Data protection week

pwc

Opening Conference

@PwC_CI • @JerseyOIC

#KeepMyDataSafe • #DataProtectionWeek

pwc J.DPA Jersey Data Protection Association Government of Jersey OFFICE OF THE INFORMATION COMMISSIONER LEAN-JSY Efficient & Effective Jersey Business Expertise. Shared. Channel Islands Financial Ombudsman CALLINGTON CHAMBERS DIGITAL JERSEY JRA Jersey Retail Association CIISF CHANNEL ISLANDS INFORMATION SECURITY FORUM

Data protection week

Welcome

Follow us on social media

@JerseyOIC @Office of the Information Commissioner

#KeepMyDataSafe • #DataProtectionWeek

David Carney

PwC Director and J.DPA Chairman

pwc

J.DPA

JERSEY DATA PROTECTION ASSOCIATION

Jacob Kohnstamm

Chair, Jersey Data Protection Authority

Dr Jay Fedorak

Information Commissioner

OFFICE OF THE INFORMATION COMMISSIONER

#KeepMyDataSafe

Data protection week

pwc

Opening Conference

@PwC_CI • @JerseyOIC

#KeepMyDataSafe • #DataProtectionWeek

pwc J.DPA Jersey Data Protection Association Government of Jersey OFFICE OF THE INFORMATION COMMISSIONER LEAN-JSY Efficient & Effective Jersey Business Expertise. Shared. Channel Islands Financial Ombudsman CALLINGTON CHAMBERS DIGITAL JERSEY JRA Jersey Retail Association CIISF CHANNEL ISLANDS INFORMATION SECURITY FORUM

Brexit and Data Protection

Stephanie Peat
Director, Digital and Telecoms Policy
Office of the Chief Executive

Jersey has long recognised the importance of protecting personal data

- Jersey has had Data Protection legislation since 1987
- The Data Protection (Jersey) Law 2005 provided equivalent protection to that in the UK and Europe
- Jersey is a third country for the purpose of EU Data Protection Law
- In 2008 the EU confirmed that Jersey offers an essentially equivalent level of protection to the EU (2008/393/EC)
- This ‘adequate’ status allows frictionless data flows between Jersey and EU member states

And is an ‘adequate’ third country for the purposes of data protection

- The EU’s new data protection standard the General Data Protection Regulation (GDPR) became enforceable from May 2018
- Jersey’s new legislation came into force at the same time. It is essentially equivalent to the GDPR
- Jersey’s adequacy status has ‘rolled over’ and a review of Jersey’s current adequacy decision will be undertaken by the European Commission by 2020
- Brexit will not affect Jersey’s current adequate status

After Brexit the UK's position will change

- When the UK leaves the European Union it will no longer be a member state for the purposes of data protection
- While the UK has committed to seeking an adequacy decision from the EU this will not be in place prior to 29th March 2019
- The UK Department for Culture, Media & Sport has confirmed that the UK remains committed to a high level of data protection
- And the EU (Withdrawal) Act 2018 (EUWA) retains the GDPR in UK law

There are implications for data flows under any Brexit scenario

- In the event of an orderly transition *or* a no-deal Brexit, the UK will become a third country for data protection purposes
- But the future of data flows between the UK and the EU is likely to depend on the manner of Brexit
- Under any scenario there are potential risks to the continued free flow of personal data between Jersey and the UK
- Mitigating this risk is crucial as many Jersey businesses rely heavily on the unrestricted flow of personal data with the UK

Government is seeking to maintain frictionless data flows with the UK

- The States of Jersey has proposed amendments to the Data Protection (Jersey) Law 2018 to ensure that when the UK leaves the EU, data controllers and processors may continue to treat data transfers to the UK in the same way as those to EU Member States
- The provision will remain in effect until the end of December 2020 and can be found in Regulations 3 of the draft European Union (United Kingdom Exit – Miscellaneous Amendments) (Jersey) Regulations 201-
- This amendment effectively maintains the status quo and allows for data to continue to flow freely between Jersey and the UK

Conclusion

- Adequacy remains of paramount importance to Jersey and we are committed to taking action that will assist with maintaining our adequacy status
- We think we are in a strong position in relation to the review that will take place by 2020
- We are prepared for both the UK leaving with a withdrawal agreement in place and a no-deal Brexit
- We are continuing to monitor the situation with Brexit and will make plans accordingly

Dr Jay Fedorak

Information Commissioner

OFFICE OF THE INFORMATION COMMISSIONER

#KeepMyDataSafe

Data protection week

pwc

Opening Conference

@PwC_CI • @JerseyOIC

#KeepMyDataSafe • #DataProtectionWeek

pwc J.DPA Jersey Data Protection Association Government of Jersey OFFICE OF THE INFORMATION COMMISSIONER LEAN-JSY Efficient & Effective Jersey Business Expertise. Shared. Channel Islands Financial Ombudsman CALLINGTON CHAMBERS DIGITAL JERSEY JRA Jersey Retail Association CIISF CHANNEL ISLANDS INFORMATION SECURITY FORUM

How to survive a data breach

Advocate Davida Blackmore, Callington Chambers

“Death and taxes and childbirth.
There’s never a convenient time
for any of them.”

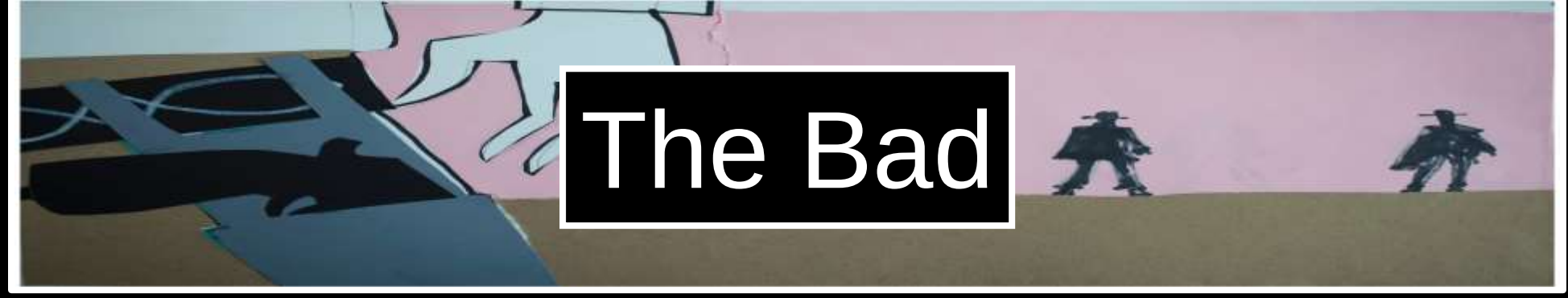
–Scarlett O’Hara in Gone With the Wind
By Margaret Mitchell

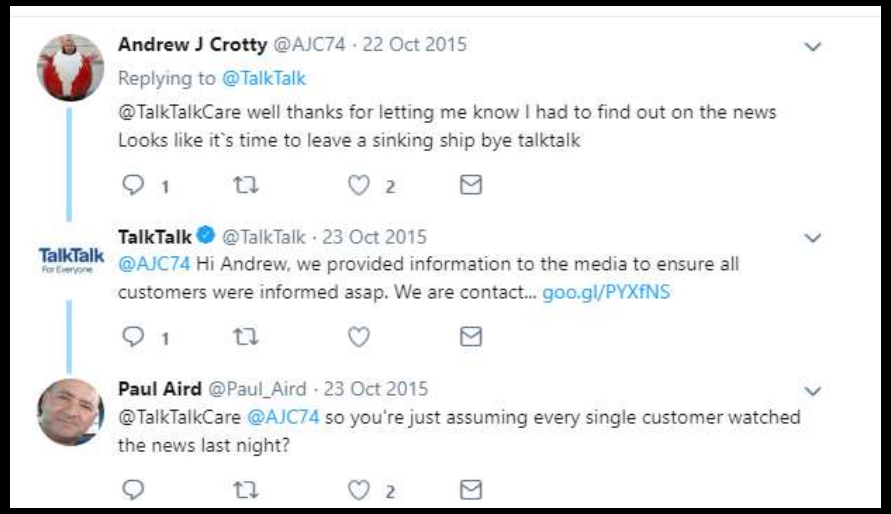

The good, the bad and the ugly
(in reverse order)

