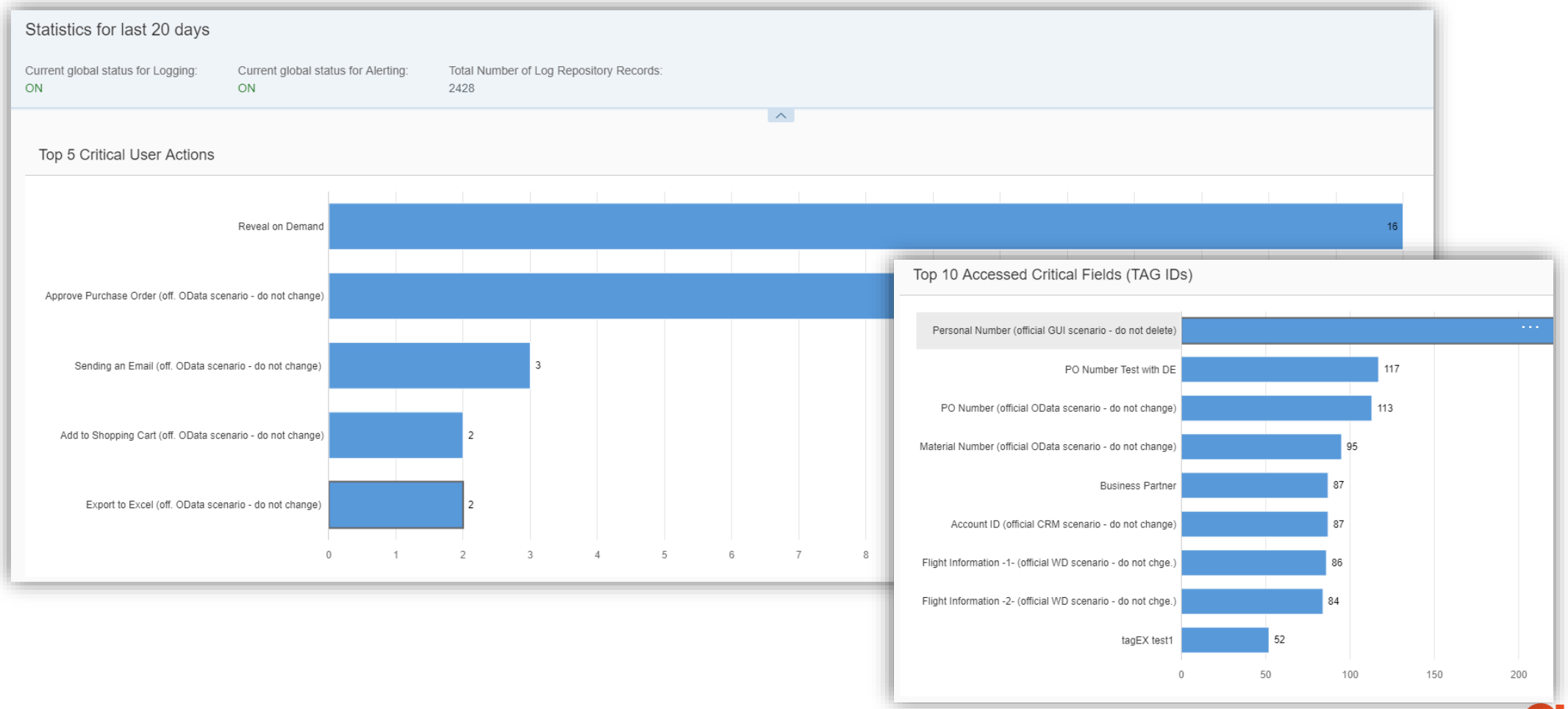




© 2020 ASUG Confidential

# UI Logging: Fiori Applications for the DPO (Data Protection Officer)

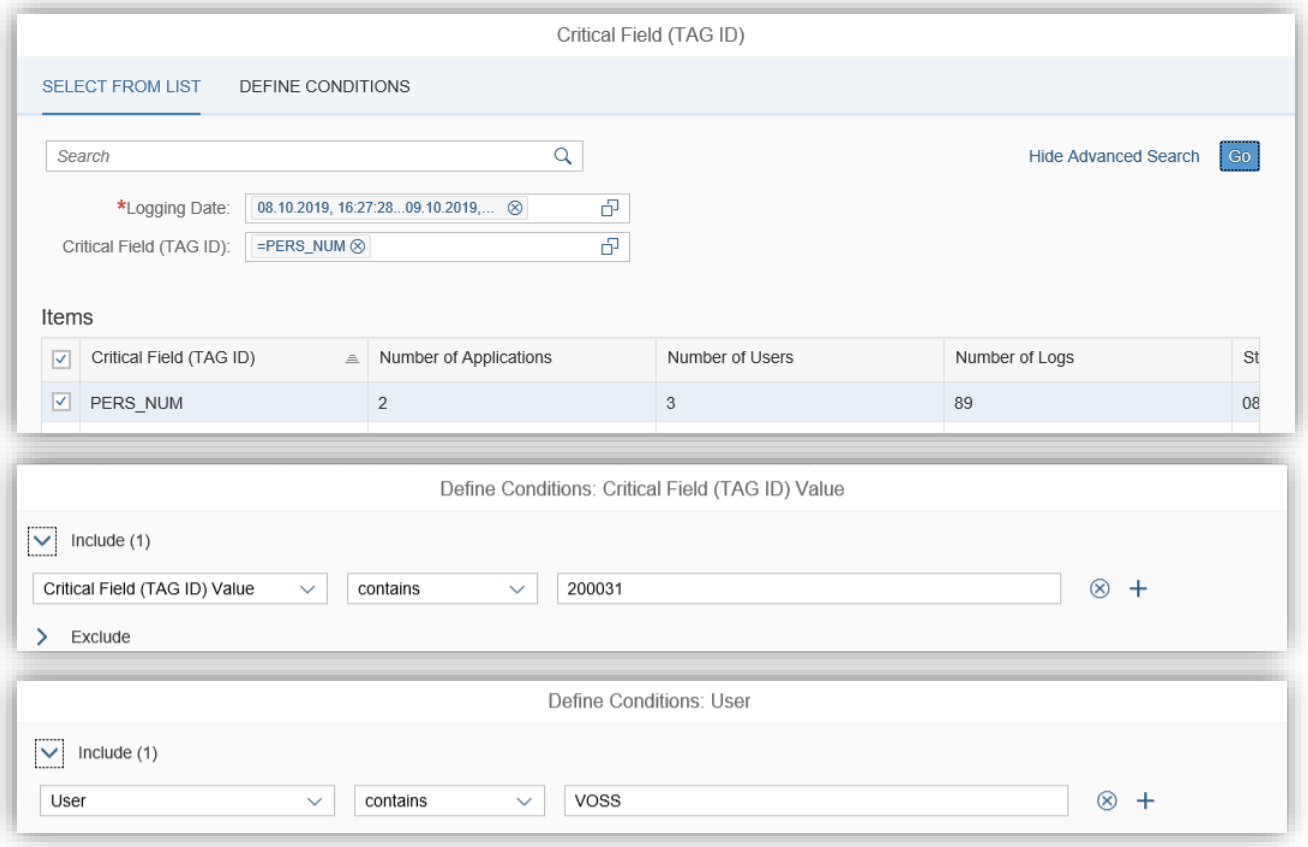
Security personnel can get an overview of system status as well as statistics concerning data usage (top n logged users, top n accessed critical data fields (data types), top n triggered actions, and more)




 © 2020 ASUG Confidential

# UI Logging: Fiori Applications for the DPO (Data Protection Officer)
## Analysis of UI Logs

Security personnel can conduct exploratory analysis of access to data types.
They gain a comprehensive view on data usage as multiple screen fields of the same type (e.g., social security number) can be aggregated or grouped by “tags”. Filter criteria allow for a more granular display of accessed data objects, and accessing users.



