



Business Continuity Management is inherent part of EU-GDPR

-

How to link both domains?



- What could be a minimal format to link BCM and GDPR
 1. Assure for resilient GDPR processes in relation to rights and freedoms, breach notification,...
 2. Know which business processes make use of “high-risk” / “risk” processing’s
 3. Always perform a breach-check at any compromising event (technical or physical event)
 4. Make BCM part of the technical and organisational measures used to assure GDPR compliance

- How is Business Continuity mentioned in GDPR?
 - many places
 - like article 32...

Art. 32 GDPR – Security of processing

...and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data; **the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;**

...the ability **to restore the availability and access to personal data in a timely manner** in the event of a **physical or technical** incident;

EU-GDPR addresses “resilience” explicitly

Restoring capabilities & DRP !

Not only “technical” events !

- What are the eye-catchers?

**EU-GDPR : assure rights & freedoms,
breach management, data
availability, data accuracy**

**Not being able to assure this
capability...can cause a breach
situation!**

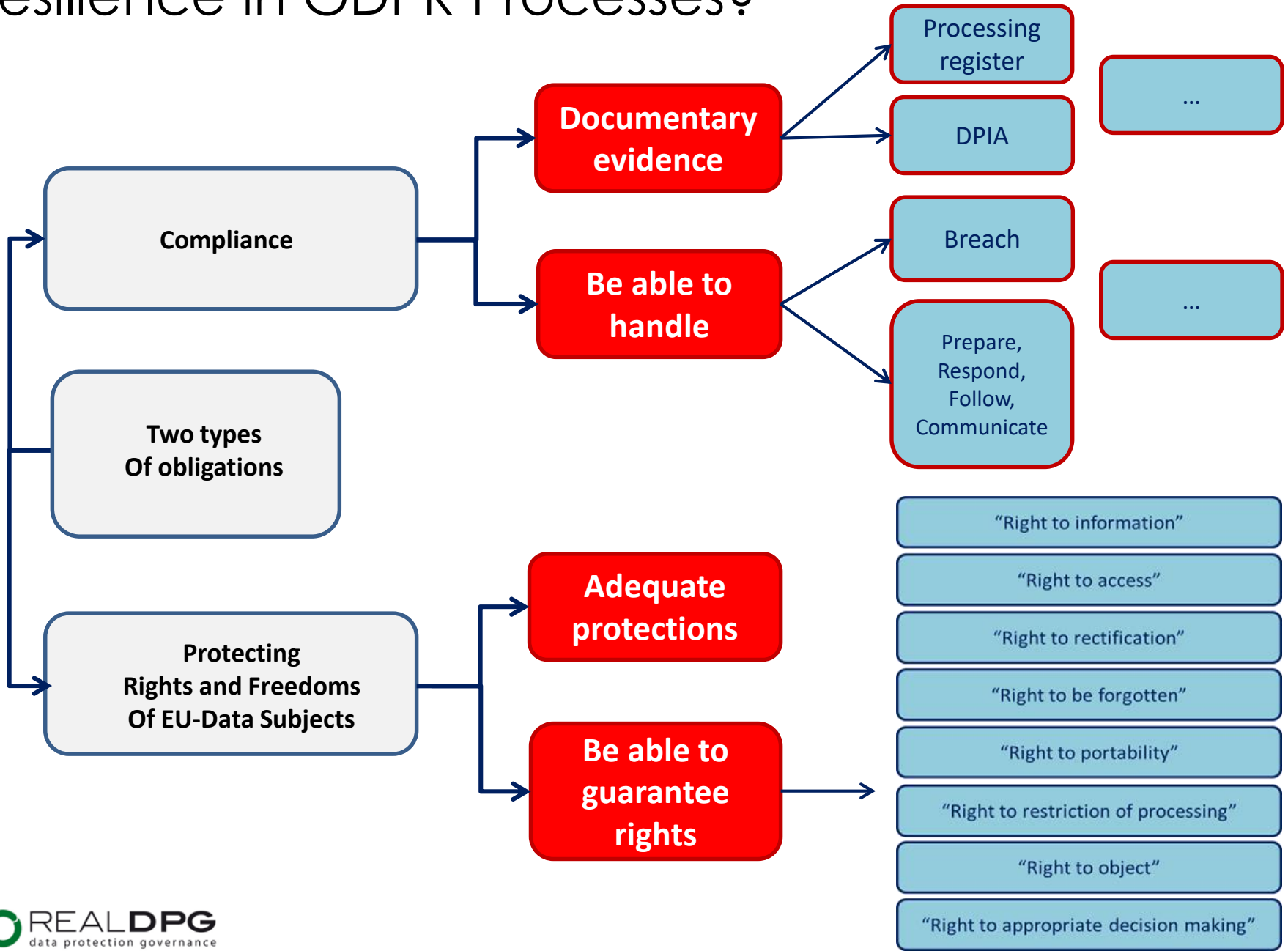
**It is not only about the personal
data and the Data-Subjects...it is
also about processes!**