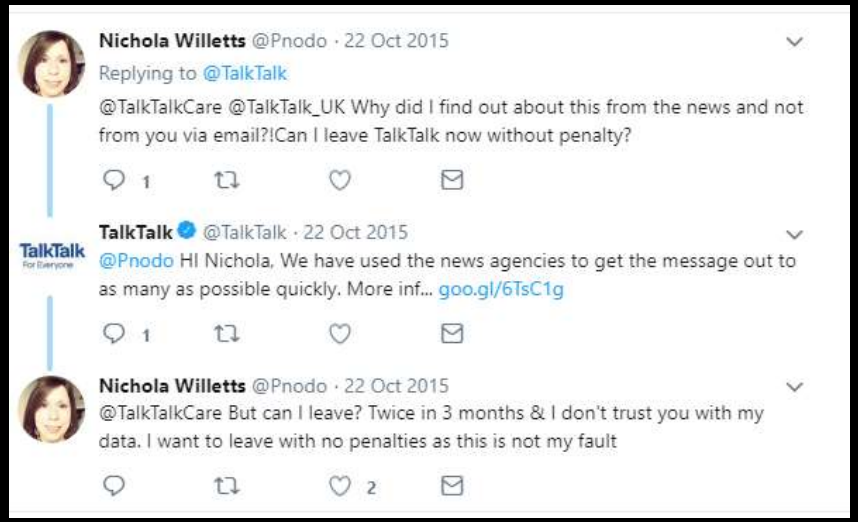
The Ugly

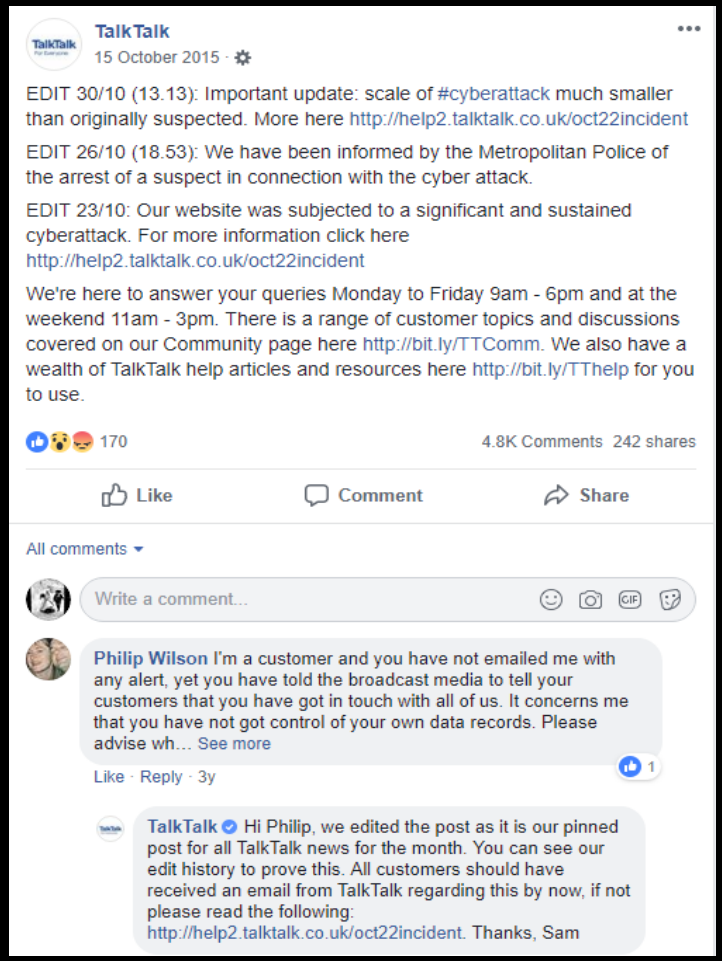
- Failed to patch known vulnerability in open source Apache Struts
- 143m US customers exposed. In May 2017
- Executives sell off $1.8m of shares on 29 July 2017

EQUIFAX


The Bad


Andrew J Crotty @AJC74 · 22 Oct 2015
Replying to @TalkTalk
@TalkTalkCare well thanks for letting me know I had to find out on the news Looks like it`s time to leave a sinking ship bye talktalk
1
2
TalkTalk @TalkTalk · 23 Oct 2015
@AJC74 Hi Andrew, we provided information to the media to ensure all customers were informed asap. We are contact... goo.gl/PYXfNS
1
Paul Aird @Paul_Aird · 23 Oct 2015
@TalkTalkCare @AJC74 so you're just assuming every single customer watched the news last night?
2


Nichola Willetts @Pnodo · 22 Oct 2015
Replying to @TalkTalk
@TalkTalkCare @TalkTalk_UK Why did I find out about this from the news and not from you via email?!Can I leave TalkTalk now without penalty?
1
TalkTalk @TalkTalk · 22 Oct 2015
@Pnodo HI Nichola, We have used the news agencies to get the message out to as many as possible quickly. More inf... goo.gl/6TsC1g
1
Nichola Willetts @Pnodo · 22 Oct 2015
@TalkTalkCare But can I leave? Twice in 3 months & I don't trust you with my data. I want to leave with no penalties as this is not my fault
2


TalkTalk
15 October 2015 ·
EDIT 30/10 (13.13): Important update: scale of #cyberattack much smaller than originally suspected. More here http://help2.talktalk.co.uk/oct22incident
EDIT 26/10 (18.53): We have been informed by the Metropolitan Police of the arrest of a suspect in connection with the cyber attack.
EDIT 23/10: Our website was subjected to a significant and sustained cyberattack. For more information click here http://help2.talktalk.co.uk/oct22incident
We're here to answer your queries Monday to Friday 9am - 6pm and at the weekend 11am - 3pm. There is a range of customer topics and discussions covered on our Community page here http://bit.ly/TTComm. We also have a wealth of TalkTalk help articles and resources here http://bit.ly/TThelp for you to use.
170
4.8K Comments 242 shares
Like
Comment
Share
All comments
Write a comment...
Philip Wilson I'm a customer and you have not emailed me with any alert, yet you have told the broadcast media to tell your customers that you have got in touch with all of us. It concerns me that you have not got control of your own data records. Please advise wh... See more
Like · Reply · 3y
1
TalkTalk Hi Philip, we edited the post as it is our pinned post for all TalkTalk news for the month. You can see our edit history to prove this. All customers should have received an email from TalkTalk regarding this by now, if not please read the following: http://help2.talktalk.co.uk/oct22incident. Thanks, Sam

The Good?

- Dedicated website
- Dedicated call centre
- Paid for web monitoring for a year
- Kept information updated

Preparation is EVERYTHING

- Map out response plan IN ADVANCE
- Store plan offline in case of catastrophic breach
- Identify key players
- Define roles
- Train staff (identify, notify and/or respond, as appropriate)
- STRESS TEST (in advance)

What should your plan look like?

