
DEBT RECOVERY
EMPLOYMENT & HR
CONSTRUCTION & ENGINEERING
DEPENDABLE
COMMERCIAL
CLIENT SERVICES
LANDLORD
FOR YOU
DISPUTE RESOLUTION
COMMON SENSE
WILLS & ESTATES
RIGHTS

Understanding GDPR and how to make your business compliant Part 3

Adam Gilbert - Partner, Head of Corporate and Commercial

Ex-Shoosmiths and Shakespeares

vasanta group

wilko

Joined Else in 2015

Created numerous data protection, data breach and subject access request policies and procedures

Created, trained and helped businesses implement those procedures

Advised clients on data breaches and dealing with the ICO

else SOLICITORS

What we are going to cover in Part 1?

- What is the GDPR?
- Who does it apply to?
- Principles under GDPR
- Conditions for Lawful Processing - Overview

else SOLICITORS

What is the "GDPR"?

- GDPR stands for the General Data Protection Regulations
- Due to come into force on 25 May 2018
- It will replace the current Data Protection Act 1998

else
SOLICITORS

31 Days left
or
744 hours....

Let's get it over with....

- FINES - 4% of turnover or 20 million Euro.
- BUT... its not just about the fines.
- Great opportunity to re-engage with your customers/clients
- ICO have said that fines will be similar for similar offences under DPA

else SOLICITORS

Who does the GDPR apply to?

- 'Controllers' **and** 'Processors'.
- The definitions are broadly the same as under the DPA
- A controller says how and why personal data is processed
- Processor acts on the controller's behalf.

else SOLICITORS

What information does the GDPR apply to?

Personal data

The GDPR's definition is more detailed and makes it clear that information such as an online identifier – eg an IP address – can be personal data.

"personal data' means any information relating to an **identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

else SOLICITORS

What information does the GDPR apply to?

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data".

"racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

else SOLICITORS

Principles of GDPR

(a) processed **lawfully, fairly and in a transparent** manner; (***lawfulness and fairness***)

(b) collected for **specified, explicit and legitimate purposes**; (***legitimate purposes***)

(c) **adequate, relevant and limited to what is necessary**; (***limited processing***)

(d) **accurate and, where necessary, kept up to date**;(***accuracy***)

(e) for **no longer than is necessary** for the purposes for which the personal data are processed; (***necessity***)

(f) **using appropriate technical or organisational measures**. (***security***)

else
SOLICITORS

Conditions for Lawful Processing

- 6(1)(a) – **Consent** of the data subject
- 6(1)(b) – Processing is necessary for the **performance of a contract**
- 6(1)(c) – **Legal obligation**
- 6(1)(d) – **Protect the vital interests** of a data subject or another person
- 6(1)(e) – **Public interest or in the exercise of official authority vested in the controller**
- 6(1)(f) – **Legitimate interests**

else SOLICITORS

Specific rules regarding **sensitive data** - not enough time today but main ones are:

- Explicit consent
- necessary for carrying out obligations under employment, social security or social protection law
- necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care