What processes?

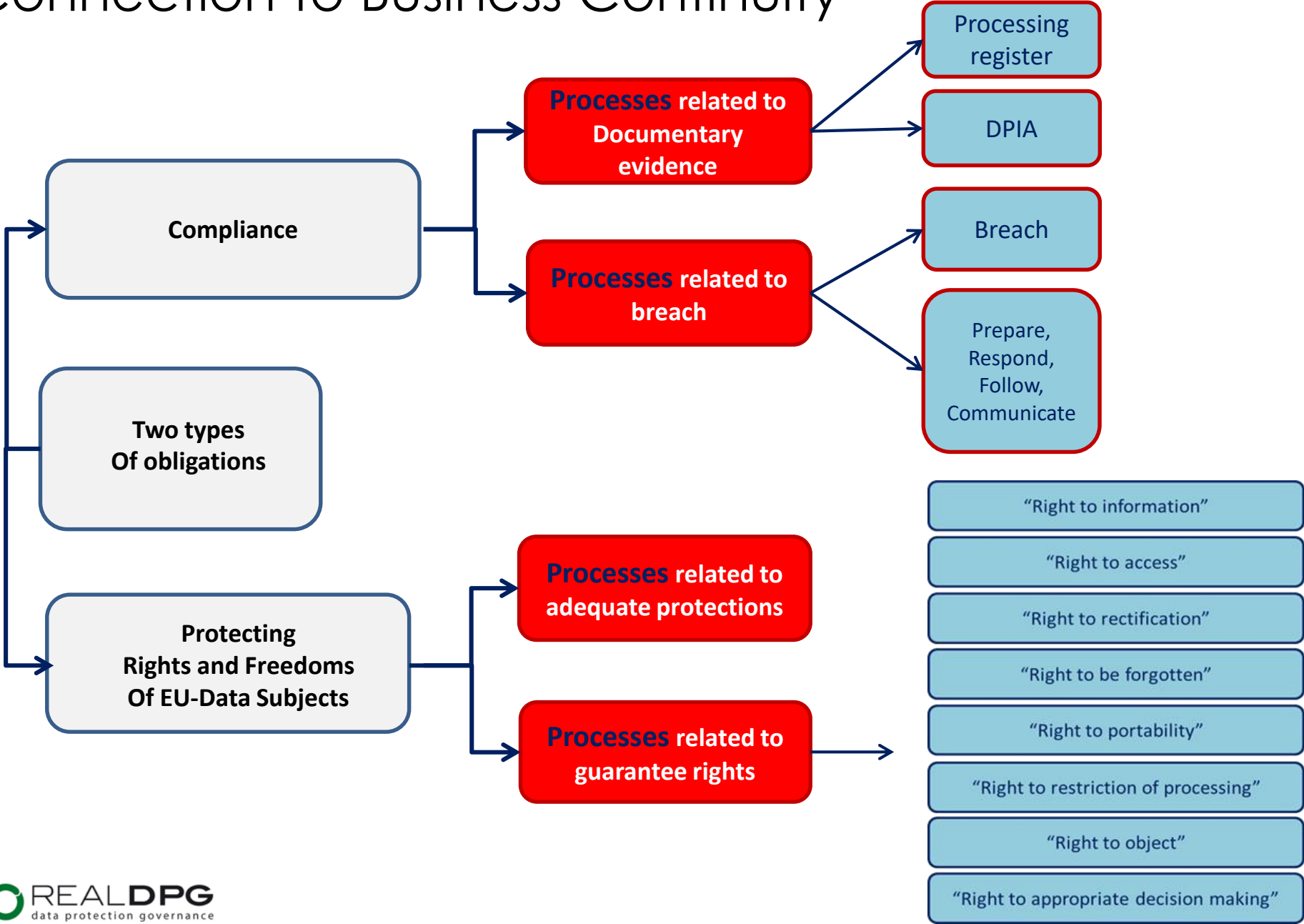
- **GDPR related processes**
- **GDPR sensitivity in business
processes**