- What is a breach? How can staff identify one?
- Clear escalation procedures and reporting lines
- Identify team members and responsibilities
- Include details of external consultants
- Tailor to different types of breach and different actions
- How to deal with affected individuals
- How/when to contact law enforcement/regulators
- How/when to deal with other entities (eg your controller)
- Breach record
- Insurer notification process
- Review and remediation strategy post-breach


LOW
AVERAGE
HIGH
MAXIMUM
DATA BREACH
Level

“In the case of a personal data breach, the controller must, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach in writing to the Authority in the manner required by the Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.”

Art.20(1)

Key players

- Leader
- Internal response team
  - IT
  - DPO
  - Senior management
  - Communications/PR
- Insurers
  - May take control
- External consultants

Containment

- Contain the breach
  - Change passwords
  - Shut down computers
  - Halt any traffic
  - Restore from backups
- BUT make sure you don’t do anything that may impact on forensic work

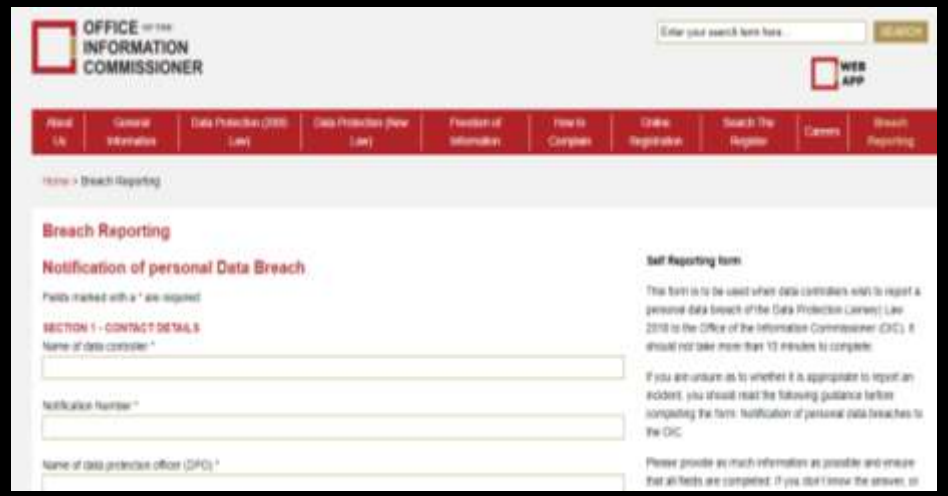
What should your investigation look like?

- What has been breached, how, when and by whom?
- How did you become aware?
- How many data subjects affected?
- How many records?
- Likely consequences? Risk assessment. Harm to subjects.
- Plan response, contain the breach, recover from the impact
- Must log all breaches internally

What do I need to say?

To the JOIC

- How many people affected
- How many records
- What type of info (sensitive?)
- What did you have in place to prevent breaches? (security measures/training?)
- What have you done to contain/remedy the breach? What are you going to do?
- Do you have policies/procedures?
- Has anyone affected already complained to you?



What do I need to say?

To data subjects

- The name and contact details of the DPO or other contact point where more information can be obtained
- A summary of the likely consequences of the Breach
- A description of the measures taken or proposed to be taken by the data controller to address the Breach
- A description of the measures a data subject could take to mitigate any possible adverse effects of the Breach

Review

- What have you learned from the breach?
- What have you done/should you do to improve your practices?
- What have you done/will do to prevent similar breaches from happening again?

Final thoughts

- Data breaches are inevitable
- Companies targeted on a daily basis
- Ignoring vulnerabilities, expecting users to deal with fall-out and selling assets when you have information of a breach won’t help
- Be honest
- Put yourselves in the shoes of the data subject

CALLINGTON
CHAMBERS

Advocate Davida Blackmore, Partner

T: +44 1534 510250

E: davida.blackmore@callingtonchambers.com

W: www.callingtonchambers.com

Twitter: @Callington_law

Final thoughts

- Data breaches are inevitable
- Companies targeted on a daily basis
- Ignoring vulnerabilities, expecting users to deal with fall-out and selling assets when you have information of a breach won’t help
- Be honest
- Put yourselves in the shoes of the data subject

Review

- What have you learned from the breach?
- What have you done/should you do to improve your practices?
- What have you done/will do to prevent similar breaches from happening again?

What do I need to say?

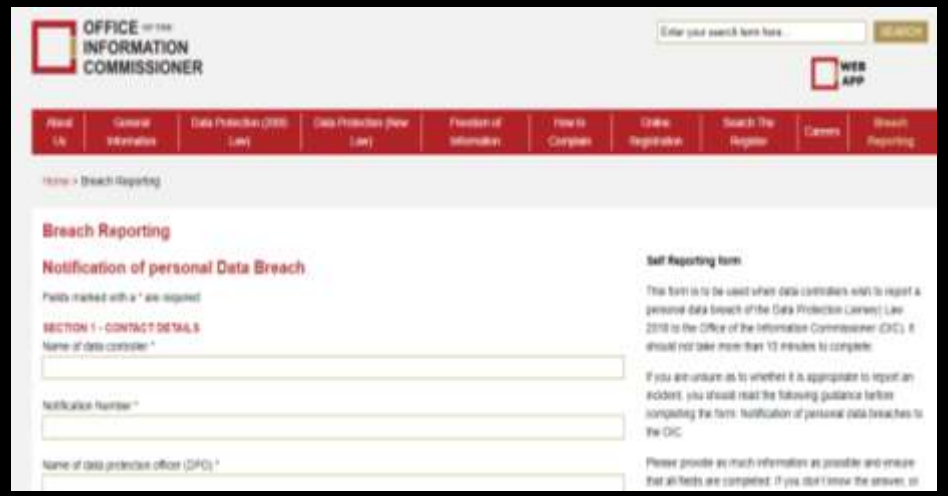
To data subjects

- The name and contact details of the DPO or other contact point where more information can be obtained
- A summary of the likely consequences of the Breach
- A description of the measures taken or proposed to be taken by the data controller to address the Breach
- A description of the measures a data subject could take to mitigate any possible adverse effects of the Breach

What do I need to say?

To the JOIC

- How many people affected
- How many records
- What type of info (sensitive?)
- What did you have in place to prevent breaches? (security measures/training?)
- What have you done to contain/remedy the breach? What are you going to do?
- Do you have policies/procedures?
- Has anyone affected already complained to you?



What should your investigation look like?

- What has been breached, how, when and by whom?
- How did you become aware?
- How many data subjects affected?
- How many records?
- Likely consequences? Risk assessment. Harm to subjects.
- Plan response, contain the breach, recover from the impact
- Must log all breaches internally

CALLINGTON
CHAMBERS

Advocate Davida Blackmore, Partner

T: (00 44) 1534 510250

E: davida.blackmore@callingtonchambers.com

W: www.callingtonchambers.com

Follow us on Twitter: @Callington_law

Data protection week

pwc

Opening Conference

@PwC_CI • @JerseyOIC

#KeepMyDataSafe • #DataProtectionWeek

pwc J.DPA Jersey Data Protection Association Government of Jersey OFFICE OF THE INFORMATION COMMISSIONER LEAN-JSY Efficient & Effective Jersey Business Expertise. Shared. Channel Islands Financial Ombudsman CALLINGTON CHAMBERS DIGITAL JERSEY JRA Jersey Retail Association CIISF CHANNEL ISLANDS INFORMATION SECURITY FORUM

Data Protection

Key Issues for the Board

Huw Thomas

Counsel, Jersey

CAREY OLSEN

The law of privacy

"The Right to Privacy" Warren and Brandeis Harvard Law Review Vol. IV December 15, 1890 No. 5

"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone" .

Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."


