## 10 Things You Need to Know and Do

### Awareness
- Inform the Board
- Assign clear responsibility
- Communicate to and engage all staff
- Create a strategy with reporting to the Board

### Know your data
- Why do you process data?
- Whose data?
- What data do you process?
- When do you obtain it?
- Where is it kept/ transferred?
- How long is it kept?

### Accountability
- Onus on business to demonstrate and document compliance:
  - lawful, fair & transparent,
  - purpose limitation,
  - data minimisation,
  - accuracy, storage limitation, integrity and confidentiality

### Transparency
- Inform Data Subjects:
  - who you are;
  - why you process data;
  - what you will do with it;
  - how long will you keep it.
- Advise them of their rights and how to exercise them.

### Consent
- New rules for obtaining and withdrawing consent
- Additional rules for children
- Clear plain language
- Tangible evidence of consent

### Security
- Adopt measures to ensure ongoing confidentiality, integrity, availability and resilience
- Ability to restore timely access after incident
- Regularly tested

### Data Protection Officers (DPO)
- If required appoint a DPO with knowledge
- Reports to highest level of management
- Cannot be instructed
- Duties cannot conflict

### Privacy by Design/DPIAs
- DP requirements ‘designed in’ to any new project from outset
- Mandatory DP Impact assessments and prior authorization
- Involve DPO

### Rights
- New and enhanced
- Free to exercise with reduced compliance time
- Right to object, data portability & more

### Scope/Penalties
- IOM law by May 2018
- Equivalent to EU General Data Protection Regulation
- Applies to Data Processors as well as Data Controllers
- Fines up to 4% of turnover

---

www.inforights.im  May 2017