VISION SOLUTIONS

GDPR – some hints and tips

Stephan Leisse
Solution Architect
stephan.leisse@visionsolutions.com

GDPR Overview

- General Data Protection Regulation (GDPR) is upcoming Regulation (EU) 2016/679 of The European Parliament and the Council of the European Union.
- Giving individuals (‘natural persons’) control over information concerning them (‘personal data’)
- Protection of that information with respect to processing and movement of data.
- Adopted on April 27, 2016
- Comes into force on May 25, 2018.

- Non-compliance can lead to fines.

  Penalties can be severe: Failure to protect data can result in fines of up to 1M Euro or 4% of the world wide revenue

  Essential step to strengthen citizens' fundamental rights in the digital age and facilitate business

VISION SOLUTIONS

Who Does it Apply To?

The regulation applies to two categories of organizations:

Controllers: Organizations of any kind or individuals that transmit, maintain, or process personal information.

Processors: Organizations of any kind or individuals that “process personal data on behalf of the controller.

For example, if :

- Personal data is stored or transmitted through a system under your control you are a Processor.
- Or, if you provide personal information to other organizations likes 3rd party IT service providers or organizations host their own clouds you are a Processor.

The Regulation

- The GDPR is structured in 173 ‘recitals’ and 99 articles.
- Of these, 14 recitals and 11 articles mention or imply the need for data protection technologies, which can be grouped into the following categories:

- Protection of Data
- Privacy and Confidentiality of Data
- Integrity of Data
- Encryption and Pseudonymization
- Access Control, Malicious and Accidental Damage
- Compliance to Regulations
- Risk Assessment
- Logging and Auditing
- Security Settings and Policy

Original Sections of the GDPR and their Corresponding Categories

Section in GDPR	Category
Recital (6)	Protection
Recital (7)	Protection
Recital (15)	Protection
Recital (28)	Encryption
Recital (39)	Privacy, Access control
Recital (49)	Damage, Integrity, Access control
Recital (71)	Privacy, Risk
Recital (78)	Compliance, Encryption
Recital (83)	Risk, Encryption, Damage, Privacy, Integrity, Access Control
Recital (84)	Risk
Recital (87)	Settings, Log/Audit
Recital (90)	Risk, Settings, Protection, Compliance
Recital (108)	Protection
Recital (162)	Access Control
Article 5 1(f)	Integrity, Privacy, Damage
Article 6 4(e)	Encryption
Article 24	All categories
Article 25	Protection, Encryption, Access Control
Article 28	All categories
Article 30	Log/Audit, Security settings
Article 32	Risk, Encryption, Integrity, Security settings, Damage, Privacy, Access Control
Article 34	Encryption
Article 35	Risk, Settings
Article 47	Integrity, Protection
Article 71	Security Settings

VISION SOLUTIONS

Protection of Data

- Protection of data is expressly mentioned or strongly implied in recitals 6, 7, 15, 90, and 108; and in articles 24, 25, 28, and 47,
- The responsibility for data protection falls on both the controller and the processor
- Techniques and data protection principles mentioned to achieve the protection of data included pseudonymization, purpose limitation, data minimization, limited storage periods and data quality.

There are several ways to protect data on IBM i; we would like to discuss the **Object Authority** approach within IBM i

Protection of Data

Object Level Security:

- Traditional way of securing on IBM i
- Powerful capability but complex
- Must have someone on staff with working knowledge of IBM i security schemas
- Many application packages implement Full Access to everyone
- Object level security does not differentiate between internal and external access to the file
- How do you check your settings remain as you set them - assure object level security stays in place

Protection of Data

File Level Security:

- Object Level Security is an extremely powerful tool
- However, it can be bypassed/neutralized by users with powerful user profiles (of which there are too many in most organizations)
- Organizations therefore are looking for full role based access to sensitive DB2 Files to control privileged users
- IBM offers an exit point but you have to write program
- Management infrastructure is needed to optimally use it

VISION SOLUTIONS

Integrity of Data

Data integrity comes up in recitals 49 and 83; and in articles 5, 32 and 47

- Technical measures to ensure integrity and to protect personal data against accidental loss destruction or damage.
- Audit/alerting measures

