
DPPC 2024
EMPOWERING YOU
THROUGH INFORMATION
ico.
Information Commissioner's Office
#DPPC24
ico.org.uk/DPPC


DPPC
2024
ico.
Information Commissioner's Office
#DPPC24
ico.org.uk/DPPC

Choosing and using AI

How to do it safely

Slido

Choosing or using?

Where are you in your AI journey?

Why are we here?

In this session, we will discuss:

- What AI is;
- What data protection risks arise from procuring AI tools;
- How to manage those risks so you can benefit from AI;
- Who to involve within your organization to get the most out of using AI;
- How the ICO can help you.

Who are we?

Meet the presenters and the topic for today

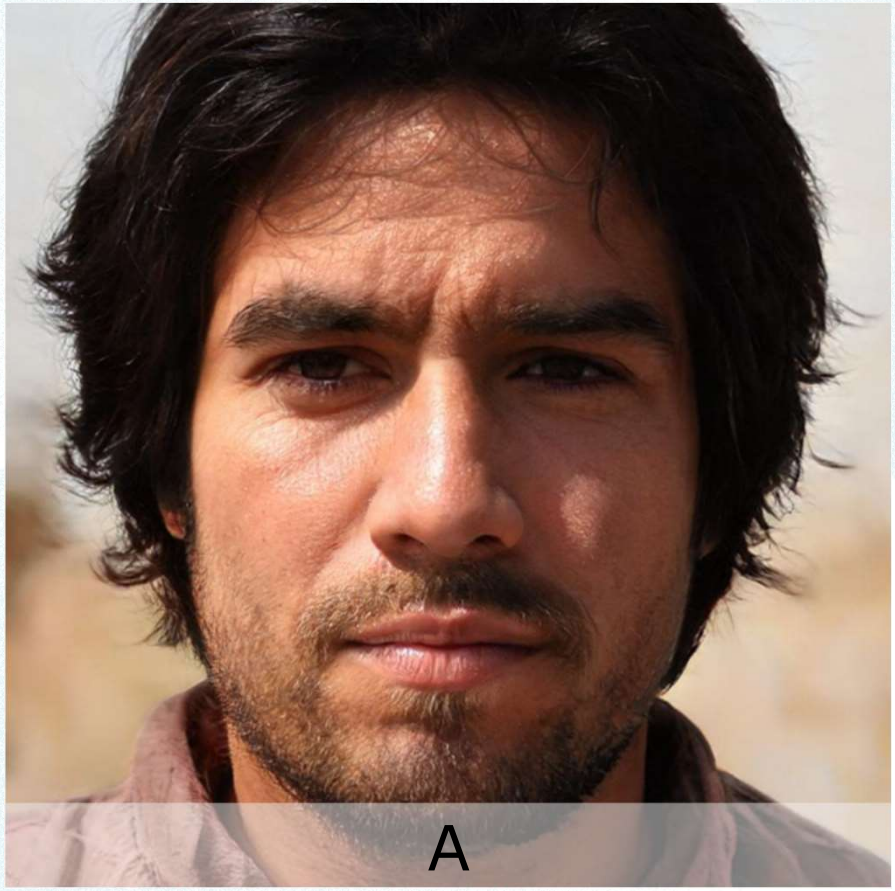
ico.org.uk/DPPC

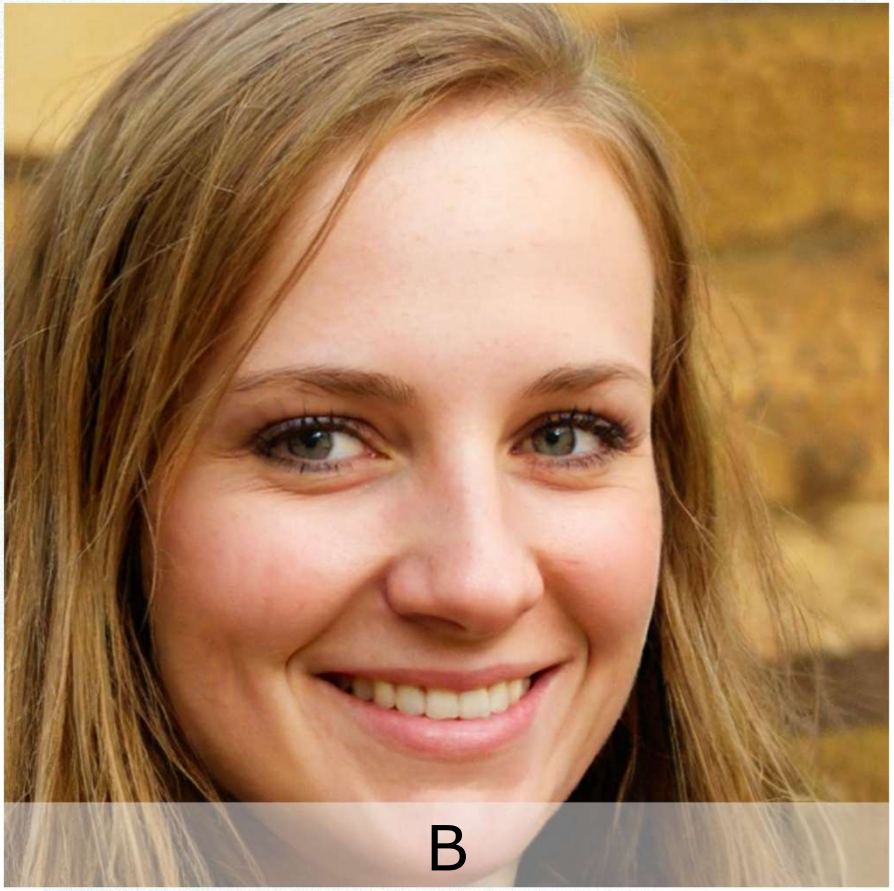
#DPPC24

