GDPR ALIGNMENT HE SECTOR

WARWICK

25th MAY 2018

Information and Data Director, Senior Solicitor DPO for

The University of Warwick

GDPR: IMPLICATIONS

- Group Liability.
- Penalties for violations are significant: breaches & non compliances.
- Broader territorial reach.
- Burden of accountability on institutions is much higher.
- Actively need to demonstrate compliance.
- DPIA/Consent.
- Contractual liabilities – indemnity.
- Claims for compensation & Legal claims.

WARWICK

ALIGNMENT WITH THE GDPR

- DP by design and default– Article 25, Article 5 *all processing activities.*
- Have your DPIA embedded in key processes. Procurement/ethics approval/partnerships . Don't forget your screening questions. Article 35
- Ensure you are relying on the appropriate lawful basis for processing. C=P.
- Art 30 – Records of processing/IAR – blueprint/data inventory.
- Ensure your agreements meet the requirements of the GDPR Art- 28/32/35.
- Adhere to data subject rights & the principles – ICO's 12 steps .
- Look at your data capture points – Enrolment / Research/Employment – PN.
- Aim to have single repositories with role based restricted access to avoid duplication, BCDR, ease of adherence to data subject rights.

ALIGNMENT WITH THE GDPR

- Documented policies and procedures for data protection and information security.
- Robust systems to store data.
- Privacy notices.
- Enforced mandatory training for all staff.
- Data classification policy.
- Records management policy.
- Record retention policy.
- Embedding DP by design and default across all appropriate University policies and procedures /implementation and enforcement of those policies.
- Breach response plan with a procedure for staff to report – only 72 hours to respond.

- The following risk-factors will should be used by the data protection team to identify high priority contracts: Formulaic approach to this :
    - Processing of biometric data.
    - Processing of special category data.
    - Processing of children’s data.
- International transfers of data.
- Profiling.
- Volume of data processed.
- Value of the contract.
- Contractual indemnities – processor.

TASKS OF THE DATA COMPLIANCE TEAM

Accountability Processes & Governance	To implement compliance Create a governance structure to support accountability requirements– eg procurement process .
DP Bill	Respond to the requirements of the UK Data Protection legislation when the DP Bill when it comes into force.
E-privacy Regulation	Respond to the requirements of the E-Privacy Regulation when it comes into force.
GDPR Gap Analysis	Identify what needs to be updated or newly introduced to comply with the GDPR compliance requirements after the outcome of the data inventory.
Implementation	Create a compliance programme to address the compliance gaps and an assurance programme on which the DPO can rely.
Contracts	Contracts contain data protection provisions to meet GDPR requirements and address accountability, privacy by design and default.
Cross-Border Data Transfers	Review legal mechanisms for cross-border data transfers from the EEA .
Systems	Review of key systems
Data Subjects' Rights	Prepare policies and procedures to ensure requests to exercise rights can be handled effectively.
Data Breach Notification	Breach Response plan. Prepare a policy, a breach notification procedure and process
Carry out Departmental Audits	To have in place audit/monitoring compliance plan

DATA TRANSFERS OUTSIDE THE EEA

Transfers within the EEA

Permitted.

Transfers outside of the EEA on the basis of adequacy ruling from the EU

Permitted - countries deemed by commission as having appropriate protection for rights and freedoms of its citizens :

Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay

Transfers subject to appropriate safeguards – third countries

Model Contracts
Condition of contract/consent/vital interests
BCR

Processing centre/office abroad/ representative office abroad

Check local jurisdiction . If you are the DPO you may need to register locally – Singapore.
Check your obligations for DP under any partnering arrangement.
Representative staff – encrypted devices – are they routinely transferring personal data to you from outside the EEA. China – regular info sec assessment.

YOUR MAIN DATA SUBJECT POOLS ARE

Students

Privacy notice enrolment process/application process cross refer it to your data life cycle.
Data Flow maps System Supplier Due Diligence.

Research

Consent Privacy Notice Data Flow Map System supplier Due diligence.

HR – applicants /employees

You should be relying on performance of a contract / LI for employment type matters – anything else which falls outside of this will require consent.
Consent Privacy Notice Data Flow Map System Supplier due Diligence.

Effectively balancing the need to meet GDPR expectations whilst continuing with institutional targets

- SMT to adequately resource the data protection function
- DPO – ability to act independently and has a budget
- Multi disciplinary team
- Legacy arrangements an issue – huge deluge of live contracts which requires technical resource
- Risk Register
- Data Strategy/ Road Map – documented

REVIEW

- Local data handling practices and procedures – document.
- Email circulations – mass emailing policy .
- Access controls.
- Clear desk policy.
- Confidential waste.
- Secure deletion.
- Encrypted devices.

DATA HELD

- What data is it?
- Why are you holding it held? Goes to the Purpose Principle.
- Where did it come from? Data subject or did you buy a list?
- Who are you sharing the data with?
    - Review your data sharing terms with third parties, including those processing data on your behalf.
    - Review details of transfers to third countries – check whether you are legally allowed to do this.
- What is the lawful basis for processing?
- Retention?
- Secure?
    - Consider technical and organisational security measures (how is the data handled/transferred/stored?) – encryption? Clear desk? Shredders? Confidential waste?

WORKING GROUP – GDPR DPO HE SECTOR

Have established a DPO working group with support from the ICO comprising of JISC and key stakeholders from the HE sector – multi partner DPO team.

Aim – offer practical guidance through a collaborative approach so there is consistency in the sector with a view to influence codes of practice.

Templates - e.g PN/ Security Measures / Consent.

Contact

My details are available on the Warwick University Website on our Data Protection Policy