

# Delve into Data protection week

Monday 28 January –  
Friday 01 February 2019

**#KeepMyDataSafe**

The week of events is kindly being supported by many local businesses.



The views expressed by speakers during presentations at the Jersey Office of the Information Commissioner (JOIC) events are those of the speaker and not necessarily of the JOIC. Presentations at the JOIC events do not constitute an endorsement of the speaker's views, products or services.



**LEAN-JSY**  
EFFICIENT & EFFECTIVE

# Data Protection Compliance for the Hospitality Sector

Paul Byrne - Director

## What we will cover.

- Key findings of the compliance survey
- Understand the impact of the Data Protection (Jersey) Law 2018 & GDPR on your business and how the regulation impacts data processing.
- Requirements for your website
- Prepare for and cope with the rights of individuals (like the right to Access)
- Explain the responsibilities of a Data Controller and Data Processor.
- Data Breaches
- Use of CCTV
- Road map to compliance

## About the Survey

- We identified 377 establishments including hotels, Guesthouses, campsites, tourist attractions/activities and restaurants, cafes and pubs.
- We contacted 276 companies inviting them to complete the on-line survey.
- The survey consisted of 15 questions and ran from 14/09/2018 – 19/10/2018.
- 59 completed surveys received, giving a response rate of 21%.

