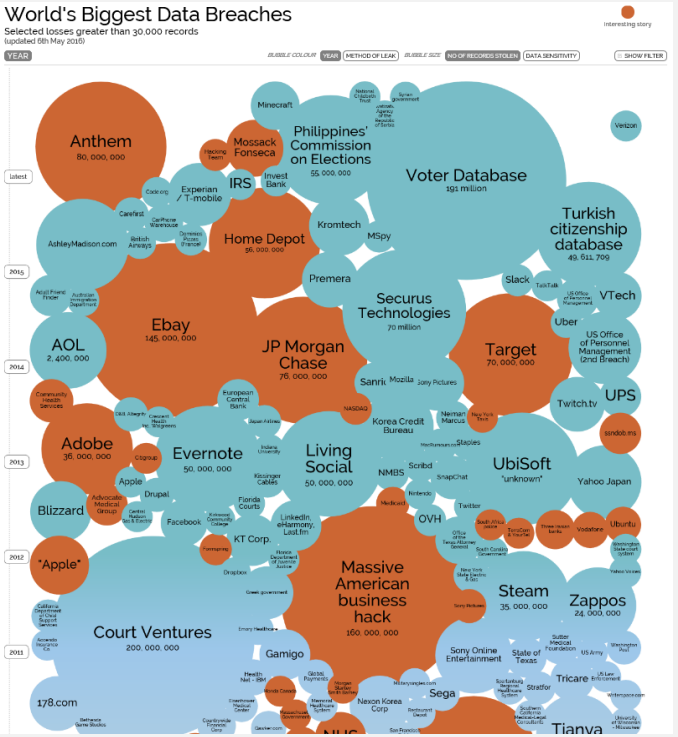
TURNING THE PRIVACY CHALLENGE TO YOUR ADVANTAGE

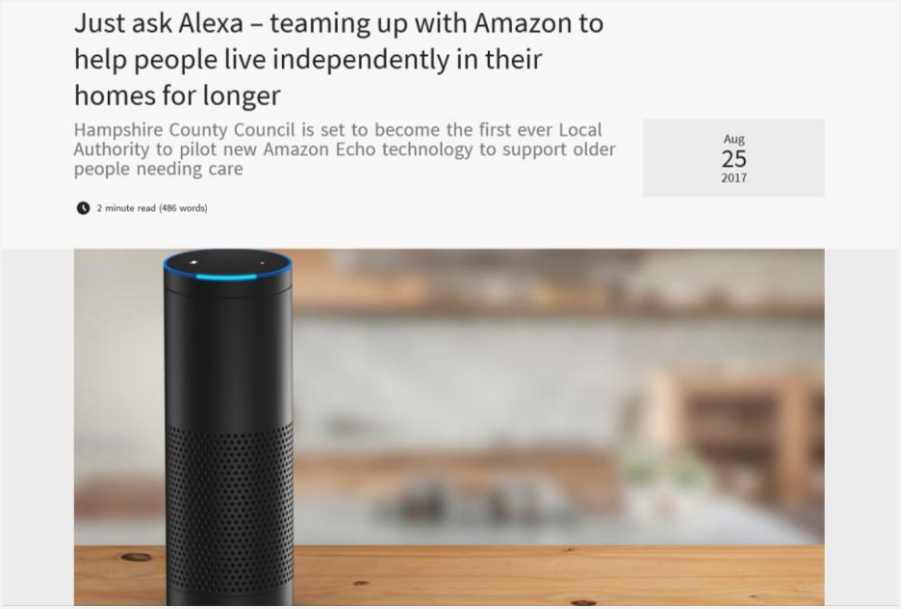
Higher and greater personal data breaches are forcing the debate on privacy protection

- For charities the damage of a personal data breach is not just the in terms of legal penalties or reputational damage, but in terms of the impact on that a person's life
- Covering campaigning, fundraising, or providing services to beneficiaries
- A breach of personal data could put someone who is already vulnerable at risk of harm, financial loss or even blackmail
- If you think cyber criminals don't target charities…
- Last year, the Information Commissioner's Office reported that the charity sector was responsible for 21 data security incidents in just one quarter.



Data-driven technologies are reshaping society and benefiting many

- Adoption of new technologies such as Alexa are helping make lives easier
- Join Dementia Research portal or the NIHR collaboration hub, are accelerating research into conditions that affect millions
- To operate in this data-rich world and reap the benefits for clients, charities need to take data protection seriously.