1. Assure for resilient GDPR processes in relation to rights and freedoms, breach notification,...

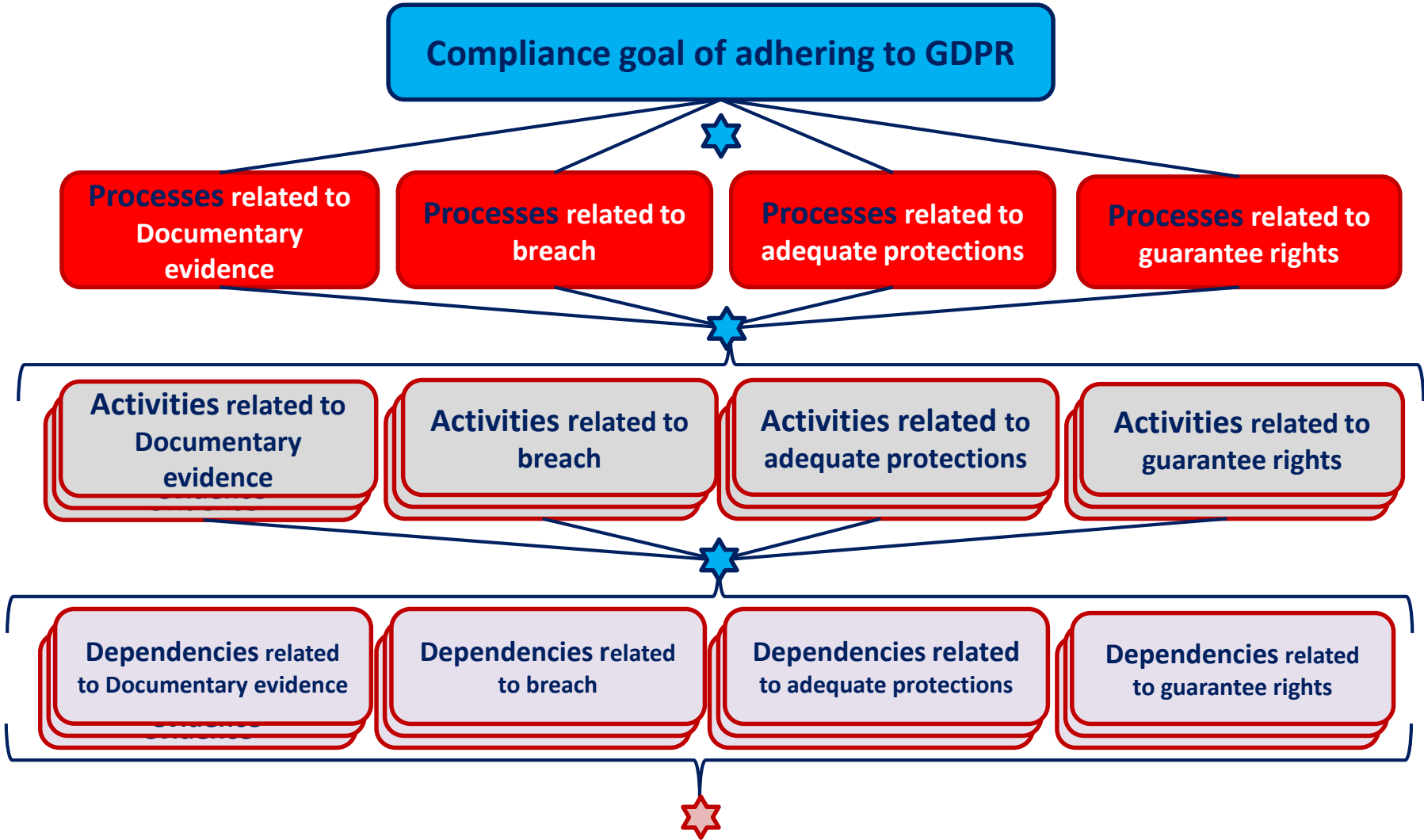
Resilience in GDPR Processes?



