GDPR Compliance for Bin Sponsors, Programme Managers and Wallet/Card Processors

Q1 2018

BIN Sponsors
- Ensure you have contracts in place with all your programme managers and Wallet/Card Processors inside and outside of the EU.
- Ensure you work towards complying with GDPR over security and transparency

Programme Managers
- Keep records of any processing taking place.
- Ensure consent is in place for marketing messages and processing taking place
- Update privacy statements
- Identify all EU residents

Wallet/Card Processors
- Ensure all your contracts with Data Controllers includes Data Protection wording and joint liabilities
- Data Controllers to sign revised contracts and send them back.
- Ensure breach policy and process has been tested and validated
- Keep records of all processing taking place

Post GDPR

BIN Sponsors
- Review data security features
- Test Subject Access Request process along with deletion of data
- Test data breach process in tandem with PMs

Programme Managers
- Test data breach process
- Test Subject Access Request process along with deletion of data.
- Start keeping records of all data coming into and out and destination
- Use DPIA for new schemes using data in connection with BIN sponsors

Wallet/Card Processors
- Keep copies of what processing has taken place
- Test security processes
- Test Subject Access Requests and breach reporting

Ongoing

BIN Sponsors
- Self audit all GDPR processes and policies to ensure you can prove the level of GDPR compliance is correct if asked to in conjunction with PMs
- Continue to review processing and privacy statements
- Review contracts as new PM's and Wallet/Card Processors come on board

Programme Manager
- Self audit all GDPR processes and policies to ensure you can prove the level of GDPR compliance is correct if asked to, in conjunction with BIN sponsors
- Continue to review processing and privacy statements
- Submit practise audit of Wallet/Card Processors

Wallet/Card Processors
- Continue to keep records of all processing and be available for audit
- Continue to keep security up to date with the latest security updates
- Test security features as part of an ongoing assessment

Development Phase

Existing customers
- Can you prove you have clear explicit permission
- for all uses of the data you hold?
- Have you informed them of their rights to:
  - I. Object to profiling?
  - II. Erase data?
  - III. Transfer their data to someone new?
- If the answer is No to any of these questions you
- may need to 'refresh' your consents

New customers
- Start sending the new data protection policy
- setting out the new rights and a new fair processing
- notice
- Data protection safeguards must be built into products and services from the earliest stage of development

(Privacy by Design) (See also step 3 if additional IT functionality required)

Annual contracts
- Start sending customers new data protection
- policies which set out their new rights and a new
- fair processing notice

Checking Phase

Consider & review:
1. What consents do you have and are they GDPR
2. compliant?
3. Customer journeys and terms and conditions
4. Marketing, competitions and promotions
5. Fair processing notices
6. Privacy Policies
7. Website terms
8. Who is your current DPO

Existing customers
- Can you prove you have clear explicit permission
- for all uses of the data you hold?
  - I. Have you informed them of their rights to:
  - II. Object to profiling?
  - III. Erase data?
  - IV. Transfer their data to someone new?
- If the answer is No to any of these questions you may need to 'refresh' your consents

New customers
- Continue sending the new data protection policy setting out with the new rights and a new fair processing notice
- Data protection safeguards must be built into products and services from the earliest stage of Development (Privacy by Design)

12 Step 24HR Data Breach Response Plan

1. Mobilise crisis management team with support from communications and legal advisers,
2. Record the date and time when the breach was discovered, as well as the current date and time when response efforts began, i.e. when someone on the response team is alerted to the breach
3. Alert & activate everyone on the response team
4. resources, to begin executing your incident response plan
5. Secure the IT systems affected by the cyber attack to help preserve evidence
6. Stop additional data loss. Take affected equipment offline but do not turn them off or start probing into the computer until your forensics team arrives
7. Document everything known so far about the attack
8. Protect your reputation with an internal and external communications
9. strategy, supported as necessary by crisis communications specialists and/or reputation lawyers
10. Interview those involved in discovering the breach and anyone else who may know about it
11. Review protocols regarding disseminating information about the breach for everyone involved in this early stage
12. Notify ICO, if needed, after consulting with legal counsel and upper management and insurance broker(s) to ensure compliance with policy terms
13. Report to police, if/when considered appropriate

Written and Published by David Parker and Simon Hinks of Polymath Consulting. Contact: davidparker@polymathconsulting.com & simonhinks@polymathconsulting.com

polymath consulting