# Handling of data protection

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

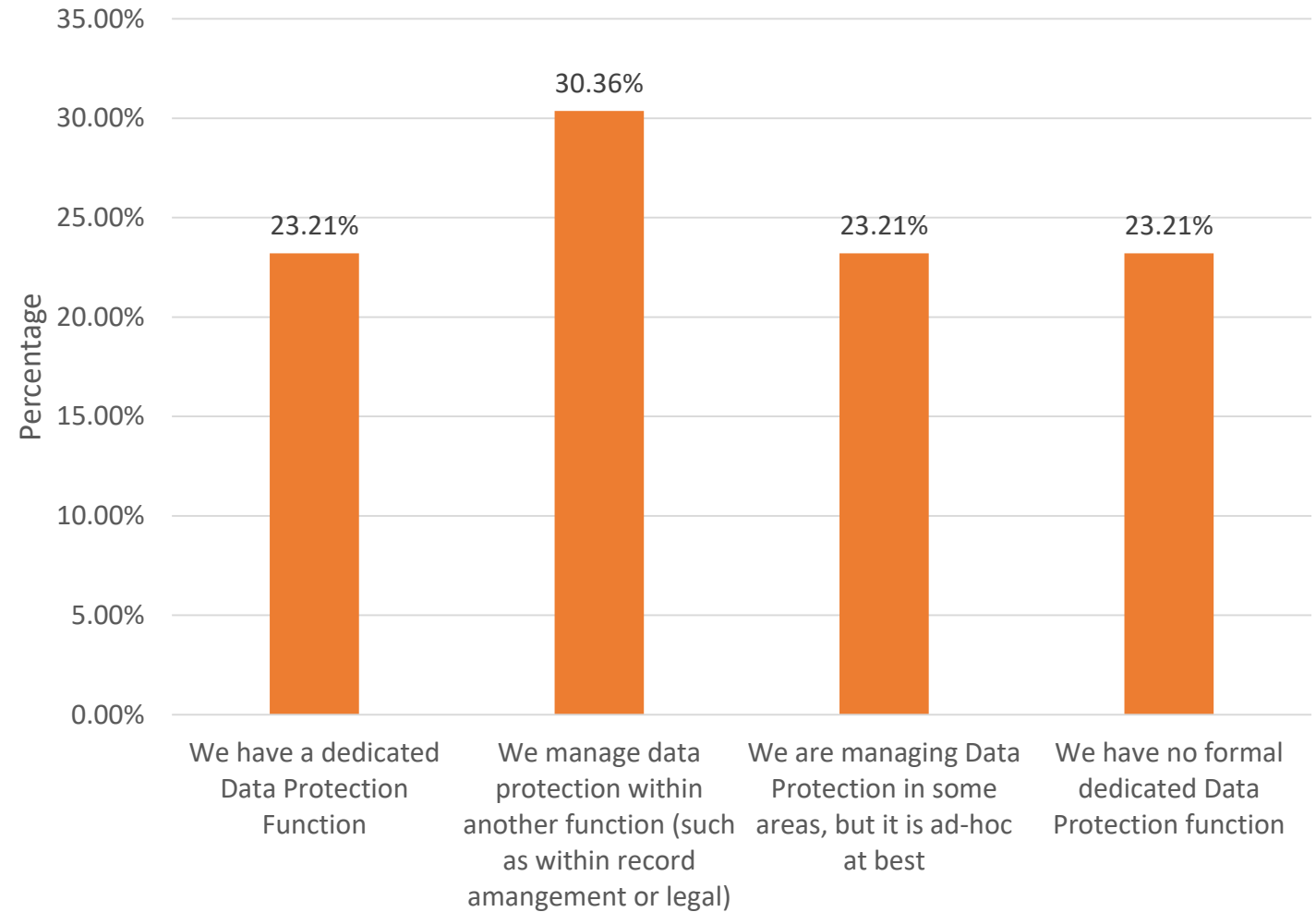
55% because it's a legal requirement

16% Risk of being fined

