The EU General Data Protection Regulation (GDPR) is Coming - What you need to do *now*

May 23, 2017

Rafi Azim-Khan, Partner & Head, Data Privacy, Europe

Steve Farmer, Counsel

Content

- GDPR Overview – “Noise”, Myths and Mis-selling “Tools”
- Key concepts e.g. Accountability
- Processing data (Principles, Legitimate Basis, Consent)
- Data subject rights
- Privacy by design and default
- Data security
- Service providers
- International transfers – BCRs (GDPR blessed, seriously consider)
- Data breach
- Key takeaways – GDPR Programs: What to do now & What NOT to do

pillsbury

GDPR Overview | In a nutshell…

- In force 25 May 2018 – direct effect
- Builds on existing concepts
- Key new rights for individuals and new obligations on both ‘data controllers’ and ‘data processors’
- Regulation: Harmonises DP law across the EU (and the UK will almost certainly continue post Brexit)
- Significantly extends territorial reach
- Supplier organisations face challenges
- Fines of up to EUR20m or up to 4% of worldwide turnover/revenue
- Biggest fines for inability to *show actual tailored advice and actions*
- *No “cookie-cutter” or software quick fix approach*

pillsbury

Overview | Likely impacts

GDPR will require most companies to:

- Change how they collect, use and globally transfer personal data
- Make changes to existing IT systems and software or implement new ones
- Update systems and controls
- Update privacy policies and terms and conditions
- Update data collection notices and consents
- Update websites and social media
- Change how they engage in marketing and advertising
- Change internal HR practices and training of employees
- Make changes to existing supplier and customer contracts

pillsbury

Overview | Accountability

- Accountability…

  "…is at the centre of all of this"

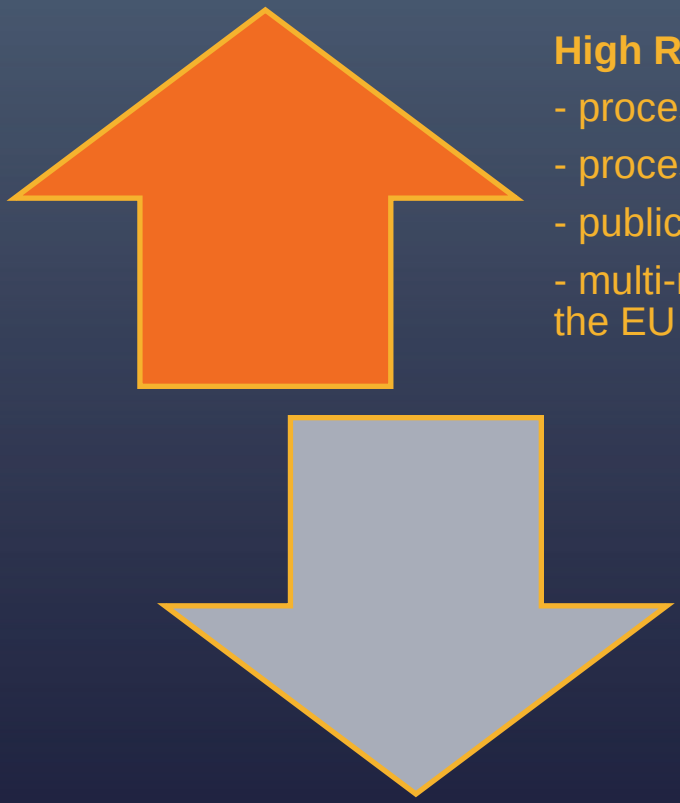
  "…cannot be bolted on: it needs to be part of the company's overall systems approach"

  [Elizabeth Denham – UK Information Commissioner, 17 Jan 2017]

- Comply AND demonstrate/prove compliance
- Increased focus by controllers on the types and amounts of data being collected and used

pillsbury

Overview | Risk factors for GDPR?



High Risk Entities:

- process consumer data
- process special category (sensitive) personal data
- public/government bodies
- multi-national companies headquartered outside the EU

Low Risk Entities:

- B2B entities (but not a pass)
- small amounts of consumer data
- entities with Binding Corporate Rules (BCRs) given synergy with GDPR obligations

pillsbury

Overview | Will my business be caught?

