Peer Support & Data Protection
Key considerations & minimum standards

Aedrian Bekker
Aviation and Clinical Psychologist

Centre for Aviation Psychology
www.centreforavaitionpsychology.com

Alternative title:

PSPs & GDPR
Important things you need to know about, but were too bored/ scared to ask...

About

Clinical Psychologists

Leaders in Aviation Mental Health (EPPSI & EAAP, etc)

Specialise in Peer Support Programmes (PSPs)

± 20 000 pilots/ 11 languages/ >22 AOCs

About

Clinical Psychologists

Leaders in Aviation Mental Health (EPPSI & EAAP, etc)

Specialise in Peer Support Programmes (PSPs)

± 20 000 pilots/ 11 languages/ >22 AOCs

PSPs, GDPR & me

Data Protection Officers & Impact Assessments (DPIAs)

Lack of SMEs in *both* PSPs and

GDPR Fundamentals Standard (similar to ISO 27001)

About

CAP

Centre *for* Aviation Psychology

Clinical Psychologists

Leaders in Aviation Mental Health (EPPSI & EAAP, etc)

Specialise in Peer Support Programmes (PSPs)

± 20 000 pilots/ 11 languages/ >22 AOCs

PSPs, GDPR & me

Data Protection Officers & Impact Assessments (DPIAs)

Lack of SMEs in *both* PSPs and

GDPR Fundamentals Standard (similar to ISO 27001)

Health warnings

A lay person's view

A new(ish) world

Consult your DPOs, lawyers and insurers

Local terms may differ

Share your learning, pls…

PSPs and GDPR

Overview

- Protection of data of individuals residing in the EU & EEA

- Irrespective of an organization's global location, GDPR still applies when dealing with data of EU & EEA individuals

- We live in a digital world, leaving multiple data trails in transit, process or storage

- Yet, confidentiality & trust paramount to success of PSPs

- Consider PSP data = medical data

- Lack of knowledge or awareness for those establishing & overseeing PSPs

PSPs and GDPR

Why does it matter?

- It's the law x 2!

- Penalties: €20m or up to 4% of turnover – whichever is the greater

- PSPs deal with personal *and* sensitive data in a safety critical industry

- Impossible (?) for PSPs not to process data trail *and* be compliant with GDPR 2018 & CAP.GEN.MPA 215

- Data breach risks

- PSPs are data controllers i.e. responsibilities & liabilities

PSPs and GDPR

Useful concepts

- Supervisory Authority e.g. UK ICO

- Data controller vs. data processor

- Legal basis for processing data

- Consent (informed, affirmative and evidence of it)

- Personal <u>and sensitive</u> data

- Subject Access Request/ withdrawal/ erasure

- Data retention, deletion, breach (and related SOPs)

Former GDPR Compliance strategies...

Typical questions…

Accessing PSP

How? (Website/ Phone number? Internal/External?)

How is consent provided & documented?

Who controls data and contact and distribution platforms?

What personal data is requested, transmitted, stored (and logged)?

Typical questions…

Accessing PSP

How? (Website/ Phone number? Internal/External?)

How is consent provided & documented?

Who controls data and contact and distribution platforms?

What personal data is requested, transmitted, stored (and logged)?

Peer Support

Phone/SMS/WhatsApp/email?

Who owns devices, numbers & addresses?

Who else has access to device/ accounts?

What logs kept?

What notes are kept and how?

Centre *for* Aviation Psychology

Typical questions…

Accessing PSP

How? (Website/ Phone number? Internal/External?)

How is consent provided & documented?

Who controls data and contact and distribution platforms?

What personal data is requested, transmitted, stored (and logged)?

Peer Support

Phone/SMS/WhatsApp/email?

Who owns devices, numbers & addresses?

Who else has access to device/ accounts?

What logs are kept?

