



# Ways to Interpret Security Standards - What We Can Learn From the Law

**JOHN ELLIOTT**  
**BLACKFOOT UK**

Session ID: GRC-207

Session Classification: Intermediate

**RSACONFERENCE**  
**EUROPE 2012**

Unfair dismissal

Explosion

Murder



Drinking

... the Lawyer and the Information Security Hero...



# Which is the worst?

**serious**  
vulnerability

**priority**  
vulnerability

**critical**  
vulnerability

**major**  
vulnerability

**significant**  
vulnerability



# The bear market\* for regulation

Stop  
hackers

Breach  
notification

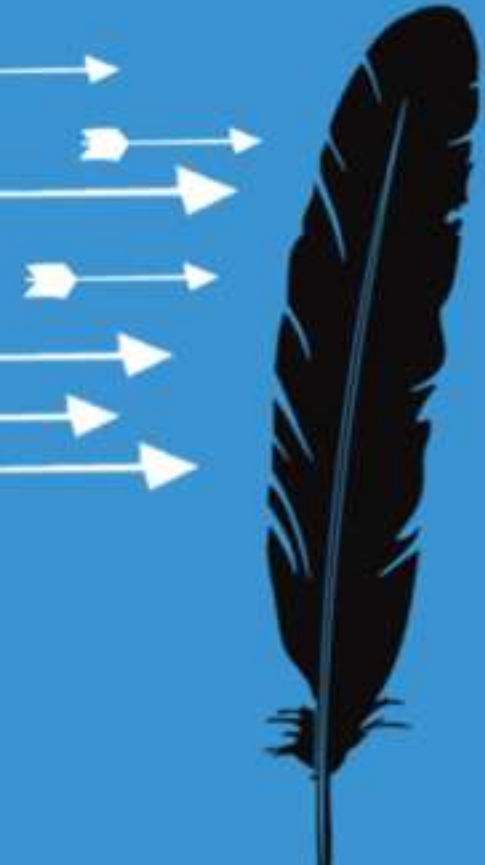
Reasonable  
security

Standards  
as legal  
requirements

\*Stewart Room, Butterworths Data Security Law & Practice



# Information Security in Law



# Massachusetts 201 CMR 17.00

- Secure user authentication protocols ...
- Secure access control measures ...
- Encryption of personal data on public networks
- Reasonable monitoring
- Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions.



# Oregon Senate Bill 583

- Technical safeguards including:
  - Assesses risks in network and software design
  - Assesses risks in information processing, transmission and storage
  - Detects, prevents and responds to attacks or system failures
  - Regularly tests and monitors the effectiveness of key controls, systems and procedures



# PCI Compliance

- Nevada NRS 603A.215
  - If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the PCI DSS.
- Washington House Bill 1149
  - If.. the processor, business, or vendor was certified compliant with the PCI DSS ... . A processor, business, or vendor will be considered compliant.





# Information Commissioner's Office

“Lush took some steps to protect their customers’ data but failed to do regular security checks and did not fully meet industry standards relating to card payment security. Had they done this, it may have prevented the fraud taking place and could have saved the victims a great deal of worry and time invested in claiming their money back. **This breach should serve as a warning to all retailers that online security must be taken seriously and that the Payment Card Industry Data Security Standard or an equivalent must be followed at all times.**”

**Making soft-law (PCI) into hard-law (DPA)**



# Italian Data Protection Code

- a password shall consist of at least eight characters...
- an ID code, if used, may not be assigned to another person in charge of the processing even at a different time
- Authentication credentials shall be de-activated if they have not been used for at least six months ...

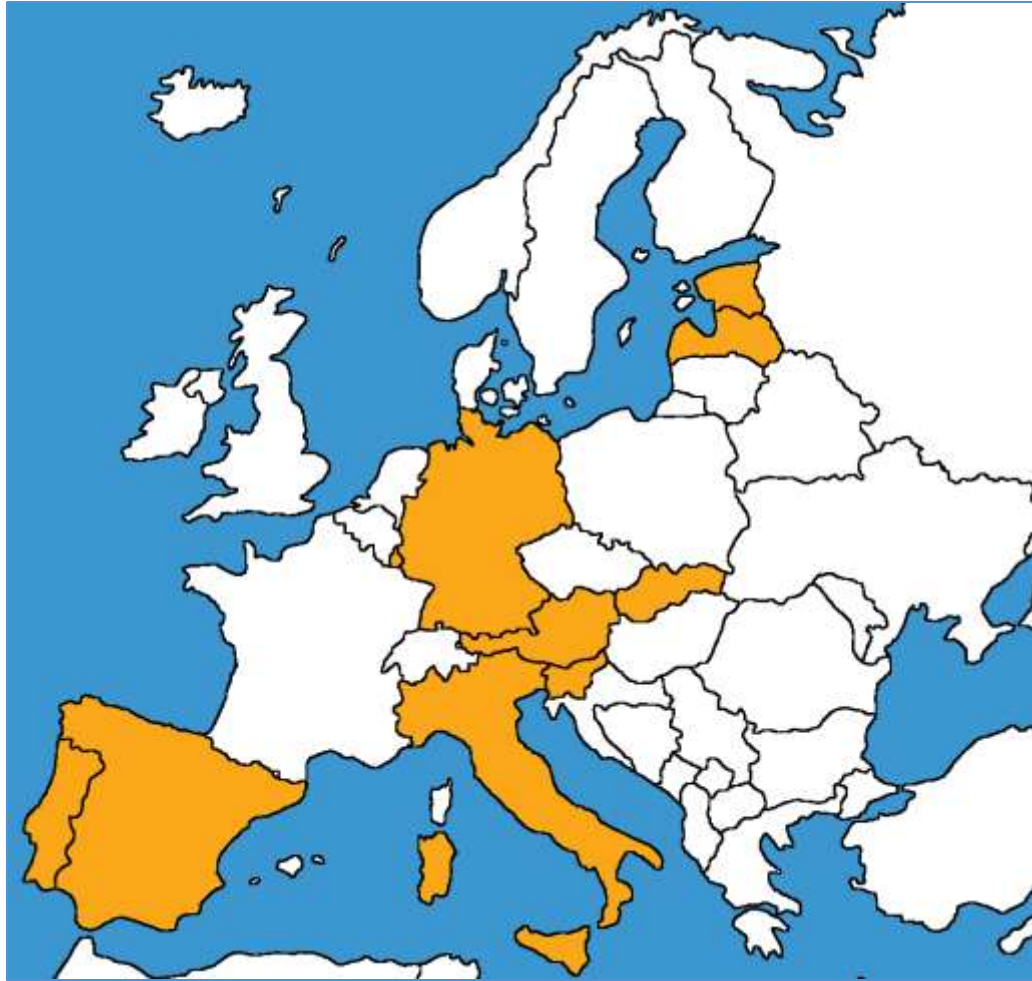


# Spanish Organic Data Protection Law

- There are three levels of security measures, basic, medium and high.
- **Basic:** ... mechanisms to avoid a user being able to access resources ...
- **Medium:** ... limit the possibility of repeated attempts of unauthorised access ...
- **High:** ... for each attempt at access ... identification of the user, date, time and whether authorised or denied ...