Higher fines for non-compliance for personal data breaches for EU resident citizens

An organisation risks fines of up to **4%** of the annual global turnover or **€20M**, whichever is greater

The following will, among other things, be considered when deciding the amount of the fine**:**

The **nature, gravity and duration** of the breach	The **character of the breach**, whether intentional or negligent	The **actions taken to mitigate the damage** suffered by individuals due to the breach	**Previous** breaches	Degree of co-operation with authorities to remedy the breach or **mitigate the adverse effects**

The growing scope of what is regarded as personal data

- Any information relating to an identified or identifiable person

Special categories of personal data considered sensitive include:

- Data concerning race or ethnic origin
- Data concerning political opinions
- Data concerning religious or philosophical beliefs
- Data concerning trade union membership
- Processing of genetic data or biometric data to uniquely identify a person*
- Data concerning health, sex life or sexual orientation*
- Identifiers such as location data or online identifiers

** Member States are given the right to introduce further conditions/limitations*

Overview of the major changes

Who?

Reach outside of EU:

Applicable to data leaving the EU

Strengthening the individuals rights:

The right of erasure

Capabilities within the organisation:

Data Protection Officer

How?

Proactive third-party information governance

Unambiguous consent

Privacy impact assessment

Privacy by design/default

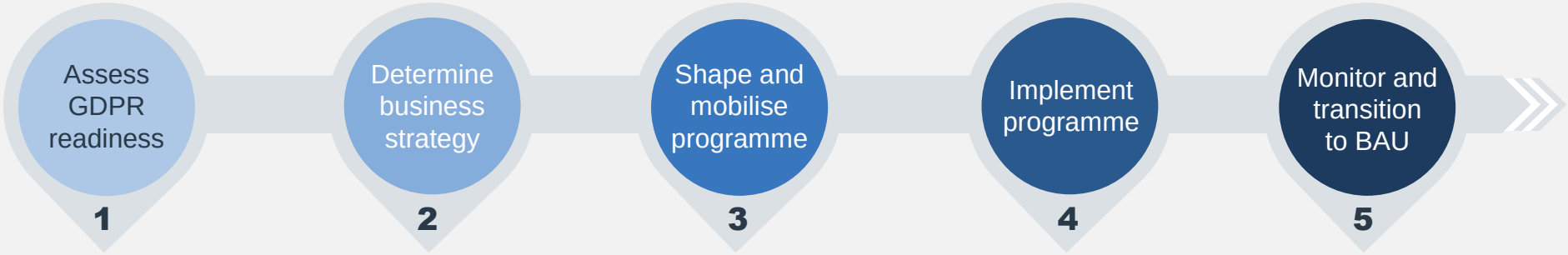
What?

Liability extension

Breach notification

Higher fines for non-compliance

Approach to GDPR from risk assessment to business as usual



- Assess maturity against GDPR
- Identify gaps for remediation
- Identify owners for mitigating actions

- Identify key business areas and processes
- Determine business opportunities
- Define consent model

- Determine priorities
- Build programme roadmap
- Create governance mechanisms and resource requirements