There are many ways to ensure data integrity on IBM i, here we want to focus on the area of securing IBM i data being accessed by users from **TCP/IP** environment

Integrity of Data

TCP/IP Security:

- The OS/400, now IBM i was architected before the advent of PC connectivity
- A user is able to access the IBM i through the network, change or delete data he wants without being detected
- A person with a user profile and password is restricted in the interactive environment by menus
- TCP/IP Back Door: With the same user name and password through TCP/IP tools this user can bypass menu security and get to resources the menus would not allow him to access interactively

Integrity of Data

TCP/IP Security:

- OS Audit capabilities are not adequate to track such activity
- Putting in security at PC level is too complicated
- Object Level security is (usually) not the answer, especially in terms of
  - reporting required for regulatory compliance
  - expertise required to maintain it
  - applications often not being able to work with it

Integrity of Data

TCP/IP Security:

- Exit Points - WRKREGINF
  - Tools like FTP, ODBC, RMTCMD, IFS etc.

- Need structure to manage the exit programs – role based, layered

- What if there are no Exit Points?
  - For ways of TCP/IP access where IBM is not providing Exit Points they need to addressed too:
  - Examples SSH, SFTP
  - Socket or Packet Level

GDPR: Encryption and Pseudonymization

- The need for encryption and pseudonymization is referred to in recitals 28, 78 and 83; and articles 6, 25, 32 and 34.
- Clearest defined GDPR requirement
- Pseudonymization = Masking or Scrambling or Shuffling

GDPR: Encryption and Pseudonymization #2

- Assuring sensitive data is not seen by unauthorized eyes

- Credentialed or Non-Credentialed User

  -Non credentialed – cryptography cards, IFS directory encryption

  -Credentialed – role based and at field level

- Encryption used to be complicated task, requiring changes to applications, copying files (especially on the decrypt) etc.

VISION SOLUTIONS

- Field Encryption/Masking - Evolution within IBM i

Before IBM i 7.1

Needed to make changes on applications, especially on the decrypt

IBM i 7.1: Field Procedure

- Called at database level

Advantages

- Control on almost everything related to the field:
- encryption/decryption
- Masking
- Scrambling
- Field Audit
- Field Security

Disadvantage

- CPU intensive

IBM i 7.2: RCAC (Row Column Access Control)

- Pure IBM internal DB functionality
- Different masking views fields and records for different users
- Regulates access by data in the row according to user authority

Advantage

- Good and fast performance

Disadvantages

- No Encryption
- No Scrambling
- No Field Auditing

VISION SOLUTIONS

Access Control, Malicious and Accidental Damage

- Access Control is a central component of any data protection requirement. Explicit references to access control exist in, in recitals 39, 49, and 162; and article 25

- Ensuring that personal data is accessible for processing only when necessary

- This implies access control with respect to when, where and two whom access to the data is allowed.
- Access based on need to know

There are many ways for securing data based on need know, one area we would like to zoom in on is **securing** access to **commands**

Access Control, Malicious and Accidental Damage

Command Security & Monitoring

- Security exposure of everyone having access to commands.
- Monitoring of commands is possible in QAUDJRN but at User level
- Individual users need to be configured for *CMD auditing with CHGUSRAUD command.
- Limit access to command line (FTP command line still bypasses, powerful user)
- Another option is to use the exit point IBM provides - allows you to have role based management infrastructure as well as an
audit trail

Privacy and Confidentiality of Data

- The privacy or confidentiality of data is mentioned or strongly implied in recitals 39, 71 and 83; and in articles 5, 28 and 32
- Preventing unauthorized disclosure of or access to such data
- Personal data should be processed in a manner that ensures appropriate security and confidentiality using appropriate technical or organizational measures.

There are several ways to address security and resulting confidentiality on IBM i; here we would like to pay attention **session time out**

Privacy and Confidentiality of Data

Session Timeout:

- Do not want to leave work stations with access to critical data open & unattended
- Role Based not System wide

Compliance to Regulations

- Recital 90 requires assessment of compliance with the regulation.

This requires:

- Defining Controls
- Proof that these are being maintained intact
- In an Automated Way

Manual daily processes to check the settings

Risk Assessment

- Recitals 71, 83, 84, and 90; and articles 32 and 35 refer to risk assessment, incl. measures taken against risks, as necessary to determine the level of security required.