# Other EU States With Technical Security Requirements in Data Protection Law





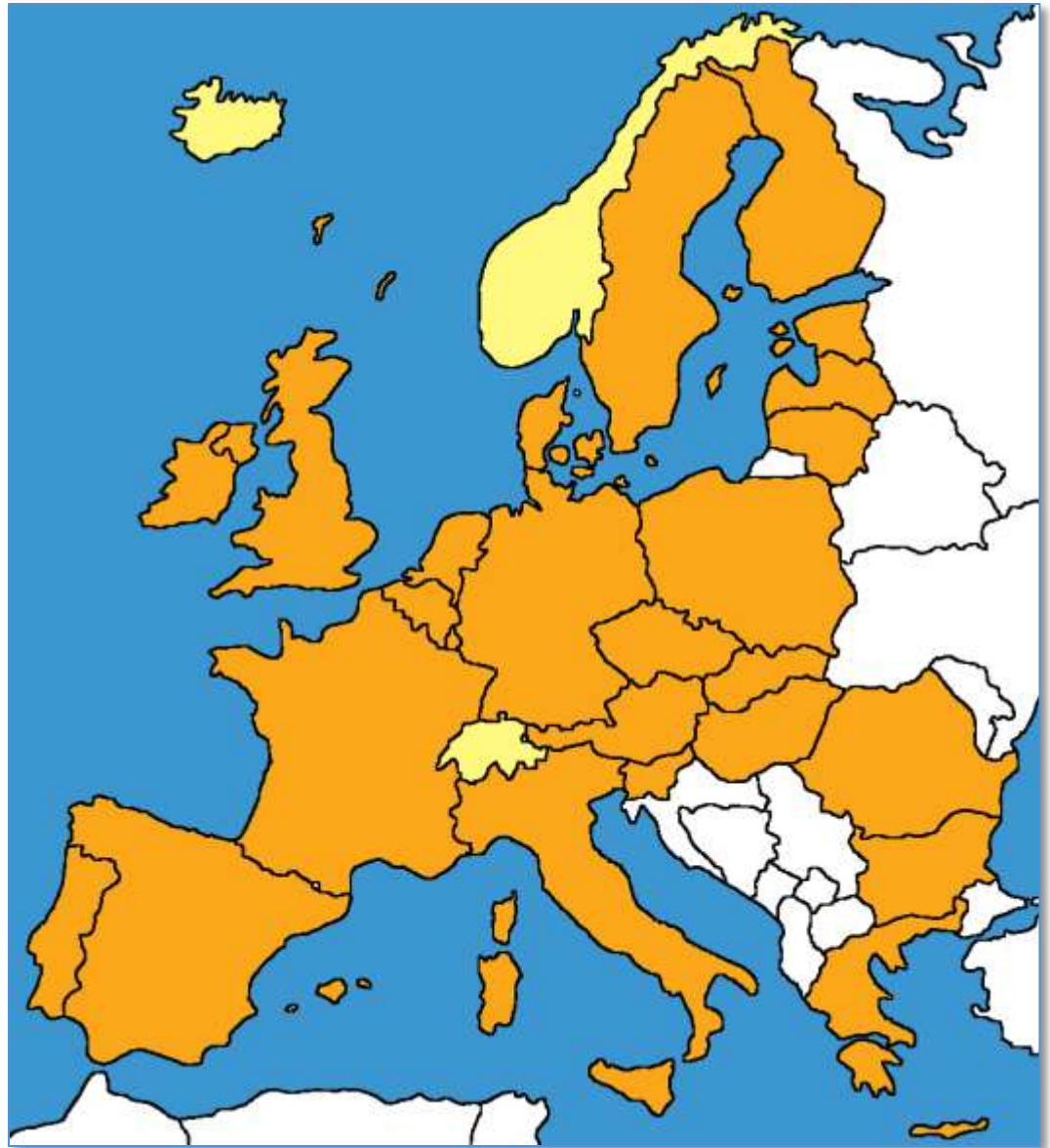
# Proposed EU Data Protection Regulation

- A regulation applies EU-wide
  - Current data protection law was established with a directive
  - Implemented differently in each country
- One set of data protection rules for the entire EU
- What about information security?



# A Regulation ...

-  applies directly
-  would probably be adopted



# Proposed EU Data Protection Regulation

- **Article 30(3)**

The Commission shall **be empowered to adopt delegated measures**... for the purpose of further specifying the criteria and conditions for the **technical and organisational measures** ... including the determinations of **what constitutes the state of the art** ... in particular taking account of developments in technology and solutions for privacy by design and data protection by default



