GDPR – what is the accountability principle and the role of the Data Protection Officer?

13 June 2019
What we’ll cover today

- Awareness and the accountability principle
- The role of the Data Protection Officer
Awareness and Accountability
Awareness and Accountability

- Raising Awareness in your organisation

  - Induction procedures vitally important – you may do things differently to a previous employer or there may be no awareness at all of the issues and risks.
  
  - Ensure that all staff have access to and take part in training activities making sure that these are relevant as possible to the education sector.
  
  - Make sure the Governing Body / Board of Trustees take data protection and risk management seriously – ensure regular reporting with the DPO present and serious consideration is given to financial investment/budget allocation for data protection issues.
  
  - Data protection can be looked at as an additional feature of the safeguarding duties you hold.
Awareness and Accountability

- What do we mean by accountability?

- Accountability is one of the data protection principles – it makes you responsible for complying with GDPR. You must be able to demonstrate your compliance.

- There are a number of measures that you can, and in some cases must, take including:
  - adopting and implementing data protection policies;
  - taking a ‘data protection by design and default’ approach;
  - putting written contracts in place with organisations that process personal data on your behalf;
  - maintaining documentation of your processing activities;
Awareness and Accountability

• Measures to take continued:
  • implementing appropriate security measures;
  • recording and, where necessary, reporting personal data breaches;
  • carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals’ interests;
  • appointing a data protection officer; and
  • check whether suppliers commit to any relevant code of conduct or signing up to certification schemes.
Awareness and Accountability

- Accountability:
  - lies with the Governing Body/Board of Trustees; and
  - cannot be sub-contracted – so outsourcing the DPO role does not address the risks of data protection non-compliance.
The role of the DPO
The Data Protection Officer
Roles, responsibilities and relationships

Why you need a DPO:

• Section 69 DPA
• Article 37 GDPR
• Good governance
• Common sense!
The Data Protection Officer
Roles, responsibilities and relationships

The DPO’s Tasks:

• Inform and advise
• Monitor compliance with GDPR and policies
• Provide advice on DPIA’s
• Co-operate with the ICO
• Act as a point of contact for the ICO
• Receive SAR’s and complaints
• Record keeping
• Promote a data protection culture within a school
The Data Protection Officer
Roles, responsibilities and relationships

Who should be the DPO?

- Expert knowledge of DP law and practice
- Ability to perform the tasks described above
- Expertise should be commensurate with the sensitivity, complexity and volume of data the organisation processes
- Good understanding of the processing and information systems
- Sound knowledge of the administrative rules and procedures of the organisation
- Well placed to promote a data protection culture within a school
The Data Protection Officer
Roles, responsibilities and relationships

Supporting the DPO:

• Must ensure the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data

• Must provide the DPO with the necessary resources and access to personal data and processing operations to enable the DPO to perform the tasks and maintain expert knowledge

• The DPO must report to the highest management level of the organisation

• Early involvement in DPIA’s

• Invite DPO to regular management meetings

• DPO should always attend when DP issues are being discussed
The Data Protection Officer
Roles, responsibilities and relationships

Supporting the DPO continued:

- Give due weight to DPO’s opinion
- Consult DPO promptly when a breach or other incident occurs
- Finance and training
The Data Protection Officer
Roles, responsibilities and relationships

Independence of the DPO:

• Should be a degree of separation between those in charge of the ecosystem and the DPO
• The organisation must not instruct the DPO how to deal with a matter
• The DPO must have no decision-making power
• Cannot be dismissed or penalised for performing the DPO’s tasks
The Data Protection Officer
Roles, responsibilities and relationships

Liability / accountability of the DPO:

• The Controller is liable for compliance with GDPR/DPA
• But there is no express exemption for DPO’s
• Article 29 Working Party Guidance – DPO’s are not personally liable for non-compliance
• Employment contracts/SLA will set out the job description or specification, so performance measured against that
The Data Protection Officer
Roles, responsibilities and relationships

If you outsource or share the role:

• Have you a contract in place?
• Did you perform due diligence as required by GDPR when entering into the contract;
• Is the contract clear on risk allocation – you are paying the provider to manage certain of your risks after all;
• What parts of the service come at additional cost e.g. privacy impact assessments; and
• What financial liabilities are accepted by the outsourcing business – does it carry insurance to support its activities?
If you outsource or share the role continued:

- Be aware that its arguable penalties imposed by ICO cannot be indemnified – but you should be able to claim for costs involved in managing the issues arising; and
- Having outsourced, how do you promote a “data protection culture in your school” (see page 43 of the Toolkit).
questions and answers

Chris Bowen
Associate – Commercial
E: christopher.bowen@wardhadaway.com
T: 0330 137 3459 / M: 07769 677 577