LTCM
SM
The financial technology company

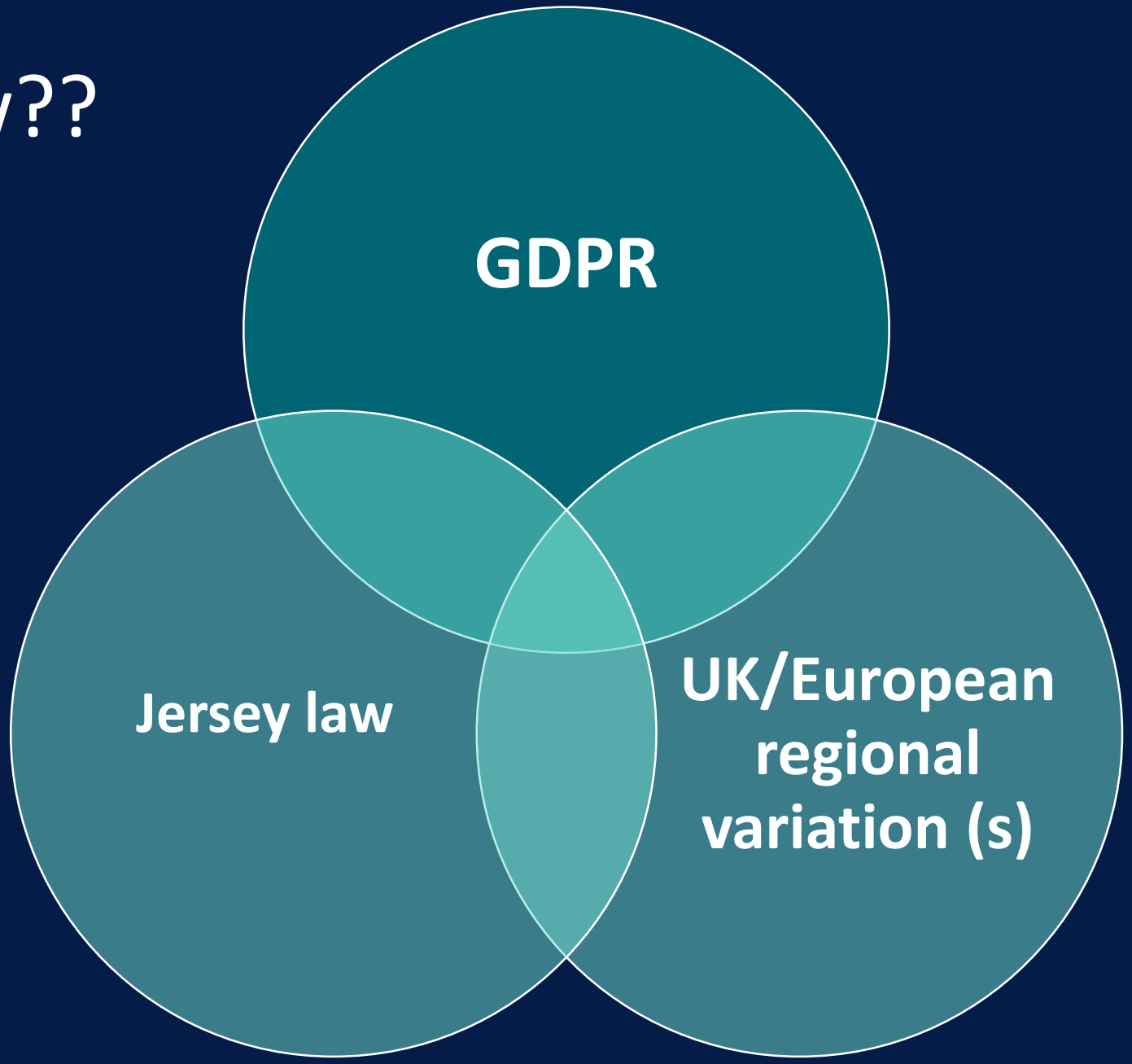
Target

"If we send someone a catalog and say, 'Congratulations on your first child!' and they've never told us they're pregnant, that's going to make some people uncomfortable,"

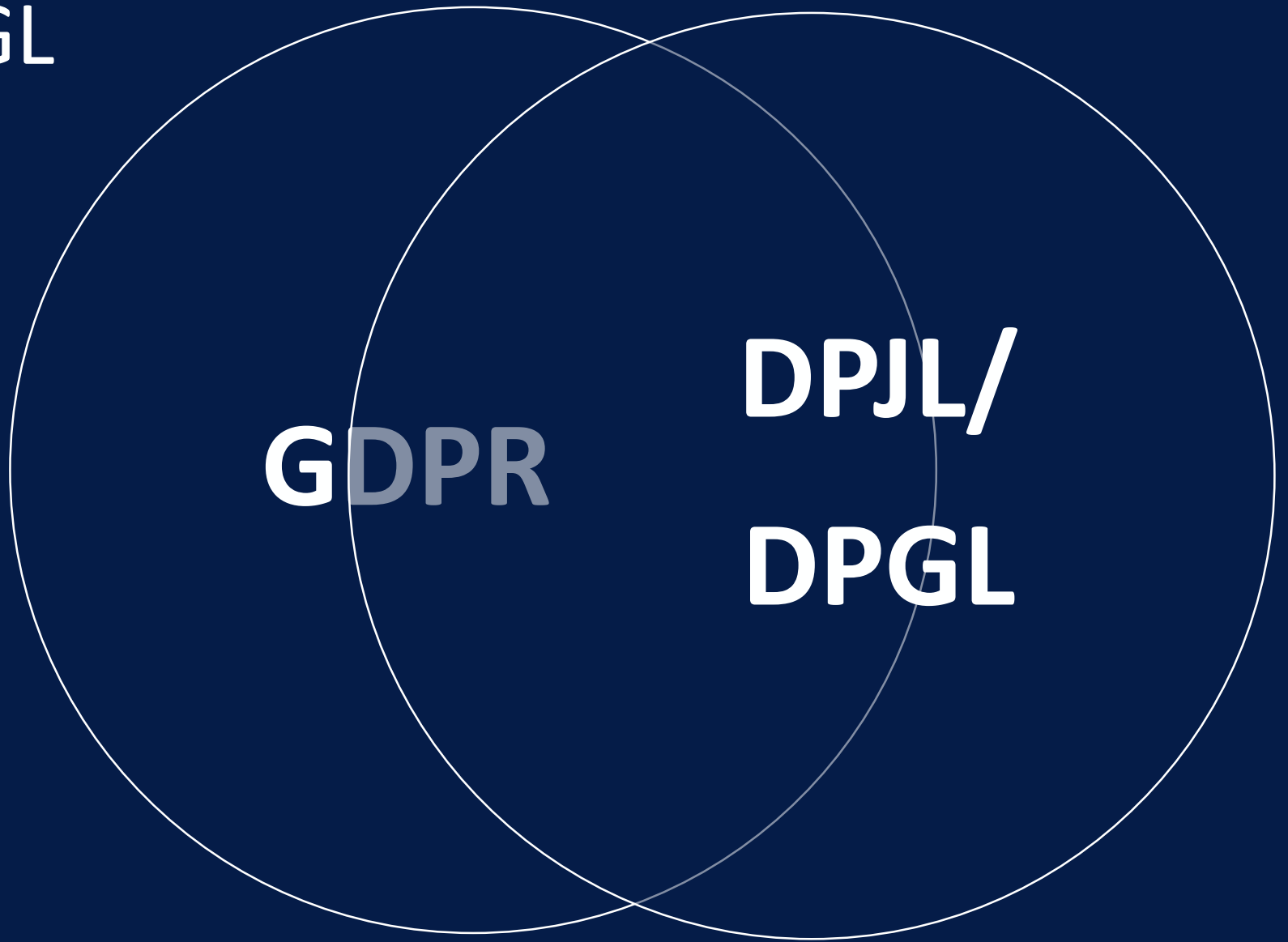
"We are very conservative about compliance with all privacy laws. **But even if you're following the law, you can do things where people get queasy.**"


Lawfulness, fairness and transparency
Purpose Limitation
Data Minimisation
Accuracy
Storage Limitation
Integrity & Confidentiality
Accountability

Which Law??



