Breakout session:
Managing risk - information security and the data supply chain

ICO Adtech Fact-Finding Forum 2
19 November 2019

ico.
Information Commissioner's Office

ico.org.uk

The main issues...

Confirmed: lack of clarity over controller/processor (and joint controller) arrangements

Confirmed: inconsistent contractual arrangements / terms

Confirmed: over-reliance on contracts as 'guarantees' of security

Confirmed: lack of specific details on security measures

Confirmed: Inadequate and inconsistent DPIAs

A reminder that the law has certain demands

Information Security: Security Principle

GDPR Article 5(1)(f):

"Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"

Do you have the right controls in place?

Information Security: Security of Processing

GDPR Article 32(1):

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk"

Are you confident that security controls for you and your supply chain are appropriate to the level of risk?

Integrating Safeguards: Data protection by design

GDPR Article 25(1):
"Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures [...] in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

Are the technical and organisational controls for you and your supply chain appropriate to the level of risk?

ico.
Information Commissioner's Office

ico.org.uk

Integrating Safeguards: Data protection by default

GDPR Article 25(2):

"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed…"

Do you undertake continuous assessment throughout the lifecycle?

Assessing risk: Data protection impact assessments

GDPR Article 35(1):

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data…"

Are you using DPIAs effectively?

ico.
Information Commissioner's Office

ico.org.uk

Who does what: controllership in RTB

GDPR Article 4(7):

"'Controller' means the natural or legal person [...] which, alone or jointly with others, determines the purposes and means of the processing..."

GDPR Article 4(8):

"'Processor' means the natural or legal person [...] which processes personal data on behalf of the controller"

Article 26
Joint controller arrangement?

Article 28
Controller/processor arrangement?

Do you know who does what, and what this means?

ico.
Information Commissioner's Office

ico.org.uk

A reminder... the main issues

Confirmed: lack of clarity over controller/processor (and joint controller) arrangements

Confirmed: inconsistent contractual arrangements / terms

Confirmed: over-reliance on contracts as 'guarantees' of security

Confirmed: lack of specific details on security measures

Confirmed: Inadequate and inconsistent DPIAs

How can you mitigate these issues?

1. **Controller/Processor:** What are the challenges in determining controller/processor status? For each, how can you meet (and demonstrate you have met) your obligations?

2. **Security controls** What security measures and controls (governance and technical) can you put in place to respond to the nature of ***RTB*** and the issues we identified?

3. **Risk management** How can DPIAs be completed that are tailored to and effective in addressing the issues ***RTB*** presents?

4. How can you bring your contracts into line with the specific requirements of the GDPR and also ensure that any processors are capable of handling personal data securely?

Keep in touch

@ICOnews

ico.
Information Commissioner's Office

ico.org.uk