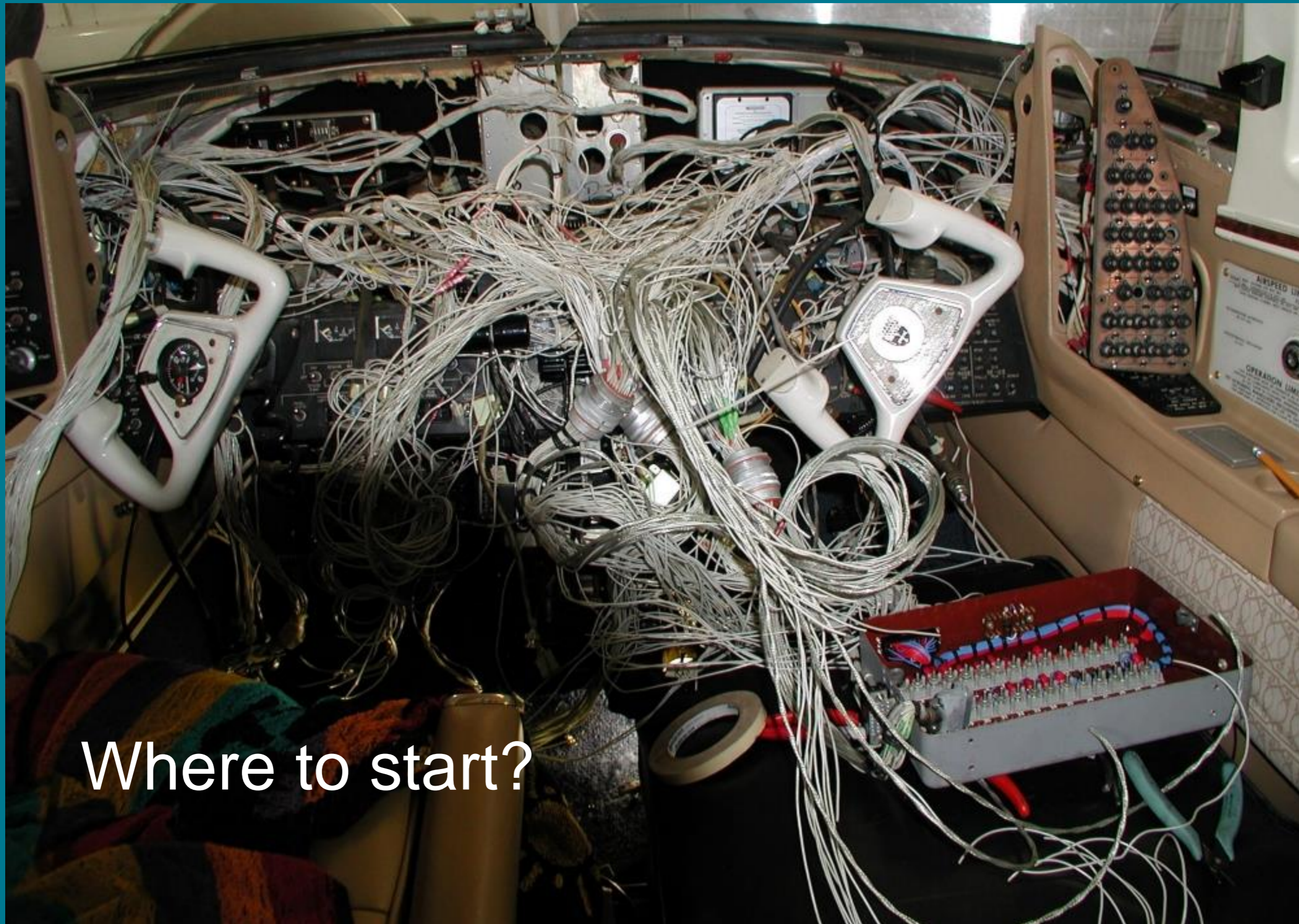What notes are kept and how?

Processing

Escalation policy?

MHP supervision documented?

Subject access request process?

Aggregated data?

Data deletion?

IT security?

Centre *for* Aviation Psychology

Where to start?

Centre *for* Aviation Psychology

PSPs and GDPR

Key policies required

- GDPR policy including :
  - Legal framework
  - Principles & Accountability
  - Method of consent gained
  - Rights of service users
  - Data breach management

- Confidentiality policy (incl note keeping and MHP input)
- (Safety critical) Escalation policy
- Information security policy
- Peer Code of Conduct
- Profess. Indemnity Insurance
- Record taking, storage, retention & deletion

Becoming GDPR compliant

Internal PSPs

Becoming GDPR compliant

Internal PSPs

- Get professional help (easier than DIY);

- Decide on who the data controller is;
- Document within the governance model;
- Map data flow (incl. note keeping; safety critical escalations; MHP interactions);
- Develop & document a thought through GDPR policy and supporting; documentation and processes;
- Train and update peers re GDPR; requirements – esp. personal devices, data breach;
- Peers agree to a code of conduct;
- Professional indemnity cover for

Becoming GDPR compliant

Outsourced PSPs

Becoming GDPR compliant

Outsourced PSPs

Ask for evidence of:

- Registration with the national data/supervisory authority
- Data Protection Impact Assessment including:
  - Data flow
  - Method of consent
  - Data transmission, storage, retention & deletion
  - Safety issue escalation re GDPR
  - Process & documentation for: subject access request; complaints; compliance requests
  - Peer training re GDPR

Thank you!

Aedrian Bekker
Aviation and Clinical Psychologist

Centre for Aviation Psychology
www.centreforavaitionpsychology.com

Centre *for* Aviation Psychology