Extensive Consultancy required for analyzing current situation and recommend settings

Logging and Auditing

Article 30 - ‘Records of processing Activities’ mandates maintaining a record of processing activities

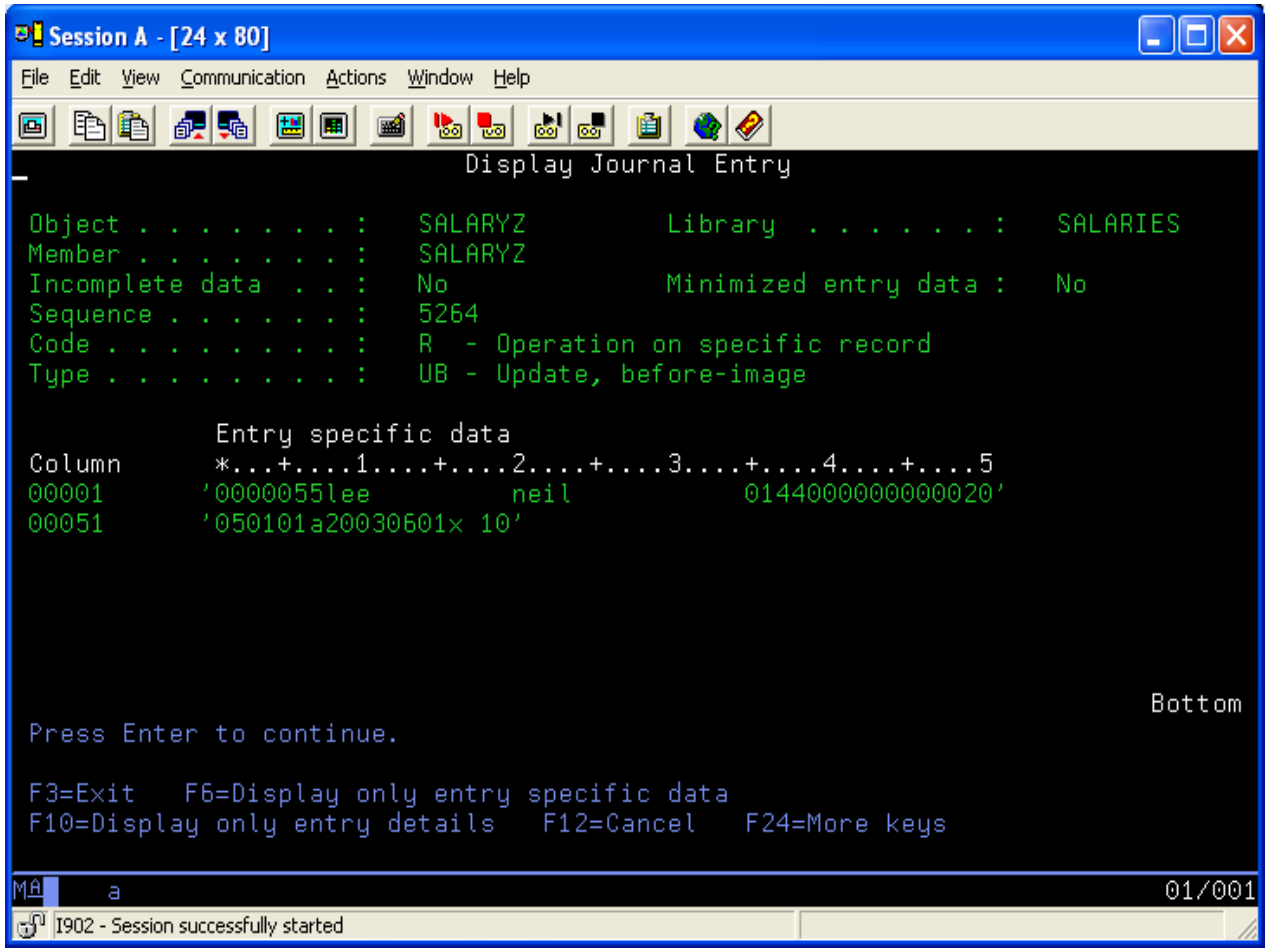
Logging and Auditing

Auditing:

- OS contains many journals and logs that contain a wealth of information
- Challenge is to present this information in a user friendly and comprehensive way

- Example File Journal – information is spread out over various screens
- File Journal- file information, but what about read data events?
- SQL – running this log without management tools is setting up for performance problems
- SQL – problem with ??? in SQL Statements

Logging and Auditing - Example



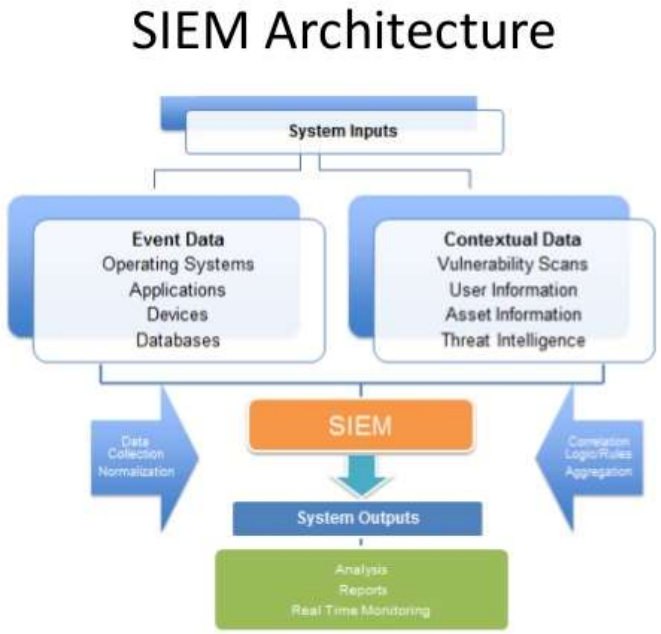
- No indication of the PC that accessed the file
- No indication of the SQL statement
- No separation of field values
- No display of non-character fields
- No indication that this was breach rather than legitimate update

VISION SOLUTIONS

Logging and Auditing

Challenge of Maintaining a Record:

- Amounts of Data
- Journal Receivers need to be taken offline, restoring them for forensics needs can be at cross purposes with operational needs.
- Storage on a Production Server – SIEM (Security Information & Event Management)



Security Settings and Policy

Articles 30, 32, 35, and 71 relate to the maintenance and reporting of a security policy and an assessment of that policy.

- Automatic comparisons between IT configurations and policies.
- stand-alone security risk assessment
- Reporting/predefined reports

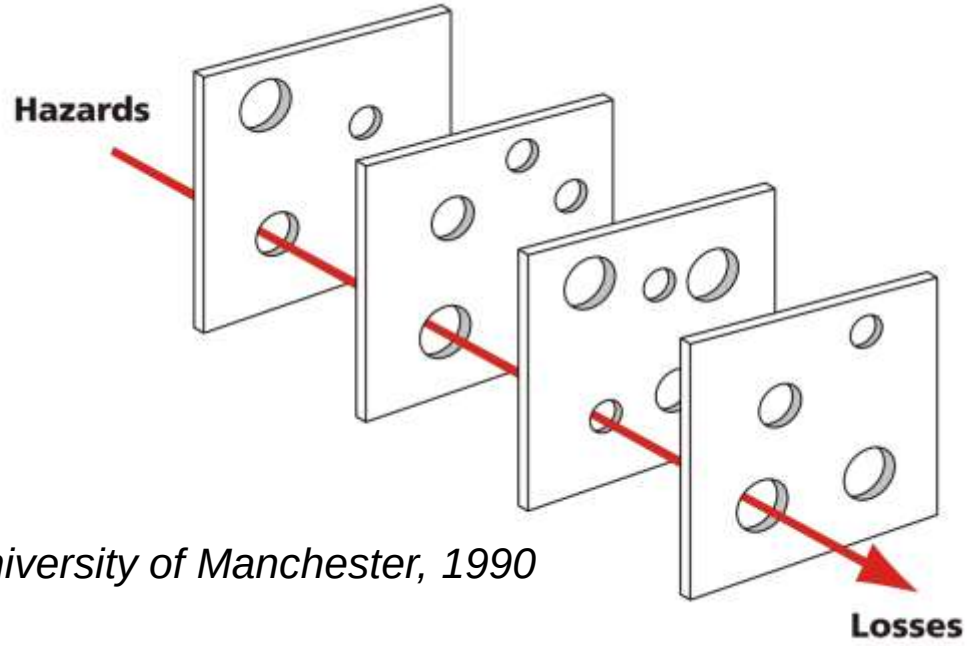
Manual run Reports and daily processes to check the settings

