



Addressing 5 Critical GDPR Data Protection Requirements

EU GDPR

Are you prepared?

Agenda



GDPR Explained

Key GDPR Requirements

Addressing 5 Critical GDPR Requirements

- Data Protection Impact Assessment
- Purpose Limitation
- Data Protection
- Incident Response
- Breach Notification

GDPR Explained

“GDPR is a complex set of regulations specifying how organizations must protect EU citizens’ personal data. Here are six fundamental principles of the GDPR.”



Expands and standardizes data protection rules across entire European Union

Gives EU citizens “ownership” of their personal data

Broadly defines personally identifiable information (PII)
“any data that can be used to identify a person”

Organizations must seek permission from citizens to use their personal data

GDPR Explained



EU citizens can withdraw right of an organization to use their personal data

EU citizens can monitor the use of their data, decide who can use it, and can demand its return to them

In summary: they have the right to be “forgotten”



Key GDPR Mandates

“GDPR is complex but the key mandates can be broken down to eight major points.”



1. Big Fines

GDPR compliance violations can be huge: 4% of global revenue or €20 million whichever is greater

2. Data Protection Officer Required

Organizations >250 employees must have Data Protection Officer who will be personally liable for data breaches

3. Strict Breach Notification

Organizations must notify authorities within 72 hours of a data breach



Key GDPR Mandates



4. Global Reach

Any organization anywhere in the world collecting EU citizen personal data must comply

5. Comprehensive Monitoring and Security Controls

Organizations must establish strict PII access monitoring, documentation, and security controls

6. On-Demand Demonstration of Data Security

Organizations must be able to demonstrate their data protection process at any time

Key GDPR Mandates



7. Data Protection Impact Assessment

Organizations must assess the scope, purpose, and sensitivity of data processed

8. Applies to Organization Affiliates

GDPR rules apply to a company's partners, vendors, subcontractors, and cloud providers who store or access PII

GDPR Compliance is Challenging



- GDPR compliance violations can be big
4% of revenue or €20 million whichever is greater
- GDPR requirements are complex
- Data environments are large, complex, and distributed
- PII is often stored in many applications and
databases across the enterprise



GDPR Data Protection and Compliance Solution



Monitor - Detailed audit/alerting of PII usage – “Who, What, Where, When and How”



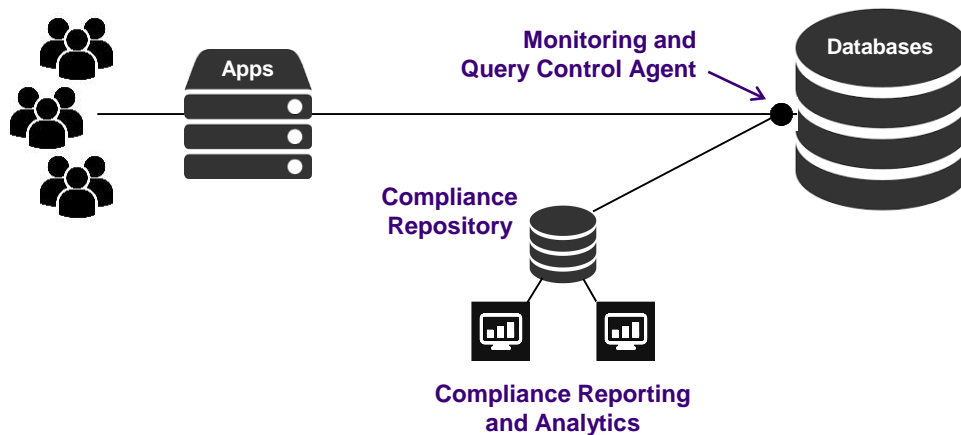
Report/Analyze - Out-of-the-box GDPR compliance reports and alerts. Analysis of users, organizational context, applications, PII access for audit and breach forensics



Protect - 70 granular access policies automatically mask or block inappropriate access to PII



