

# 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 Jersey Retail 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.
- 3<sup>rd</sup> Party agreements
- Data Breach
- Requirements for CCTV security systems
- Requirements for your website
- Prepare for and cope with the rights of individuals (like the right to Access)
- Apply the regulation to your business with a step-by-step guide
- Gain confidence in your approach to compliance



## 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.

## Island Global Research – April-May 2018

### Loyalty card ownership (Jersey)

% that owned store loyalty card – 67% in Jersey

### Levels of trust in organisations that handle personal data (Jersey, Guernsey, Isle of Man)

40% do not trust Store Retailers - 26% do trust

37% do not trust online retailers – 28% do trust

37% do not trust government depts – 32% do trust

7% do not trust doctor – 80% do trust

### Level of concern compared to a year ago (Jersey)

45% more concerned about the privacy and security of their personal data

54% about the same as a year ago

1% less concerned

### Areas of Concern (Jersey, Guernsey, Isle of Man)

62% concerned about contactless payment

65% Unsolicited direct marketing

69% targeted advertising

83% identity theft

### Effected by loss or misuse of personal data (Jersey, Guernsey, Isle of Man)

45% know someone or have been personally affected

53% of those personally affected incurred financial loss

## What is the Impact to your business

- One of the most vulnerable to data breaches (Verizon 2017 Data Breach Investigations). It is no surprise that the industry accounted for the fourth largest share of security breaches in 2017.
- It is imperative that Retail businesses upgrade their data protection processes, or they face the risk of severe financial penalties, reputational damage and business disruption.
- £38 million in GST during 2017, Tourists spent £15 Million
- Retail employs 7,760 people in Jersey



# 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 2**  
Data mapping  
& audit

**Step 4**  
Staff training and  
awareness

**Step 5**  
Business support  
and monitoring  
compliance

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

**LEAN-JSY**  
EFFICIENT & EFFECTIVE



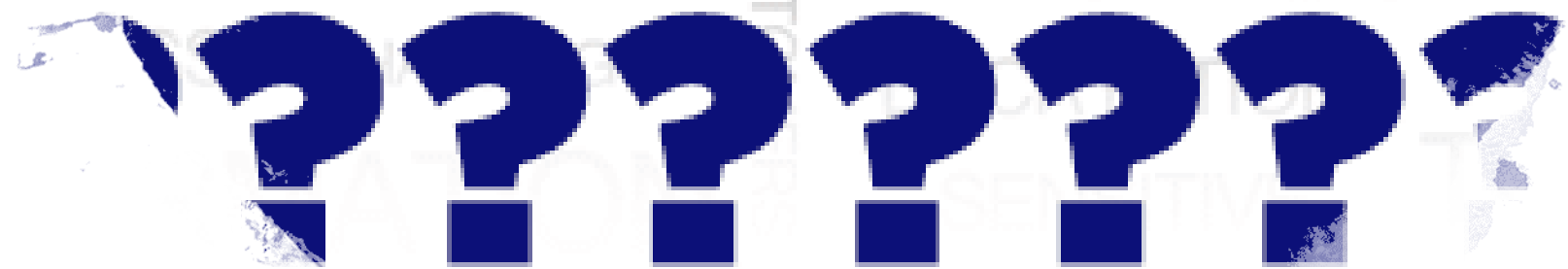
# Marketing



- **Capturing and using personal data** Personal data must be collected for specified explicit and legitimate purposes.
- **The Retail sector must ensure customers are aware of the particular uses of their data.**
- **Employ a strategy to obtain consent** (if this is the legal basis used) 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.**



