

## CEO



## ORGANISATION



## RISKS



## PROCESSES



## TECHNOLOGY



- ✓ I take a front seat and ensure that my board fully supports and understands GDPR
- ✓ We have a Data Protection Officer or a dedicated go-to resource to manage our obligations under the GDPR
- ✓ We know which and how departments will be impacted across the business
- ✓ We have assessed and updated our Privacy Policies
- ✓ We have allocated a budget for GDPR compliance management
- ✓ We have allocated internal resource to help manage compliance
- ✓ We have identified our third party suppliers and understand their policies

- ✓ We understand our level of corporate risk
- ✓ We understand that fines of up to €20m or 4% of annual turnover aren't the only risk - reputational damage is also likely
- ✓ Our dedicated DPO manages our evolving risk profile, covering:
  - Consent
  - Transparency
  - Data Minimisation
  - Data Portability
  - Right to be Forgotten

- ✓ We have mapped the inbound and outbound flow of data for our organisation
- ✓ We can identify the source of all data
- ✓ We know what kind of personal data we're holding, including sensitive data
- ✓ We are open and transparent about how we use and share the personal data we hold
- ✓ We can demonstrate that we have obtained consent to use this data
- ✓ We have processes in place to delete data when it is no longer required, when our intended use of the data has changed or when the data subject asks for it to be erased
- ✓ We have created systems to manage a data breach
- ✓ All data is encrypted and stored securely
- ✓ We can fulfil subject access requests

- ✓ Using Sytorus' PrivacyEngine, we easily track and manage all of our data processes across the organisation
- ✓ We can be fully accountable in one click should the ICO come knocking!
- ✓ We can demonstrate that our systems have privacy by design built-in