Security 101: Layered Security Fundamentals

Layered Security: The Swiss Cheese Model

We Assume There Are Holes, We Can't Plug All Of Them

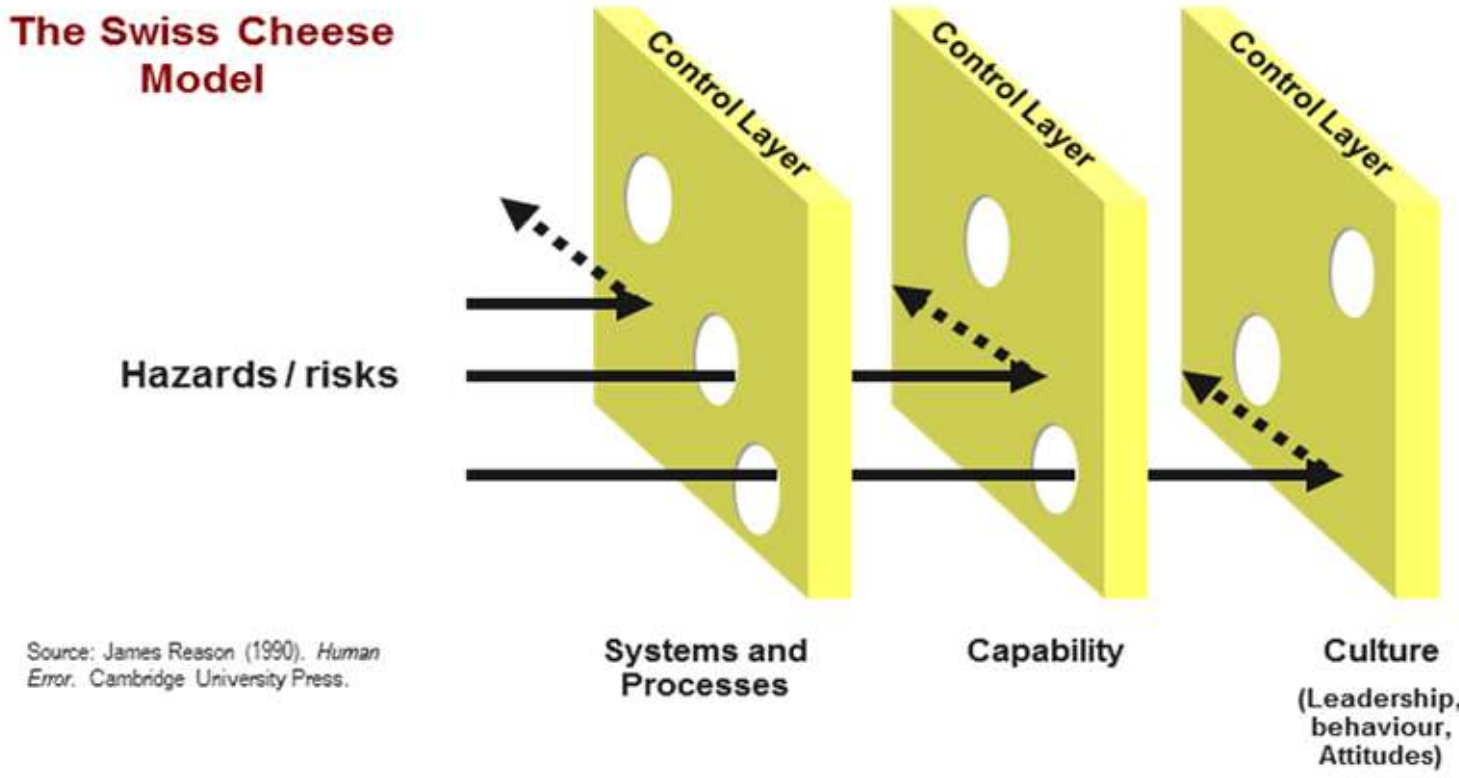
The Goal Is Not To Plug All The Holes



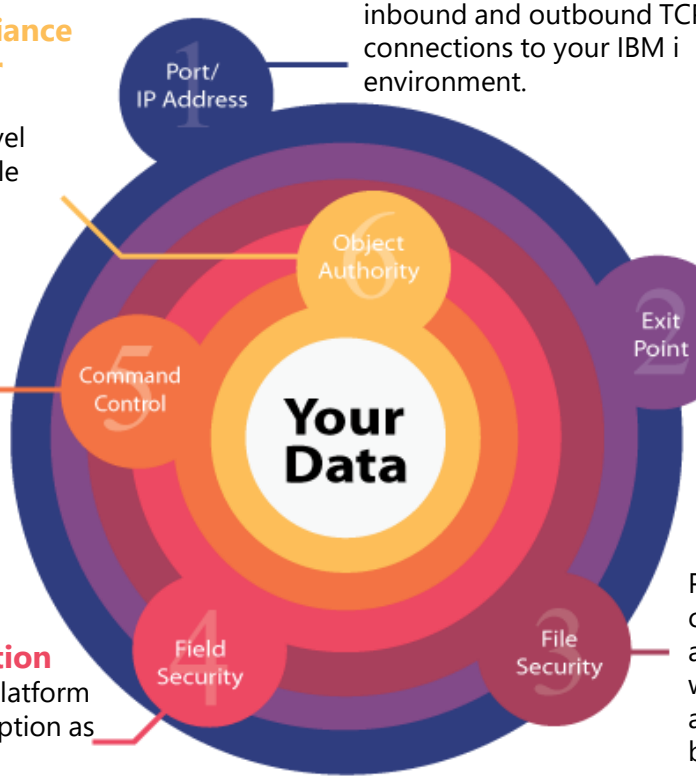
James T. Reason, University of Manchester, 1990

Security 101: Layered Security Fundamentals

The Goal is to Prevent a Breach



Layered Security for IBM i



Firewall/IP Packet Filtering
Allows you to monitor and secure all inbound and outbound TCP/IP connections to your IBM i environment.

Policy Compliance Manager
Provides a way to monitor object level security and enable updates from GUI interface.

Application Access Control
Provides auditing and protection from unauthorized activity coming to or from the TCP/IP network through exit poitns

Command Control
A layer of access control to system commands that is applied in addition to the object authority controlled by the operating system.

File Protection Layer
Powerful feature that allows you to control record level access internally and externally to file objects in a way that complements the control afforded by the operating system's built in object authority.

Field Encryption