16% Risk of damage to reputation

13% Losing business to competitors

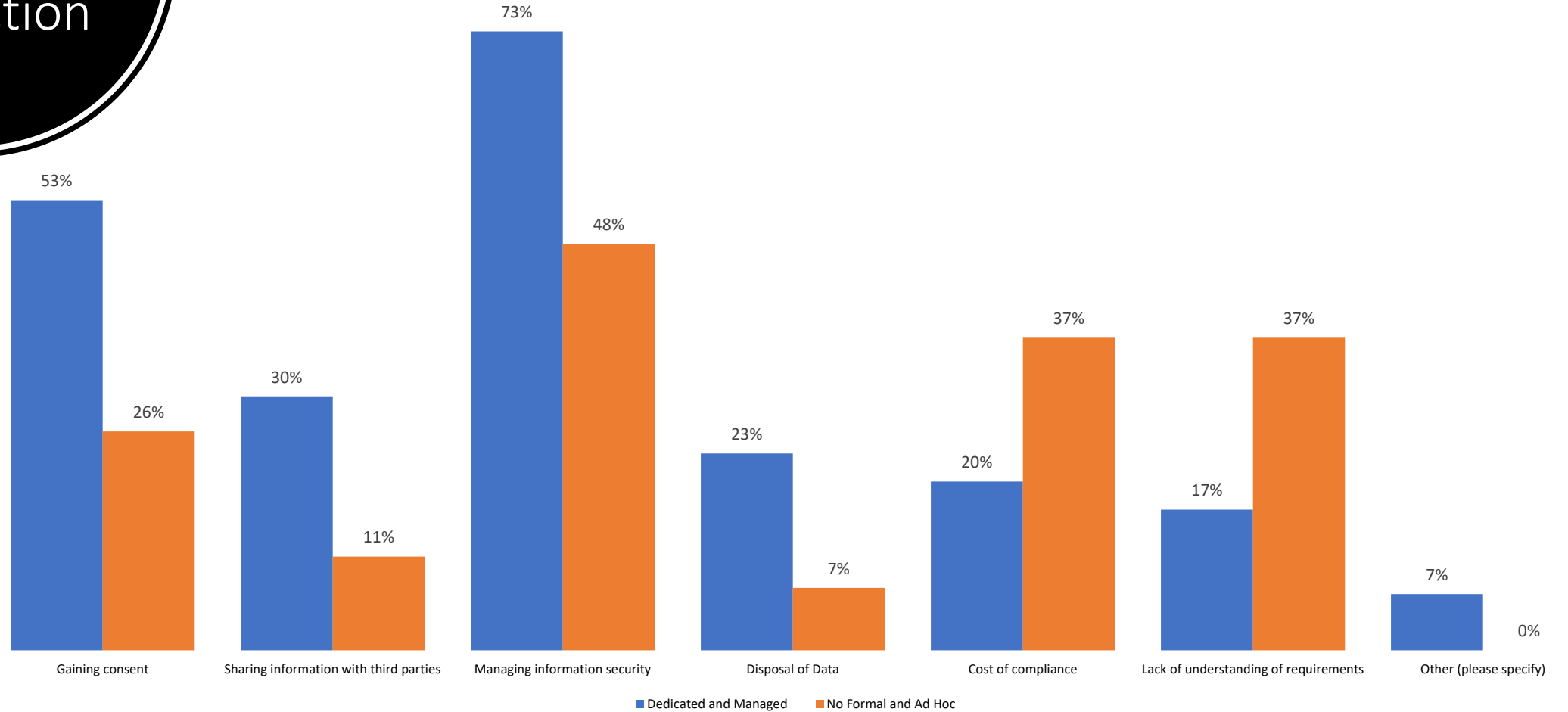
## How is Data Protection Handled in your organisation?