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



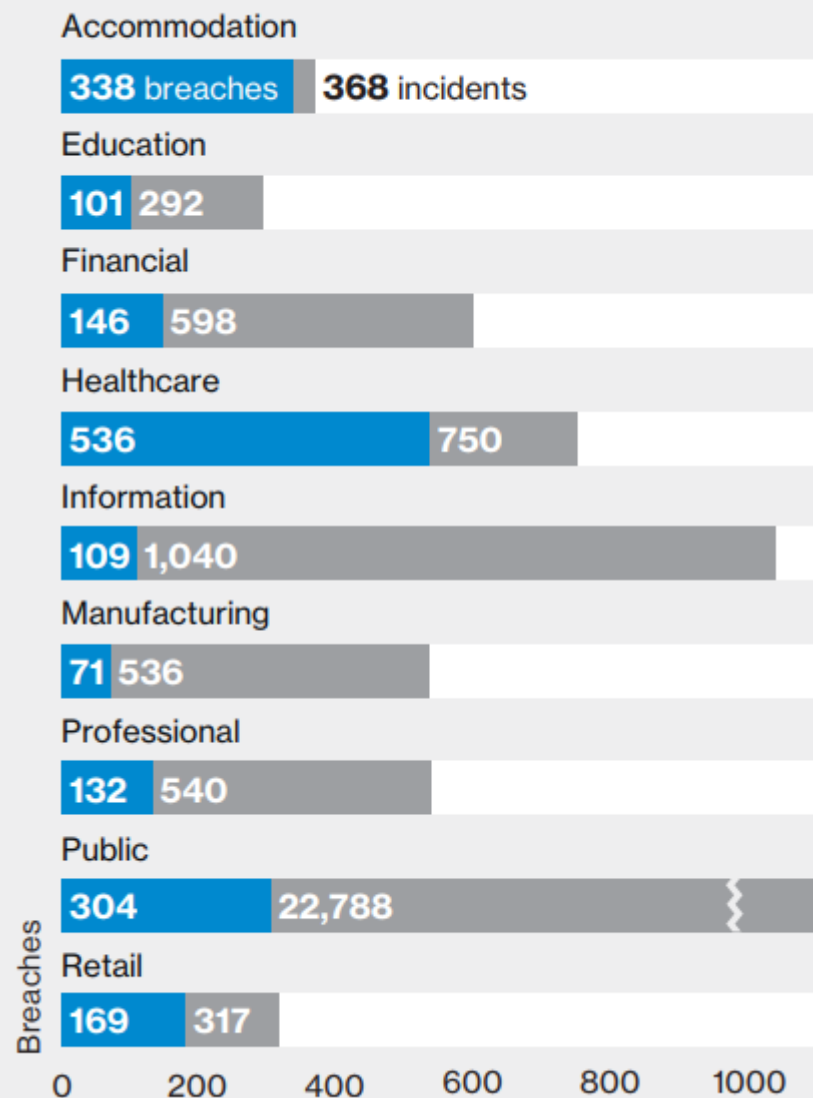
- Have a clear Policy and Procedure in place
- Not all breaches need to be notified, only if there is significant harm to the rights and freedom of the data subjects involved
- 72 hours to notify the Office of the information commissioner



- 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



## Retail

**Who** 91% external, 10% internal

**What** 73% payment, 16% personal, 8% credentials

**How** 46% hacking, 40% physical



In terms of data theft, web application attacks leveraging poor validation of inputs or stolen credentials came top. But it's not just the theft of data you need to worry about. Denial of service attacks can have serious consequences, including preventing transactions being processed and slowing down your website and in-store systems.

