ADVICE & ACTION POINTS ON CYBER THREATS

Industry Colleagues Make Tech Fly list advice on what actions to take to avoid an incident

1. **Review how and where you receive data**
   Identify the digital interfaces through which you receive data and assess who is sending it to you.

2. **List all data exchanges within your operation**
   e.g. Handling Requests, Fuel Orders, Catering, or any other operational data transfers. EASA Part IS already requires this level of understanding.

3. **Analyse the type of data being received**
   Determine what the data contains, whether it includes Personal Identifiable Information (PII), and whether it is coming from secure or insecure sources such as unencrypted email.

4. **All Data Requires Protection. Personal Data demands the Highest Level Security**
   The UK Data (Use and Access) Act 2025 and GDPR require strict protection of personal data. The Information Commissioners Office, ICO provides a useful guide *here*. You are responsible for any PII you hold, and the ICO can issue fines of up to £17.5m or 4% of global turnover for breaches in security.

5. **Example**

   You receive an email containing PII where the sender has 'cc'd all'. Your email system now contains sensitive data. If a staff member loses a phone or your emails are compromised that data is at risk.

   Action

   - ***Delete the source data*** and request that the sender removes the PII if it is not relevant to you. ***Consider if you need the PII*** – eg: can you manage the request with just a surname?

   Ensure you can anonymise or securely store required data

   - If the PII data ***is*** required, confirm your server can anonymise the data.

   Notify Affected Data Subjects

   - Ensure you inform the data subjects (eg; pax/clients/guest) that their data is on your system. They can conduct a subject data request, SAR. The ICO website offer guidance on SAR compliance.

6. **Storage of handling requests** or such like on your email inbox or transfer into a spreadsheet must ensure there are no PII in the workflows

7. **Anti-virus software** must be maintained on all IT networks, password managers and VPN's. Check that this software is rigorous for detecting a data breach and cyber-attacks. Regularly run vulnerability scans on your websites and email systems.

8. **Storing and using PII has** evolved under GDPR laws globally. Names, passport data and financial details must be handled **securely**.