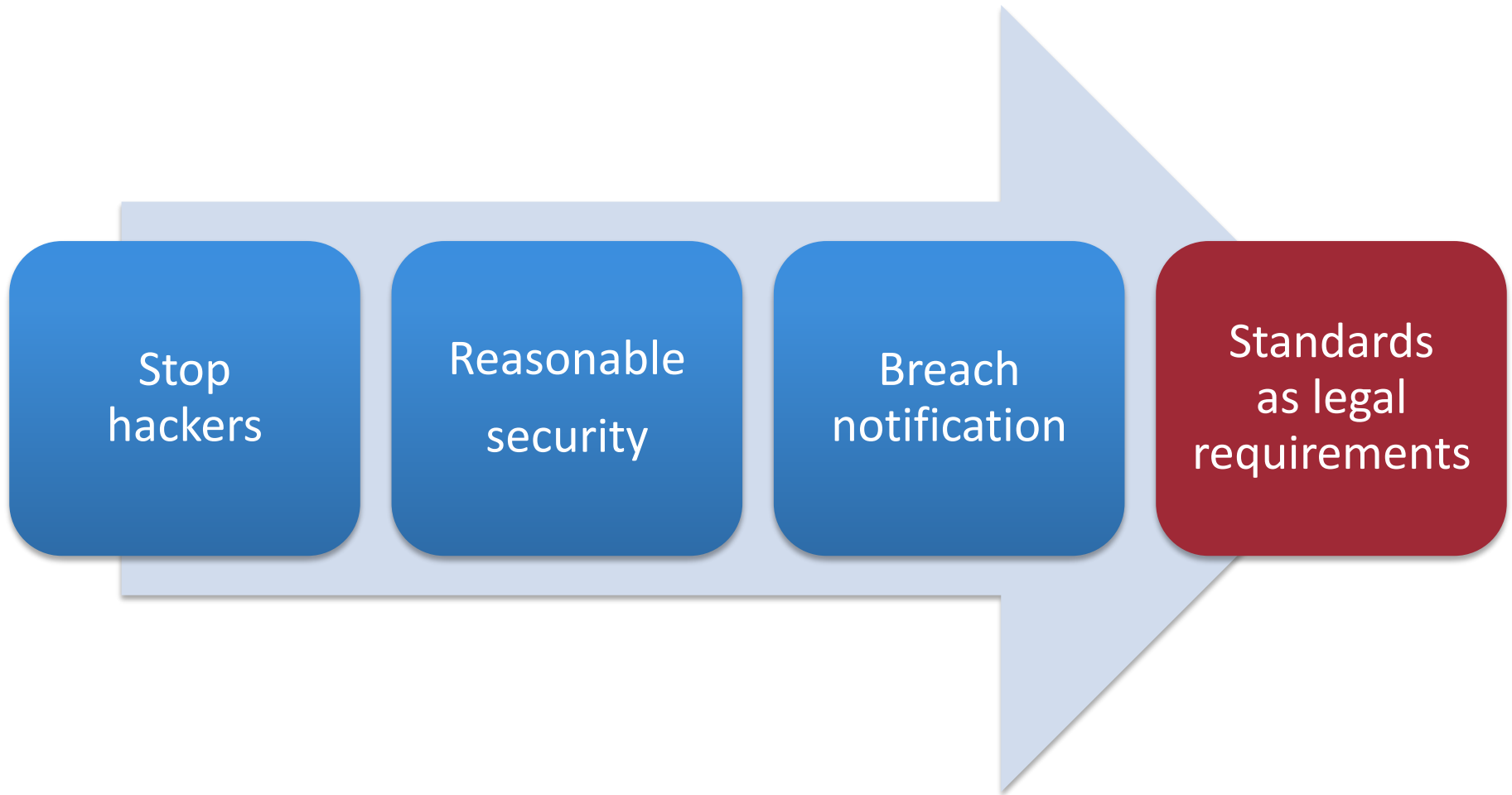
# Proposed EU Regulation- Article 36

- The Member States and the Commission shall **encourage** the establishment of **data protection certification mechanisms** and of **data protection seals** and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors
- The Commission **may lay down technical standards** for **certification mechanisms** and **data protection seals** and marks ...





# A Challenge for Information Security



# Words can have many meanings

The Commission may lay down technical standards for certification mechanisms and **data protection seals** and marks ...



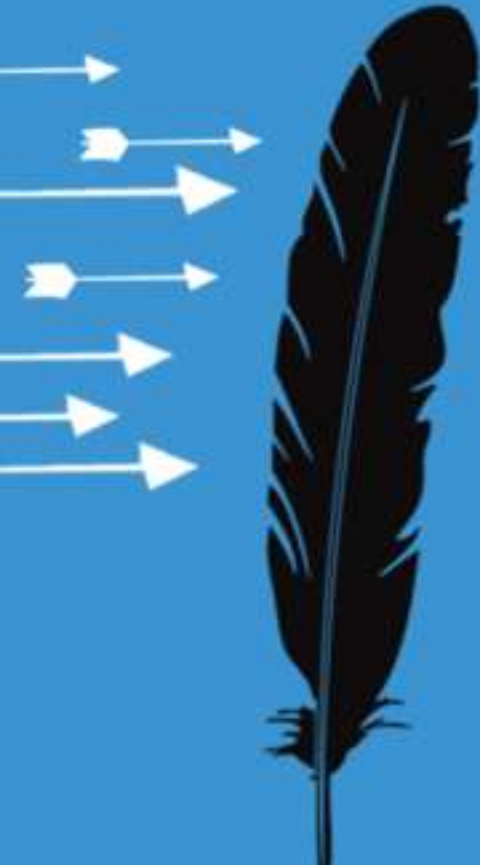
navy seal



data protection seal



# The Rules Lawyers Use



# What We Can Learn From The Law

- 500 years of written history
- Parliament passes statutes (acts)
- Judges have to interpret statutes
- They have developed a number of approaches (rules)



# Road Traffic Act 1988

- *[An insurance policy] must insure such person, persons or classes of persons as may be specified in the policy in respect of any liability which may be incurred by him or them in respect of the death of or bodily injury to any person or damage to property caused by, or arising out of, the use of a vehicle on a **road** in Great Britain...*  
145(3)(a) Road Traffic Act 1988



# Cutter v Eagle Star Insurance Company

- Mr Cutter was sitting in a car parked in a multi-story car park
- Lighter fuel had leaked on to the back seat
- The driver returned and lit a cigarette
- Mr Cutter was injured

The car was not being used on a **road** so the insurance company was not liable.



# Literal Rule

- Words must be given their plain, ordinary meaning



# Administration of Estates Act

- *The residuary estate of an intestate shall be distributed in the manner .. mentioned in this section, namely:*
- *If the intestate leaves issue but no spouse or civil partner, the residuary estate of the intestate shall be held on the statutory trusts for the issue of the intestate*

s46(ii) Administration of Estates Act 1925





# Re: Sigsworth

- Mary Ann Sigsworth died intestate
- She had one son, Thomas Sigsworth
- who murdered his mother



Thomas Sigsworth could not inherit.



# Golden Rule

- Words must be given their plain, ordinary meaning
- UNLESS that produces an ABSURDITY or an affront to public policy




# Licensing Act

- *Every person who is drunk while in charge on any highway or other public place of any carriage, horse, cattle, or steam engine, or who is drunk when in possession of any loaded firearms, shall be liable to a penalty ..., or in the discretion of the court to imprisonment for any term not exceeding one month.*  
s12 Licensing Act 1872



# Corkery v Carpenter

- Shane Corkery was arrested for being drunk in charge of a bicycle on the highway
- It was argued that a bicycle was not a carriage



Binge  
drinking

It won't be a stylish marriage,  
I can't afford a carriage,  
But you'll look sweet, upon the seat  
Of a bicycle made for two.