Territorial scope

1. Do you have an establishment in the EU?
2. Are you offering goods and services to data subjects residing in the EU (even if no payment is required by data subject)?
3. Are you monitoring data subjects residing in the EU?

If "**yes**" to any of those questions, GDPR will apply

pillsbury

Overview | What should I be doing now?

pillsbury

Overview | Parallels with NY Cybersecurity Requirements

- Policies, procedures and risk assessments
- Managerial involvement
- Chief Information Security Officer/Data Protection Officer
- Application security/privacy by design
- Focus on services providers
- Breach notification
- Separately, consider other State laws in the mix to dovetail if possible
- Benefits of uniform approach if possible (note also shifting global trends e.g. S. Africa, Australia, Singapore etc. positive view of BCRs)

Overview | UK developments

- The UK regulator has indicated that EU rules will apply to UK regardless of Brexit
- If UK leaves single market, it will need an “adequacy decision” to receive personal data from the EEA, hence adopting GDPR

pillsbury

GDPR

KEY CONCEPTS

pillsbury

Key concepts | Personal data

- Four-step test

any information

Includes data with meaning such as technical and transactional data

Form is not relevant

relating to

Content related to a person, i.e. name, job title, address etc.

Includes opinions of a natural person or information about their actions

an identified or identifiable

"Identifiable" includes the use of additional information held by a third party

Data which has been assigned random numerical identifiers may still be considered Personal Data

