Data Protection and COVID-19 Seminar*

Checklists for organisations

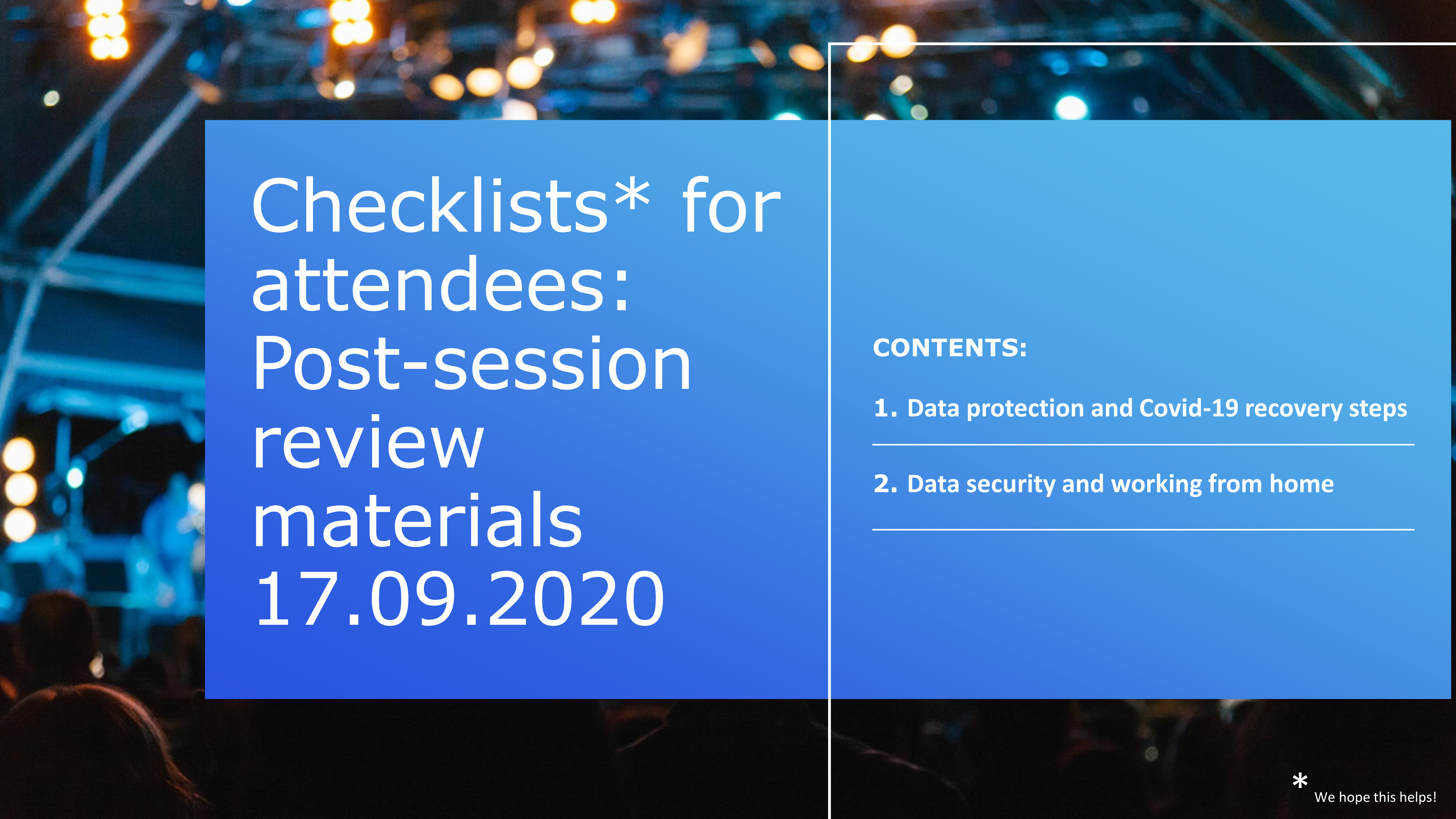
dentsu
AEGIS
network

Mahisha Rupan: Legal Director
Nikita Saini: Legal Counsel

17 September 2020

TrustLaw
COVID-19 RESPONSE

* Thanks for listening!



Checklists* for attendees: Post-session review materials 17.09.2020

CONTENTS:

1. **Data protection and Covid-19 recovery steps**

2. **Data security and working from home**

* We hope this helps!

Checklist:
Data protection and Covid-19 recovery steps

1. Only collect and use the personal data which you absolutely need, and nothing more

(data minimisation, purpose minimisation)

- Do you really need the information?
- Could you achieve the same result without collecting personal information?

2. Keep the data to a minimum

(data minimisation)

- Only collect the information needed to implement your measures appropriately and effectively

3. Communication is key. Be clear, open and honest with individuals about their data

(lawfulness, transparency)

- Communicate why you wish to use their personal data
- Communicate the purposes for which you’re handling their personal data
- Communicate who you will share this information with
- Communicate for how long you intend to keep the data

Checklist:
Data protection and Covid-19 recovery steps

4. Treat individuals fairly and be accountable for your decision making

(accountability, fairness)

- Document your decision-making process
- Make sure your approach doesn’t cause discrimination

5. Focus on data security, and keep people’s personal data safe and secure

(integrity and security)

- Keep data secure and hold it for only for as long as necessary
- Have a retention policy in place that sets out when and how personal information needs to be reviewed, deleted or anonymised

6. Individuals must be able to exercise their rights

(accountability, lawfulness)

- Inform people of their rights in relation to their personal data
- Individuals must have the option to exercise those rights
- Individuals must be able to discuss any concerns they may have with you

Data security and working from home

Checklist:
Data security and working from home

1. Establish and follow policies, procedures and guidance

- Ensure that data is adequately protected
- Avoid the temptation to do things in a way that may be seen as more convenient (such as sending emails through your personal account or using the video conferencing app that you use with friends for work calls)

2. Only use approved technology for handling personal data

- This will provide the best protection for personal data
- This equally applies to both hardware and software!

3. Consider confidentiality when holding conversations or using a screen

- You may be sharing your home working space with other family members or friends
- Try to hold conversations, where they are less likely to overhear you
- Try to position your screen where it is less likely to be overseen
- Consider measures like a screen for your laptop

Checklist:
Data security and working from home

4. Take care with print outs

- Safely store print outs until you can take them into the office and dispose of them securely

5. Don’t mix your organisation’s data with your own personal data

- If you have to work using your own device and software, keep your organisation’s data separate to avoid accidentally keeping hold of data for longer than is necessary
- Where possible, if provided, rely on your organisation’s secure technology

6. Lock it away where possible

- Put print outs and devices away at the end of the working day if possible
- This will avoid any data loss or data theft!

7. Be extra vigilant about opening web links and attachments in emails or other messages

- Remember not to click on unfamiliar web links or attachments!
- There is a rise of scams, particularly in relation to “important coronavirus updates” – please keep an eye out for these and be wary of your information sources

Checklist:
Data security and working from home

8. Use strong passwords

- Remember to make your passwords hard to guess.
- Remember to use different passwords for different services too

9. Communicate securely

- Use the communication facilities provided to you by your organisation where available
- If you need to share data with others then choose a secure messaging app or online document sharing system
- If you have to use email, which isn't always secure, consider password protecting documents and sharing the passwords via a different channel, like text

10. Keep software up to date

- Keep your security software up to date to make it more difficult for hackers to get in
- If your organisation has provided you with technology to work from home, this should be managed for you

Many thanks to all attendees

Remember:
There’s more guidance on the ICO website! www.ico.org.uk