Image credit: Yutong Liu & Kingston School of Art / Better Images of AI / Talking to AI / CC-BY 4.0

Slido

Human or AI?





Case study: Bougie Ltd and SparkAI

Bougie Ltd makes scented candles. It receives many emails from customers: positive reviews, questions, complaints and refund requests. It also receives some emails which are meant for Boogie Ltd, a disco ball manufacturer, which customers have sent to the wrong address.

Bougie Ltd has heard of SparkAI, an AI tool which analyses customer correspondence and triages it.

Bougie would like SparkAI to answer all the positive reviews and emails intended for Boogie Ltd and escalate all other emails to the customer service department.

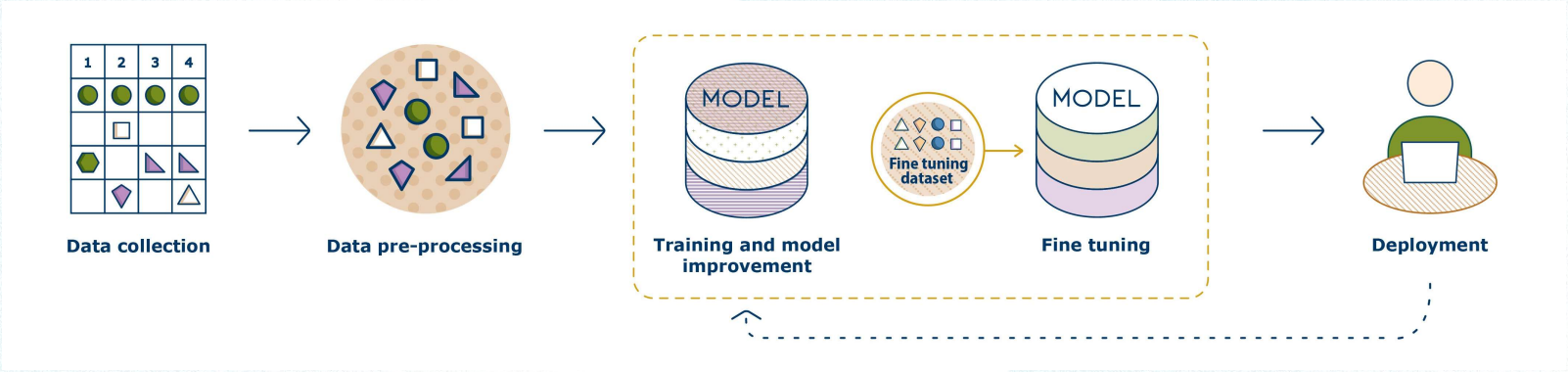
Slido

Risks to consider?