How is Data Protection Handled in your organisation?

# Handling of data protection

## Main areas of Concern by how companies handle data protection





## Key Findings

- 23% of Respondents said they had a dedicated Data Protection function. These respondents also said that their main areas of concern with regard to data protection 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). These same respondents said that their main areas of concern with regard to Data Protection 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.
  - 66% said they had no provision for Subject Access Requests on their websites
- We conducted an audit of all companies which we had sent the survey to who had a website and we found that out of 237 Tourism businesses websites we looked at, only 57 privacy/cookies notices were up-to-date on their websites.



## What is the Impact to your business

- one of the most vulnerable to data breaches (Verizon 2016 Data Breach Investigations). It is no surprise that the industry accounted for the second largest share of security breaches in 2016.
- it is imperative that hotels upgrade their data protection processes, or they face the risk of severe financial penalties.

# Data Protection (Jersey) Law 2018 GDPR road map

**Step 1**  
Set out a clear  
Project Plan  
and time lines.

**Step 3**  
Policy review and  
development

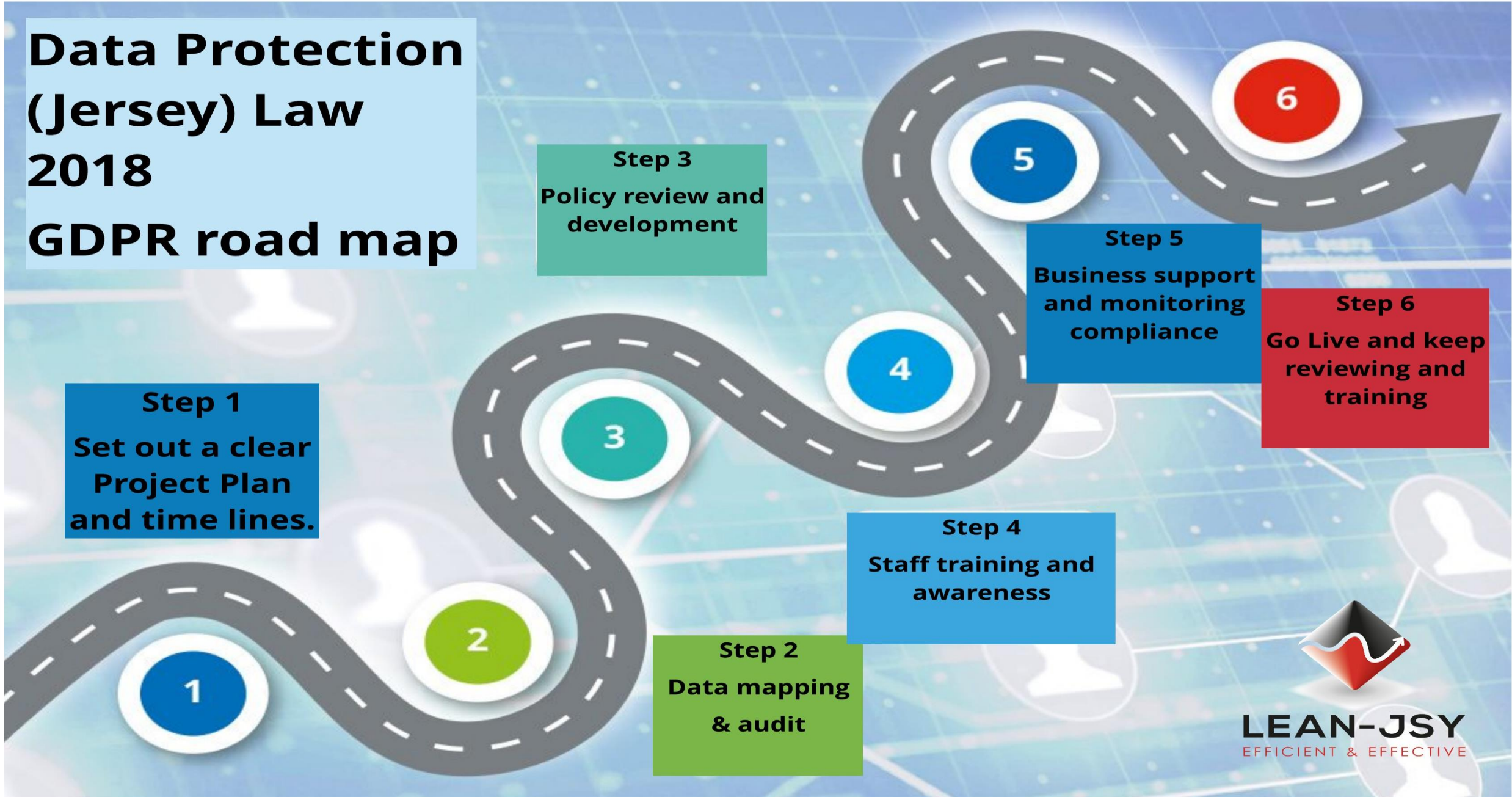
**Step 5**  
Business support  
and monitoring  
compliance