GDPR v DPJL/DPGL



Data Protection – Issues for the Board

- **Criminal**
  - Secondary liability under DPJL/DPAJL for directors, manager, secretary or similar officer or someone purporting to act in such capacity is personally guilty of an offence in addition to the corporate body if:
    - offence was committed with his/her consent or connivance; or
    - The offence is attributable to any neglect on his/her part.

Civil

Individual Rights

- Subject access
- The right to erasure or to be forgotten
- The right to rectification
- The right to restriction of processing.
- The right to object to processing
- Data portability
- Right to object to automated individual decision making (including profiling)
- Claims for loss/distress

Civil

Remedies

Individuals may have the following civil remedies:

- The right to lodge a complaint with the Authority where their data has been processed in a way that does not comply with the DPJL;
- The right to bring civil proceedings against controllers in the Royal Court;
- The right to compensation from a relevant controller or processor for loss, damage or distress resulting from infringement of the DPJL.

Controllers may also have contractual claims against **processors** arising from processing agreements.

Regulatory

FCA Guidance:

"Compliance with GDPR is now a board level responsibility, and firms must be able to produce evidence to demonstrate the steps that they have taken to comply. The requirement to treat customers fairly is also central to both data protection law and the current financial services regulatory framework. When the FCA makes rules, we take into account how our requirements will affect the privacy interests of individuals such as firms' customers and employees, and are open and transparent on why we have made rules in the way that we have."

Regulatory

GDPR Sanctions

- Up to **€20 million or 4% of annual global turnover** (prior year), whichever is greater, for more serious breaches
  - Basic conditions of processing, consent, data subjects' rights, international transfers, non-compliance with an order of a Supervising Authority
- Up to **€10 million or 2% of annual global turnover** (prior year), whichever is greater, for less serious breaches
  - Obligations of the controller/processor (design/default), representative of non-EU controller, choice of processor, record keeping, breach notification, data security, etc.)

Regulatory

Jersey Sanctions

A **sanction** may be:

- A **reprimand**; or
- A **warning**; or
- An **order**

Administrative fines are a separate regime.

Regulatory

Jersey Fines

- The limits on fines are:
  - the **lower threshold** (**£5 million**)
  - the **upper threshold (£10 million**)
- Subject to an overall limit of 10% of annual global turnover or £300,000 (whichever is the greater)
- Crossover with fines in other jurisdictions?

Operational Issues

Disruption to operations caused by:

- Exercise of individual rights
- Regulatory sanction
- Cyber security breaches
- Information governance as a broader commercial issue

GDPR overview

"High impact" changes

- Extra territoriality
- Breach notification
- Sanctions
- Organisational measures:
  - Privacy by design / by default
  - Accountability
  - DPIAs
- Consent
- Data protection officers
- Enhanced individual rights - (Disclose/Delete/Freeze/Correct It)
- Duties on processors

GDPR & Information Security

Some specific issues

GDPR Requirement

Information Security

- The Regulation requires data controllers and data processors to take a **risk based approach** to the implementation of **security measures** to protect against loss or unauthorised disclosure of personal data
  - Extends to behaviours of investors/subscribers/NEDS?
  - Personal security issues of individuals?
  - Recitals add new concept
    - Confidentiality
    - **I**ntegrity
    - **A**vailability
    - **R**esilience (new concept)

Cyber Security - Dear CEO Letter

February 2016

- Engages:
  - Corporate governance
  - Systems & Controls
  - Record Keeping
- Requires assessment of third party risk

Cyber Security - Dear CEO Letter

- A registered person should understand (and document) the risk of a cyber-attack on their business and take appropriate documented measures to mitigate this risk; the level and type of risk mitigation should be appropriate and proportionate to the type, potential impact and likelihood of the risks identified
- The registered person should have in place appropriate contingency arrangements that they can deploy in the event of a cyber-attack, for example maintaining service levels for clients or informing relevant parties about the attack and its impact

Cyber Security - Dear CEO Letter

- A registered person should keep these matters under review and test their effectiveness at appropriate intervals
- Boards of Directors (or equivalent) of registered persons will take overall responsibility for ensuring that their firm adequately addresses cyber-security risks.

Where do the risks come from?

- Hackers
- Competitors
- Media
- Insiders
  - Malicious
  - Non malicious

But remember

- Quis custodiet ipsos custodes?
- People risk in relation to senior management/board members is in a category of its own
  - Knowledge of systems
  - Lack of oversight
  - Authority to override rules
  - Lack of consequences
  - Ability to engage in “high impact” misconduct

Non Executive Directors

CAREY OLSEN

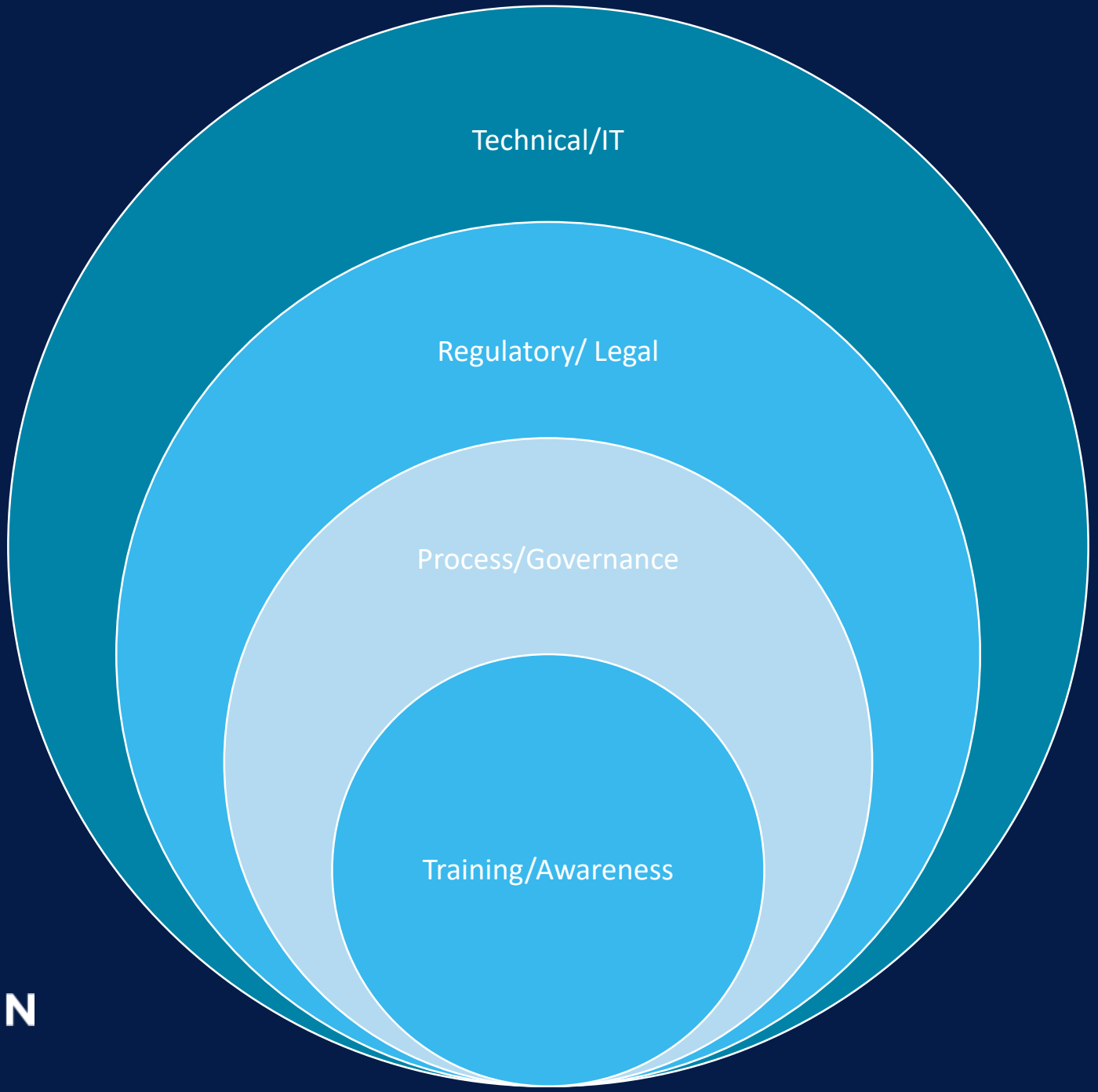
Status

- Data Contollers?
- Data Processors?
- Agents?