What data protection risks should Bougie Ltd consider?

Accountability: SparkAI's developer (1/3)

- Controller and processor, joint controller, separate controllers…and for which phase?
  - Split it up: development phase, live use phase, improvement phase
  - Who is doing which part of the processing?
  - Who has access to Bougie Ltd's customer data? And for what purpose?



Accountability: SparkAI's developer (2/3)

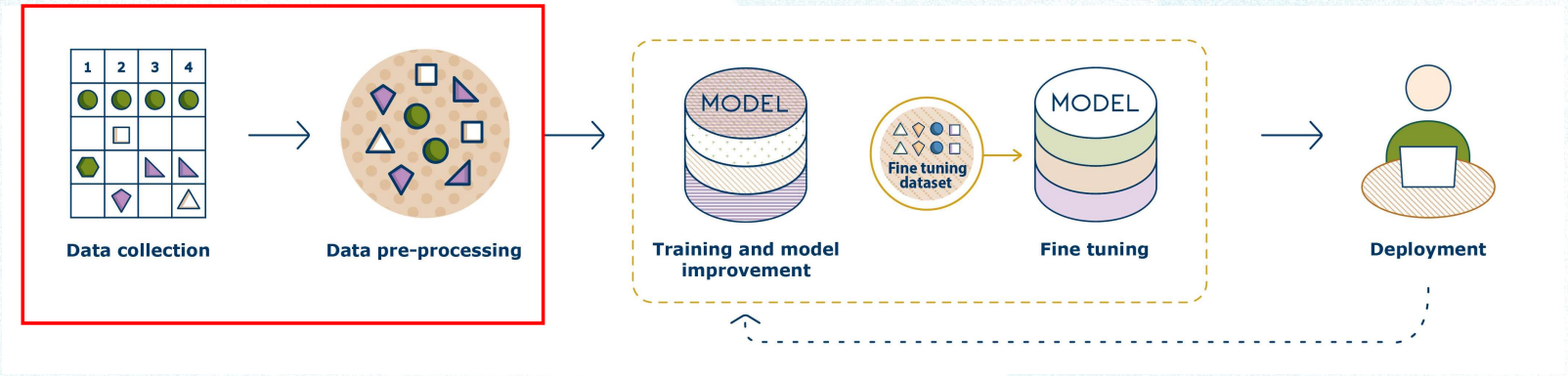
- DPIA
  - Could SparkAI's developer support with it?
  - If not, will Bougie Ltd meaningfully be able to assess and document the risks?

