Addressing 5 Critical GDPR Data Protection Requirements

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

teleran

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”

teleran

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

teleran

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

teleran

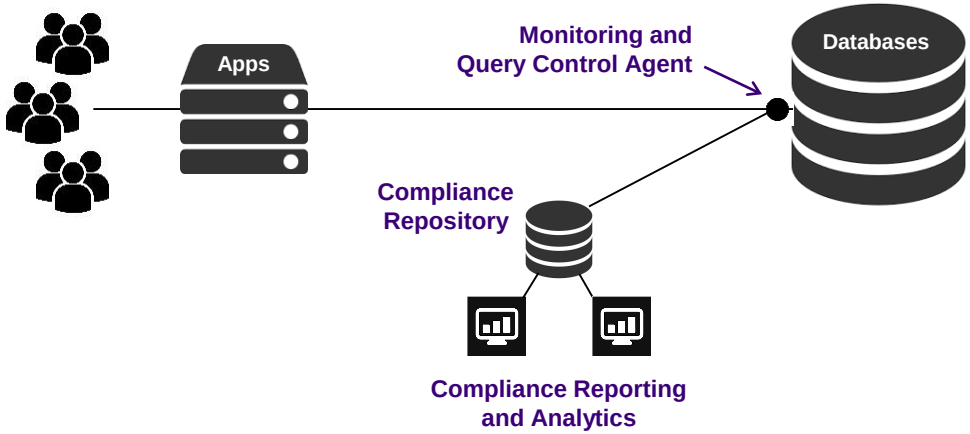
GDPR Data Protection and Compliance Solution

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

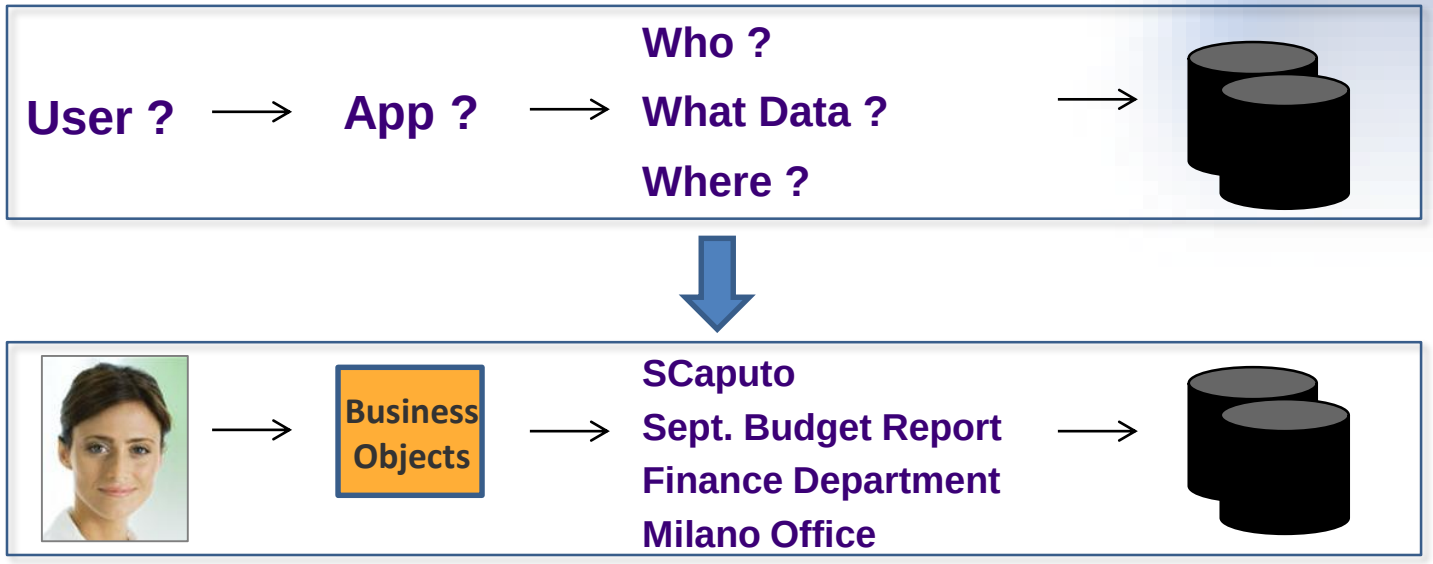
GDPR Data Protection and Compliance Solution



- 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 Data Protection and Compliance Solution