GDPR Data Protection and Compliance Solution

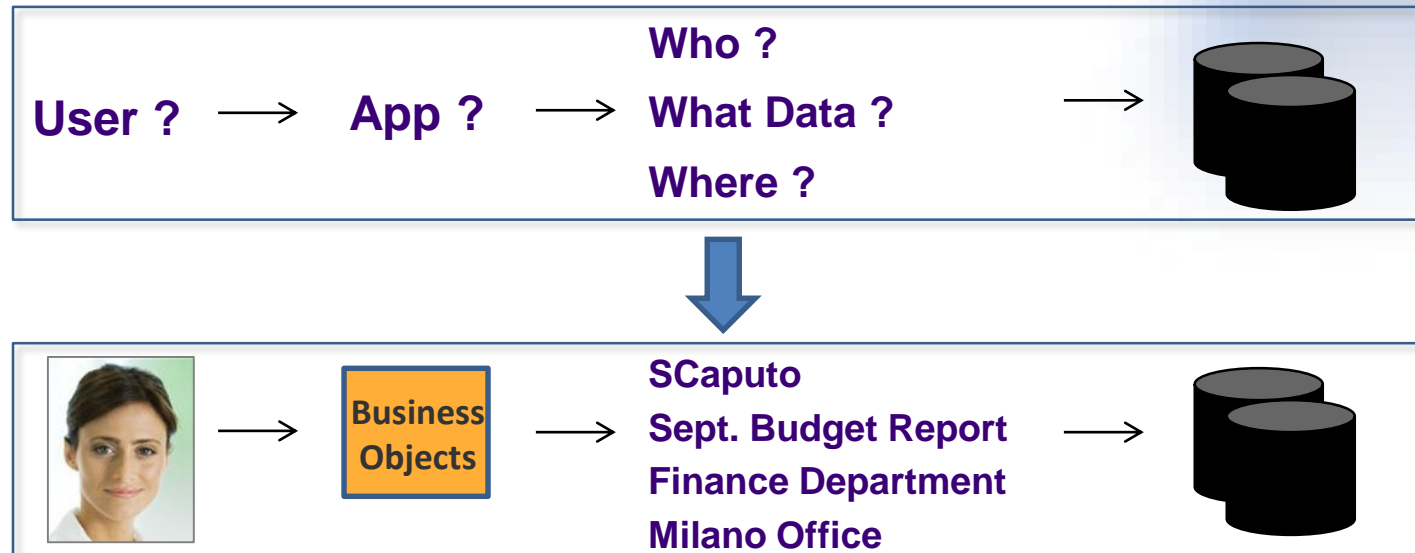


- Unobtrusive
- Comprehensive
- Quick to Install
- Low Admin Effort

GDPR Data Protection and Compliance Solution



Establishes “business context” for comprehensive, accurate compliance and effective protection





GDPR Data Protection and Compliance Solution



Addresses Five Critical GDPR Requirements



Impact
Assessment

(Article 35)



Purpose
Limitation

(Article 5-1b)



Data
Protection

(Article 5-1f)



Incident
Response

(Article 5-2)



Breach
Notification

(Articles 33/34)



GDPR Data Protection and Compliance Solution



GDPR Impact Assessment – organizations need to conduct audit of what is PII, how it is used, and by whom to confirm and attest they are GDPR-compliant

Teleran addresses by:

- Enabling a “GDPR Readiness Assessment” by discovering sensitive PII and auditing/documenting who is accessing PII, with which application, and for what purpose
- Applying appropriate data masking and access control policies to protect PII, ensure compliance