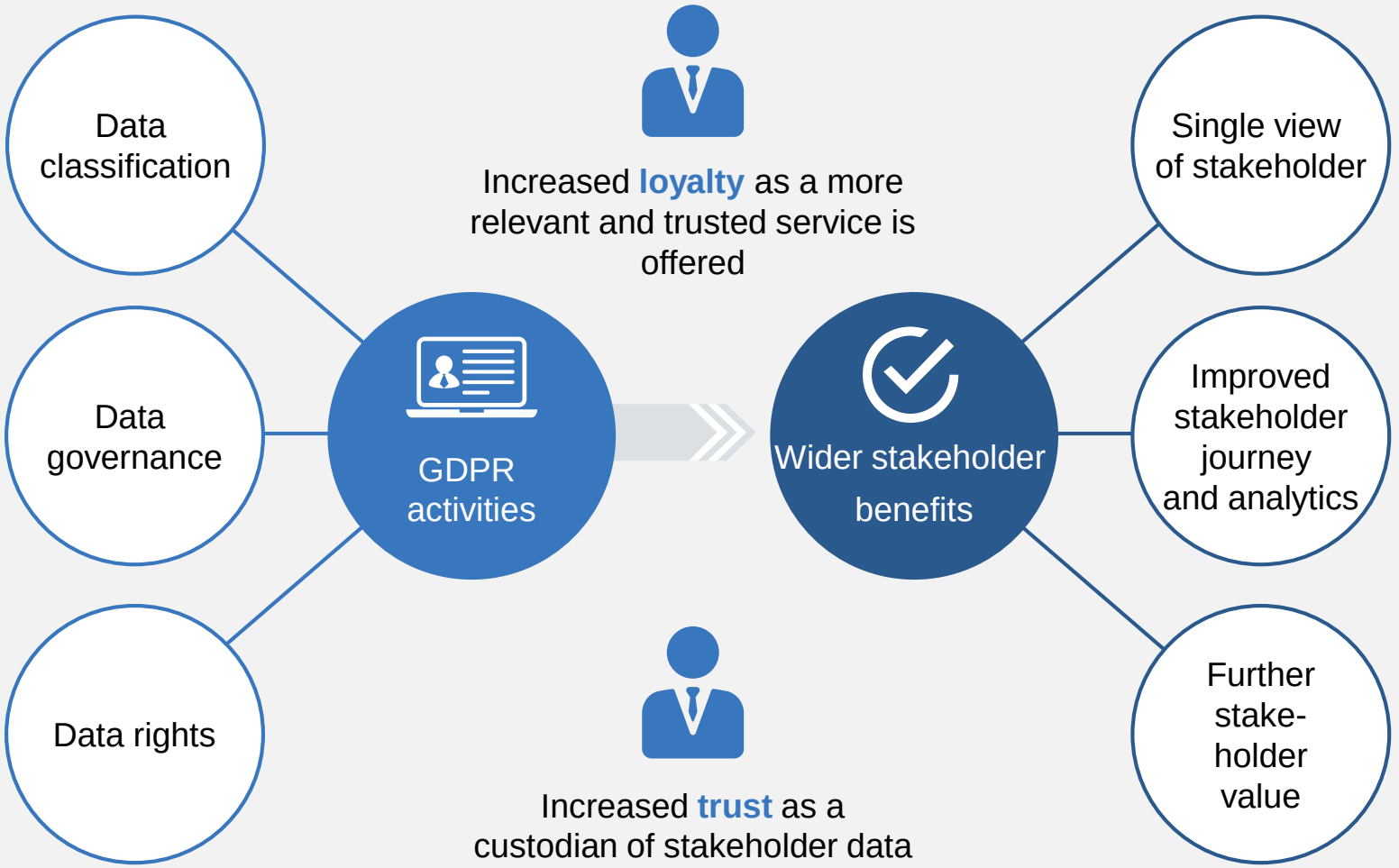
- Embed strategic, tactical and operational measures
- Optimise ‘ways of working’
- Determine transition to BAU (business as usual)

- Define KPIs and metrics for compliance reporting
- Establish monitoring mechanisms
- Operate as BAU

What are the key issues for charities?

- Fundraising - storing and using personal information to take donations and send out direct marketing material or using publicly available information to research and contact new supporters, either via post, emailing them, or sending them a text message
- Under GDPR this is processing personal data and you have legal obligations and responsibilities - you can only send direct marketing to individuals if you are able to do so under one of the 6 lawful bases
- **Consent** has to be a freely given, specific, informed and unambiguous indication of the individual's wishes
- **Legitimate interest** allows a charity to send direct marketing (post and live telephone calls) as long as an individual has not said 'no' to being contacted and it does not cause harm or override an individual's privacy rights
- Don't forget your employees, beneficiaries and volunteers…..

Privacy compliance should help, not hinder charities



Identifying and mapping where your personal data is within the organisation is a fundamental principle

Maintain inventory of personal data holdings

Identify the different types of data held (the nature of employee data, customer data, client-owned data, and data co-owned with another organisation) and where the personal data is held (eg servers, mobile devices, desktops, in the cloud, and geographic location)

Classify holdings by type

Agree legal basis for processing data

Work with each business unit to identify and agree the legal basis for processing personal data

This needs to consider options such as what would happen if the user decides to take back consent

Maintain flow charts for data flows

Agree data transfer mechanism

Identify cross-border flows, tracking its use of, and compliance with, cross-border transfer mechanisms

Once categorised, a set of remediation activities needs to address the risks

Prioritise all risks / activities according to set criteria and rate as high, medium and low

Absolute priority to address before May 2018

High risk example: Information security – maintain technical security measures (eg intrusion detection, firewalls, monitoring)

High risk example: Human resources (HR) process – there is a risk that physical document and record stores that hold personal information are not destroyed following the required business or regulatory holding period