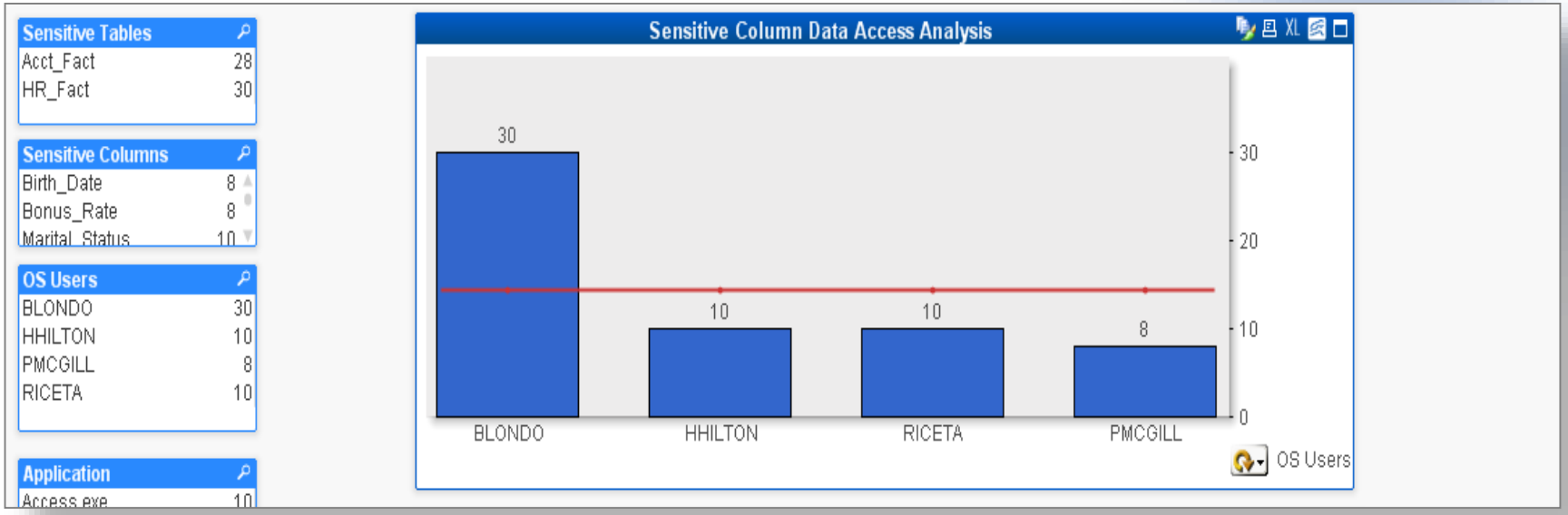
Purpose Limitation - personal data use must be limited to stated purpose and no other