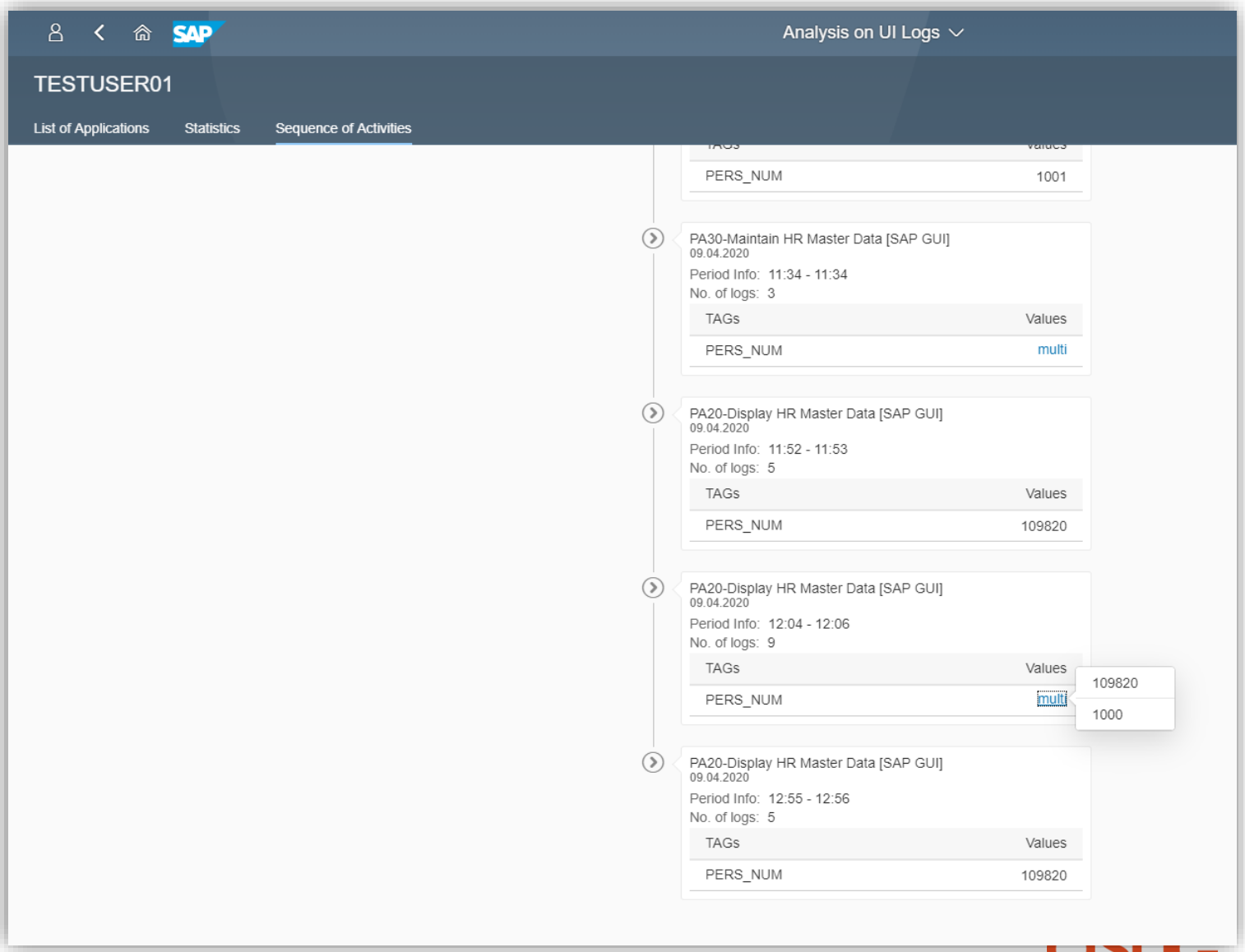

 © 2020 ASUG Confidential

# UI Logging: Fiori Applications for the DPO (Data Protection Officer)

## Analysis of UI Logs

Security personnel can analyze deeper into access and behavior of specific users, through a list of applications in which they accessed critical objects, and more in detail also into the sequence of activities.

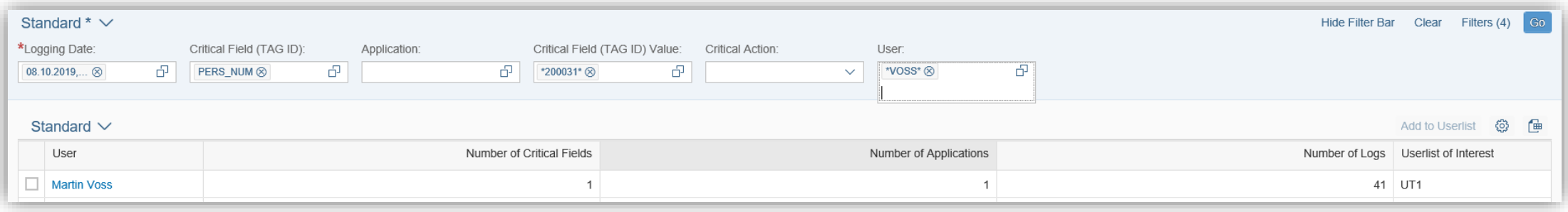
For deeper research on more detailed level,  jump points are provided into SAP GUI analysis applications.