IP addresses and online identifiers may be considered Personal Data

natural person

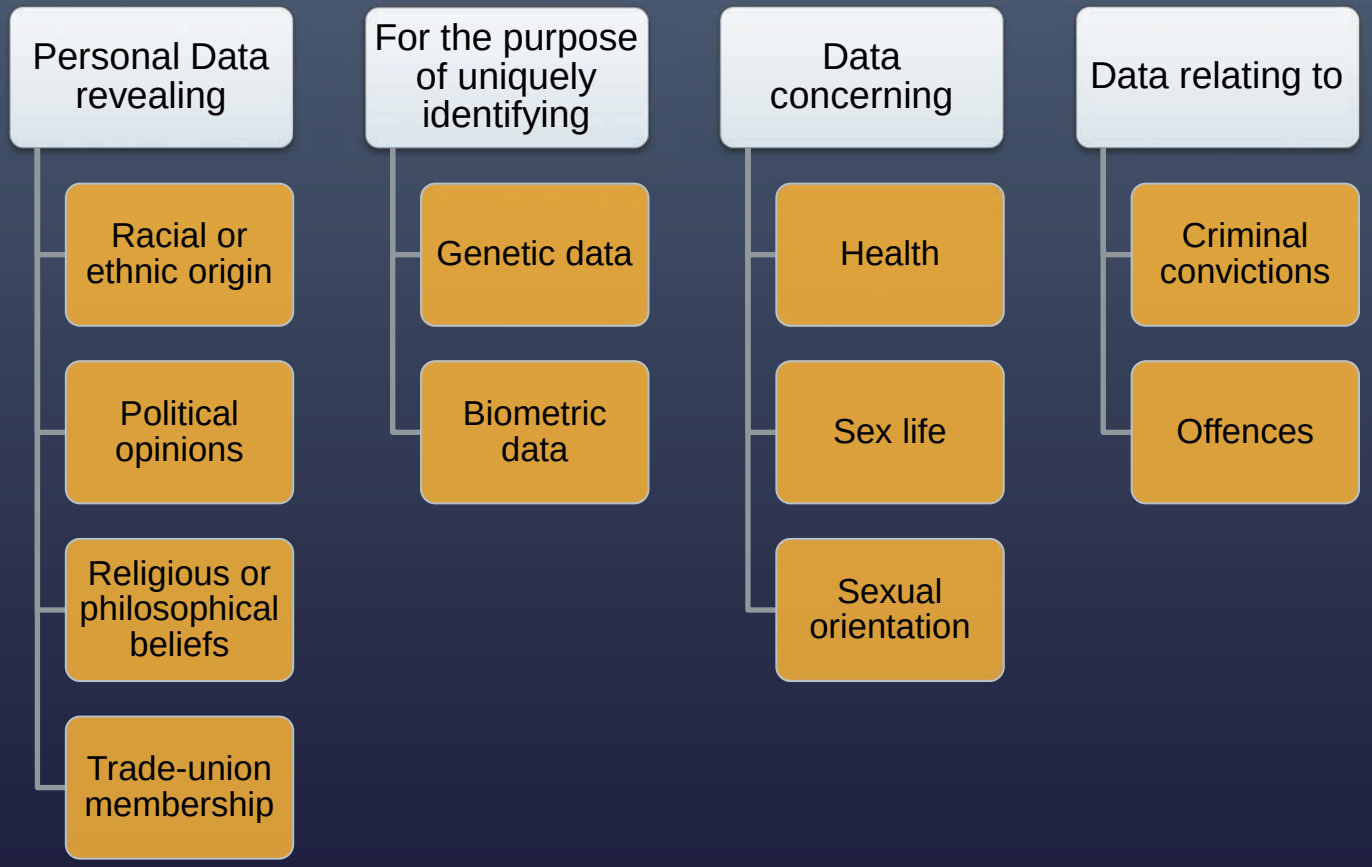
Only living natural person

Does not apply to legal persons

Will apply to sole traders

pillsbury

Key concepts | Special (sensitive) personal data



pillsbury

Key concepts | Data protection roles

Supervisory Authority

Data Processor

Data Controller

Data Subject

pillsbury

Key concepts | Controller and Processor

Data Controller

- A natural or legal person, public authority, agency or other body
- Alone or jointly with others
- Determines the purposes and means of the processing
- Wider legal obligations

Data Processor

- A natural or legal person, public authority, agency or other body
- Processes personal data on behalf of the controller
- Accountability obligations

GDPR

PROCESSING DATA

pillsbury

Processing data | Principles

- Data protection principles are broadly unchanged:

1	Lawful, fair, transparent	4	Accuracy
2	Specified, explicit & legitimate purpose	5	Storage limitation
3	Data minimization	6	Integrity and confidentiality

- Transparency Controller must provide more information to individuals about its processing of their data

pillsbury

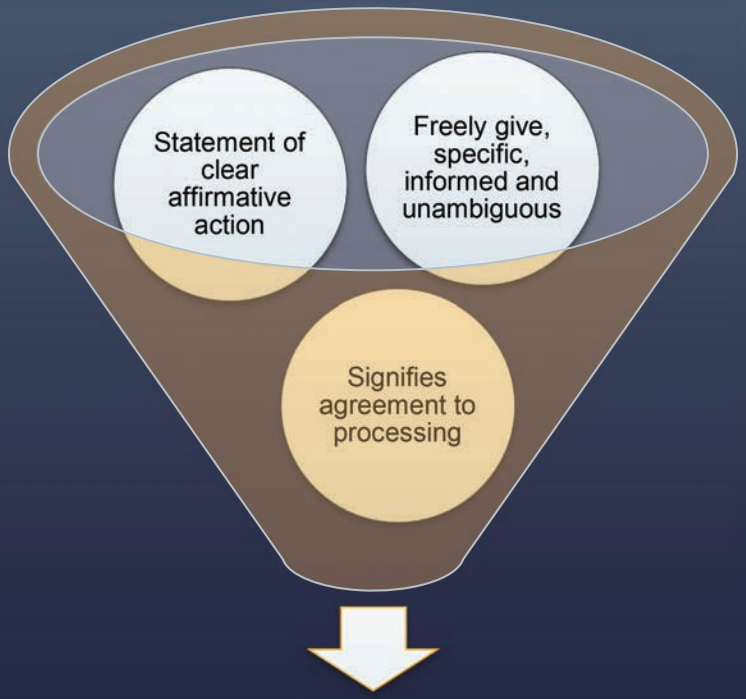
Processing data | Legitimate basis

- Legitimate basis

Consent **Contract** **Legal Obligation** **Vital Interests** **Public Interest** **Legitimate Interest**