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

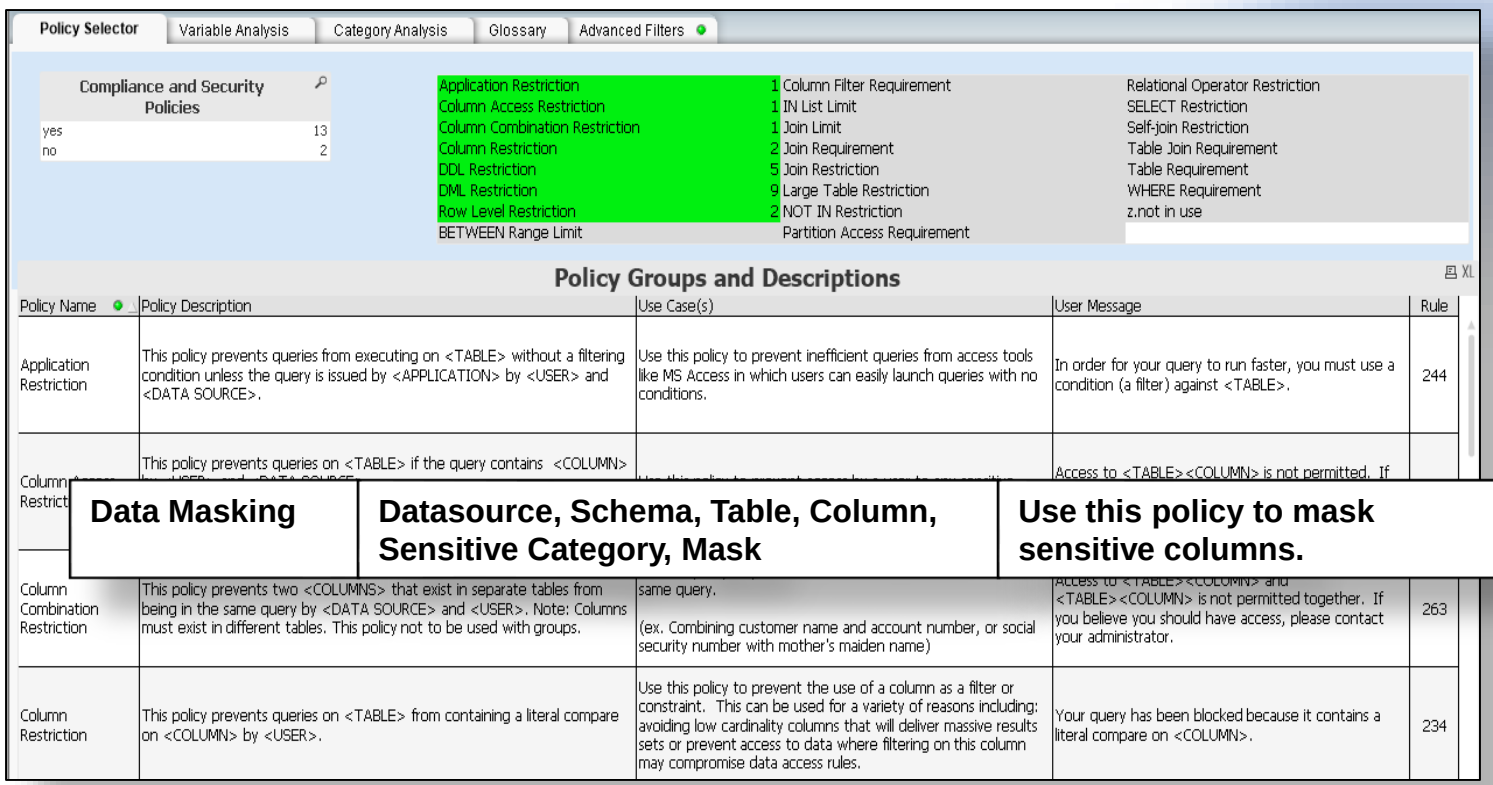
GDPR Purpose Limitation Monitoring



Report showing sensitive column data access

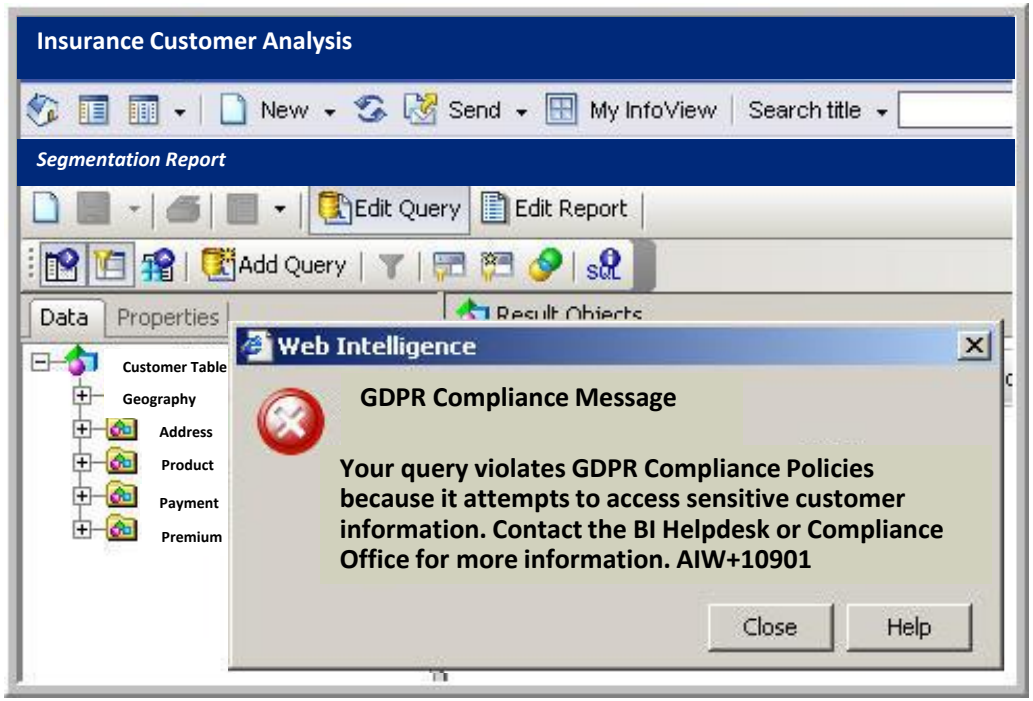
GDPR Data Protection and Compliance Solution

Purpose Limitation PII Access Controls



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

Application DML Activity

Application exe	Select	Insert	Update	Delete	DDL	DML
Totals	**59,885**	**3,432**	**572**	**132**	**1295**	**144**
SQLBUILDER.EXE	3	0	0	0	0	0
ODBCAD32.EXE	10	0	0	0	0	0
QV.EXE	28	0	0	0	0	0
ORAMANAGER.EXE	36	0	0	0	6	0
TOAD.EXE	116	0	0	0	0	0
DATABASEBROWSER.EXE	248	0	0	0	13	0
JREW.EXE	571	0	0	0	33	0
NAVICAT_LITE.EXE	956	290	1	0	66	0
JAVA.EXE	2,009	0	0	6	179	0
SQLPLUSW.EXE	371	56	2	0	40	2
SQLTOOLS.EXE	18,746	1,564	58	2	341	49
SQLPLUS.EXE	36,791	1,522	511	124	617	93