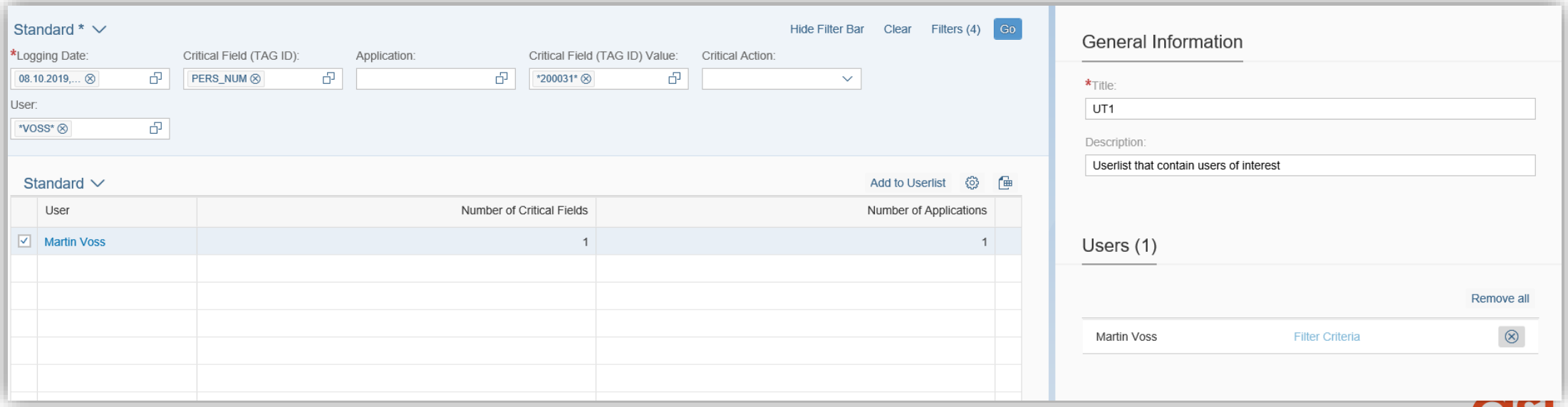



 © 2020 ASUG Confidential

# UI Logging: Fiori Applications for the DPO (Data Protection Officer)
## Analysis of UI Logs

Security personnel can identify users whose data access and actions are worth noting, and can add them to a list of “users of interest” which can be edited until it is “published” (for handing over to other departments who may take additional steps).