else SOLICITORS

PART 2
How to become compliant and Updates

else
SOLICITORS

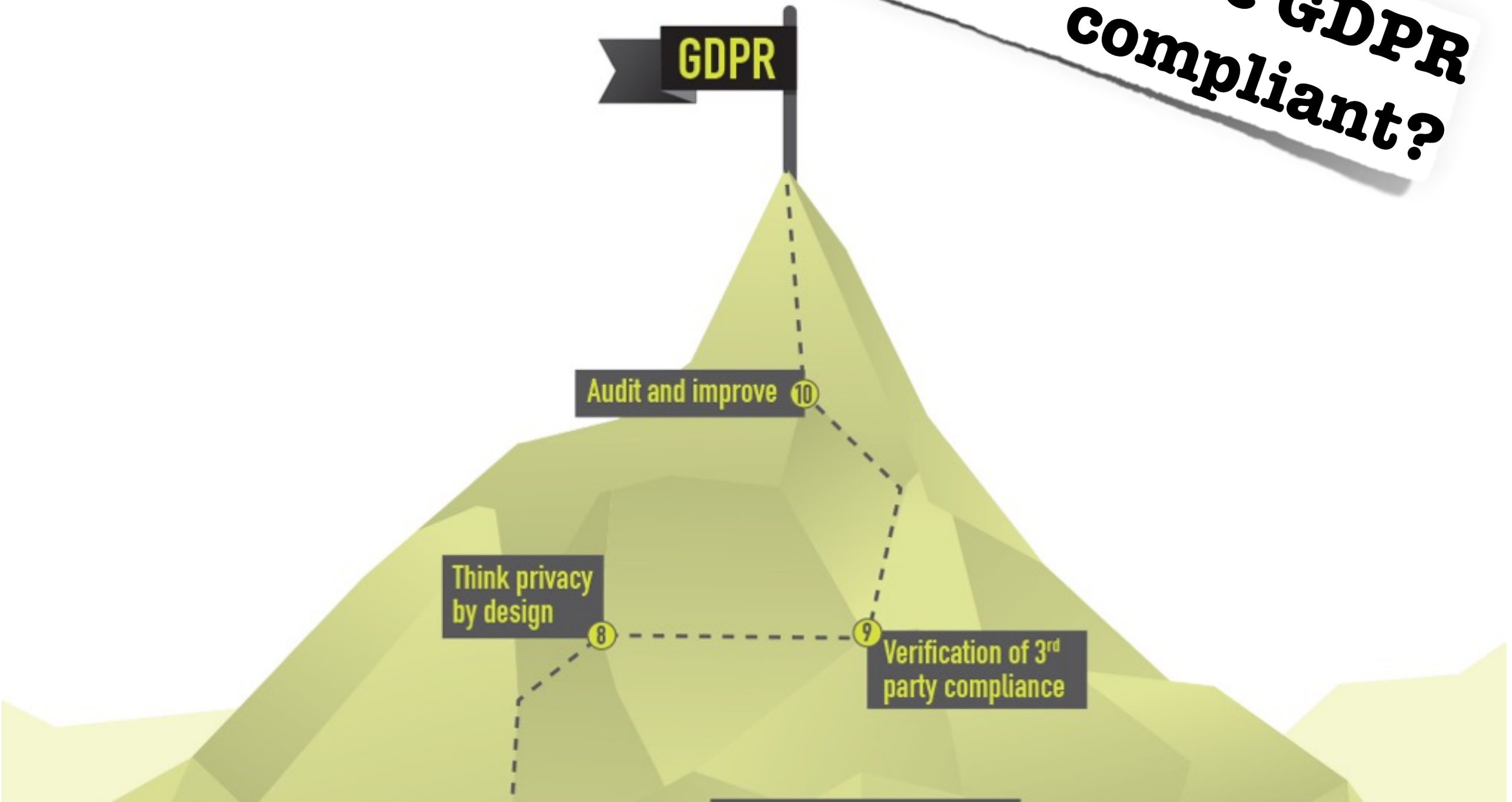
What we are going to cover in Part 2?

- How to become compliant - more details
- Conditions for Lawful Processing specifically:
  - Consent;
  - Contracts
  - Legitimate Interests
- Q&A

else SOLICITORS

else
SOLICITORS

How can you become GDPR compliant?



10 Steps to GDPR Compliance

else SOLICITORS

1. Become aware, gain commitment
2. Map your data, conduct a risk assessment
3. Deliver the specifics of the GDPR for your business
4. 3rd Party processing & security
5. Employee engagement & awareness
6. Policy, process & security that's fit for purpose
7. Robust breach management

party compliance

Policy, process & security that's fit for purpose

6

Robust breach management

7

Employ engage & awar

5

3rd Party processing & security

Map your data, conduct a risk assessment

2

1

Become aware, gain commitment

3

Deliver the specifics of th GDPR for your business

Following the Risk Assessment...

- What data are you holding?
- On what lawful basis are you processing it?
- It is imperative you start with the "right' basis
- You most select the most appropriate lawful basis (or bases) for each activity.
- Is it necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.
- Document the decision - which lawful basis applies to you to demonstrate compliance.
- Include the information about both the purposes of the processing and the lawful basis for the processing in your privacy notice.

else SOLICITORS

Is it….Consent?

- The most confused area….
- Consent may not be the best basis.
- You can't contact clients IF THEY HAVE REFUSED CONSENT
- Don't be tempted to use GDPR as a guise to contact those that do not want to be contacted.

Is it....Consent?

else SOLICITORS

NEWS

Home | UK | World | Business | Politics | Tech | Science | Health | Family & Education

Technology

Flybe fined for sending 3.3 million unwanted emails

29 March 2017

Flybe did not obtain people's consent before sending the marketing emails.

Royal Mail fined for sending 300,000 nuisance emails

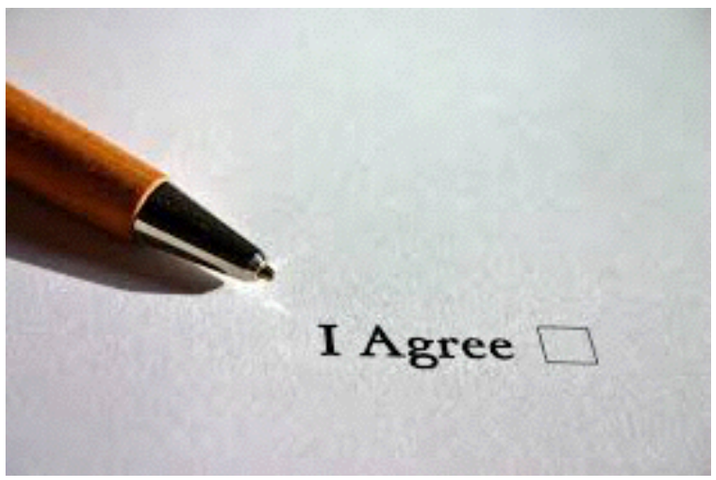
6 April 2018

Share

Royal Mail has been fined £12,000 for sending 327,000 nuisance emails to people who had opted out of receiving such information.