A bicycle is a carriage.



# Mischief and Purposive Approach

- What was the state of the law before the act?
- What was the mischief Parliament wanted to remedy?
- What is the purpose of the act

“We do not sit here to pull the language of Parliament to pieces and make nonsense of it. We sit here to find out the intention of Parliament and carry it out and we do this better by filling in the gaps and making sense of the enactment than by opening it up to destructive analysis” *Denning LJ*



# Transfer of Undertakings (Protection of Employment)

- “to provide for the protection of employees in the event of a change of employer, in particular, to ensure that their rights are safeguarded . . . .”
- *Any reference. . . above to a person employed in an undertaking or part of one transferred by a relevant transfer is a reference to a person so employed **immediately before the transfer**...*  
S5(3) TUPE



# Litster v Forth Dry Dock and Engineering

- Employees (unfairly) terminated at 15:30
- Business sold at 16:30
- Employees therefore not employed immediately before the transfer

Unfair dismissal

Read as:

“employed immediately before the transfer or would have been so employed if he had not been unfairly dismissed”



# Teleological Approach

- Used in interpreting European law
- Consider aims
- Follow the spirit of the legislation





# Summary of Rules

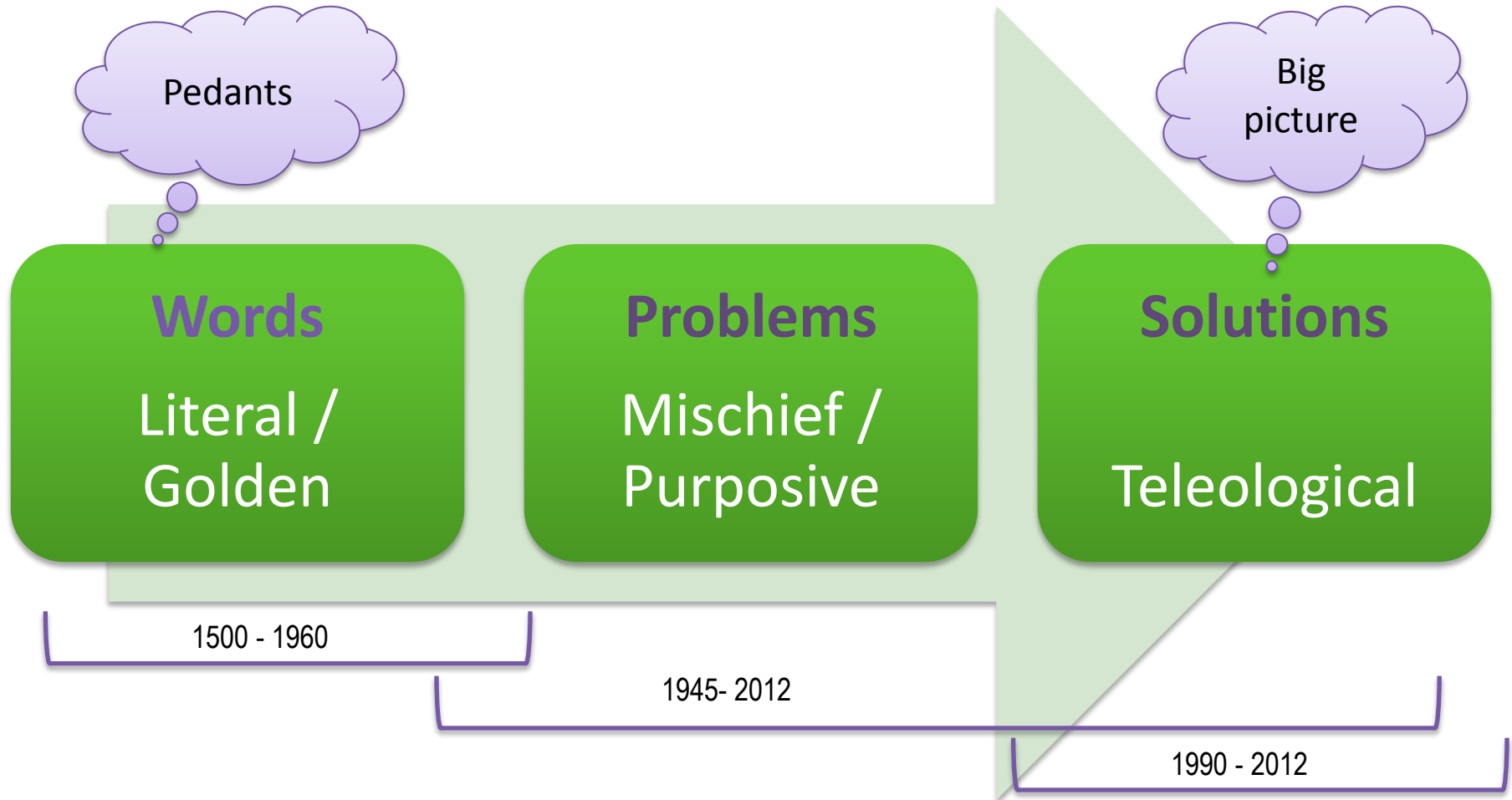
- Literal
- Golden
- Mischief / Purpose
- Teleological approach