Images are Personal Information

Placement of signage to let customers know you have CCTV in operation

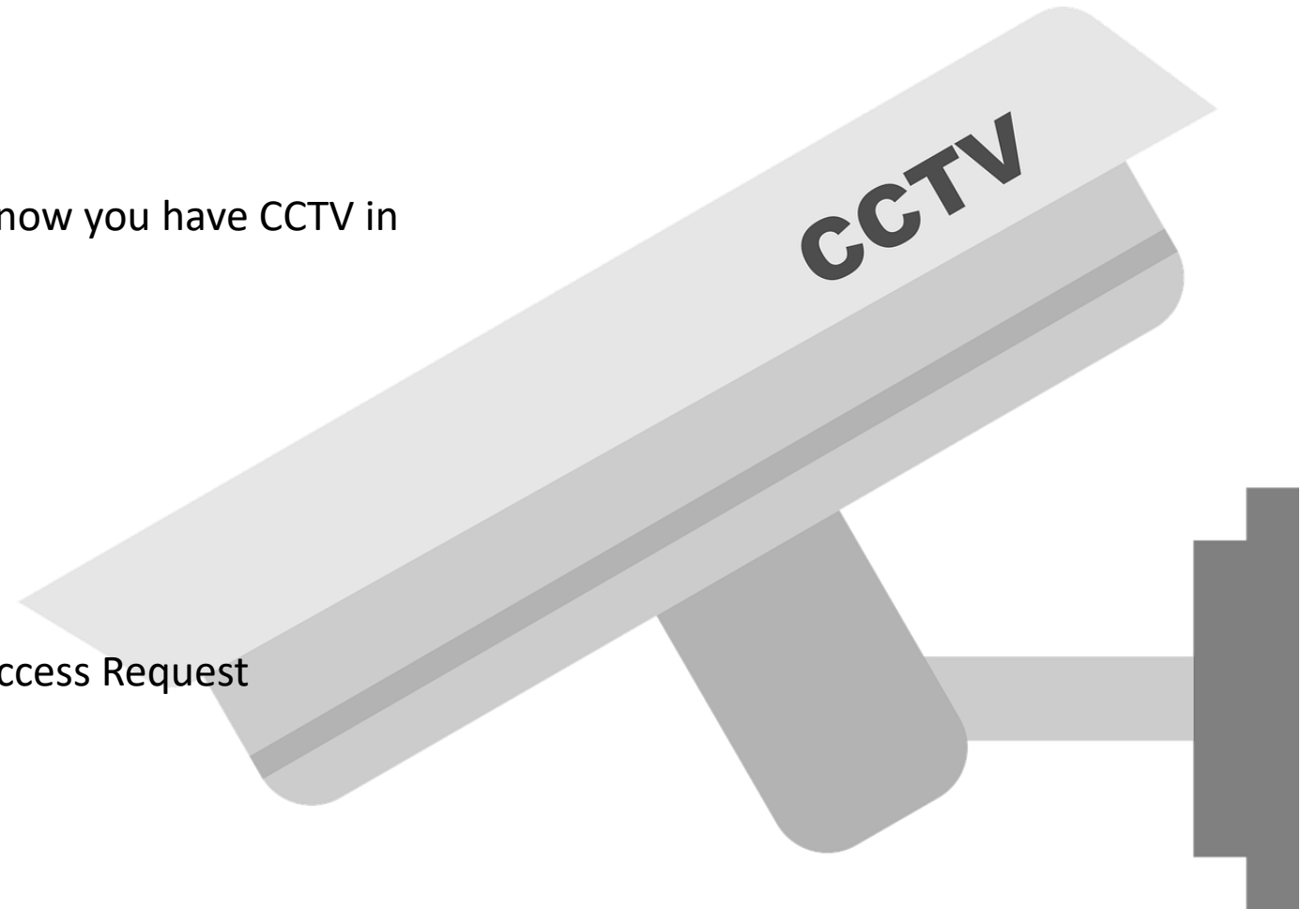
Contact details of system operator

Keep for 30 days maximum

Must be provided as part of a Subject Access Request

No cameras in private areas

Placement of viewing monitors

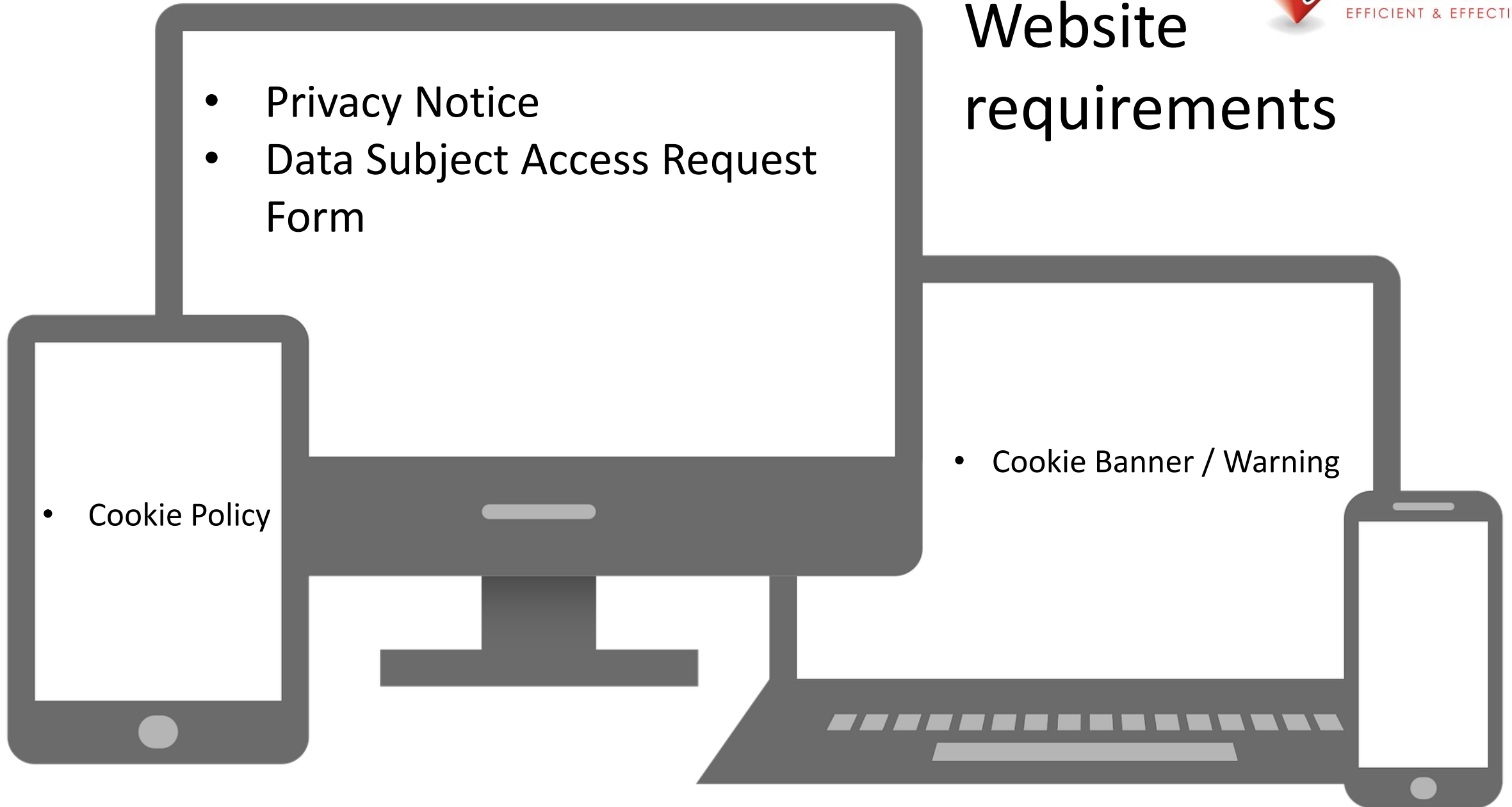


# Website requirements

- Privacy Notice
- Data Subject Access Request Form

- Cookie Banner / Warning

- Cookie Policy

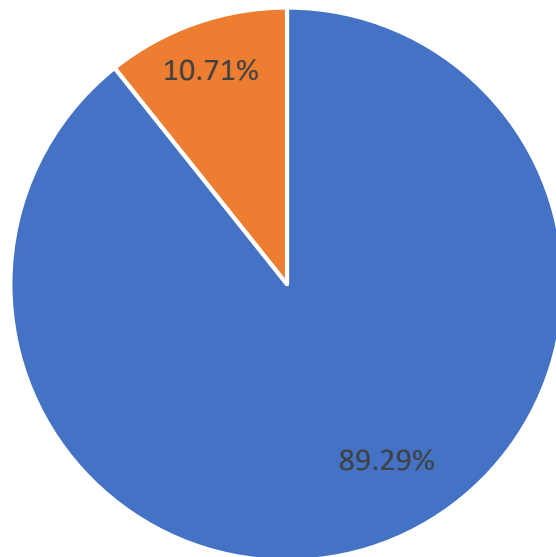






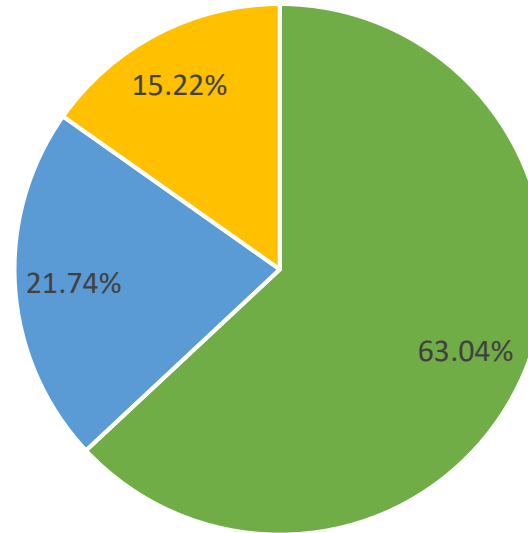
Website

Do you have a website for your business?