**Step 6**  
Go Live and keep  
reviewing and  
training

**Step 2**  
Data mapping  
& audit

**Step 4**  
Staff training and  
awareness

**LEAN-JSY**  
EFFICIENT & EFFECTIVE



# Marketing

- **Capturing and using personal data** Personal data must be collected for specified explicit and legitimate purposes.
- **The hotel, Guest House and Restaurants/pubs must ensure customers are aware of the particular uses of their data.**
- **Employ a strategy to obtain consent in appropriate form through proper documented communications.**
- **The regulation stipulates that customers have to “opt-in” to an email marketing service, as opposed to the previously and widely-used “opt-out” system.**

# Website requirements

- Privacy Notice
- Data Subject Access Request Form

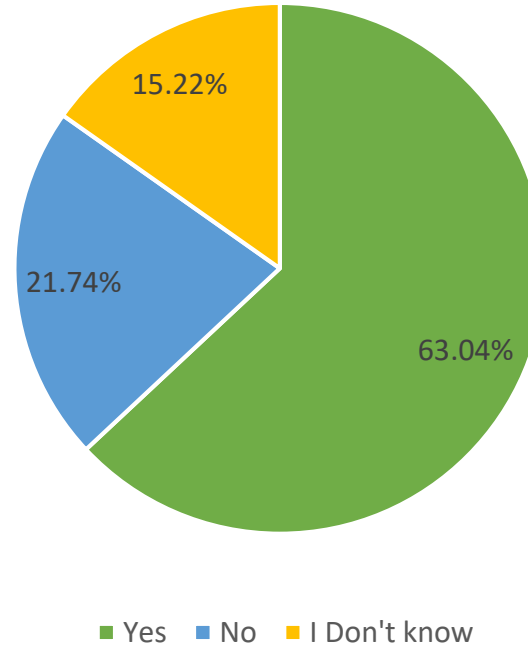
- Cookie Banner / Warning

- Cookie Policy

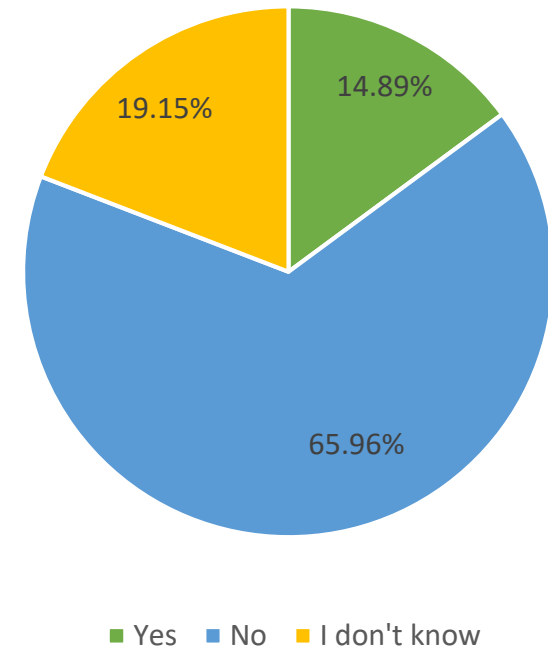




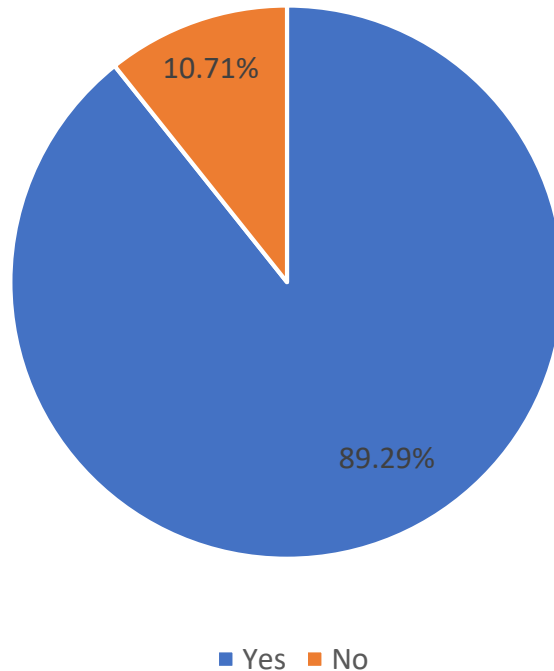
Do you Have an up-to-date Privacy & Cookies Notice/ Policy on your website?



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



Do you have a website for your business?





# Data Protection (Jersey) Law 2018 & GDPR Data Subject Rights

1

Right to be Informed  
– you have the right to know how your data is collected, by who, for what, for how long, where it is stored and how it is deleted. This is covered in a Privacy Notice

What should I know?

2

Right to Access  
– you have the right to request a copy of the information that we hold about you. You will receive a response within 4 weeks.

What can I get?

3

Right of Rectification  
- you have a right to correct data that we hold about you that is inaccurate or incomplete

Can I correct inaccurate data?

4

Right to be Forgotten  
– in certain circumstances you can ask for the data we hold about you to be erased from our records.

Can I delete my data?

5

Right to Restrict Processing  
– where certain conditions apply you have a right to restrict the processing.

Can I stop my data from being processed?

6

Right of Portability  
– you have the right to have the data we hold about you transferred to another organisation.

Can I move my Data?

7

Right to Object -  
– you have the right to object to certain types of processing such as direct marketing.

Can I stop some processing?

8

Right to Object to Automated Processing, including Profiling -  
– you also have the right not to be subject to the legal effects of automated processing or profiling.

Can I ask a Person?

# DATA SUBJECT ACCESS



- No fee can be charged, unless the request is repetitive
  - 4 weeks to provide a response
  - Provide a response in the format in which it is stored – so electronic, memory stick or paper, copies.
  - You do not have to decipher bad writing
  - If a key is required, you should provide it.
- 
- Form not mandatory to use
  - Can be in any format and does not have to say ‘subject access request’ As long as it is clear the person is requesting their own information, it is a DSAR.

## Data Controller

- “controller” means the natural or legal person, public authority, agency or other body that, whether alone or jointly with others, determines the purposes and means of the processing of personal data, and where those purposes and means are determined by the relevant law, the controller or the specific criteria for its nomination may be provided for by such law;

## Data Processor

- “processor” means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller, but does not include an employee of the controller;





# Controller vs. processor Who is responsible & what for?



Taking all necessary  
measures to comply  
BUT...

Determines the means and  
processing purposes

Processors (suppliers) are  
more liable now, as they  
have to:

- Maintain the documentation
- Conduct assessments
- Pay fines as well

Hiring other processors?



Carries out processing


Contract

# Contracts with third parties

---

- If a controller uses a processor then you need a contract:
  - What and how long
  - Why
  - Types of data
  - Types of data subject
  - Obligations and rights of controller
- Must be in writing.