GDPR Data Protection and Compliance Solution



GDPR Data Protection Impact Assessment

GDPR Readiness Dashboard											
Exception Analysis		Exception SQL Analysis					Filters	Statistics			
Overall Assessment											
Large Volume Transaction	DML/DDL	DB Errors	Multiple IPs	Data Pattern Change	Transaction Pattern Change	SELECT *	Sub-SELECT	Query Complexity	Distinct SQL	Total Executes	
●	●	●	●	●	●	●	●	●	483	2,435	
Overall Assessment											
Large Volume Transactions	DML/DDL	DB Errors	Multiple IPs	Data Pattern Change	Transaction Pattern Change	SELECT *	Sub-SELECT	Query Complexity	Application exe	Total Executes	
2.7%	13.3%	25.5%	4.8%	72.5%	13.0%	13.0%	5.8%	7.5%	SQLPLUS.EXE	667	
Negative Issue Activity											
Application exe	Large Volume Transactions	DML/DLL	DB Errors	Multiple IPs	Data Pattern Change	Transaction Pattern...	SELECT *	Sub-SELECT	Query Complexity		
EXCEL.EXE	●	●	●	●	●	●	●	●	●		
JOBSERVERCHILD.EXE	●	●	●	●	●	●	●	●	●		
MSACCESS.EXE	●	●	●	●	●	●	●	●	●		
PDTM.EXE	●	●	●	●	●	●	●	●	●		
PERL.EXE	●	●	●	●	●	●	●	●	●		
PYTHON.EXE	●	●	●	●	●	●	●	●	●		
SQLDEVELOPER.EXE	●	●	●	●	●	●	●	●	●		
SQLPLUS.EXE	●	●	●	●	●	●	●	●	●		
									SQLPLUS.EXE	667	
									PDTM.EXE	324	
									SQLDEVELOPER.EXE	299	
									PERL.EXE	293	
									JOBSERVERCHILD.EXE	271	
									MSACCESS.EXE	240	
									EXCEL.EXE	199	
									PYTHON.EXE	142	



GDPR Data Protection and Compliance Solution



Purpose Limitation - personal data use must be limited to stated purpose and no other

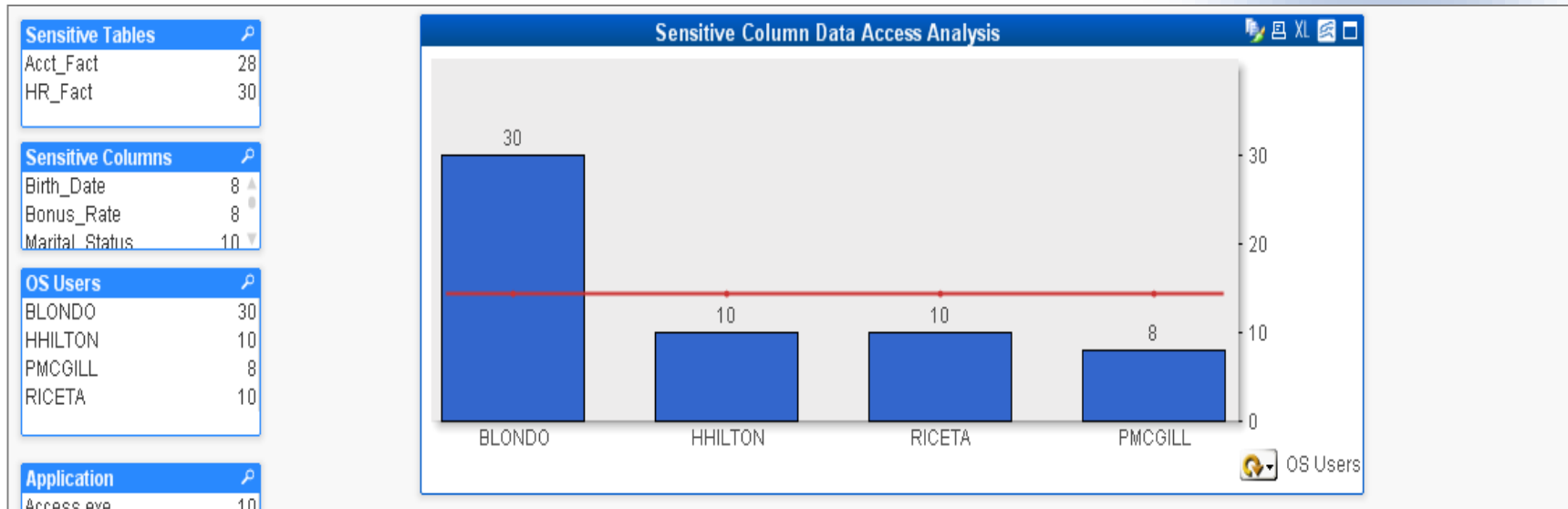
Teleran addresses by:

- Auditing PII access to ensure it is limited to stated use and no non-compliant access is occurring
- PII protection policies enforce purpose limitation by allowing only authorized users to access PII
- All other attempted access is prevented



GDPR Data Protection and Compliance Solution

GDPR Purpose Limitation Monitoring



Report showing sensitive column data access

GDPR Data Protection and Compliance Solution



Purpose Limitation PII Access Controls

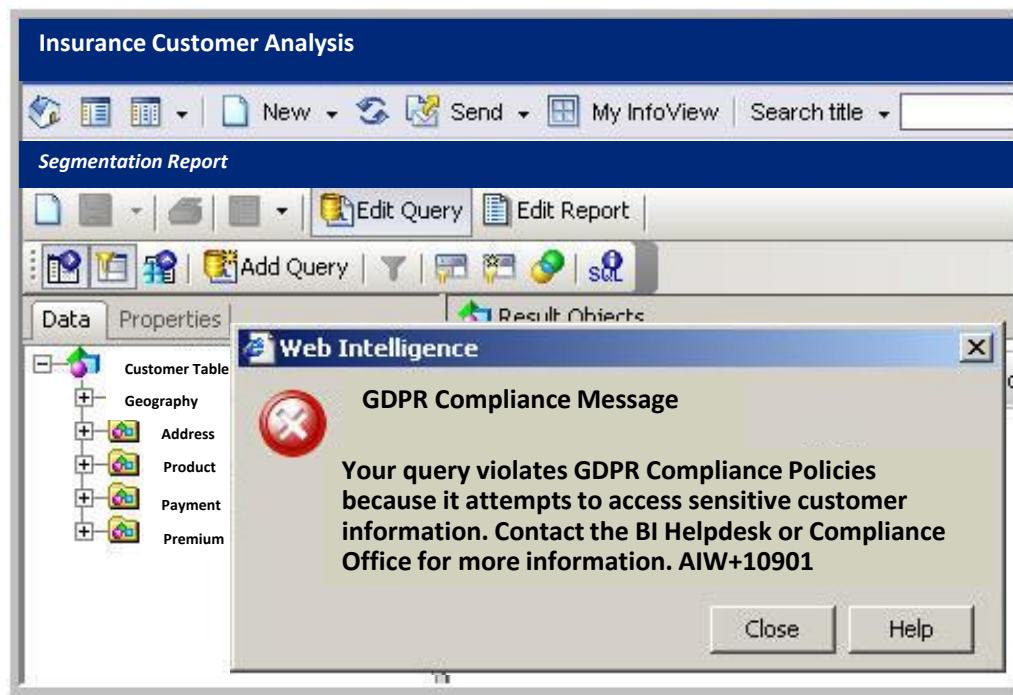
Policy Selector				
Variable Analysis		Category Analysis		Advanced Filters
Compliance and Security Policies yes 13 no 2		Application Restriction Column Access Restriction Column Combination Restriction Column Restriction DDL Restriction DML Restriction Row Level Restriction BETWEEN Range Limit	1 Column Filter Requirement 1 IN List Limit 1 Join Limit 2 Join Requirement 5 Join Restriction 9 Large Table Restriction 2 NOT IN Restriction Partition Access Requirement	Relational Operator Restriction SELECT Restriction Self-join Restriction Table Join Requirement Table Requirement WHERE Requirement z.not in use
Policy Groups and Descriptions				
Policy Name	Policy Description	Use Case(s)	User Message	Rule
Application Restriction	This policy prevents queries from executing on <TABLE> without a filtering condition unless the query is issued by <APPLICATION> by <USER> and <DATA SOURCE>.	Use this policy to prevent inefficient queries from access tools like MS Access in which users can easily launch queries with no conditions.	In order for your query to run faster, you must use a condition (a filter) against <TABLE>.	244
Column Restriction	This policy prevents queries on <TABLE> if the query contains <COLUMN>		Access to <TABLE><COLUMN> is not permitted. If	
	Data Masking	Datasource, Schema, Table, Column, Sensitive Category, Mask	Use this policy to mask sensitive columns.	
Column Combination Restriction	This policy prevents two <COLUMNS> that exist in separate tables from being in the same query by <DATA SOURCE> and <USER>. Note: Columns must exist in different tables. This policy not to be used with groups.	same query. (ex. Combining customer name and account number, or social security number with mother's maiden name)	Access to <TABLE><COLUMN> and <TABLE><COLUMN> is not permitted together. If you believe you should have access, please contact your administrator.	263
Column Restriction	This policy prevents queries on <TABLE> from containing a literal compare on <COLUMN> by <USER>.	Use this policy to prevent the use of a column as a filter or constraint. This can be used for a variety of reasons including: avoiding low cardinality columns that will deliver massive results sets or prevent access to data where filtering on this column may compromise data access rules.	Your query has been blocked because it contains a literal compare on <COLUMN>.	234