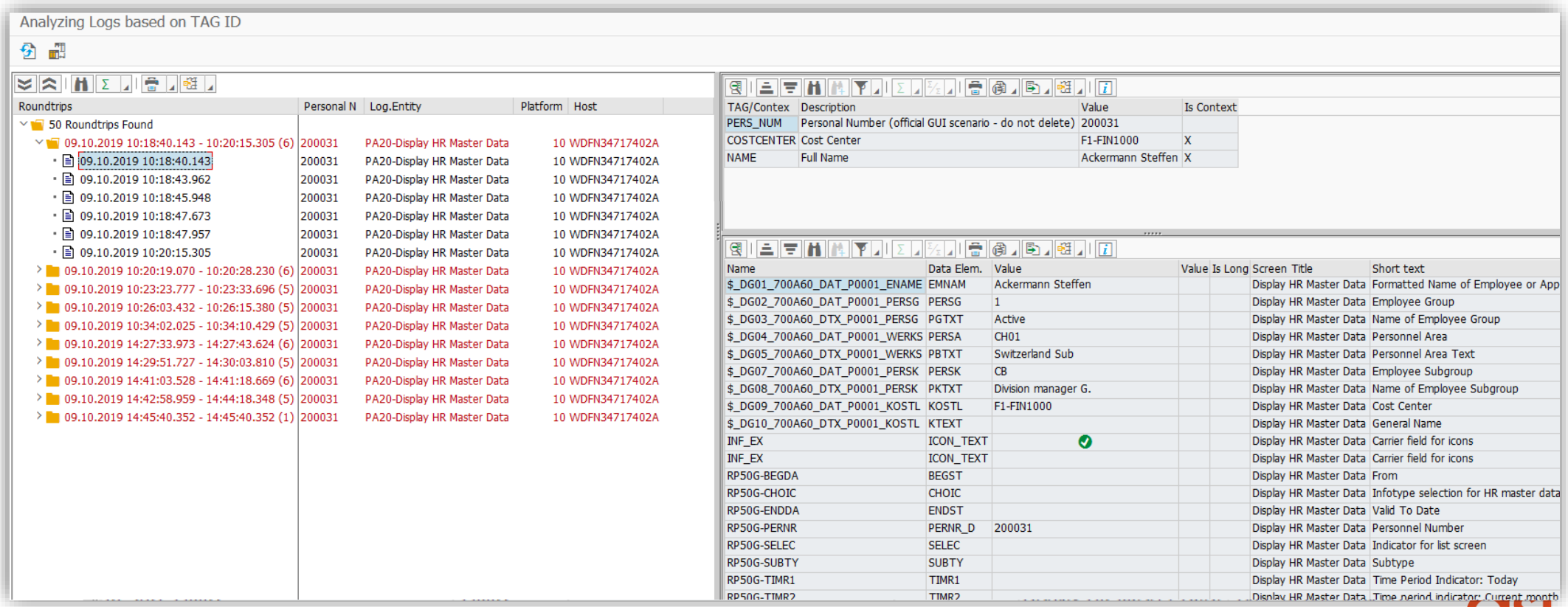



 © 2020 ASUG Confidential

# UI Logging
## Classic Analysis: TagAnalyzing

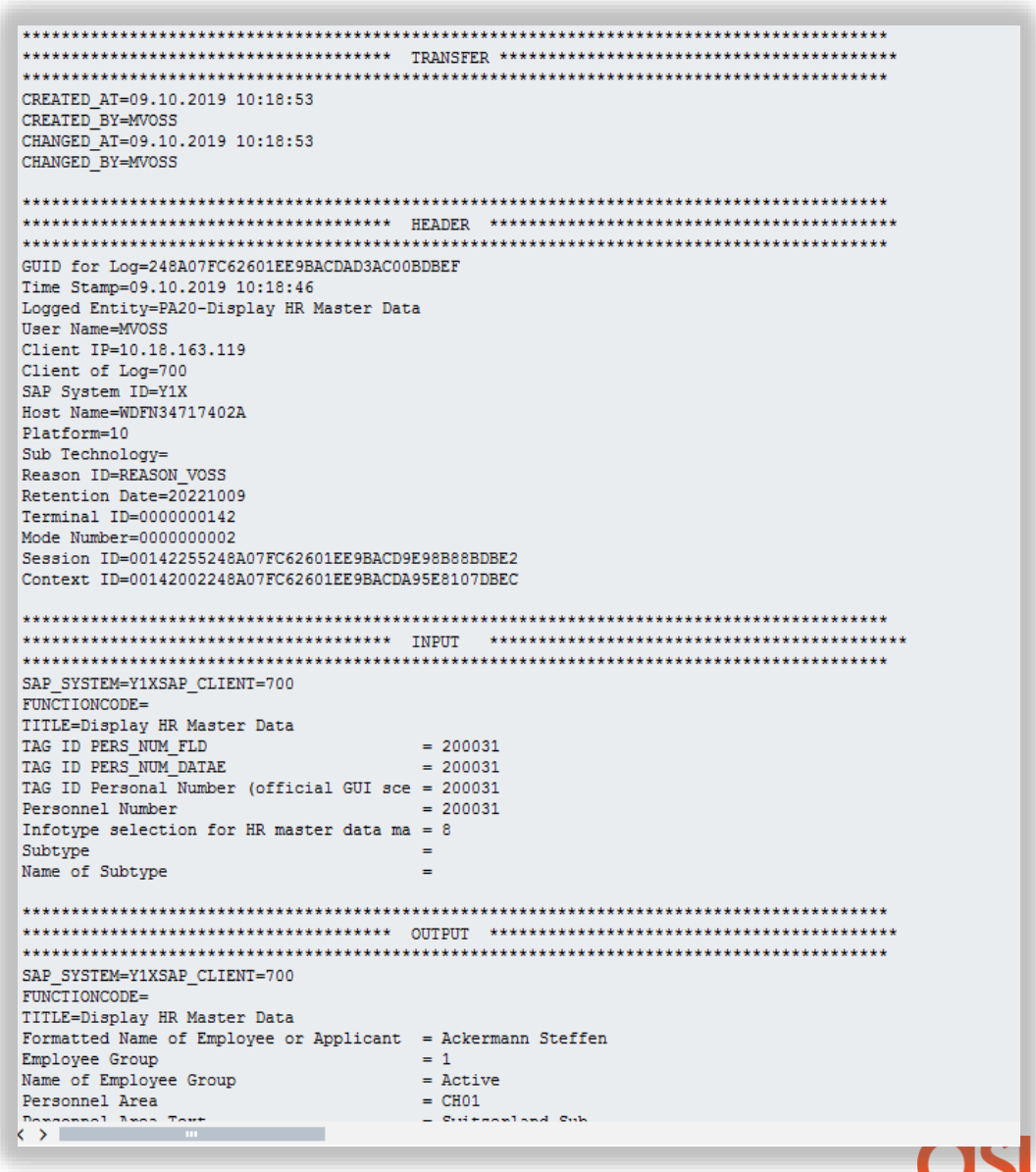
In addition to the Fiori based analysis apps, analysis can be conducted through the classical tools if desired. Relevant roundtrips are grouped by user sessions (Extended Passport). Per roundtrip, the relevant log data is displayed in the bottom left section, and additional data fields that may be assigned to tags are specified in the top right section. Technical field names are enhanced by more telling labels where available.