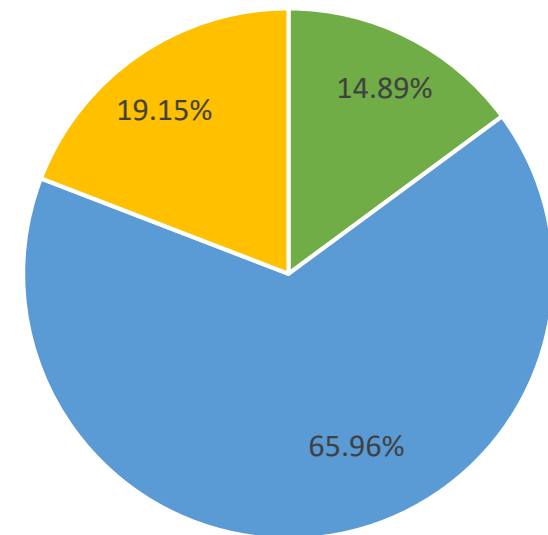
■ Yes ■ No

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



■ Yes ■ No ■ I Don't know

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



■ Yes ■ No ■ I don't know

# 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 and/or Vexatious
  - 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.



## 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 faint text, including the word "Signature" and "Statut". 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

# 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





**LEAN-JSY**  
EFFICIENT & EFFECTIVE