GDPR Data Protection and Compliance Solution



Purpose Limitation PII Access Control



Compliance Message to application user attempting to access sensitive data



GDPR Data Protection and Compliance Solution



Data Protection – personal data must be secure and remain unchanged. Security audits must be documented

Teleran addresses by:

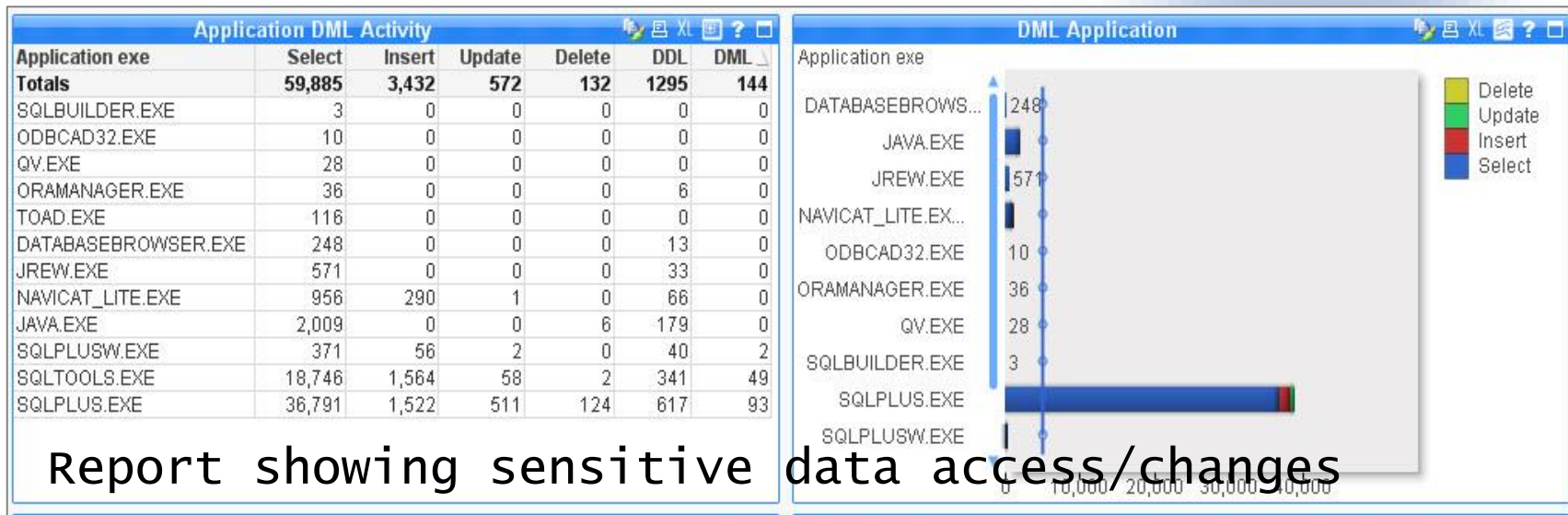
- Monitoring access to ensure personal data is unchanged or destroyed
- Audit reporting documents data security and integrity measures are in place
- Data protection policies prevent data manipulation or destruction of personal data