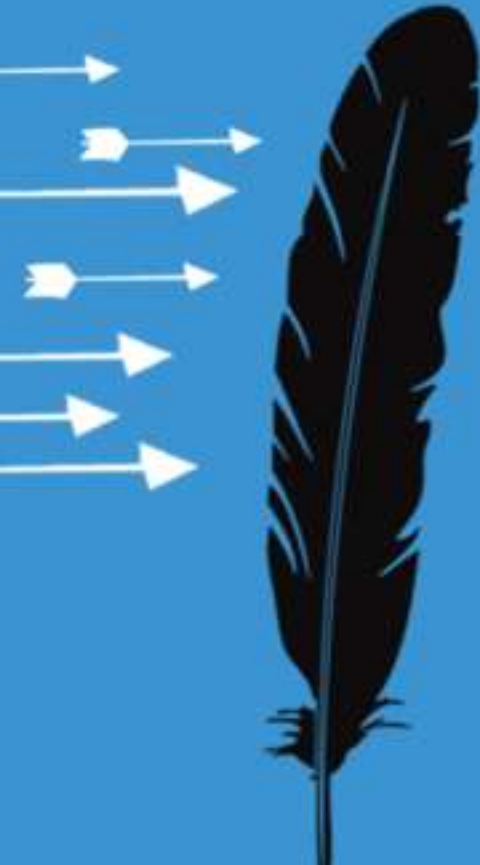


Integrated



# Emphasis on





# An Example: PCI DSS\*

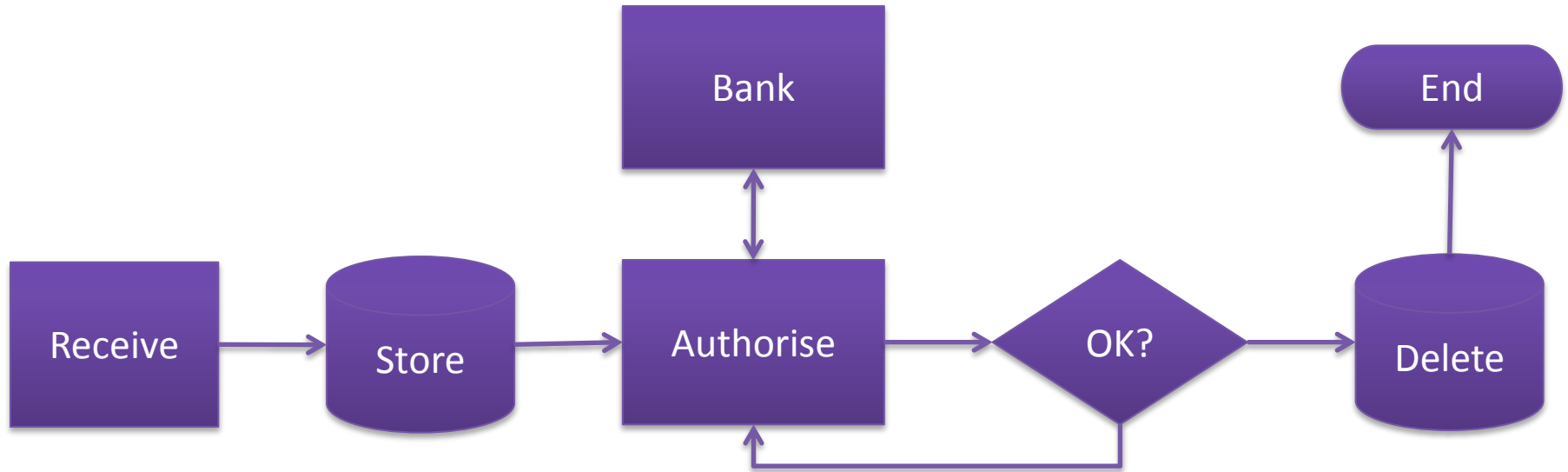
- \* Which is most likely to be used as the basis of a law

# PCI DSS - an example

- 3.2 Do not **store** sensitive authentication data **after** authorization (even if encrypted).
- 3.2.2 Do not **store** the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.

