



LAW SOCIETY

> **FINUAS** Network



Annual In-house and Public Sector Conference

Adrienne Harrington

The Law Society Finuas network is funded by member companies and the Finuas Networks Programme, managed by Skillnets, funded from the National Training Fund through the Department of Education and Skills.



LAW SOCIETY
> **FINUAS** Network




Takeaways

- However, if you have been compliant with the Directive/Act(s), the GDPR is more of an incremental step
- Ability to demonstrate compliance is key
- Systems must implement Data Protection by Design and by Default


You should not be the DP Officer!

25 May is not negotiable - no transitional arrangements!

Data Subjects Rights

1. Processed lawfully, fairly and in a transparent manner
 2. Collected for specified, explicit and legitimate purposes and for further processed in a manner than is incompatible with those purposes
 3. Adequate, relevant and limited to what is necessary
 4. Accurate, and where necessary, kept up-to-date
- 

Data Subjects Rights

5. Kept in a form that permits identification of DS for no longer than is necessary
 6. Processed in a manner that ensures appropriate security of the personal data
 7. Controller shall be responsible for, and to able to demonstrate compliance with DP principles
- 

Data Subject Rights


- . How many of these rights apply to data in your systems?

Subject access requests- do you know where all the data is?


How would you “forget” someone from your systems? Would you be prepared to certify to this?

Are your systems capable of enforcing restricted processing?


Data Subject Rights

- Are workflows to support these rights built in to your systems?
 - Can you easily rectify data across all systems?
 - What about unstructured data?
- 


Data Breach Notification

- ◆ Are you ready for a data breach?
 - ◆ Have you an incident response plan?
 - ◆ Is it tested?
 - ◆ How would you know if you had a breach? Do you review security events and alerts?
 - ◆ How quickly could you mobilise an incident response team with all the necessary skills? Who'd be on your team?
- 


Data Breach Notification

- ◆ What about your processors?
 - ◆ Do you keep records of data breaches and security incidents?
 - ◆ Mandatory reporting
- 


3rd Parties/Data Processors

- ◆ The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the Regulation and ensure the protection of the rights of the data subject.
 - ◆ Controller must only appoint a processor under a binding written agreement.
 - ◆ Regulation is quite prescriptive on what this agreement must contain.
 - ◆ Does your standard contract reflect GDPR requirements?
- 

3rd Parties/Data Processors

- ◆ How well do you know your supply chain? What about sub-processors?
 - ◆ Are there written contracts with all processors and sub-processor?
 - ◆ Have they been given instructions on what security controls are expected?
 - ◆ What happens on termination of a contract?
 - ◆ Do you have a right to audit? Will you exercise this right?
- 

Cloud Service Providers (CSP)


- ◆ Cloud services not precluded by GDPR
 - ◆ Some CSPs advertise as improving your GDPR compliance
 - ◆ OGCIO framework 'Advice Note: Considering Cloud Services'
- 

Demonstrate Compliance


The controller shall be responsible for, and be able to demonstrate compliance with, data protection principles ('accountability')

- ◆ Privacy Impact Assessment
- ◆ Keep records of your processing activities
- ◆ Adhere to codes of conduct where applicable
- ◆ Follow WP29 advice
- ◆ NB Document your due diligence and risk assessment
- ◆ Adopt internal policies and adhering to them
- ◆ Follow lead of DPO once in place

Where are you on Action Plan?

1. Inventory and map your data
 2. Supply Chain Audit
 3. Review processor and sub-processor contracts
 4. Assess your current systems
 1. Access control
 2. Auditing
 3. Right to be Forgotten
 5. Review infrastructure and system resilience
- 

Action Plan contd

6. Review Disaster Recovery/Business Continuity Plans
 7. Review/create security audit plans
 8. Create Incident Plan/Team
- 

Action Plan contd

9. Enshrine Privacy by Design, new and existing systems

10. Document as you go

11. Staff training - check central provisions

12. Is GDPR on your Risk Register?

13. DPO?