GDPR Data Protection and Compliance Solution



Data Integrity Reporting and Controls



Report showing sensitive data access/changes

DELETE Restriction	Prevents queries containing DELETE on <TABLE> or <COLUMN>.	Use this access policy to prevent deleting sensitive data.
---------------------------	-------------------------------------------------------------------------------	-------------------------------------------------------------------



GDPR Data Protection and Compliance Solution



Breach Identification / Notification – organizations need to put in place process to be aware of and notify authorities and citizens if and when a breach occurs

Teleran addresses by:

- Identifying and alerting staff to suspected or actual data breaches
- Documenting breach for purposes of notification and preventing further breach activity
- Applying additional data masking and access control policies to prevent future breaches



GDPR Data Protection and Compliance Solution



Suspicious Activity Alerting

---Security Alert---

From: Teleran [mailto:501458408@chicisapp429v.corporate.gr.com]

Sent: Saturday, July 23, 2019 3:22PM

To: rsimone@gr.com

Subject: GDPR Compliance Event Alert

Exception Activity: INSERT sensitive data to TEMP TABLE queries run 7/23/19 3:20 PM by User ID: DB Administrator.

Download event report pdf.

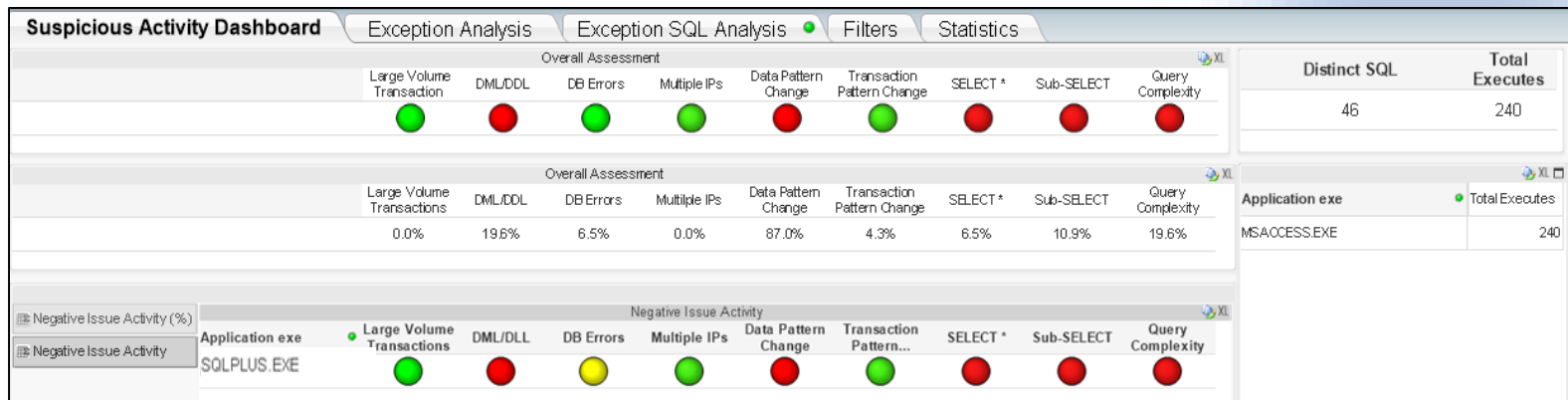




GDPR Data Protection and Compliance Solution



Data Breach Identification



Suspicious Activity Dashboard identifying the possible GDPR violation of accessing and moving sensitive data