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

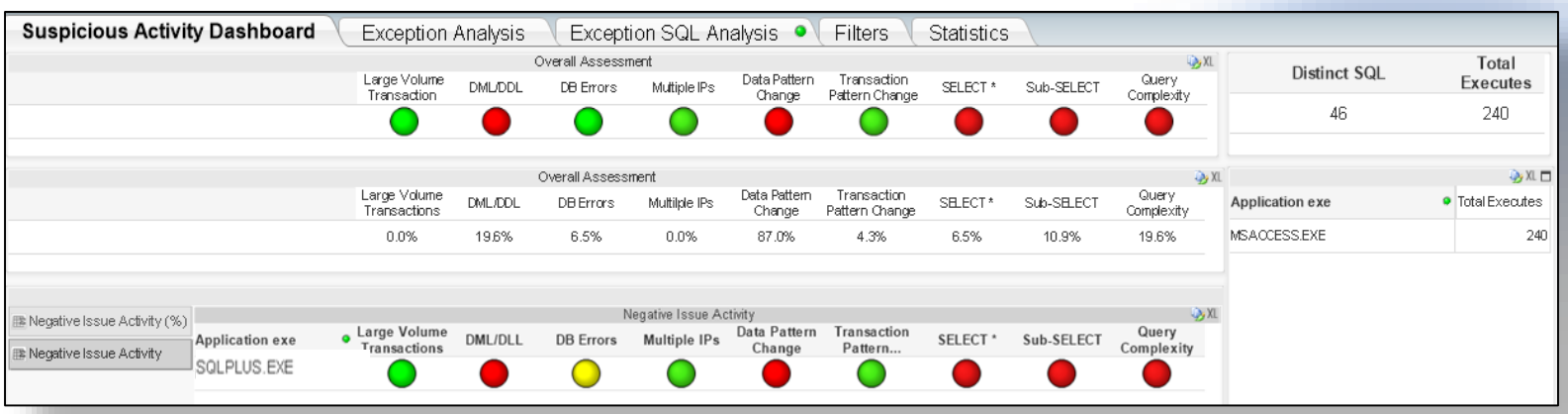
GDPR Data Protection and Compliance Solution

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

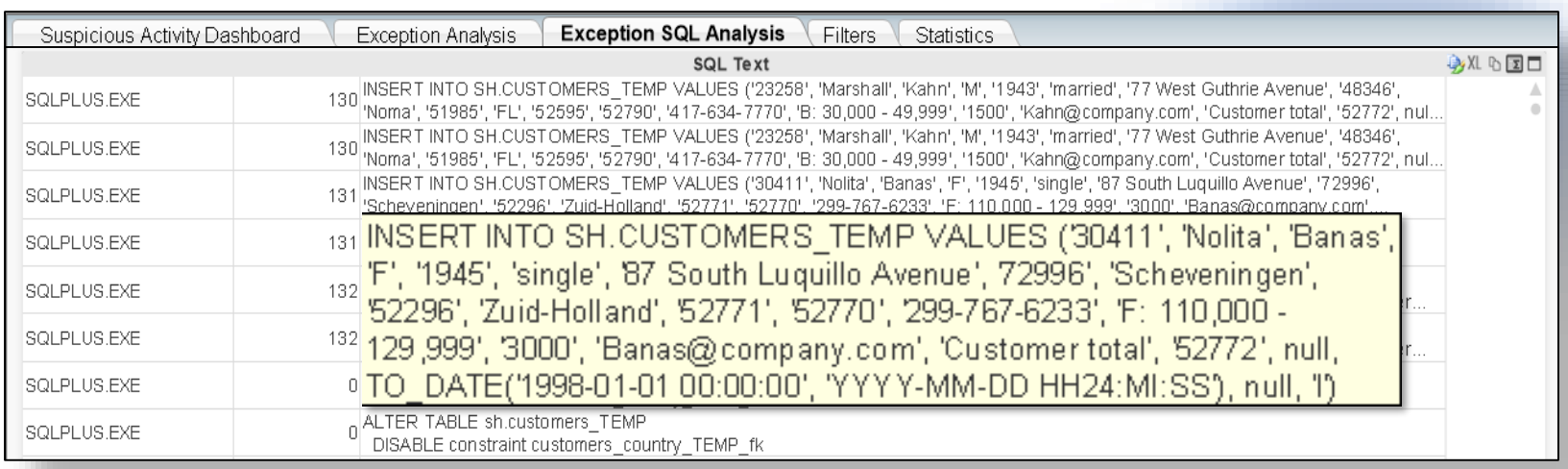
Data Breach Identification



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



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