Issues

- Retention of
  - board packs (Class G Guidance)
  - Notes on business/employees
  - Disciplinary/grievance packs
- Cyber/communications security
- Mixed data

What to Do?


Technical/IT
Regulatory/ Legal
Process/Governance
Training/Awareness

CAREY OLSEN

- Data protection by design/Default
- Right to be forgotten
- Subject Access
- Data Portability
- Accountability – record keeping
- Security
- Breach management

- Monitoring guidance/developments
- Foreign legal systems
- Data Protection Officer
- Data processing agreements
- Data transfer
- Privacy notices
- Lawfulness of processing
- Data sharing/disclosure
- Subject Access
- Breach management
- Data Protection Impact Assessment

- Data Protection Officer
- Board
- Customers
- Third Parties
- Employees/prospective employees

- Board ownership/skills
- Data Protection Impact Assessment
- HR processes
- Data sharing/disclosure
- Data transfer
- Data Protection Officer
- Data protection by design/Default
- Right to be forgotten
- Subject Access
- Accountability – record keeping

CAREY OLSEN

Questions

CAREY OLSEN

Speaker

Huw Thomas

Counsel, Jersey

D +44 1534 822224

E huw.thomas@careyolsen.com

CAREY OLSEN

OFFSHORE LAW SPECIALISTS

BERMUDA BRITISH VIRGIN ISLANDS CAYMAN ISLANDS GUERNSEY JERSEY

CAPE TOWN HONG KONG LONDON SINGAPORE

careyolsen.com

Data protection week

pwc

Opening Conference

@PwC_CI • @JerseyOIC

#KeepMyDataSafe • #DataProtectionWeek

pwc J.DPA Jersey Data Protection Association Government of Jersey OFFICE OF THE INFORMATION COMMISSIONER LEAN-JSY Efficient & Effective Jersey Business Expertise. Shared. Channel Islands Financial Ombudsman CALLINGTON CHAMBERS DIGITAL JERSEY JRA Jersey Retail Association CIISF CHANNEL ISLANDS INFORMATION SECURITY FORUM

LEAN-JSY

EFFICIENT & EFFECTIVE

Data Protection Compliance for the Hospitality Sector

Survey conducted :

September - October 2018

Why the Jersey hospitality sector?

- Tourism plays a significant role in Jersey's economy.
- The latest report from the 'Economic Contribution of Tourism to Jersey' found that tourism activity supported more than 5,000 jobs in Jersey.
- Jersey had 727,000 visitors in 2017 with main areas of spending being accommodation, food and beverage.
- Tourism spending raised almost £13 million GST for the Treasury
- With its reliance on point of sale recent reports have identified the tourism industry as particularly vulnerable to data breaches.

About the Survey

- 276 companies were invited to complete the on-line survey.
- The survey consisted of 15 questions.
- 59 completed surveys received, giving a response rate of 22%.

Survey results

Handling of data protection

How is Data Protection handled in your organisation?

30% Managed with another function, IT or Finance.

23% Dedicated Data Protection function.

23% No formal function or ad-hoc at best.

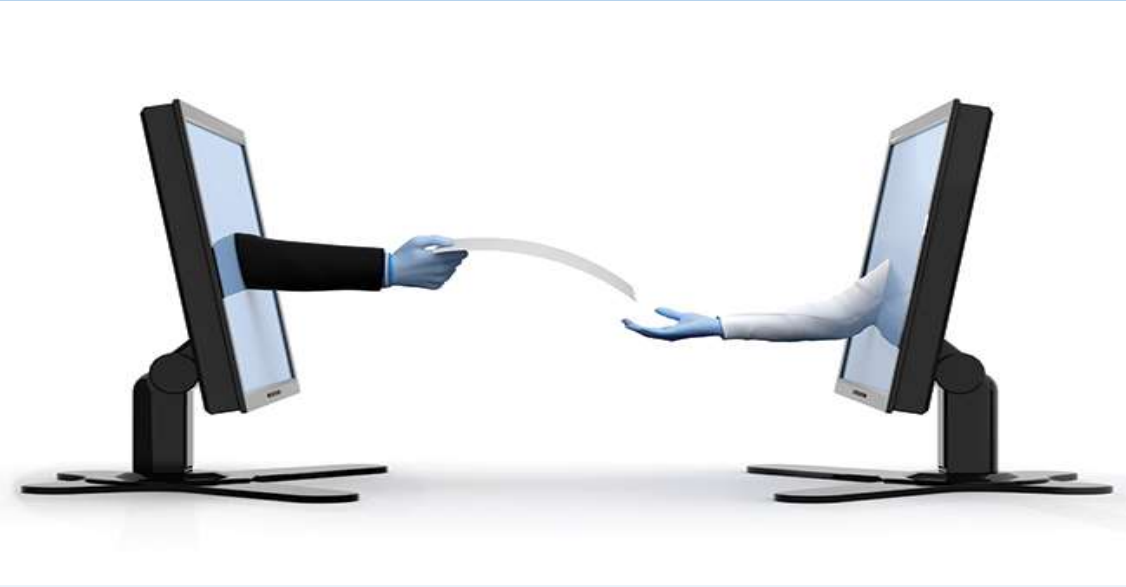
What is the primary reason for your organisation's investment in Data Protection compliance?