AI and data protection risk toolkit

AI Lifecycle Stag	ID	Risk area UK GDPR Reference	Data Protection Risk Stateme	Risk Assessment Summary	Inhere Risk Ra	Control	Control Objective	Practical steps to reduce th risk	Further ICO Guidance	Practical Steps Your Organisation Will Take	Control Owner	Current sta	Completion d
Business requirements and design	1.1	Accountability Articles 5(2), 35 and 36 and Recitals 74-77, 84, 89-92, 94 and 95.	The misidentification of risks to individual rights and freedoms caused by not carrying out a risk assessment. As a consequence, an organisation cannot put in place appropriate technical and organisational measures to prevent harms occurring to individuals.			Conduct a data protection impact assessment (DPIA)	To identify risks and implement appropriate technical and organisational measures to reduce them.	You must do a DPIA for processing that is likely to result in high risk to individuals. You must, where appropriate, consult with individuals who are likely to be affected by your AI system. If you identify a high risk that you cannot mitigate, you must consult with the ICO before you start the processing. As part of your DPIA, you should consult with the teams within your organisation who will be involved in your project to identify data protection risks of your AI project. The teams you may want to consult include the engineering team, the legal and compliance team, and any staff who will be part of the decision pipeline. You could consult with domain experts who can advise on what risks you should address.	what are the accountability and governance implications of AI? | ICO				
Business requirements and design	1.2	Accountability Articles 5(2) and 24 and Recitals 39 and 74	A lack of accountability over risks to individual rights and freedoms created or exacerbated by AI systems is caused by not clearly assigning roles and responsibilities. As a consequence, risks are left unaddressed, and individuals may suffer harm.			Assign technical and operational roles and responsibilities and provide clear direction and support on the use of AI systems and the application of data protection law	To make it clear who is accountable for mitigating and managing risks in the AI system.	You should appoint a senior owner or senior process owner to drive accountability. You should put in place operational procedures, guidance or manuals to support AI policies and provide direction to operational staff on the use of AI systems and the application of data	Accountability and governance | ICO				
Business requirements and design	1.3	Purpose limitation Article 5(1)(b), Recital 39, Article 6(4) and	Function creep over how personal data is processed is caused by not defining what purpose you will use your AI system. As a consequence, individuals lose control over how their data is being used.			Document each purpose for using personal data at each stage of the AI lifecycle, assess whether they are compatible with the originally defined purpose, and schedule reviews to reassess your purposes and whether	To define what your AI system will be used for, how personal data will be used and prevent incompatible processing taking place.	You must provide clear transparency information to inform individuals about your purposes from the outset. For example, in a privacy notice.	Principle (b): Purpose limitation | ICO				

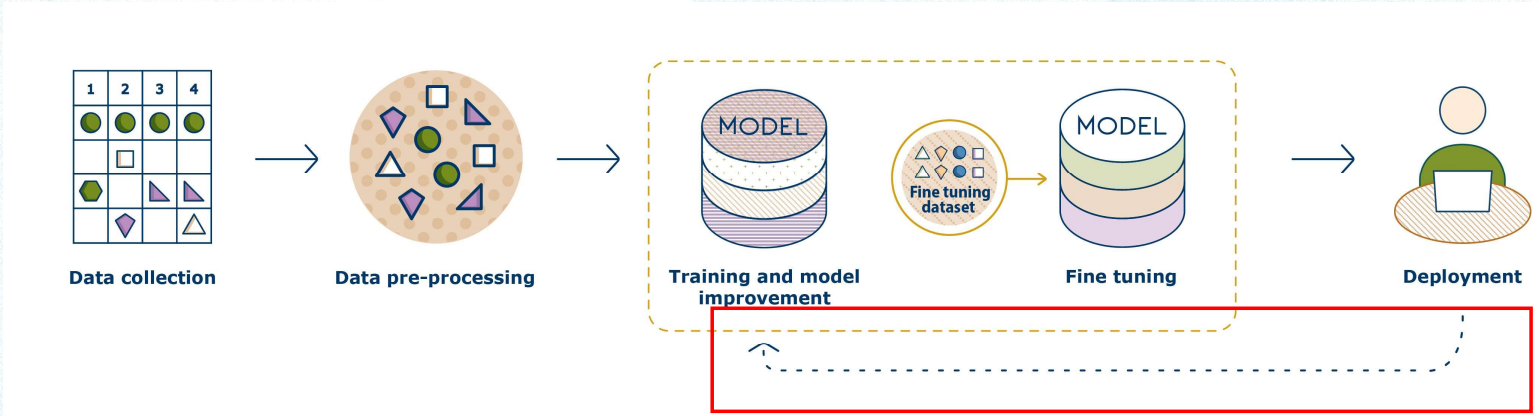
Accountability: SparkAI's developer (3/3)

- Training data: risk of leakage
  - What was SparkAI trained on?
  - Will the training data be repeated in the live outputs?
  - What contractual guarantees can the developer provide about these?