- 
- A close-up photograph of a hand holding a black pen with a gold tip, positioned over a document. The document has a signature and some text, including the word "Signature" and "interque". The background is blurred, showing a wooden surface.
- Will ensure that people working for you keep everything confidential
  - Will keep everything safe
  - Will only engage sub-processor with prior consent of controller and a written contract
  - Will assist controller with any subject access requests/when they need assistance
  - Will delete/return data to controller when requested at end of contract

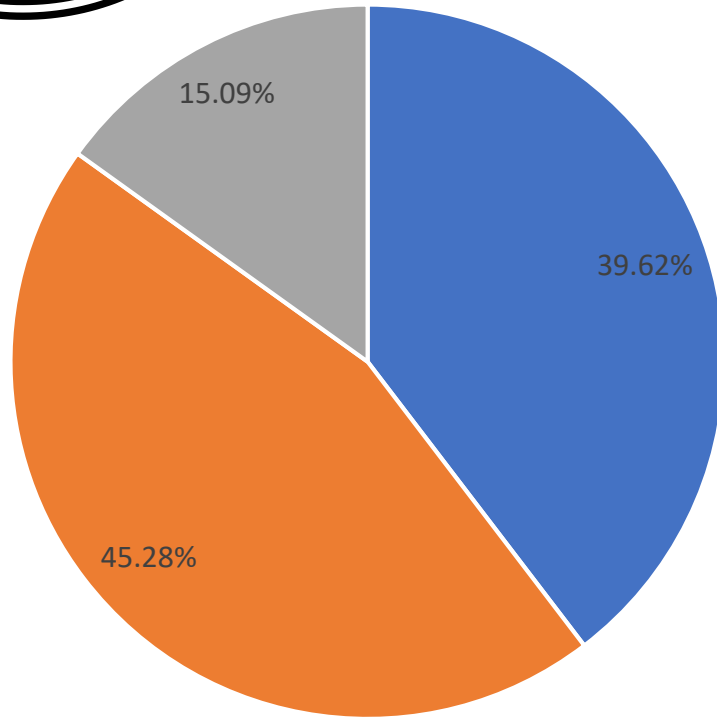
# If you're a Processor

- Register with the Authority (and pay £)
- Can't use sub-processor without controller saying it's ok
- Need to have make sure that keep things safe
- Keep records of processing activities. Doesn't apply if fewer than 250 employees
- Tell controller without undue delay after becoming aware of a breach
- Don't send data out of Jersey unless it's safe/appropriate



Processing  
data  
outside of  
Jersey

Do you process data  
outside the Bailiwick of  
Jersey?



■ Yes ■ No ■ I don't know

Do you have Controller /  
Processor agreements in  
place?

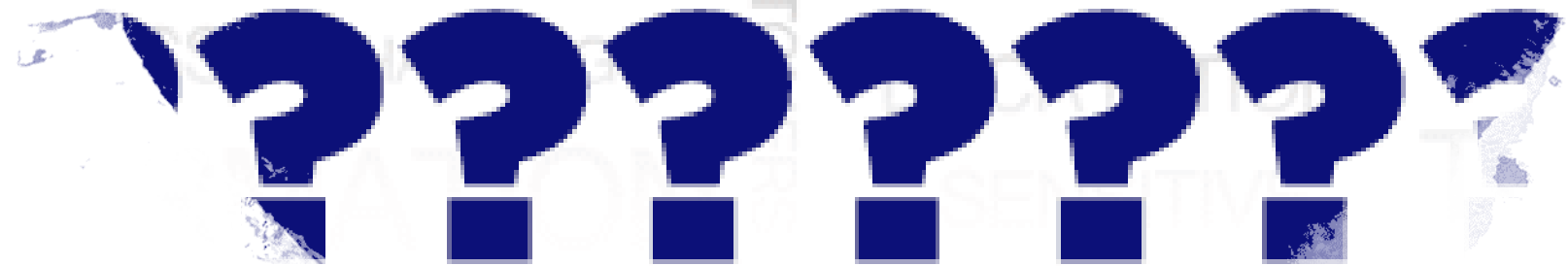
34% Nothing in place

28% All agreements in place

23% Had most of the agreements in place

15% Had some of the agreements in place

PERSONAL PERSONAL  
ONAL INCURSION  
HACKERS THEFT  
DATA BANKS  
CREDIT CARD  
ATTACK ENCRYPTIC  
CONFIDENCE  
THREAT  
LEAK  
VULNERABILITY INTERNET CRIME  
SECURITY CUSTOMER PROTECTIO