55% - because it's a legal requirement

16% - Risk of being fined

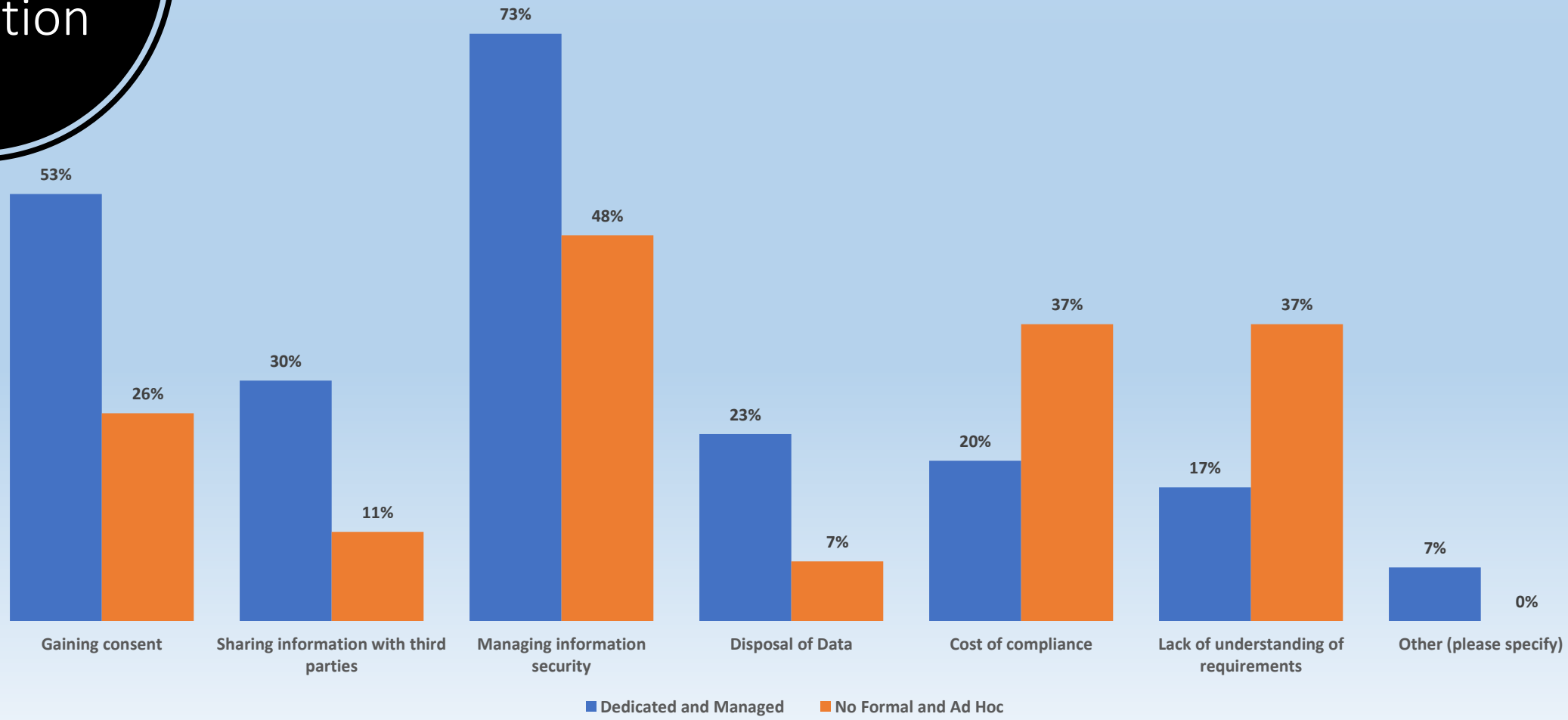
16% - Risk of damage to reputation

13% - Losing business to competitors

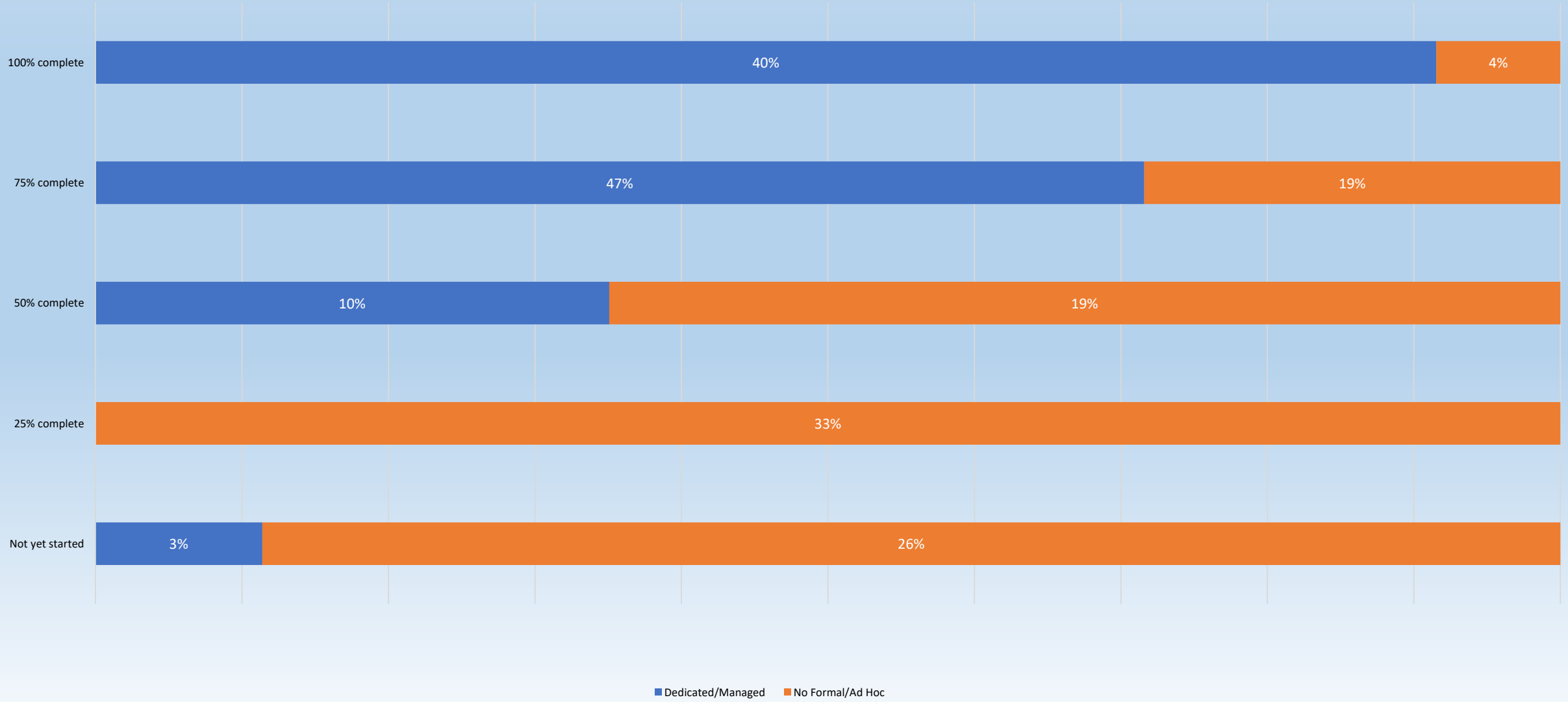


Handling of data protection

Main areas of Concern by how companies handle data protection



Compliance Progress by way in which Data Protection is Handled



What Policies, Procedures and Registers do you have in place?