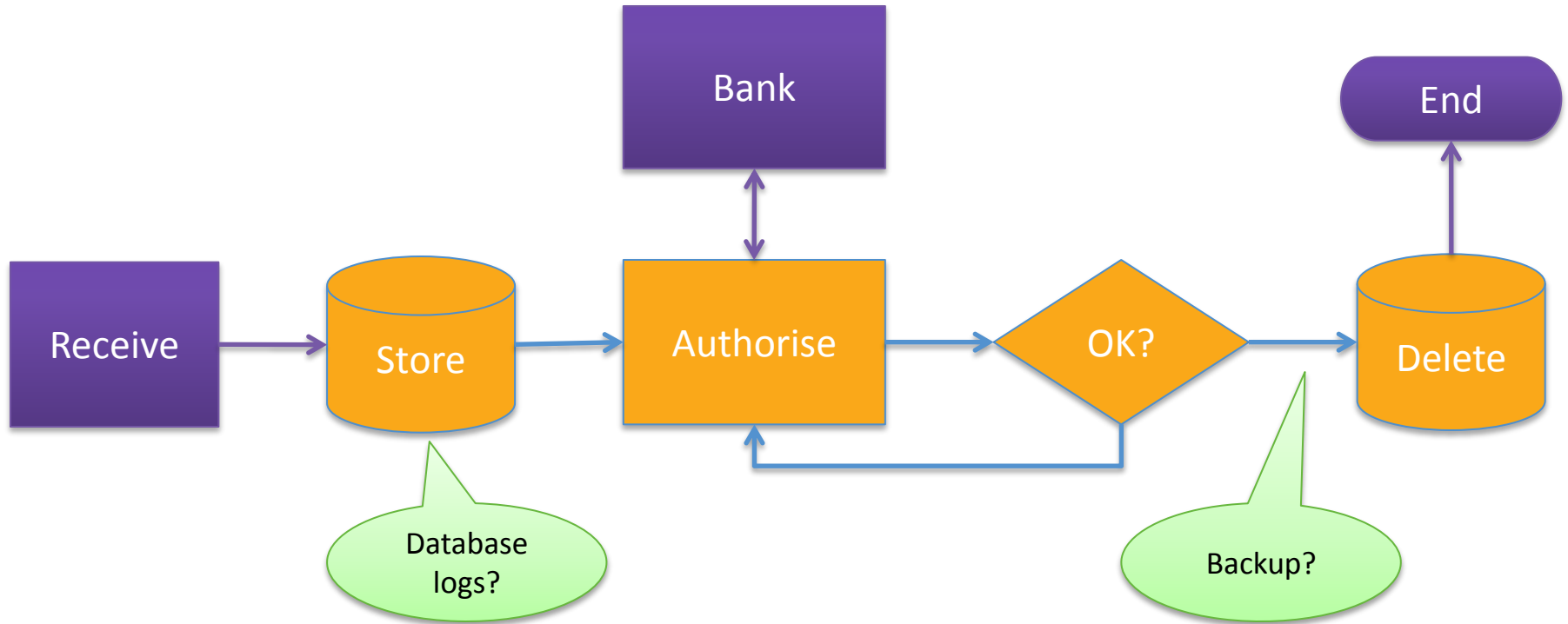


# Typical process



Do not store sensitive authentication data after authorization

# Risk



Do not **store** sensitive authentication data **after** authorization

# Literal approach: Store

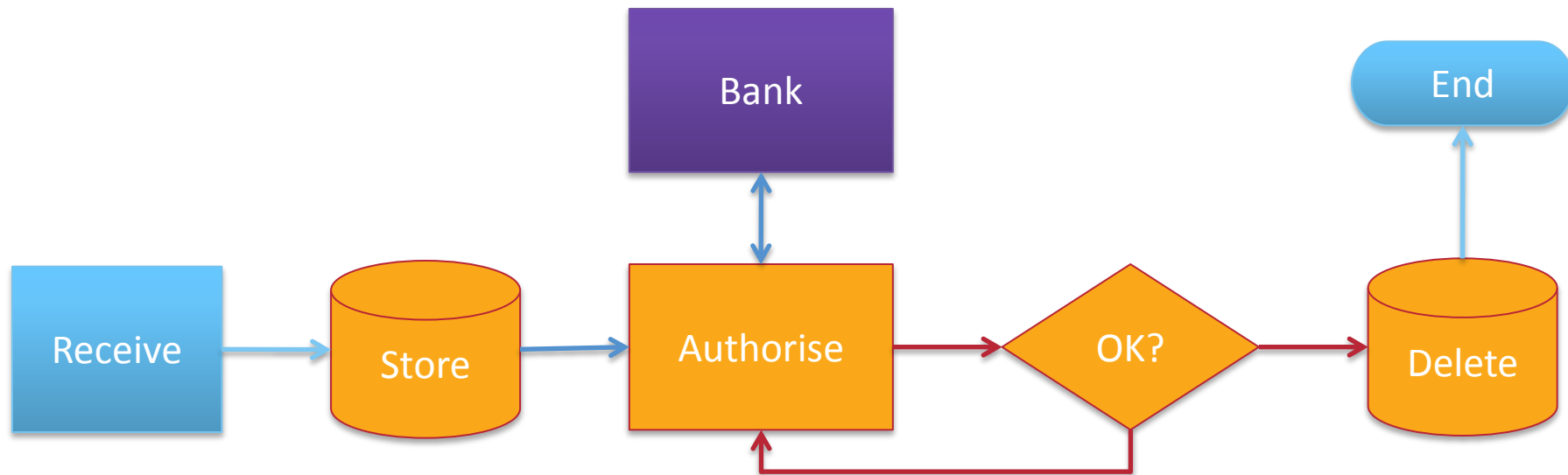
1. Keep or accumulate (something) for **future use**
2. Retain or enter (information) for **future electronic retrieval**

= write to disk



Do not **store** sensitive authentication data **after** authorization

# Literal 1



*store:*

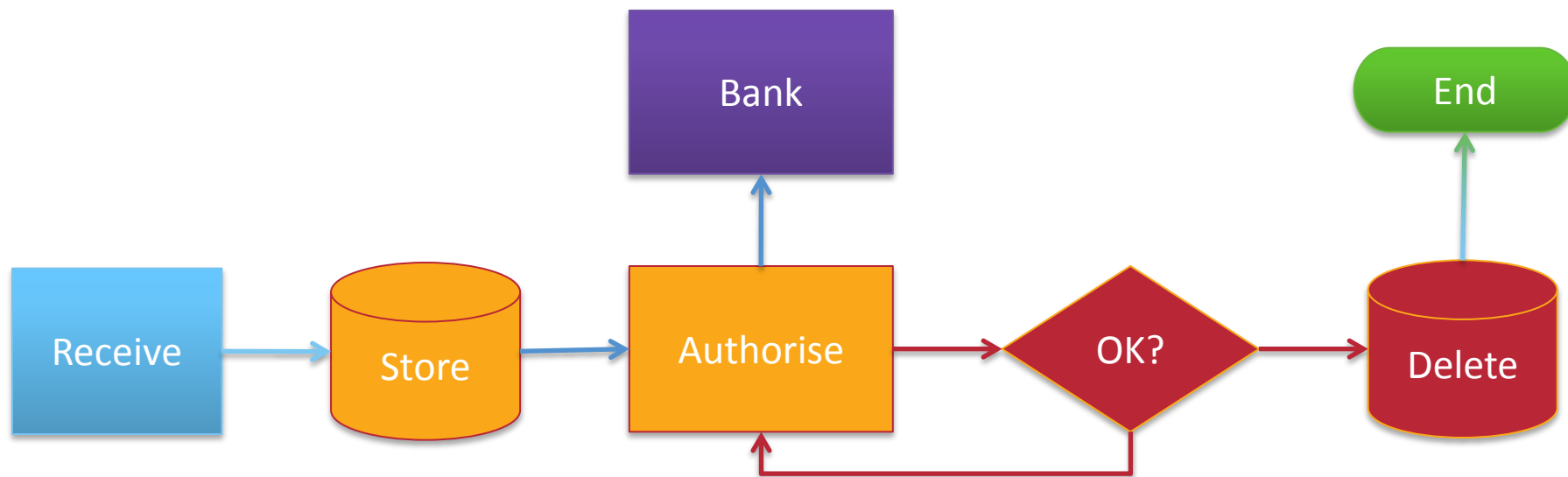
Keep or accumulate (something) for **future use**