Is it....Consent?

- Consent must be freely given, specific, informed and unambiguous.
- Is consent is the most appropriate lawful basis for processing?
- Is the consent prominent and separate from your terms and conditions?
- Don't use pre-ticked boxes or any other type of default consent.
- Is the consent clear, plain language that is easy to understand?
- Tell them, who you are, why you want the data and what you're going to do with it.
- If you are doing different things with the data, you need to ask them in a granular way
- Tell them about any third party controllers who will be relying on the consent.
- Tell individuals they can withdraw their consent.
- Can refuse to consent without detriment.
- Avoid making consent a precondition of a service.



Doesn't just end there...record, record, record

- You MUST keep a record of when and how you got consent from the individual.
- You MUST keep a record of exactly what they were told at the time.

else SOLICITORS

Doesn't just end there... manage the consent

- Regularly review consents to make sure that nothing has changed.
- Think about putting in place a process to refresh the consent including any parental consents.
- Make it easy for individuals to withdraw their consent - tell them how to do so.
- Don't penalise individuals who wish to withdraw consent.

else SOLICITORS

A bad example of gaining consent

"Dear Adam

We are writing … curre… se.

For the purposes of th… contacting you to confirm whether you would like … your data.

If you would like us … need to do anything….."

else SOLICITORS

Is it....Contract?

- Will apply if you have a contract with the individual and you need to process their personal data to comply with your obligations under the contract; or
- You haven't yet got a contract with the individual, but they have asked you to do something as a first step (eg provide a quote)
- A contract does not have to be a formal signed document, or even written down - i.e. can be verbal
- If the processing is necessary for a contract with the individual, processing is lawful on this basis and you do not need to get separate consent.
- Remember to document your decision that processing is necessary for the contract, and include information about your purposes and lawful basis in your privacy notice.

Is it....Legitimate Interests?

- This can be broken down into a three-part test:
    1. Purpose test: are you pursuing a legitimate interest?
    2. Necessity test: is the processing necessary for that purpose?
    3. Balancing test: do the individual's interests override the legitimate interest?
- A wide range of interests may be legitimate interests.
- The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list.

else SOLICITORS

When can you rely on legitimate interests?

- Legitimate interests is the most flexible lawful basis
- If you choose to rely on legitimate interests, you take on extra responsibility
- Likely to be an appropriate basis where people would reasonably expect you to use in that way and that have a minimal privacy impact.
- **You will need to conduct a Legitimate Interests Assessment**

else SOLICITORS

When can you rely on legitimate interests?

- First, identify the legitimate interest(s). Consider:
    - Why do you want to process the data – what are you trying to achieve?
    - Who benefits from the processing? In what way?
    - Would your use of the data be unethical or unlawful in any way?

else SOLICITORS

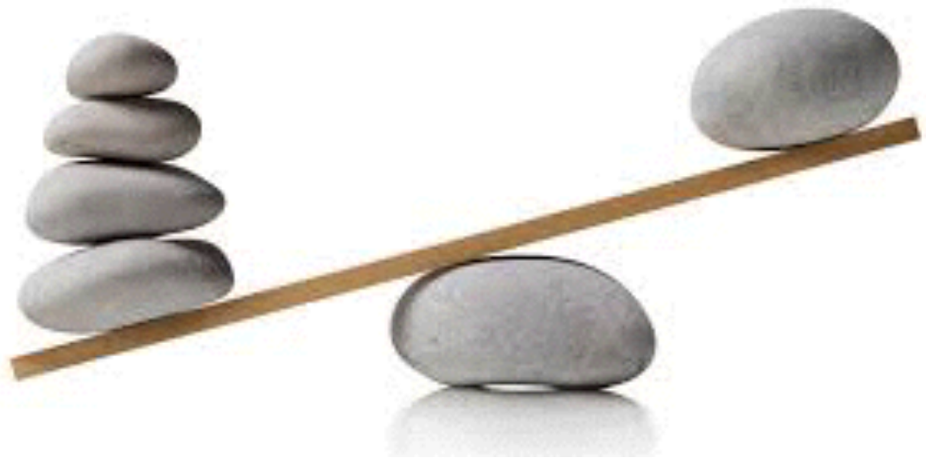
When can you rely on legitimate interests?