98% Had a Data Protection Policy

43% Had a Data Subject Access Policy and Procedure

40% Had a Data Retention Policy

27% Had a Data Breach Notification Policy and Procedure

17% Breach Register

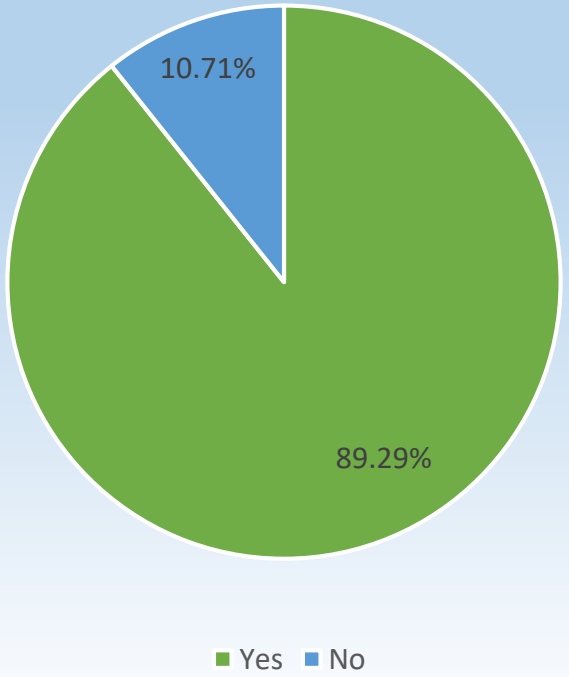
14% Data Inventory Register

14% Data Impact Assessment Register

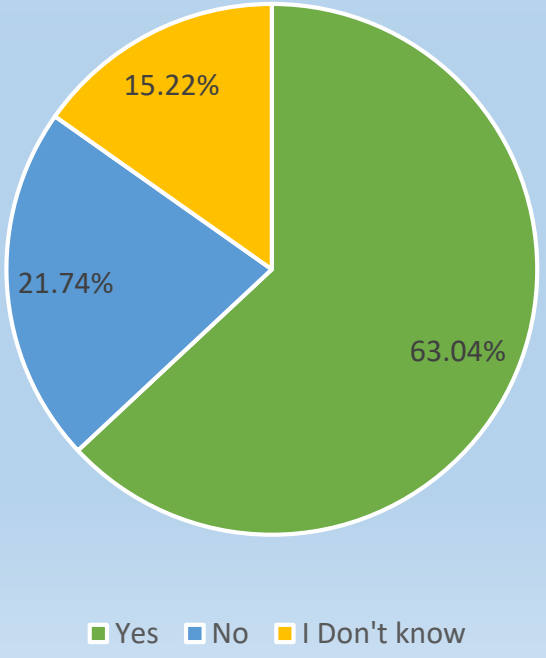
Policies, procedures and registers

Website

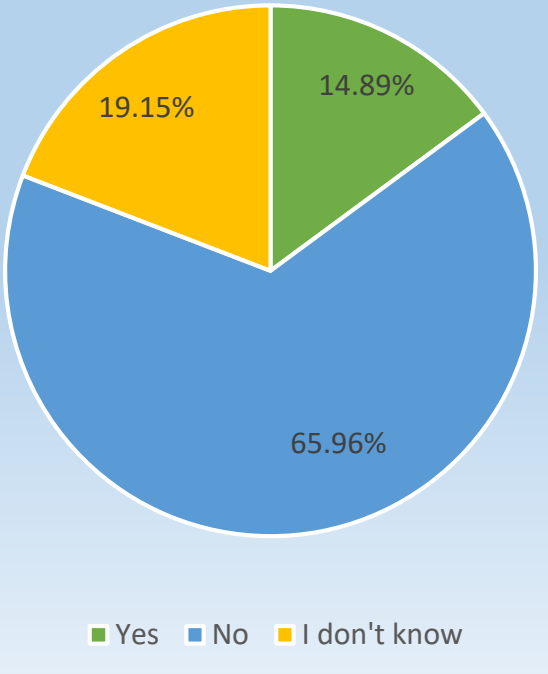
Do you have a website for your business?



Do you Have an up-to-date Privacy & Cookies Notice/ Policy on your website?

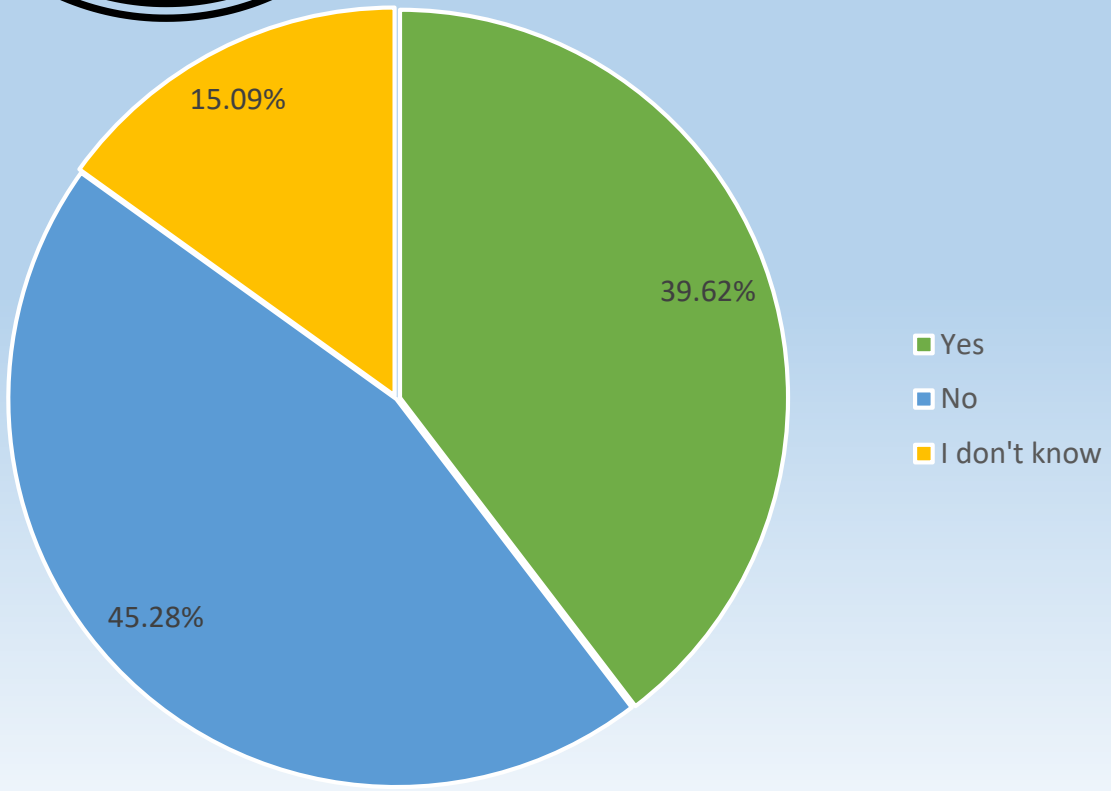


Do you have a Data Subject Access request form available on your website?



Processing data outside of Jersey

Do you process data outside the Bailiwick of Jersey?



Do you have Controller / Processor agreements in place?

34% Nothing in place

28% All agreements in place

23% Had most of the agreements in place

15% Had some of the agreements in place

Key Findings

- 23% of Respondents said they had a dedicated Data Protection function and said that their concern is gaining consent and managing information security.
- 25% of Respondents said they have no dedicated DP function (or that it is ad-hoc at best), said that their concern is the cost of compliance and a lack of understanding.
- 69% say they have no budget set for Data Protection Compliance.
- 17% of all respondents said they did nothing in the run up to the new law being implemented.
- 44% of respondents who classed their business as a guest house said they did nothing; more than any other sector.

Key Findings

- 89% of all businesses that completed the survey said they have a website for their business.
- 100% of hotels said they do have a website.
- 62% said they do have cookies/privacy policies available on their website and they are up-to-date.
- 85% said they had No or I Don't Now, when asked if they had a DSAR form on their website.

- We conducted an audit of all companies we sent the survey to who had a website and we found that only 24% of privacy/cookies notices were up-to-date on their websites.

LEAN-JSY
EFFICIENT & EFFECTIVE

There is still a lot of work to do!

Thank you

A full survey report is available from our website, just subscribe and we will send it straight out to you.

www.Lean-Jsy.co.uk

De Carteret House
7 Castle Street,
St Helier
JE23BT
01534 752982

Data protection week

pwc

Opening Conference

@PwC_CI • @JerseyOIC

#KeepMyDataSafe • #DataProtectionWeek

pwc J.DPA Jersey Data Protection Association Government of Jersey OFFICE OF THE INFORMATION COMMISSIONER LEAN-JSY Efficient & Effective Jersey Business Expertise. Shared. Channel Islands Financial Ombudsman CALLINGTON CHAMBERS DIGITAL JERSEY JRA Jersey Retail Association CIISF CHANNEL ISLANDS INFORMATION SECURITY FORUM

Building Collaborative Data Bridges

Jacob Kohnstamm

Chair, Jersey Data Protection Authority

OFFICE OF THE INFORMATION COMMISSIONER

#KeepMyDataSafe

Data protection week

Panel Discussion

Data protection week

Closing Remarks