Connection to Business Continuity



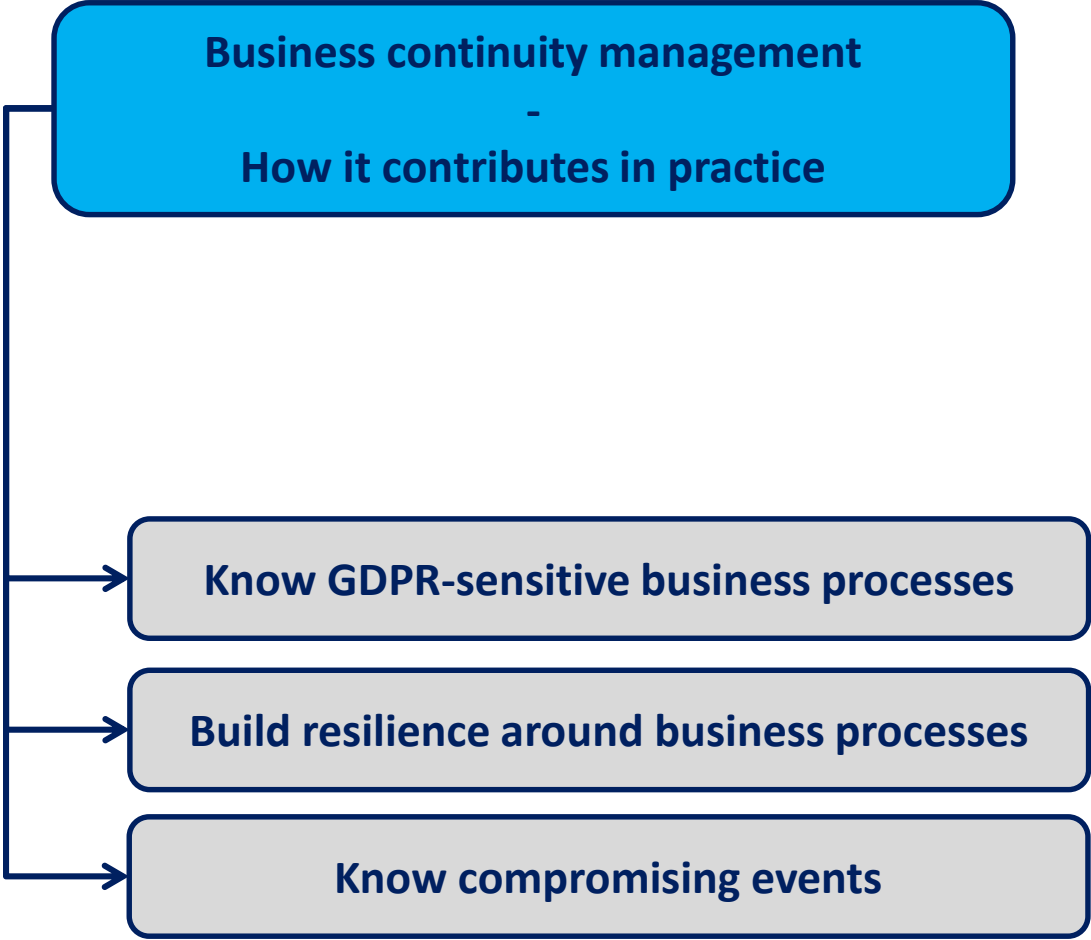
Resilience of GDPR processes



- Make the relations obvious
- Know exactly where to build GDPR-contributing resilience (BCP plans, DRP plans,...)

2. Know which business processes make use of “high-risk” / “risk” processing’s

Resilience in business processes



Integrated, relational

One place

Pocessor management...