pillsbury

Processing data | Consent

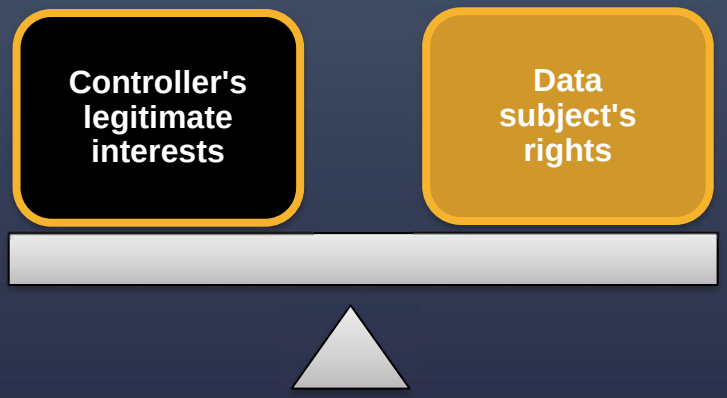


Consent

- Cannot infer from silence, pre-ticked boxes or inactivity
- Must be verifiable
- Must cover all anticipated activities
- Can be withdrawn
- May require changes to Ts&Cs and privacy notices
- International transfers, sensitive data, consent must also be ‘explicit’

pillsbury

Processing data | Legitimate interest



- Balancing test – 'careful assessment' required
- E.g. direct marketing purposes or preventing fraud
- Must inform data subject of legitimate interests pursued
- No automatic right to require controller to cease processing
- Right to object: Only continue if legitimate interests override the individual's rights

pillsbury

GDPR

DATA SUBJECT RIGHTS

pillsbury

Data subject rights | Overview

- New, enhanced and existing rights
- New or significantly enhanced rights include:
  - Transparency and information: Enhanced information to be provided to data subjects
  - Right to erasure (‘right to be forgotten’)
  - Right to data portability
- Mandated clauses: Data Processor must assist Data Controller (including through ‘technical and organisational’ means) to respond to requests

pillsbury

Data subject rights | Right to erasure

- Erasure without undue delay where e.g.:
  - Original purpose no longer applies
  - Consent withdrawn (and no other legal ground exists)
  - Objections to claimed ‘legitimate interests’ (and no overriding legitimate grounds) + Objections to direct marketing
  - Unlawful processing
- Some exceptions, e.g.:
  - Freedom of expression: Member States must balance data protection and journalism, academic artistic or literary expression
  - Compliance with legal obligations
  - Legal claims

pillsbury

Data subject rights | Right to portability

- Right to receive and transfer data to an alternative provider in a **structured, machine-readable format** (e.g. .cvs format)
- Applies where data provided by the individual and processing based on consent or pursuant to a contract
- Some types of data are excluded (e.g. resulting from website algorithms)
- Blurs line between ‘data protection’, consumer protection and competition law?
- Article 29 WP Guidance: **Broad** interpretation

pillsbury

Data subject rights | Transparency and information provision

- What is a Privacy Notice?

Format	Content
• Intelligible and easily accessible form • Clear and plain language • Conciseness • Visualisation • Free of charge • Layered online privacy notice	• Identity and contact details • Purpose and legal basis • Recipients • Intention to transfer data • Legitimate interests • Storage period • Data subjects' rights • Statutory or contractual requirement • Automated decision-making

pillsbury

GDPR

PRIVACY BY DESIGN AND DEFAULT

pillsbury

Privacy by design and default | Overview

- Key tools for demonstrating compliance under the ‘accountability’ principle
- By Design: Take measures designed to e.g.:
  - Pseudonymise and minimise data
  - Integrate necessary safeguards
  - Meet requirements of the GDPR, protect data subject rights
- By Default: Ensure by default, only personal data necessary for each specific purpose of the processing is processed

pillsbury

Privacy by design and default | Data impact assessments

- "*assessment of the impact of the envisaged processing operations*"
- Where processing is likely to result in **high risk**
- No definition of 'high risk':
  - A35(3) examples: profiling, large-scale processing of sensitive data
  - R89: new technologies, new kind and where no prior DPIA
  - R91: where could "…prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale…"
- Must consult Supervising Authority prior to processing where a DPIA indicates an unmitigated high risk