- Second, apply the necessity test. Consider:
  - Does this processing actually help to further that interest?
  - Is it a reasonable way to go about it?
  - Is there another less intrusive way to achieve the same result?

else SOLICITORS

When can you rely on legitimate interests?

- Third, do a balancing test. Consider the impact of your processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:
    - What is the nature of your relationship with the individual?
    - Is any of the data particularly sensitive or private?
    - Would people expect you to use their data in this way?
    - Are you happy to explain it to them?
    - Can you adopt any safeguards to minimise the impact?
    - Can you offer an opt-out?



else SOLICITORS

Some Examples

- Example 1 - FRAUD - An insurance company wants to process Personal Data as part of its business critical anti-fraud measures.
- Example 2 – RISK ASSESSMENT - Insurance companies need to "risk assess" potential customers to determine what products / services they can offer and the terms of those services. They also need claims information to prevent and detect fraud.
- Example 3 – WEB ANALYTICS - A social media platform uses diagnostic analytics to assess the number of visitors, posts, page views, reviews and followers in order to optimise future marketing campaigns.

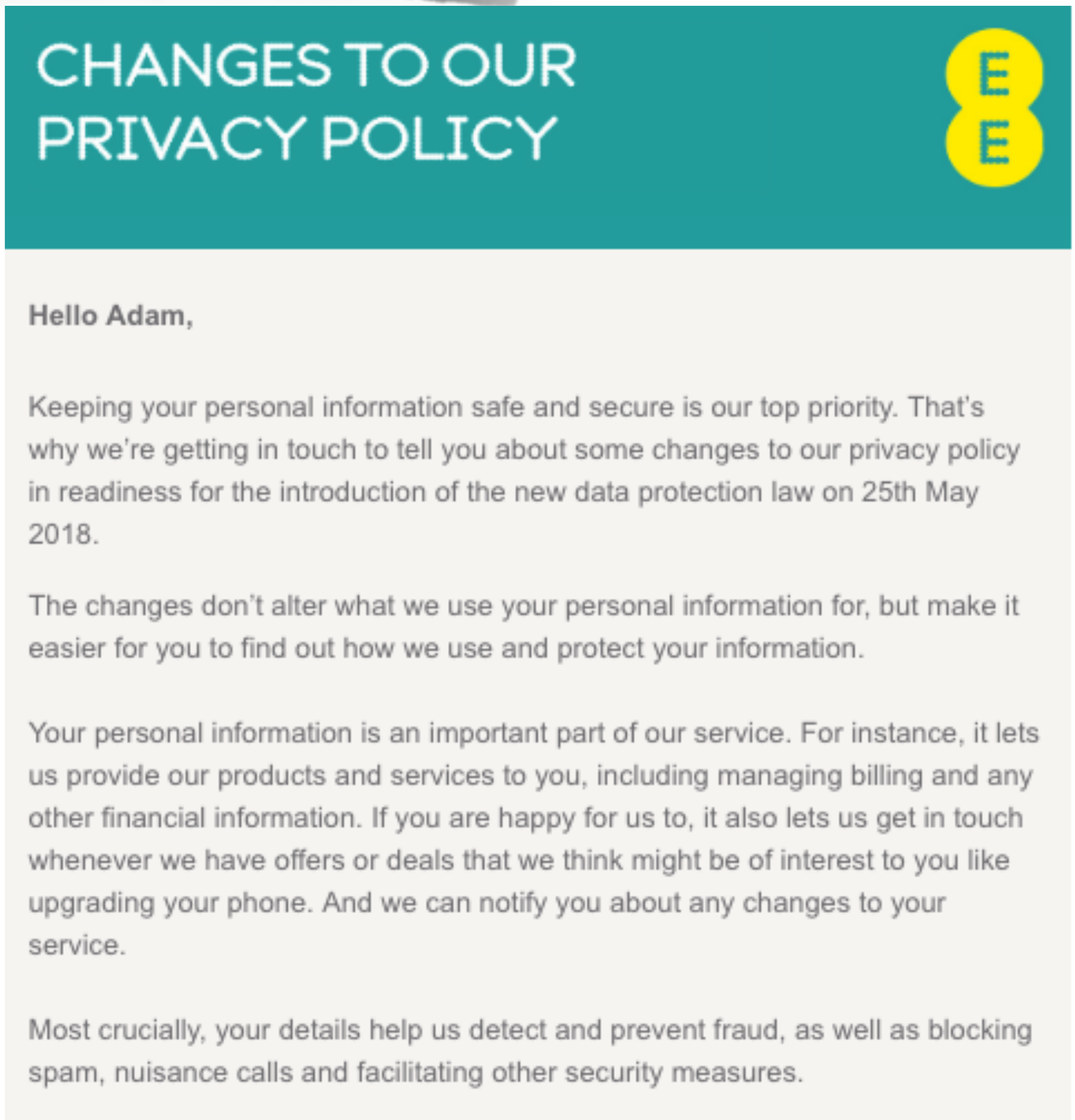
else SOLICITORS

Most obvious example - Marketing to existing customers

- You can market to customers under this basis provided:
  - They haven't opted-out
  - You only send them communications in relation to the same or similar goods and services;
  - YOU TELL THEM IN YOUR PRIVACY NOTICE
  - You must still comply with Privacy and Electronic Communications Regulations - "Soft Opt In"
  - You record the legitimate interest to evidence compliance

else SOLICITORS

A Good Example



else SOLICITORS

1. Become aware, gain commitment
2. Map your data, conduct a risk assessment
3. Deliver the specifics of the GDPR for your business
4. 3rd Party processing & security
5. Employee engagement & awareness
6. Policy, process & security that's fit for purpose
7. Robust breach management

1. Become aware, gain commitment
2. Map your data, conduct a risk assessment
3. Deliver the specifics of the GDPR for your business
4. 3rd Party processing & security
5. Employee engagement & awareness
6. Policy, process & security that's fit for purpose
7. Robust breach management
8. Think privacy by design
9. Verification of 3rd party compliance

Think privacy by design

8

9

Verification of 3rd party compliance

Robust breach management

7

6

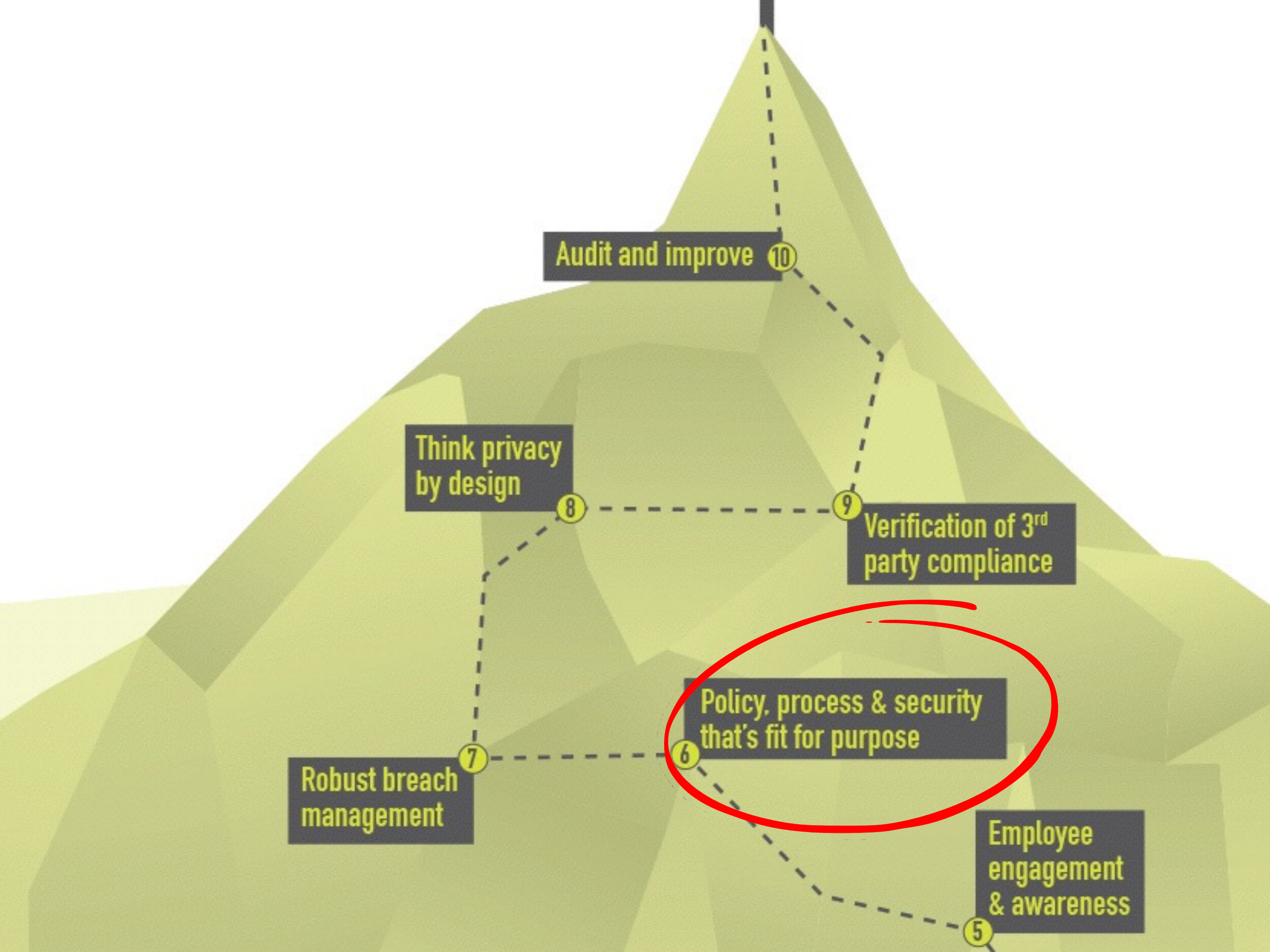
Policy, process & security that's fit for purpose