 © 2020 ASUG Confidential

# UI Logging
## Classic Analysis: LogAnalyzing

On roundtrip basis, a report can be accessed that renders logged data in a more readable way, with non-technical labels where available.



```
********************************************************************************************
************************************  TRANSFER ************************************************
********************************************************************************************
CREATED_AT=09.10.2019 10:18:53
CREATED_BY=MVOSS
CHANGED_AT=09.10.2019 10:18:53
CHANGED_BY=MVOSS

********************************************************************************************
************************************  HEADER  ************************************************
********************************************************************************************
GUID for Log=248A07FC62601EE9BACDAD3AC00BDBEF
Time Stamp=09.10.2019 10:18:46
Logged Entity=PA20-Display HR Master Data
User Name=MVOSS
Client IP=10.18.163.119
Client of Log=700
SAP System ID=Y1X
Host Name=WDFN34717402A
Platform=10
Sub Technology=
Reason ID=REASON_VOSS
Retention Date=20221009
Terminal ID=0000000142
Mode Number=0000000002
Session ID=00142255248A07FC62601EE9BACD9E98B88BDBE2
Context ID=00142002248A07FC62601EE9BACDA95E8107DBEC

********************************************************************************************
************************************  INPUT   ************************************************
********************************************************************************************
SAP_SYSTEM=Y1XSAP_CLIENT=700
FUNCTIONCODE=
TITLE=Display HR Master Data
TAG ID PERS_NUM_FLD                     = 200031
TAG ID PERS_NUM_DATAE                   = 200031
TAG ID Personal Number (official GUI sce = 200031
Personnel Number                        = 200031
Infotype selection for HR master data ma = 8
Subtype                                 =
Name of Subtype                         =

********************************************************************************************
************************************  OUTPUT  ************************************************
********************************************************************************************
SAP_SYSTEM=Y1XSAP_CLIENT=700
FUNCTIONCODE=
TITLE=Display HR Master Data
Formatted Name of Employee or Applicant  = Ackermann Steffen
Employee Group                           = 1
Name of Employee Group                   = Active
Personnel Area                           = CH01
```