GDPR Data Protection and Compliance Solution

Data Breach Forensic Audit Documentation

Suspicious Activity Dashboard		Exception Analysis		Exception SQL Analysis		Filters	Statistics
SQL Text							
SQLPLUS.EXE	130	INSERT INTO SH.CUSTOMERS_TEMP VALUES ('23258', 'Marshall', 'Kahn', 'M', '1943', 'married', '77 West Guthrie Avenue', '48346', 'Norma', '51985', 'FL', '52595', '52790', '417-634-7770', 'B: 30,000 - 49,999', '1500', 'Kahn@company.com', 'Customer total', '52772', nul...					
SQLPLUS.EXE	130	INSERT INTO SH.CUSTOMERS_TEMP VALUES ('23258', 'Marshall', 'Kahn', 'M', '1943', 'married', '77 West Guthrie Avenue', '48346', 'Norma', '51985', 'FL', '52595', '52790', '417-634-7770', 'B: 30,000 - 49,999', '1500', 'Kahn@company.com', 'Customer total', '52772', nul...					
SQLPLUS.EXE	131	INSERT INTO SH.CUSTOMERS_TEMP VALUES ('30411', 'Nolita', 'Banas', 'F', '1945', 'single', '87 South Luquillo Avenue', '72996', 'Scheveningen', '52296', 'Zuid-Holland', '52771', '52770', '299-767-6233', 'F: 110,000 - 129,999', '3000', 'Banas@company.com',					
SQLPLUS.EXE	131	INSERT INTO SH.CUSTOMERS_TEMP VALUES ('30411', 'Nolita', 'Banas',					
SQLPLUS.EXE	132	'F', '1945', 'single', '87 South Luquillo Avenue', '72996', 'Scheveningen',					
SQLPLUS.EXE	132	'52296', 'Zuid-Holland', '52771', '52770', '299-767-6233', 'F: 110,000 -					
SQLPLUS.EXE	0	129,999', '3000', 'Banas@company.com', 'Customer total', '52772', null,					
SQLPLUS.EXE	0	TO_DATE('1998-01-01 00:00:00', 'YYYY-MM-DD HH24:MI:SS'), null, 'I)					
SQLPLUS.EXE	0	ALTER TABLE sh.customers_TEMP					
SQLPLUS.EXE	0	DISABLE constraint customers_country_TEMP_fk					

Documentation of compliance violation. Inappropriate access and movement of PII to temporary database table

Summary: Teleran Addresses 5 Critical GDPR Mandates

Impact Assessment (Article 35)	Purpose Limitation (Article 5-1 b)	Data Security & Integrity (Article 5-1 f)	Accountability & Documentation (Article 5-2)	Breach Notification (Articles 33/34)
Audit where PII exists, how used, by whom. Identify / remediate gaps	Confirm PII use limited to stated purpose and no other	Protect PII from unlawful use, manipulation, destruction or loss	Demonstrate and document compliance processes	Establish process to: Identify data breaches. Notify authorities / citizens of breach
Teleran Solution				
Discovers and classifies PII. Audits who accessing PII to identify / remediate compliance gaps	Monitoring documents adherence to purpose limits	Monitoring / controlling PII access and use to ensure protection	Audit reports demonstrate, document compliant PII access / control	Identifies and alerts to suspected or actual PII breaches
Automatically applies data masking access control policies to protect PII and ensure GDPR compliance	Data masking and access controls enforce limits, prevent inappropriate use/users/apps	Delivers masking sand access policies to prevent: illegal data use, data manipulation, destruction	PII masking and access control and testing processes prove protection measures and GDPR-compliancy	Documents breach activity for notification. Applies new masking and control policies to prevent future like breaches



GDPR Data Protection and Compliance Solution



- What is your GDPR compliance strategy?
- Schedule a Teleran GDPR Data Protection Readiness Assessment now to establish your GDPR roadmap

www.teleran.com

© 2020 Teleran Technologies, Inc. All rights reserved. The Teleran logo, iSight and iGuard are trademarks or registered trademarks of Teleran Technologies, Inc. Other brand and product names are the marks of their respective owners. SO02.26.20