Employee engagement & awareness

5

3rd Party processing & security

4


Audit and improve 10
Think privacy by design 8
9
Verification of 3rd party compliance
Policy, process & security that's fit for purpose 6
7
Robust breach management
Employee engagement & awareness
5

Don't just use boilerplate policies

- Don't cut and paste from someone else!
- If you do "borrow" from others (not recommended or legal!), make sure that you at least remove the name from it
- ICO have said that one of the first places they will look is at your Privacy Notice - if its obviously someone else's then they are likely to seek enforcement action as it is not what your company/business does with data.

else SOLICITORS

Privacy Notices

- What are you holding?
- What are you doing with it?
- The different types of data
- How you will secure their data
- What you won't do with the data
- Bring it to their attention - think pop ups or links at the appropriate time
- BE TRANSPARENT!

Audit and improve 10

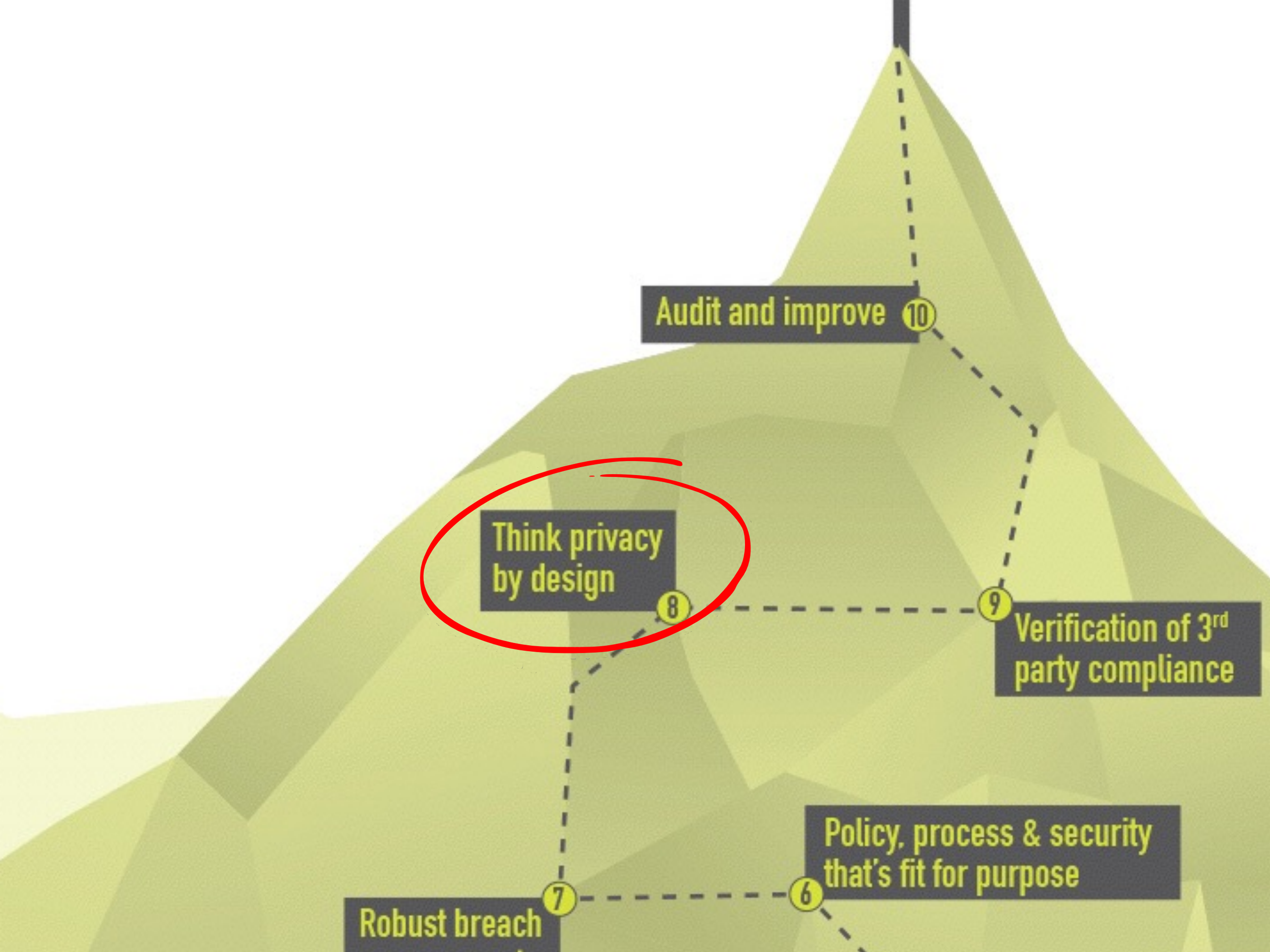
Think privacy by design 8

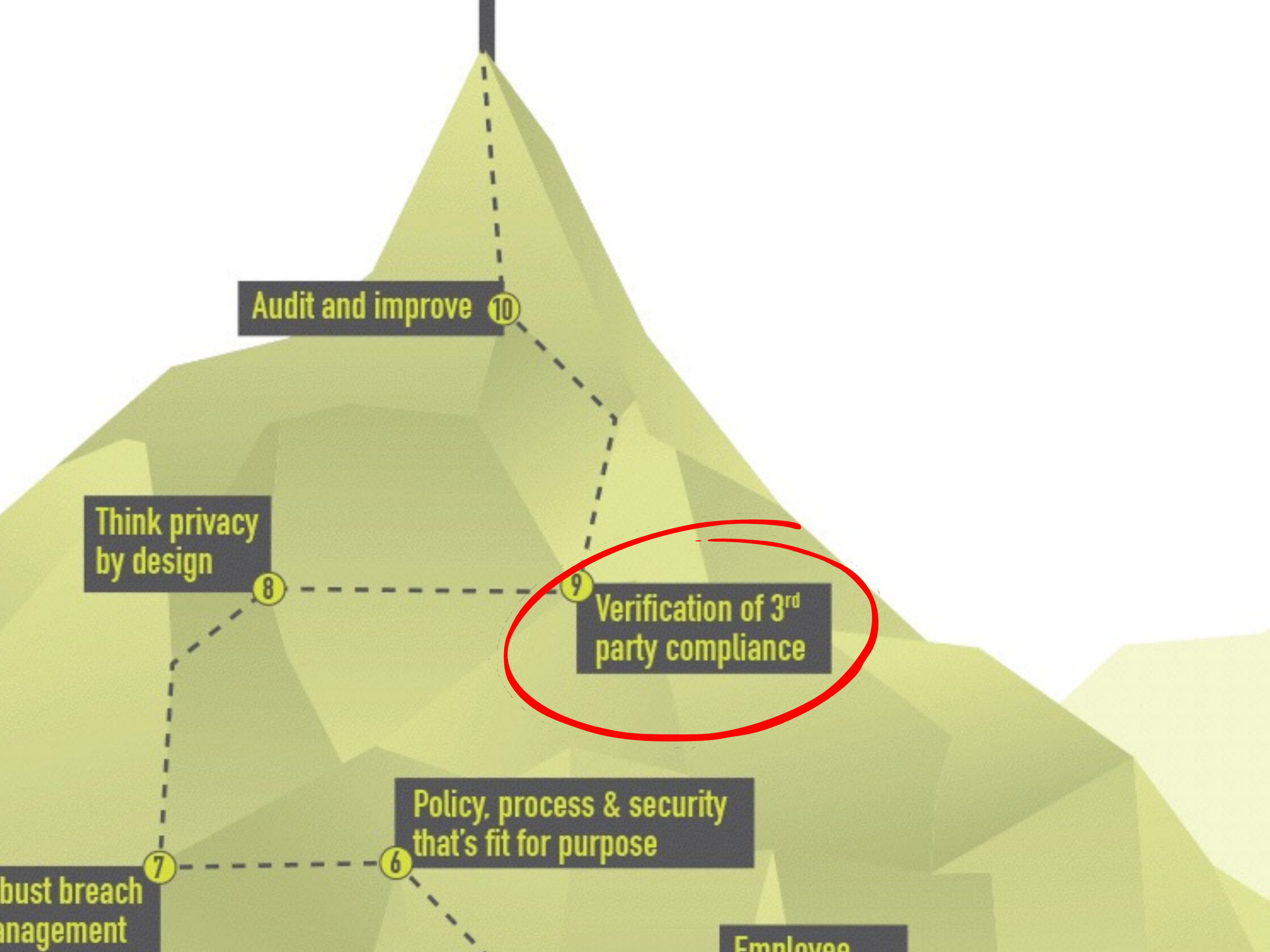
9 Verification of 3rd party compliance

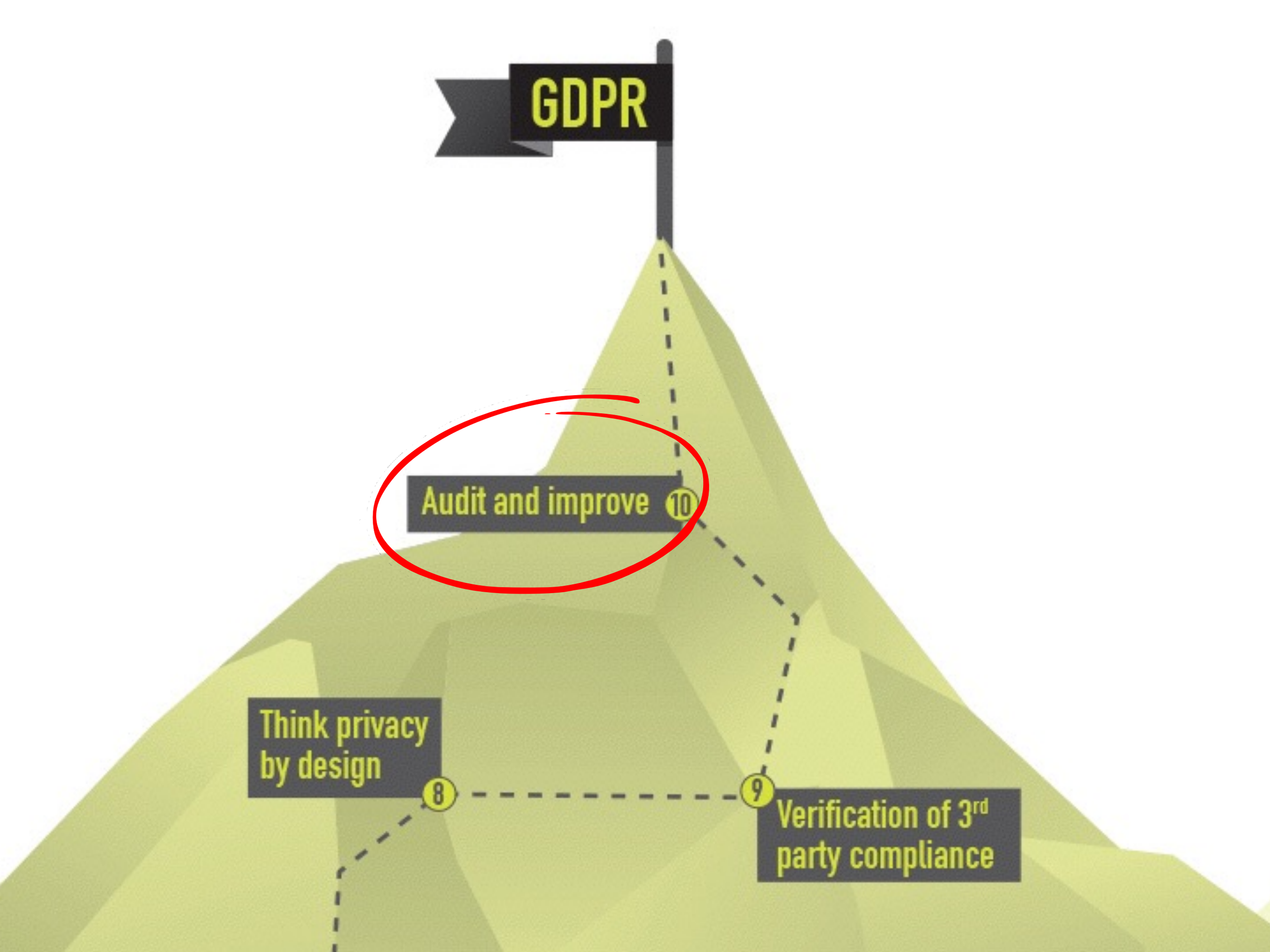
Robust breach management 7

6 Policy, process & security that's fit for purpose

Employee engagement & awareness 5


Audit and improve
10
Think privacy by design
8
9
Verification of 3rd party compliance
Policy, process & security that's fit for purpose
6
7
Robust breach


Audit and improve 10
Think privacy by design 8
9 Verification of 3rd party compliance
Policy, process & security that's fit for purpose 6
7
bust breach
anagement


GDPR
Audit and improve 10
Think privacy by design 8
9 Verification of 3rd party compliance

else
SOLICITORS

Summary -Action Plan

- Map the data
- Document lawful basis
- Review Privacy Policies
- Review consents (if relying on consent)
- Update Customer/Supplier contracts
- Train staff/inform staff
- Implement/review breach management

Q&A