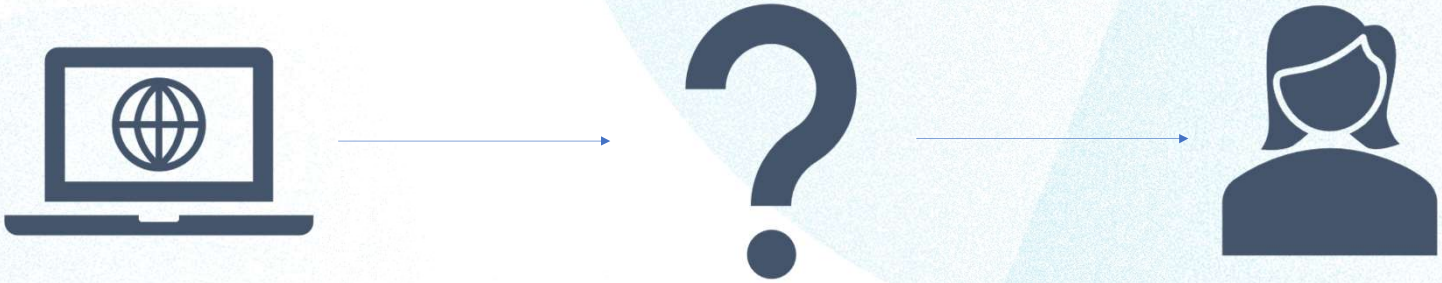
Where will Bougie Ltd's data go? (1/3)

- Access to data by SparkAI's developer
  - Does SparkAI's developer have access to the data?
  - If so, for what purpose?
  - Is Bougie Ltd comfortable with this usage?



Where will Bougie Ltd's data go? (2/3)

- Capability of SparkAI to forward customer emails?
  - Transfers to Boogie Ltd



Where will Bougie Ltd's data go? (3/3)

- Risk of jailbreaking
  - What assurances can SparkAI's developer provide?
  - What tests can Bougie Ltd carry out?

SparkAI's product offerings

	Option one	Option two
Level of customisation	No customisation	Fine-tuned with Bougie Ltd's sample data
Ongoing access to Bougie Ltd's data	Yes	No
Email forwarding functionality	No	Yes
Access to jailbreaking test results	No	Yes
SparkAI provides template DPIA	No	Yes
Price	Lower	Higher

Slido

Which option?

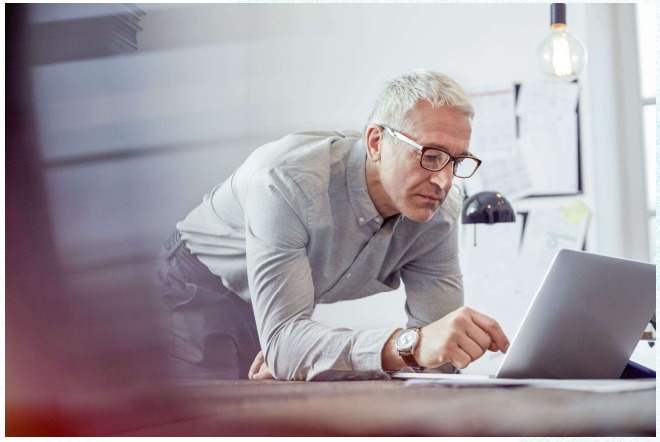
Which option would you choose, and why?

Does it work?

- What are the accuracy rates?
- What are these rates based on?
- Are the tests relevant for Bougie's business environment?
- Are there factors that typically trigger errors?
- Consider false positives and false negative rates
- Can SparkAI's developer support a live test before the full roll out?
- Does Bougie Ltd have benchmarks from previous processes?

Impact on Bougie's customers (1/3)

- Will there be any automated decisions?
  - If so, what is the effect of them?
  - Can a manual escalation process be built in?
  - Is it clear to customers that the SparkAI reply is automated?