pillsbury

GDPR

DATA SECURITY

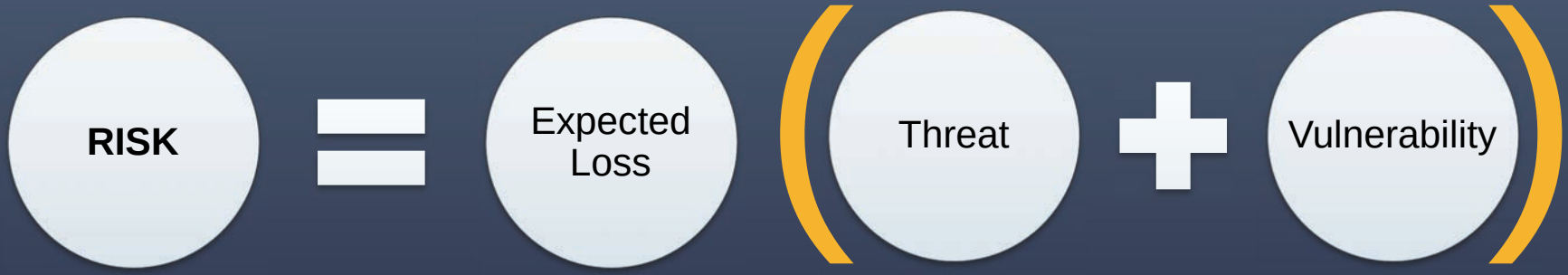
pillsbury

Data security | Overview

- The Data Controller and Data Processor shall provide…
  - appropriate technical and organisational measures
- To ensure…
  - a level of security appropriate to the risk
- Taking account of…
  - the state of the art
  - costs of implementation
  - the nature, scope, context and purposes of processing
- Adherence to an approved code of conduct or approved certification may go some way to demonstrate compliance
- Data security under GDPR is not heavily prescriptive in order to prevent the requirements becoming outdated. Organisations must conduct risk assessments and consider technological advances

pillsbury

Data security | Risk assessment factors



Key to equation

May be electronic, physical or paper-based

Threat agents may be people (not always with malicious intent), technology or acts of nature environmental factors

Digital or Physical

May include ineffective access management, unsecured communication, poor coding and configuration, or poor/lack of training awareness

pillsbury

Data security | Records of processing activities

- Records of all processing activities must be stored
- Requirement does not apply to entities or organisations which employ fewer than 250 persons unless the processing it carries out:
  - is likely to result in a risk to the rights and freedoms of data subjects;
  - is not occasional; or
  - includes special categories of data
- Records shall be in electronic form and will need to be supplied to a data authority where required

pillsbury

GDPR

SERVICE PROVIDERS

pillsbury

Service providers | Overview

- Data Controllers can only use Data Processors providing sufficient guarantees to implement appropriate technical and organisational measures
- Data Processors must show “expert knowledge, reliability and resources”
- GDPR does not mandate nature of the required ‘guarantees’:
- Arguable this is satisfied by specified security obligations
- Resist requests for onerous warranty, representation or undertaking protection

pillsbury

Service providers | Mandatory contract terms

Overarching requirement	Provision of 'sufficient guarantees'
'Core' obligations	Process on controller's instruction only
	Ensure employees keep data confidential
	Keep the personal data secure
	Flow these clauses down to subcontractors
'Information and assistance' obligations	Assist with fulfillment of data subject rights
	Security, breach, impact assessment assistance
	Delete or return personal data
	Provide information and allow for audits

pillsbury

GDPR

INTERNATIONAL TRANSFERS

pillsbury

International transfers | Overview

- Adequacy decisions
  - Findings by European Commission that certain countries, or sector within a country, adequately protect EU data by law, obviating the need for additional safeguards
- Appropriate safeguards
  - Mechanisms through which organisations can commit to protect personal data to facilitate ongoing and systematic international transfers
- Derogations
  - Limited circumstances where organisations may transfer under specific conditions

pillsbury

International transfers | Adequacy decisions

- Andorra
- Argentina
- Canada (commercial organisations)
- Faeroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay

[USA Not on list – Shield option but health warning!]

pillsbury

International transfers | EU-U.S. Privacy Shield

Who?
Organisations under FTC enforcement

What?
Voluntary self-certification programs

How?
Commitment, publicity, public disclosure, implementation and renewal

pillsbury

International transfers | EU-U.S. Privacy Shield

Privacy Shield principles

- Notice
- Choice
- Accountability and onward transfer
- Security
- Data integrity and purpose limitation
- Access
- Recourse, enforcement and liability

pillsbury

International transfers | EU-U.S. Privacy Shield

- Is Privacy Shield a viable option?