Templating-trolley

Toolkitting and -boxes

Internet content

Trainings, certifications

Technical & Org. measures

Breach management

Rights management

Complexity

Interpretations

Detailism

Concentrations on knowledge

Slow reaction times

Difficult proofing

Seeing 25 May as a stop



FAST

STRONG GOVERNANCE

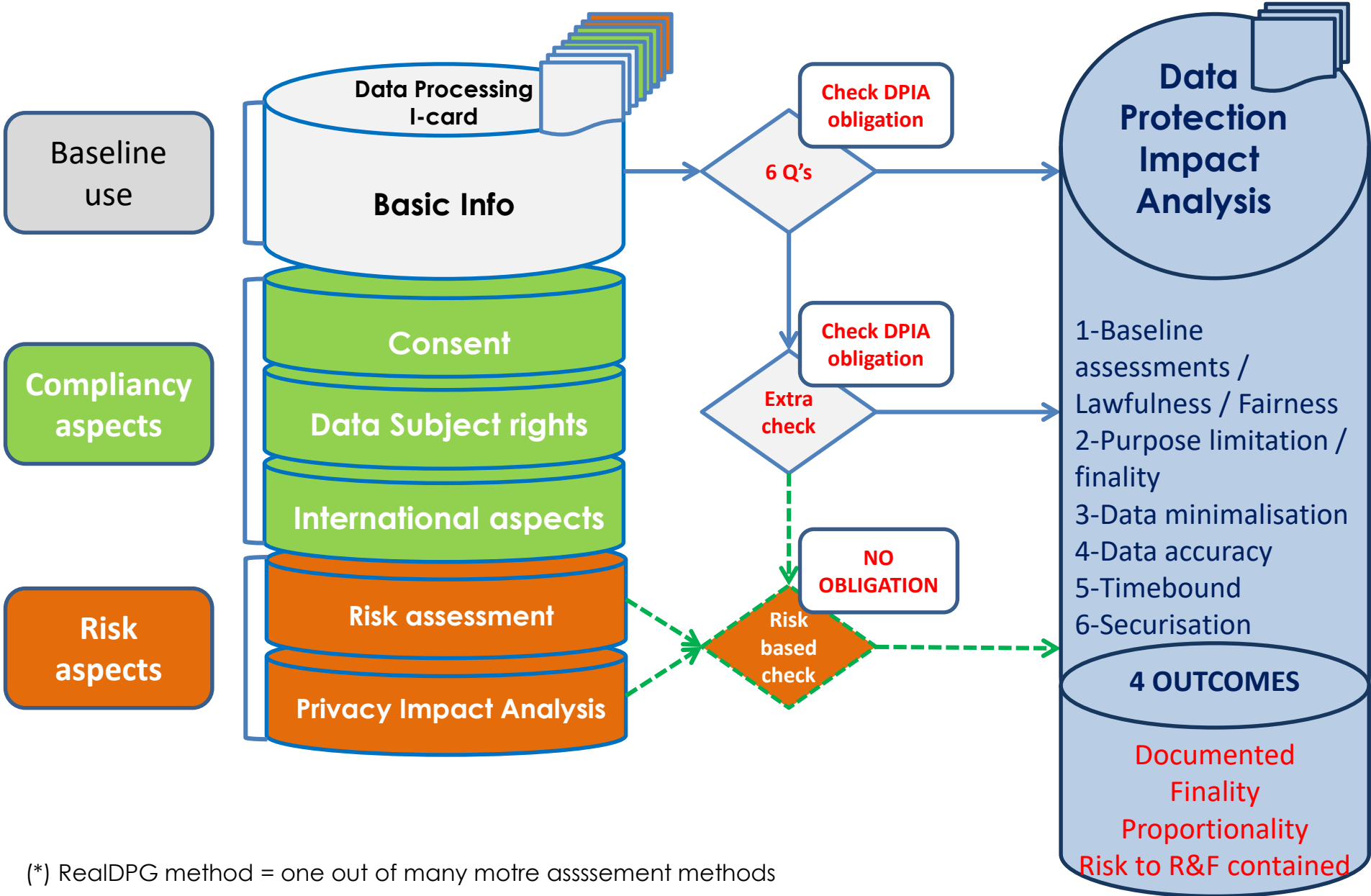
GDPR BASED

RISK BASED where needed

Compliance based where
needed

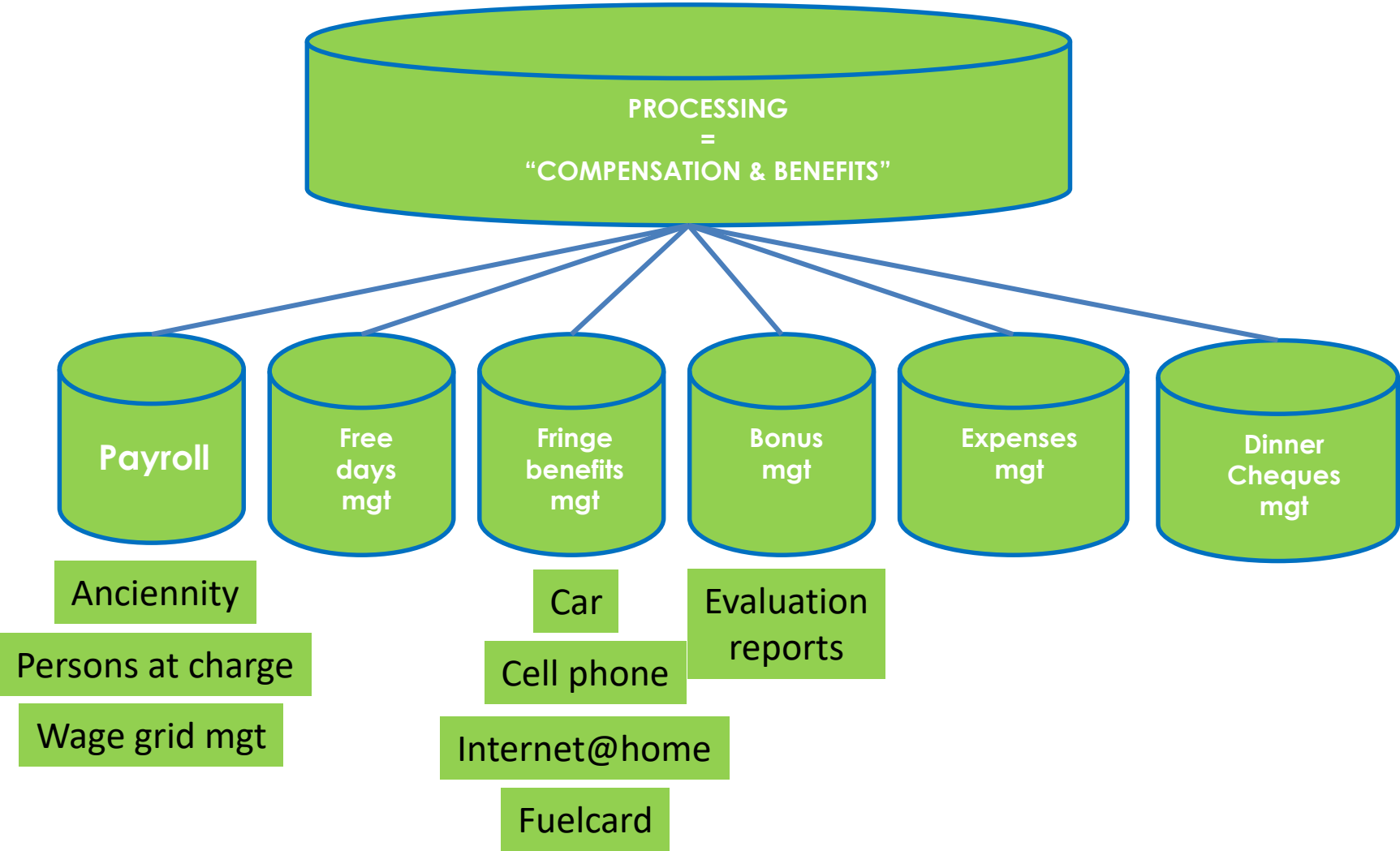
Beneficial for ALL stakeholders

Gates to the Data protection Impact Analysis (*)