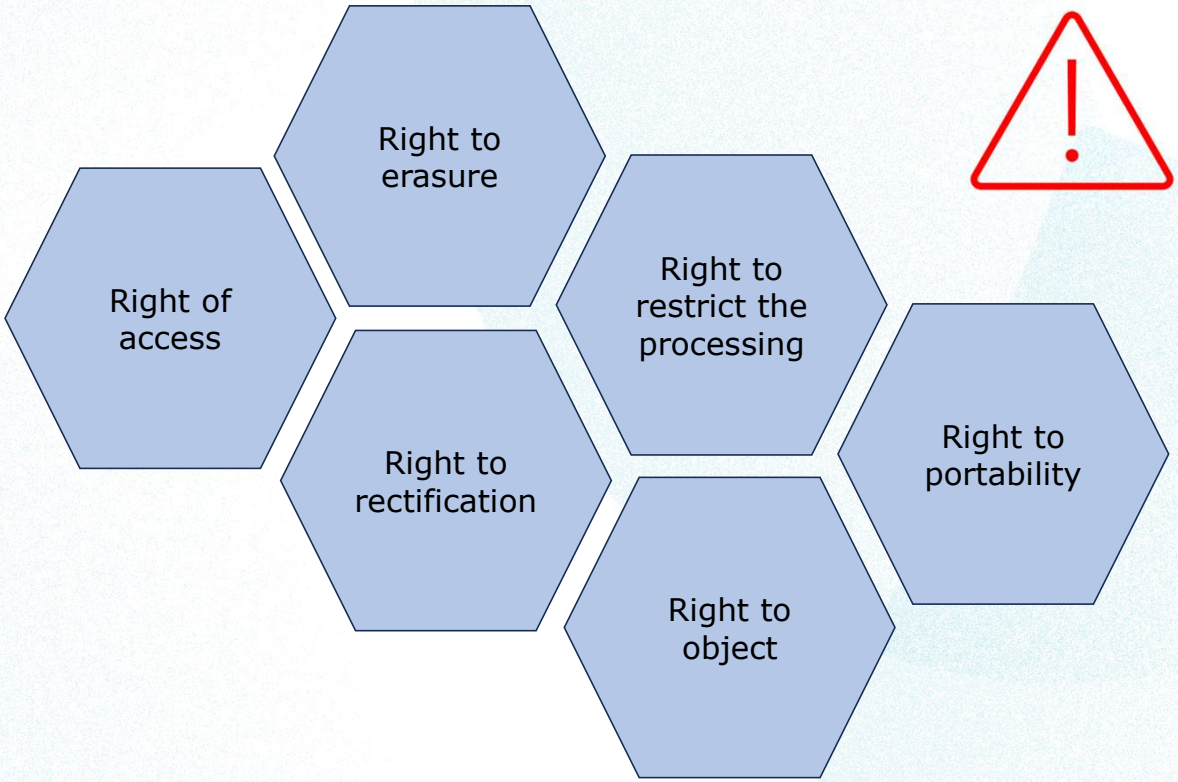


Impact on Bougie's customers (2/3)

- Are different groups of customers getting different outcomes from SparkAI?
  - Are the differences based on eg ethnicity, age, gender?
  - Are the differences fair?
  - Has SparkAI's developer tested this, and can they share the results?

Look out for:
Removing or ignoring data does not usually remove discrimination!

Impact on Bougie's customers (3/3)



Check in advance:
Can SparkAI provide these?

Slido

Who’s in the room?

Which teams could be involved in choosing SparkAI and implementing it?

ico.org.uk/DPPC

#DPPC24

Requirements and recommendations

Must: data protection requirements

- Clear accountability: controller / processor responsibilities, DPIA
- Purpose limitation: function creep, clarity on use of customer data for training
- Transparency with customers
- Security for customer data processed
- Fairness

Should or could: our top tips

- Collaborate on DPIA with developer
- Understand and discuss the risks in advance with developer and internal stakeholders
- Query all assurances
- Don’t ignore bias
- Do live tests and seek feedback
- We’re here to support you

Take away – the main one

Ensure the AI system works well for what you need it to do.

Understand what the impact of the system is on people.

As the controller, you are responsible for the processing.

Slido

Questions for us?

ico.org.uk/DPPC

#DPPC24

More resources

- ICO Innovation Services
- ICO AI and data protection risk toolkit
- ICO Guidance on AI and data protection
- DRCF AI and Digital Hub
- Government Guidelines for AI procurement

Keep in touch

Subscribe to our e-newsletter at ico.org.uk or find us on...

#DPPC24

ico.org.uk/DPPC

DPPC 2024

ico.
Information Commissioner's Office