Pros	Cons
• European Commission and US Government have tried to address Safe Harbor weaknesses • Improvements to its original version should help a bit to overcome objections from EU data protection authorities • It helps avoid cumbersome contract negotiations compared to SCC/MCC and ad-hoc contracts	• Adequacy highly likely to be challenged in the Court of Justice of European Union, so legal uncertainty will continue • There is a review process after which the EU may suspend or revoke the agreement • Continued scepticism by many EU data protection authorities • Likely to be additional compliance scrutiny from US regulators, as compared to Safe Harbor

pillsbury

International transfers | Appropriate safeguards

Standard data protection clauses (SCC/MCC model clauses)

Pros

- Freely available and no substantial drafting required
- Pre-approved as lawful transfer method across the EU
- Filing formalities relatively straightforward
- Suitable for one-off transfers

Cons

- Cumbersome as very strict non-negotiable requirements
- Unworkable for multiple and evolving transfers
- Subject to administrative requirements in most of the EU
- Risk of non-observance by data importers

Approved codes of conduct/certification mechanisms

- Binding commitments made to private, accredited third parties, for ensuring and demonstrating compliance to regulators and data subjects
- Multipurpose; incorporated throughout the GDPR
- No clear how these will work in practice

Ad hoc contractual clauses

Pros

- Greater flexibility than model clauses
- If mirroring model clauses, less likely to be challenged
- Greater likelihood of compliance with requirements
- Suitable for evolving transfers

Cons

- Greater expenditure due to bespoke drafting
- More cumbersome filing and authorisation requirements
- Delay caused by dialogue with data protection regulators
- Risk of eventual non-approval

pillsbury

International transfers | Appropriate safeguards

- Best option for many: Binding Corporate Rules (GDPR "blessed")

Who?	What?	How?	Why?
• Companies engages in joint economic activity • Corporate groups and groups of enterprises • Data Controller and Data Processors	• Internal and legally biding rules • Expressly conferred enforceable rights of data subjects	• Approval by supervisory authority • Detailed conditions for transfers	• Many benefits • GDPR approved • Much better flexibility • Global not just EU/EEA • Avoids problems of MCCs • Avoids risk of Shield • Low administrative burden post implementation

pillsbury

International transfers | Appropriate safeguards

- We are one of very few firms to have actually successfully applied and secured BCRs for clients
- New GDPR “gold standard”: BCRs are designed to allow multinational companies to adopt a policy suite with rules for handling personal data that are binding on the companies within the group
- Recital 110 allows for corporate groups and groups of enterprises to rely on approved BCRs as an appropriate safeguard to transfer data
- If the supervisory authorities approve the rules, the company is considered free to transfer personal data within its organisation around the world (better than Shield which is just transatlantic)
- Article 46 of the GDPR lists minimum requirements of BCRs e.g. application of GDPR principles
- Benefits include high flexibility and low burden post implementation