(*) RealDPG method = one out of many motre asssement methods

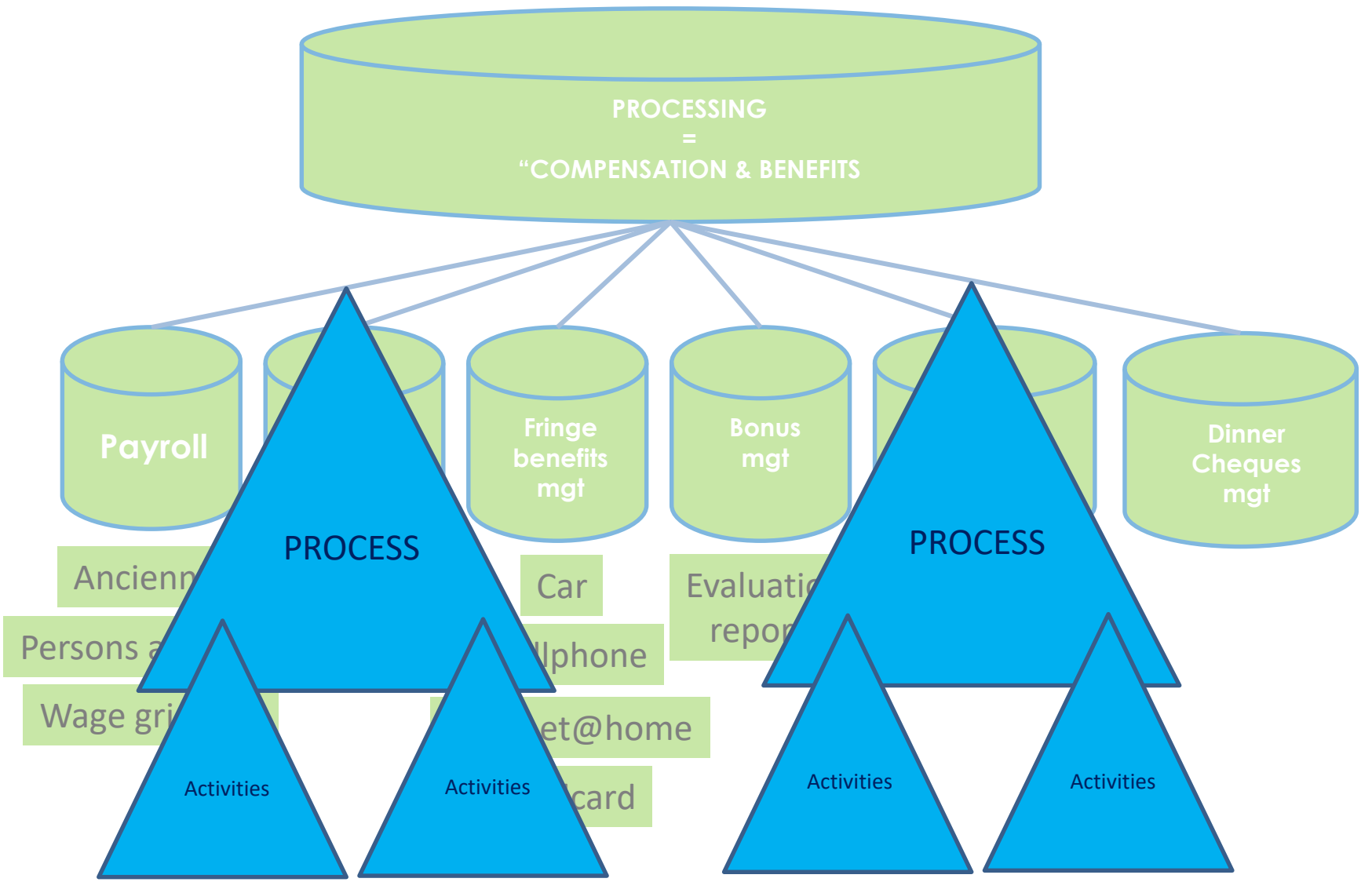
GDPR-sensitivity of business processes



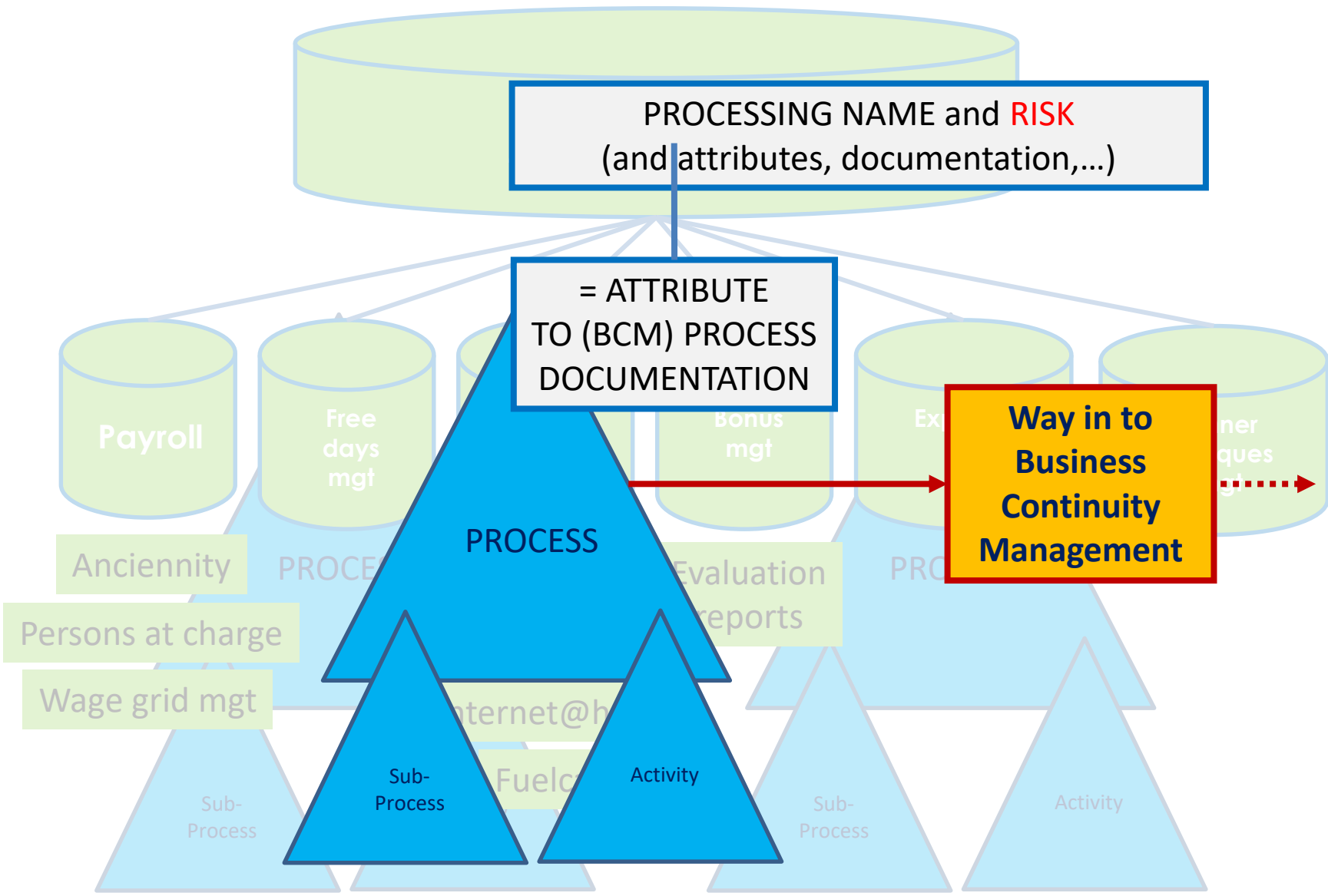
In how much detail?

Fly the right generic data-processing definition

Process >< Processing



Process >< Processing



3. Always perform a breach-check at any compromising event (technical or physical event)

- What processing(s) are involved?
- Nature of the breach (e.g. Hacking, cryptolocking,...)
- How long was the event ongoing before being confirmed?
- How many Data Subjects are affected?
- Is moral damage caused to Data Subjects?
- Is the material damage caused to the Data Subjects?
- Is physical damage caused to the Data Subjects?
- Are Rights and freedoms of the Data Subjects anyhow compromised?
- Is privacy of the Data Subjects anyhow compromised
- Is personally identifiable information becoming inaccurate?
- Is personally identifiable information becoming inaccessible?
- ...
- **Assess and make your conclusions...**

4. Make BCM part of the technical and organisational measures used to assure GDPR compliance

- Embed BCM into GDPR governance and vice versa
- Embed BCM in privacy by design / default
- Embed BCM in briefings, meetings, reviews
- Breach BCM = Breach GDPR !!

- Thank you, Any questions?



RealBCP.com
RealDPG.com
info@realbcp.com
Brochure
Quicktests