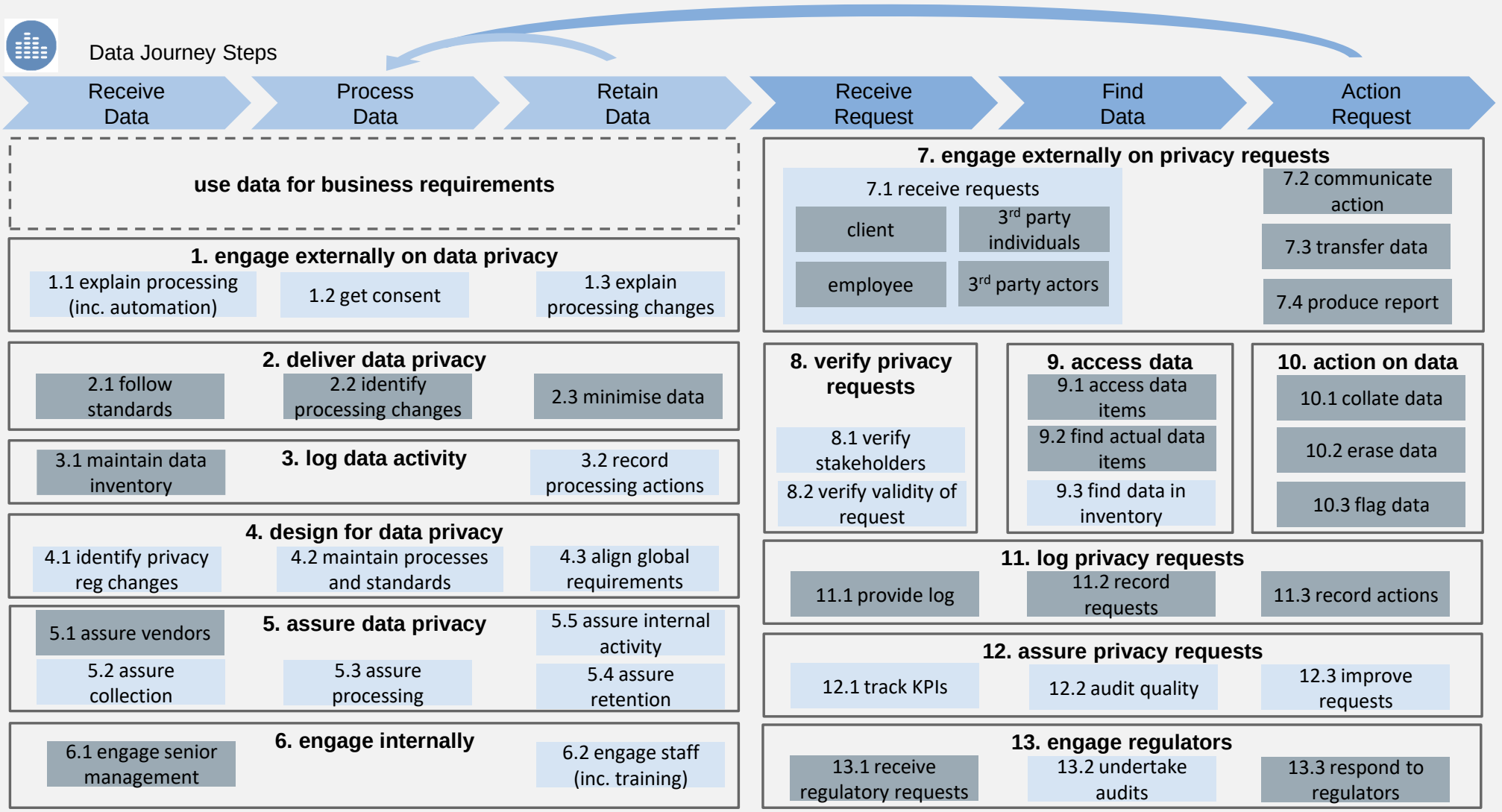
Consideration of some items before May and some after

Medium risk example: Legal – integrate data protection into practices for monitoring employees in terms of restriction and management approval

Consideration for post-May 2018

Low risk example: HR – integrate data protection into use of CCTV/video surveillance and correlation with local overriding laws on image capture

Embed privacy as business as usual



There are some key questions you should ask…

- Do you know where your fundraising contacts came from?
- Do you take personal data from social media?
- Do you know what your supply chain is doing with the personal data they hold on your behalf?
- Can your 3rd party supply chain respond within 72 hours when you have a data breach?
- Do you know if and how you are going to be targeted for information access requests?
- Have you every checked the dark web to see if personal data you have held is already out there?