 © 2020 ASUG Confidential

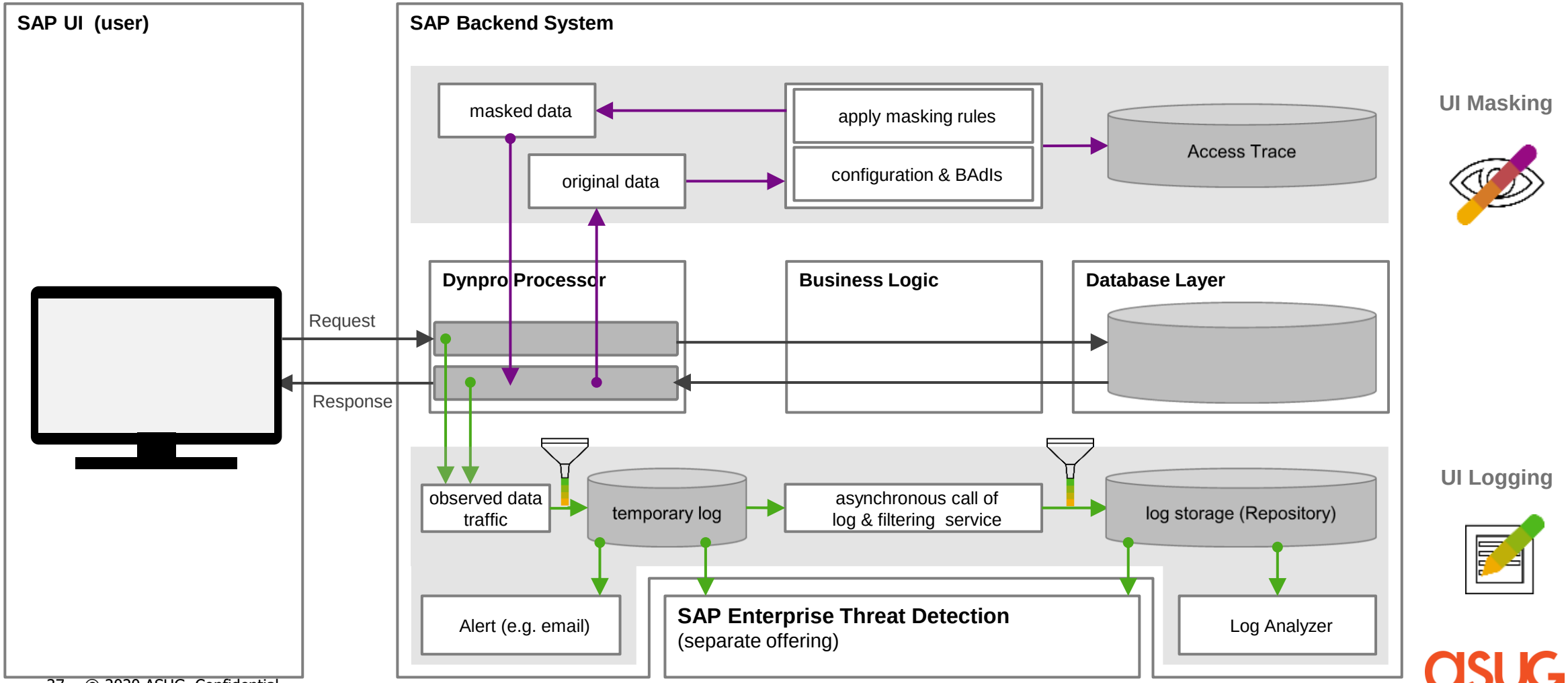
# Agenda

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| **What** | **When** | **Where** | **Next Steps** |
| Solution overview | Use cases | Architecture and availability | |

 © 2020 ASUG Confidential

# High level solution architecture

- UI Masking and UI Logging can be **used individually or jointly**, depending on the required functionality
- add-ons to SAP NetWeaver – **modification free** installation, **secure** server-based functionality with **minimal performance impact**




 © 2020 ASUG Confidential

# Coverage is based on UI technologies

| UI technology | UI Masking  | UI Logging  |
|---|---|---|
| SAP GUI for Windows / HTML / Java | ✓ | ✓ |
| WebDynpro ABAP | ✓ | ✓ |
| CRM Web Client UI | ✓ | ✓ |
| RFC/BAPI and Web Services | project based | ✓ |
| BW Access (BEx Web/Analyser, BW-IP, BICS, MDX) | project based | ✓ |
| UI5/Fiori | ✓ | ✓ |

- **Available for ECC, HEC, Suite on HANA, S/4HANA**
- **Enhancements and adaptations** can be delivered on request


© 2020 ASUG Confidential

# UI Masking: Classic vs. S/4HANA offering

| | "classic" UI Masking solutions | S/4HANA "UI data protection masking" |
|---|---|---|
| **Where to use** | ECC, classic CRM scenarios, HEC, (S/4HANA as „compatible" solutions, potential limitations) | S/4HANA |
| **How to get** | Separate installations per required UI technology | **Unified** technical installation |
| **Configuration** | Separate configurations per required UI technology | **Unified** config, automated with **data elements**; **consistent** application of protective actions over all supported UI technologies. |
| **Protective actions** | Masking of values in fields | Masking of values in fields<br>**emptying/hiding/disabling** fields/links<br>**suppression of lines** in table displays<br>**data blocking** |
| **Authorization paradigm** | Role based; attribute/rule based authorizations through BAdI implementation | Role based<br>**Policy based (attributes and rules)** |
| **Additional features** | | **Reveal on Demand (2-step authorization)** |