Do not **store** sensitive authentication data **after** authorization

## Literal 2



*store:*

Retain or enter (information)  
for **future** electronic **retrieval**

= write to disk



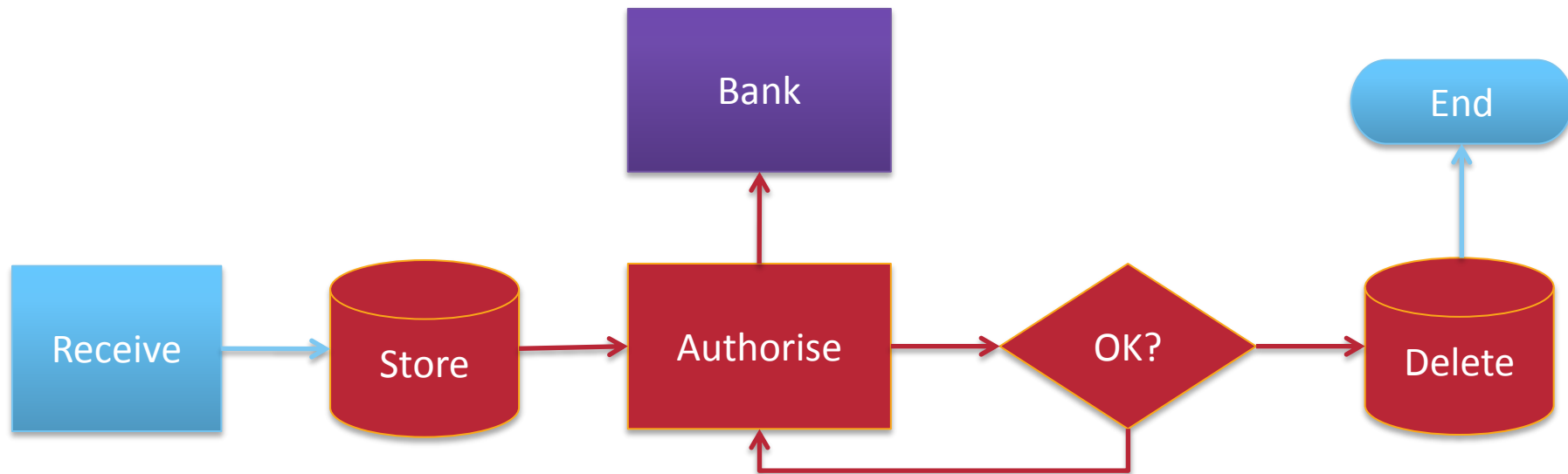
## Mischief / Purposive Approach

- The purpose of the card validation code is to protect "card-not-present" transactions—Internet or mail order/telephone order (MO/TO) transactions—where the consumer and the card are not present. ... **If this prohibited data is stored and subsequently stolen**, malicious individuals can execute fraudulent Internet and MO/TO transactions..



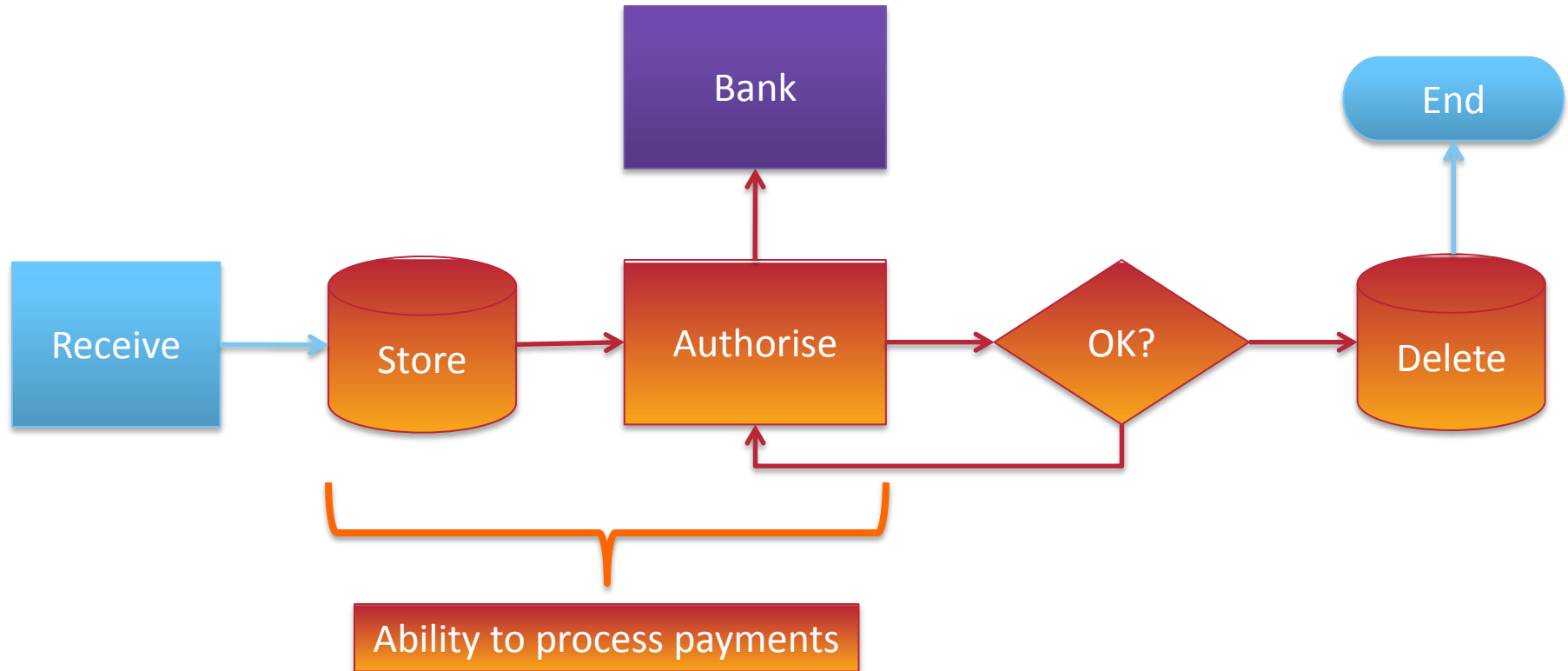
Do not **store** sensitive authentication data **after** authorization