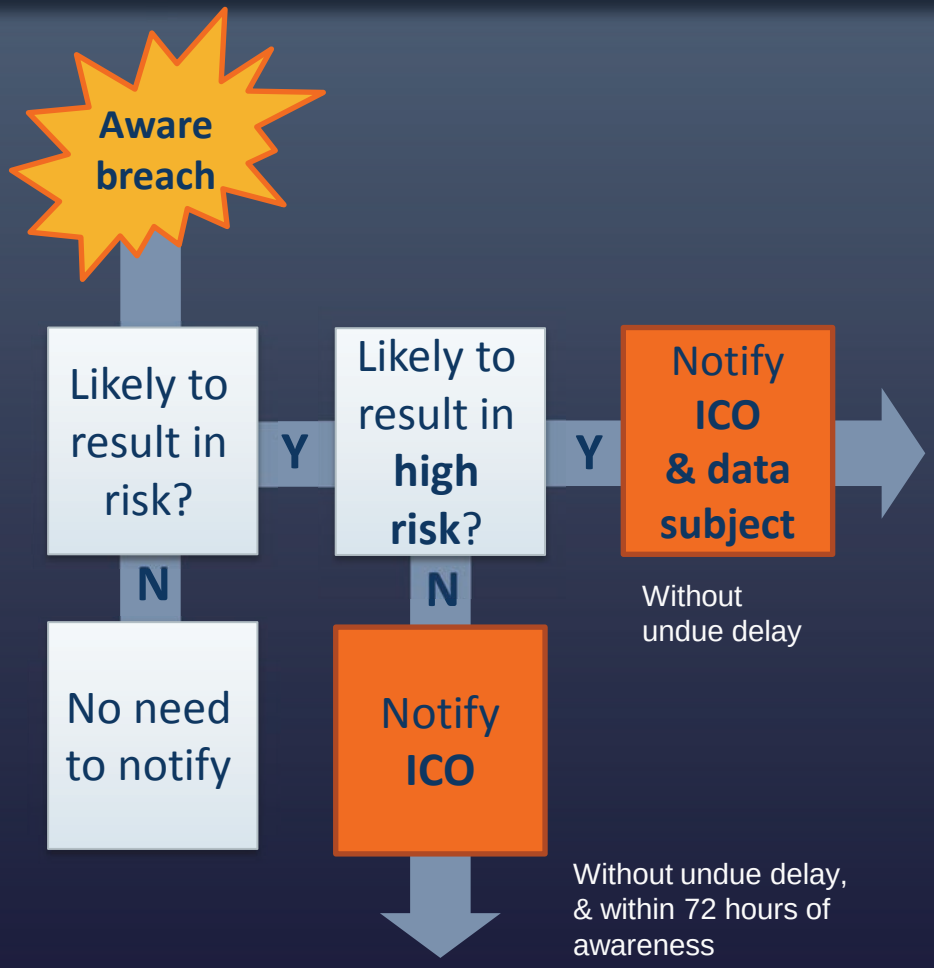
pillsbury

GDPR

DATA BREACH

pillsbury

Data breach | Appropriate safeguards



- Breach - breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access
- Risk - could include:
  - Physical, material or non-material damage
  - Discrimination, identity theft or fraud, financial loss, reputational damage, other significant disadvantage
  - Loss of sensitive data
  - Large amounts of data
- High risk - Not defined. Higher likelihood or more material consequences of the above?

pillsbury

Data breach | Appropriate safeguards

- Data Controller must notify:
  - ICO without undue delay and ‘where feasible’ within 72 hours
  - Data subject in ‘clear and plain language’ without undue delay (taking into account ’nature and gravity’ of breach)
- Limited exceptions to DS notification: e.g. data was encrypted or where notification would involve disproportionate effort (but note public communication still required)
- Data Processor must notify controller ‘without undue delay’ after becoming aware

pillsbury

Data breach | Fines

‘Serious’ breaches

- Higher of EUR20m, or 4% worldwide annual turnover/revenue
- E.g. breach of processing conditions, consent, subject rights

Other breaches

- Higher of EUR10m, or 2% worldwide annual turnover/revenue
- E.g. breach of security, engagement of processors

Contract considerations

- No settled practice yet
- Data Controllers will likely continue to seek uncapped liability for data breaches whilst seeking to cap their own liability
- Cross indemnities?
- Separate cap for breaches?
- Consider link to confidentiality

pillsbury

Key Takeaways – GDPR Program Steps

- Need to act NOW – get Board level buy in and budget – we can help
- Start GDPR Program and consult with genuine experts with close connections with key regulators/enforcers – avoid the “spin”
- Seriously consider BCRs at the same time with advice from those who have not just researched it or even applied but have secured BCRs
- Practical steps can include interviews and workshops to help you properly scope, identify and prioritise data use, flows and “to do” items
- Beware mistakes of overly relying on “tools”, cookie-cutter consultant fixes and software “solutions” that are flooding the market
- The GDPR brings potentially enormous fines and “souped-up” supervising authorities ready to enforce – not going away
- Don’t freeze in the headlights! Initial steps are small and inexpensive

pillsbury

pillsbury

Contact Details

Rafi Azim-Khan | Partner

rafi@pillsburylaw.com

London
Tower 42, Level 21
25 Old Broad Street
London, EC2N 1HQ
F +44.207.847.9519
M +44.7944.962.380

Silicon Valley
2550 Hanover Street
Palo Alto
CA 94304
F +1.650. 233.4500

Steve Farmer | Counsel

steven.farmer@pillsburylaw.com

London
Tower 42, Level 21
25 Old Broad Street
London, EC2N 1HQ
F +44.207.847.9501
M +44.7951.652.271

pillsbury