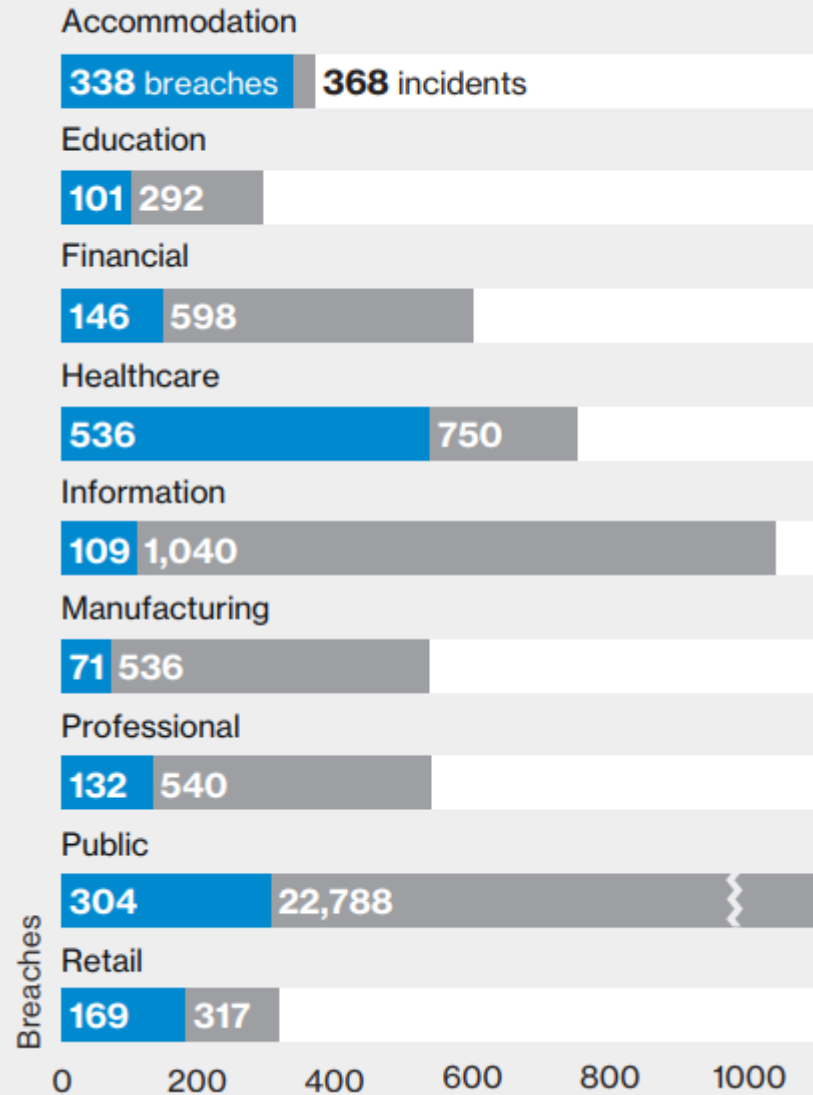


- Have a clear Policy and Procedure in place
- Not all breaches need to be notified, only if there is significant harm to the rights and freedom of the data subjects involved
- 72 hours to notify the Office of the information commissioner



- Hold and update the internal breach register
- Can be very time consuming and costly
- Make sure your staff know what a data breach is?

## Number of incidents and breaches by sector



## Accommodation

**Who** 99% external, 1% internal

**What** 93% payment, 5% personal, 2% credentials

**How** 93% hacking, 91% malware



It's pretty clear-cut where you need to focus. 90% of all breaches involved POS intrusions. In fact, you're over 100 times more likely than the median industry in our dataset to have a POS controller targeted.



Images are Personal Information

Keep for 30 days maximum

Must be provided as part of a Subject Access Request

No cameras in private areas

Placement of viewing monitors



# POLICIES, PROCEDURES AND REGISTERS

Data Protection Policy  
Data Subject Access Policy and Procedure  
Data Retention Policy  
Data Breach Notification Policy and Procedure  
Data Protection Impact Assessment Policy  
Data Security Policy

Data Activity Register  
Data Protection Impact Assessment  
Data Breach register  
Data Subject Access Register  
Data Retention Schedule



# 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

14% Data Inventory Register

14% Data Impact Assessment Register

17% Breach Register

Policies, procedures and registers