A comprehensive platform for field level encryption as well as for security, masking, and scrambling. Includes save file encryption.

Layers of Data Security

- Where are the critical assets on IBM i?
- How can you get to them?

VISION SOLUTIONS

Enterprise Security to GDPR Mapping

GDPR Category	Enterprise Security Function										
	Recital / Article	Compliance	Application Access Control	Encryption	Central Audit	Firewall	Session Timeout	Security Risk Assessment	Alert Center	Report Generator	File Audit
Protection of Data	R: 6, 7, 15, 90 A: 24, 25, 28, 47		✓	✓		✓	✓				
Privacy / Confidentiality	R: 39, 71, 83 A: 5, 28, 32		✓	✓			✓				
Integrity of Data	R: 49, 83 A: 5, 32, 47		✓		✓				✓	✓	✓
Encryption / pseudonymisa-tion	R: 28, 78, 83 A: 6, 25, 32, 34			✓							
Access Control, Malicious / Accidental Damage	R: 39, 49, 162 A: 25	✓	✓			✓	✓		✓	✓	✓
Compliance to Regulations	R: 90	✓	✓		✓						
Risk Assessment	R: 71, 83, 84, 90 A: 32, 35							✓			
Logging and Auditing	A: 30				✓	✓				✓	
Security Settings and Policy	A: 30, 32, 35, 71	✓						✓		✓	

GDPR White Paper

VISION
SOLUTIONS

VISION SOLUTIONS

GDPR – some hints and tips

Stephan Leisse
Solution Architect
stephan.leisse@visionsolutions.com