© 2020 ASUG Confidential

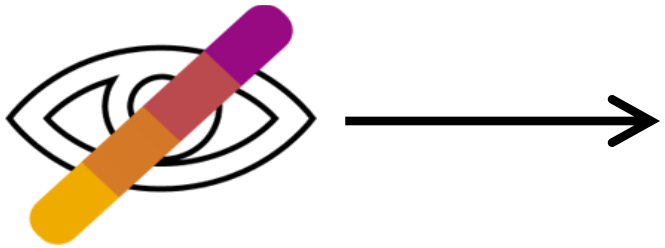
# Agenda

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| **What** | **When** | **Where** | **Next Steps** |
| Solution overview | Use cases | Architecture and availability | |

 © 2020 ASUG Confidential

# Reality and Vision: Protecting the Intelligent Enterprise: A Data Protection "Suite"

**1) mask/obfuscate what *can* be masked: with**
**UI Masking**



**2) Log what *can NOT* be masked: with**
**UI Logging**

**3) Automatically correlate and analyze the log with**
**Enterprise Threat Detection**


© 2020 ASUG Confidential

# SAP Enterprise Threat Detection

## Refine algorithms to better detect threats

Analyze and correlate logs

High-volume processing of security events

Evaluate attack detection patterns

Perform forensic investigations and discover new patterns

**Leverage machine learning to refine anomaly detection methods such as statistical methods, one-time behavior, and potential malicious sites**

Keep systems secure in a continuously changing cybersecurity threat environment

Leverage powerful and flexible monitoring, detection, and response capabilities

Receive actionable alerts in time to neutralize threats to your business-critical asset

Help prevent damage to your business and reputation


© 2020 ASUG Confidential

# Summary

## Where do we go from here?

 © 2020 ASUG Confidential

# Upcoming ASUG webinars
## Solution deep dives

**First Half Webinars**

- March 24: What You Need to Know About SAP's Offerings for Data Protection and Privacy (recording available)
- April 14: Solution highlight: SAP Privacy Management by BigID (recording available)
- April 28: Solution highlight: SAP Privacy Governance (recording available)
- May 19: Solution highlight: User interface logging and field masking solutions by SAP
- June 2: Solution highlight: SAP Enterprise Threat Detection

**Second Half Webinars – dates to be confirmed**

- Cloud Security Considerations
- Managing the identity lifecycle in hybrid landscapes
- Solution highlight: SAP Cloud Identity Access Governance
- Solution Highlight: Authentication scenarios
- Solution Highlight: Authorization scenarios
- Solution highlight: SAP Data Custodian

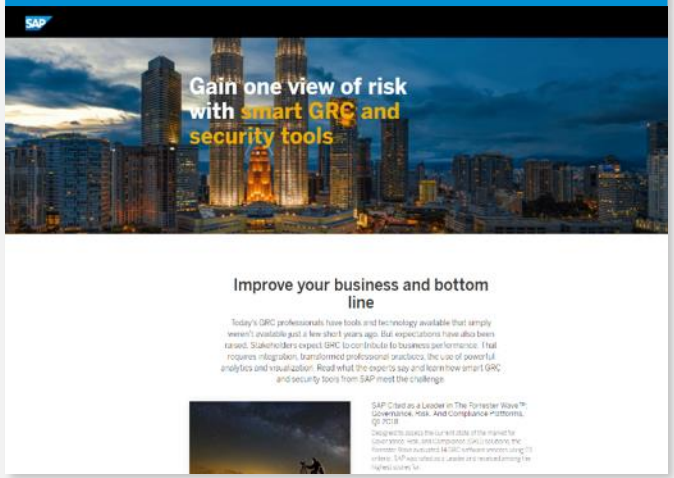

© 2020 ASUG Confidential

# More information for SAP GRC and Security solutions

Select the area of interest below

## SAP solutions for GRC & Security


## Practical Tools and Approach




## SAP Cloud Trust Center


**News Release:** SAP Receives Global Certification of Data Protection and Privacy from British Standards Institution (BSI)


© 2020 ASUG Confidential

# Questions?

For questions after this session, contact us at:

Erin Hughes
Cybersecurity Solution Advisor
Erin.Hughes@sap.com

 © 2020 ASUG Confidential

# Thank you.

Stay connected. Share your SAP experiences anytime, anywhere.
Join the ASUG conversation on social media: **@ASUG365 #ASUG**

 © 2020 ASUG Confidential