# Mischief / Purposive



Do not **store** sensitive authentication data **after** authorization

# Mischief / Purposive



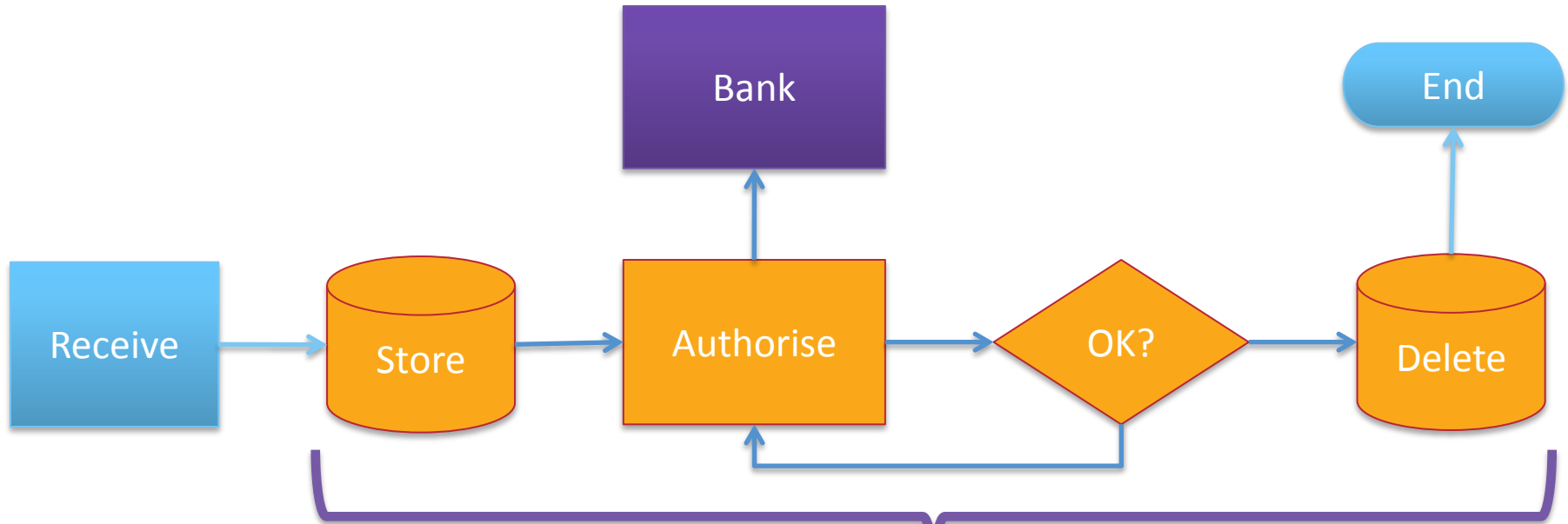
## Teleological approach

- The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to **encourage** and **enhance cardholder data security** and facilitate the broad adoption of consistent data security measures globally.



Do not **store** sensitive authentication data **after** authorization

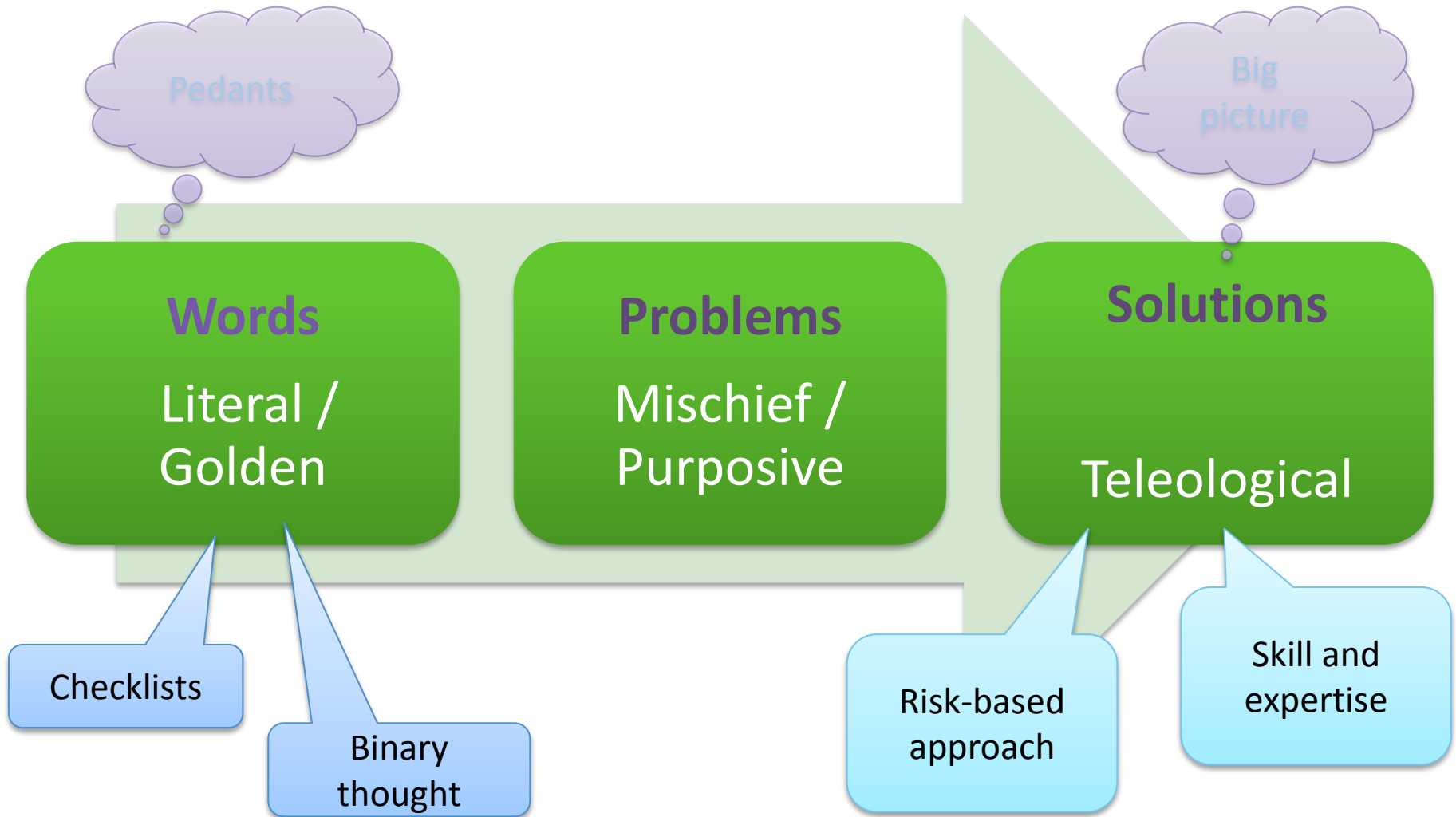
# Teleological



Store for as short a time period as possible  
Add audit controls, encrypt  
= Enhance cardholder data security



# Information security approach



# In summary

- Judges have been interpreting written statutes for more than 500 years
- A strictly literal interpretation has largely been replaced by a purposive approach
- The teleological approach is preferred when interpreting legislation that implements European law
- The most likely source of statute / regulation of written data security standards will be Europe





# How to Apply This

- Do not get injured in a car in a car park
- If you want to inherit the family wealth, do not murder your mother
- Do not ride a bicycle when drunk



... the Lawyer and the Information Security Hero...



# How to Apply This

When you get involved in a **discussion** or have to **interpret** a standard:

- Words have multiple meanings  
**Everyone might be using a different meaning**
- Test **interpretation** three ways  
**literal, purposive and teleological**
- Catalogue the written standards that you have to comply with
- Be aware of the EU Data Protection Regulation



# Questions?

